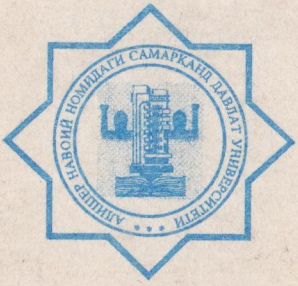
М.И. Исроилов, А.С.Солеев

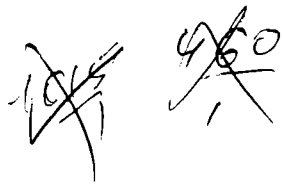
СОНЛАР НАЗАРИЯСИ



М.И.Исроилов, А.С.Солеев

СОНЛАР НАЗАРИЯСИ

УНИВЕРСИТЕТЛАР УЧУН
ЎҚУВ ҚЎЛЛАНМА



САМАРҚАНД – 2001

М.И. Исроилов, А.С. Солеев - Сонлар назарияси: Ўқув қўлланма

Ўқув қўлланма университетларнинг В-460100-математика ва В-480100- амалий математика ва информатика бакалавриат йўналишлари ўқув режасидаги "Сонлар назарияси" фанида тузилган ўқув дастури бўйича ўқитилиши мўлжалланган материалларни ўз ичига олади. Шунингдек, бу китобдан педагогик олийгоҳларнинг талабалари ҳам "Сонлар назарияси" фани бўйича ўқув қўлланма сифатида бемалол фойдаланишлари мумкин.

Китобдаги назарий маълумотларни чуқур ўрганишга имконият яратиш мақсадида, уларнинг барчаси муайян мисолларда тушунтирилган ҳамда ҳар бир бобнинг охирида мустақил ишлаш учун мисол ва масалалар келтирилган, уларнинг кўпларига жавоби билан таъминланган.

Масъул муҳаррир: ф.-м.ф.д. Тўлаганов С.Т.,
ЎзР ФА В.И.Романовский
номидаги математика
институти етакчи илмий ходими

Тақризчилар: ф.-м.ф.д., Самарқанд давлат
университети алгебра ва геометрия
кафедраси профессори Нарзуллаев Х.Н.
ф.-м.ф.д.,ЎзР ФА В.И.Романовский
номидаги математика институти
етакчи илмий ходими Шушбаев С.Ш.

МУНДАРИЖА

СЎЗБОШИ

Китоб университетлар ва педагогик олийгоҳларни сонлар назарияси фанининг дастуридаги материалларни ўз ичига олади (бўлиниш назарияси; туб сонлар ва уларнинг тақсимот қонуни; Евклид алгоритми, узлуксиз касрлар ва уларнинг тадбиқлари, биринчи даражали таққосламалар, биринчи даражали Диофант тенгламаларининг ечимларини топиш; юқори даражали таққосламаларнинг ечимларини топиш; даражали чегирмалар, бошланғич илдизлар, индекслар). Бундан ташқари ўрта мактаб ва лицей ўқитувчиларига керак бўладиган бўлиниш белгилари ва даврий касрларни даврини топиш ҳам баён қилинган. Китобни мустақил равишда ўрганиш ҳам мумкин. Шунинг учун уни иложи борича содда тарзда ёздик.

Китобда назарий маълумотларни чуқур ўзлаштириш учун уларнинг барчаси конкрет мисолларда тушунтирилган ва ҳар бобнинг охирида мустақил ишлаш учун мисол ва масалалар келтирилган, уларни айримларининг жавоби ҳам кўрсатилган. Бу мисолларнинг аксарияти ҳисоблаш характерига эга. Сонлар назариясиниг ҳозирга замон тадқиқотларига бориб тақаладиган ажойиб назарий масалалар билан қизиқадиган зукко ўқувчиларга биз И.М. Виноградов [6, 7] китобидаги масалаларни тавсия этамиз. Китобни ёзиш жараёнида биз Россия ва Узоқ хорижда чоп этилган дарсликлар ва қўлланмалардан кенг фойдаландик.

Китобда параграфлар, теоремалар ва формулалар бошидан охиригача ҳинд рақамлари билан номерланган, бундай тартиб эса китобнинг бир жойидан иккинчи жойига ҳавола қилишни соддалаштиради. Китобда теоремаларнинг асосий қисми тўла исботланган. Маълумот тўлароқ бўлиши учун айрим муҳим, лекин исботи китоб доирасидан ташқаридаги билимни талаб қиладиган, теоремалар исботсиз келтирилган.

Китоб сонлар назарияси билан биринчи марта танишаётган ўқувчиларга мўлжалланганлиги учун унинг кириш қисмида сонлар назариясининг асосий йўналишлари ва бу йўналишлар ёритилган адабиёт кўрсатилган.

Ҳар хил мисол ва масалаларни ечишда ўқувчиларга қулай бўлиши учун китобнинг охирида $p \le 97$ туб сонлар учун индекслар жадвали, бошланғич илдизлар ҳамда 6000 дан ошмайдиган туб сонларнинг жадвали келтирилган. Ниҳоят, сонлар назарияси соҳасида ўз билимларини чуқурлаштирувчи ўқувчилар учун адабиёт келтирилган бўлиб, улар уч қисмдан иборат: дарсликлар, монографиялар ва оммабоп китоблар. Келтирилган монографиялар сонлар назариясининг асосий йўналишларини ўз ичига олади.

Мазкур китоб камчиликлардан холи бўлмаса керак. Шунинг учун ҳам, китоб ҳақидаги барча фикр ва мулоҳазаларни мамнуният билан қабул қиламиз.

Муаллифлар

КИРИШ

1. *Сонлар назариясининг предмети.* Сонлар назарияси сонли системалар, уларнинг ўзаро алоқалари ва қонунлари ҳақидаги фандир. Шу билан бирга биринчи навбатда натурал ҳамдаги сонларга кўпроқ эътибор берилади, чунки улар: бутун, рационал, иррационал, ҳақиқий ва комплекс сонлар системасини тузишга асос бўлади.

Сонлар назарияси сонларни уларнинг тузулиши, ички алоқалари нуқтаи назаридан ўрганади, бир системадаги сонларни, ўзининг хоссалари билан соддароқ бўлган бошқа сонлар системаси орқали ифодалаш мумкинлигини текширади.

Натурал сонлар тушунчаси ва уларни умумлаштиришни қатъий мантиқий асослаш ҳамда улар билан боғлиқ бўлган амаллар назарияси арифметика асосларида қаралади. Арифметикани фан сифатида сонлар назарияси билан бир деб ҳисоблашади. Сонлар назариясини олий арифметика ҳам дейишади.

2. *Сонлар назариясининг асосий бўлимлари.* Сонлар назариясида вужудга келган масала ва муаммоларни, асосан, тўрт гуруҳга бўлиш мумкин.

1) *Диофант (ёки аниқмас) тенгламаларини ечиш,* яъни номаълумларнинг сони тенгламаларни сонидан катта бўлган бутун коэффицентли алгебраик тенглама ёки бундай тенгламалар системасини бутун сонларда ечиш

2) *Диофант яқинлашишлари.* Сонлар назариясининг бу бўлимида ҳақиқий сонларни рационал сонлар билан яқинлашишлари, ҳар хил кўринишдаги тенгсизликларни бутун сонларда ечиш, масалан, α-иррационал сон бўлганда $|\alpha x - y| < \frac{1}{x}$ тенгсизликни қаноатлантирадиган бутун x ва y сонларни топиш масалалари киради. Диофант яқинлашишларига *трансцендент* сонлар назарияси ҳам киради; бу бўлимда ҳар хил иррационал сонлар

синфларининг арифметик табиатини текшириб, уларни трансцендент сонларга ёки алгебраик сонларга мансублиги аниқланади.

3) *Туб сонларнинг натурал сонлар қаторида ёки бошқа сонли кетма-кетликлардаги тақсимотига оид масалалар.* Бу бўлимда натурал сонлар қаторида туб сонлар қандай жойлашган, n-туб сонни қандай топиш мумкин, кетма-кет жойлашган иккита туб сонлар орасида масофани топиш ва шунга ўхшаш масалалар қаралади.

4) *Аддитив муаммолар.* Бу муаммолар бутун сонларни махсус кўринишдаги қўшилувчиларга ёйишга тегишлидир.

Юқоридаги масалаларни тадқиқот қилиш жараёнида сонлар назариясида турли хил методлар яратилган бўлиб, бу методлар сонлар назариясининг йўналишларини ажратиш учун асос бўла олади.

Методлар асосан 5 та йўналишларга бўлинади.

I. *Сонлар назариясининг элементар методлари.* Элементар методларга шундай методлар киради, уларда асосан элементар математика ҳамда дифференцал ва интеграл ҳисобининг элементлари қўлланилади. Биринчи навбатда элементар методларга қуйидагилар киради: таққосламалар назариясининг методлари, уни буюк немис математиги К.Гаусс (1777-1855) яратган; узлуксиз касрлар методлари, уни француз математиги Ж.Лагранж (1736-1813) ривожлантирган. Элементар методларга булардан бошқа турли методлар киради.

Шуни таъкидлаш жоизки, методнинг элементарлиги бу унинг соддалигидан далолат бермайди.

Сонлар назариясида элементар методларни яратишда рус математиги П.Л.Чебишев (1821-1894), француз математиклари Ж.Лиувилл (1809-1992) ва Ш.Эрмит (1822-1901), норвег математиклари А.Туэ ва В.Брун, даниялик математик А.Селберг ва россиялик Л.Г.Шнирелман (1905-1938) ва Б.А.Венков (1900-1962) ларнинг хизматлари катта эди. (қ. [1], [5], [14], [23], [41], [46]).

2) *Аналитик сонлар назарияси.* Сонлар назариясининг бу бўлимида математик анализ, ҳақиқий ва комплекс ўзгарувчи функцияларнинг назариялари, қаторлар назарияси ва математиканинг бошқа тармоқларининг методлари қўлланилади. Аналитик сонлар назариясининг асосчиси швейцариялик олим, Петербург академиясининг академиги Л.Эйлер (1707-1783) ҳисобланади. Ҳақиқий ўзгарувчилар соҳасида аналитик методларни немис олими Л.Дирихле (1805-1859) ва П.Л.Чебишев ривожлантиришди. Комплекс ўзгарувчи функциялар назарияси билан боғлиқ бўлган аналитик методларни яратишда немис олими Б.Риман (1826-1866) нинг хизмати каттадир.

Аналитик методларни яратишда ва муҳим натижалар олишда немис математиги Г.Вейл (1885-1955), ҳинд математиги С.Раманужан (1887-1920), инглиз математиклари Г.Харди, Ж.Литлвуд, Монтгомери ва Вон, немис математиги К.Зигел, хитой математиклари Хуа-Ло-ген ва Ченнинг хизматлари катта эди. Аналитик сонлар назариясида россиялик математиклардан, хусусан, И.М.Виноградов (1891-1983), А.О.Гельфонд (1906-1968), А.А.Карацубалар кучли методлар яратишди; Ўзбекистонда бу соҳада Н.П.Романов, А.Ф.Лаврик ва М.И.Исроиловлар муҳим натижалар олишди (қ. [19-22], [26-30], [37-43], [45-47]).

3) *Алгебраик сонлар назарияси.* Бу бўлим алгебраик сон тушунчасидан бошланган бўлиб, инглиз математиги Ж.Валлис (1616-1703) ҳамда Ж.Ланграж ва Л.Эйлер ишларида вужудга келди. Бу соҳада энг муҳим методларни немис олимлари К.Гаусс, Э.Куммер (1810-1893), Л.Кроннекер (1823-1891), Р.Дедикинд (1831-1916), Г.Хассе, К.Зигел ва рус олимлари Е.И.Золотарев (1847-1878), Г.Ф.Вороной (1868-1908), Н.Г.Чеботарев (1894-1947), Б.А.Венков (1900-1962) ва И.Р.Шафаревичлар кучли методларни яратишди (қ. [1], [13], [14-15], [24]).

4) *Геометрик сонлар назарияси.* Бу назария «фазовий панжаралар», яъни берилган тўғри бурчакли координаталар

систмасида координаталари бутун сонлардан иборат бўлган нуқталар системаси қаралади. Бу назария геометрия ва кристаллографияда қўлланилади, сонлар назариясида у квадратик формалар назарияси билан боғлиқдир.

Бу назариянинг асосчиси Г.Минковский (1864-1909), Г.Ф.Вороной ва Ф.Клейн (1849-1925) лардир. Бу соҳада яратилган методларни Б.Н.Делоне, Б.А.Венков, Б.Ф.Скубенко ва ўзбекистонлик математиклар Х.Н.Нарзуллаев, С.Ш.Шушбаев ва М.И.Тўлагановалар муваффақият билан қўллашди (қ. [32-33]).

5) *Эҳтимоллик сонлар назарияси.* Бу бўлимда эҳтимоллар назариясининг методлари сонлар назариясига қўлланилади. Бу назарияни яратишда россиялик олим Ю.В.Линник ва литвалик олим И.П.Кубилюс ва ўзбек олими С.Т.Тўлагановнинг хизматлари каттадир (қ.[36]).

Мазкур методлар кўпинча бир бири билан чирмашиб кетган. Масалан, сонлар назариясининг аналитик методлари алгебраик, геометрик ва эҳтимоллик сонлар назариясида қўлланилади.

1-БОБ. БЎЛИНИШ НАЗАРИЯСИ

1-§. ҚОЛДИҚЛИ БЎЛИШ

Биз бундан кейин a, b, c,...x, y ҳарфларни фақат бутун сонлар деб тушунамиз (агар тескариси айтилган бўлмаса), улар мусбат ёки манфий, маълум ёки номаълум, ўзгармас ёки ўзгарувчи бўлиши мумкин.

Элементар арифметикадан маълумки бутун сонларнинг йигиндиси, айирмаси ва кўпайтмаси – бутун сон бўлиб, аммо иккита бутун соннинг нисбати (бўлинмаси) камдан-кам ҳолда бутун сон бўлади. Бутун сонлар ҳақида қуйидаги асосий теоремани келтиришдан олдин айрим тушунчаларни эслатиб ўтамиз.

Агар x – ихтиёрий ҳақиқий (рационал ёки иррационал, мусбат ёки манфий) сон бўлса, у ҳолда унинг бутун қисми $[x]$ ёки E(x) деб шундай бутун сонга айтиладики, унинг учун $[x] \le x < [x]+1$ ёки $x-1 < [x] \le x$ тенгсизликлар бажарилади. Агар x бутун бўлса, $[x]=x$ бўлади.

М и с о л:

$$[-5]=-5,\quad [-2{,}5]=-3,\quad [\pi]=3,\quad [e]=2,\quad [\ln 2]=0.$$

Шунга ўхшаш x нинг каср қисми деб $\{x\}=x-[x]$ га айтилади, ҳар доим $\{x\} \ge 0$.

М и с о л: $\{5\}=0$, $\{e\}=0{,}7128\ldots$, $\{-1{,}75\}=0{,}25$.

Одатдагидек $|x|$ орқали x соннинг абсолют қийматини белгилаймиз, яъни $x>0$ бўлганда $|x|=x$; $x<0$ бўлганда $|x|=-x$; $|0|=0$ бўлади.

1-т е о р е м а. Агар a ва b ихтиёрий иккита бутун сон ҳамда $b \neq 0$ бўлса, у ҳолда шундай иккита q ва r бутун сонларни топиш мумкинки, улар учун ушбу

$$a=bq+r,\ 0\le r<|b| \qquad (1)$$

муносабатлар ўринли бўлади, шу билан бирга q ва r бир қийматли равишда аниқланади.

И с б о т. Аввало фараз қилайлик a>b>0 бўлсин, бу ҳолда b га каррали бўлган 1b, 2b,...kb сонларни қараймиз. Архимед аксиомасига кўра шундай етарлича катта k натурал сон топиладики kb>a бўлади. Демак, шундай q натурал сон топиладики, унинг учун bq ≤ a бўлиб, b(q+1)>a бўлади. Энди a-bq=r деб белгилаймиз; равшанки r≥0, бундан a=bq+r келиб чиқади, лекин b(q+1)=bq+b>a, яъни bq+b>bq+r. Шундай қилиб, r<b. Бу ҳол учун теорема исботланди.

Агар a=b>0 бўлса у ҳолда q=1, r=0; агар b>a>0 бўлса, у ҳолда q=0, r=a. Агар a<0, b>0 бўлса, у ҳолда |a|=bq+r ни топамиз; демак: a=b (-q)-r, r=0 бўлганда (1)-формуланинг ўринлилиги равшан. Энди r>0 бўлсин, у ҳолда b-r=r_1 деб белгилаймиз, бундан

$$a=b(-q)-b+r_1=b(-q-1)+r_1$$

ни ҳосил қиламиз, бу эса (1)-формуланинг ўзи, чунки 0< r_1<b.

Ниҳоят, b<0 бўлганда исбот қилинганга кўра

$$a=|b|q+r,\ 0\le r<|b|$$

демак,

$$a=b(-q)+r$$

яна биз (1)-формулага келдик.

Энди q ва r бир қийматли равишда аниқланишини кўрсатамиз. Фараз қилайлик, биз икки усул билан қуйидагиларни топдик:

$$a=bq+r=bq_1+r_1,\ 0\le r<|b|,\ 0\le r_1<|b|,$$

бундан

$$bq-bq_1=r_1,\ b(q-q_1)=r_1-r.$$

Бу ерда ўнг томон абсолют қиймати билан $|b|$дан кичик, $q-q_1\neq 0$ бўлганда чап томон абсолют қиймати бўйича ≥|b|. Демак, $q-q_1=0$, $q=q_1$, $r_1=r$.

Теорема тўлиқ исботланди.

И з о ҳ. Берилган (мусбат) a ва b сонлар бўйича q ва r ни топиш одатдаги «қолдиқли бўлиш» бўлиб, унинг элементар арифметикада ўрганишади. Биз бу ерда ихтиёрий a ва b бутун сонлар учун q ва r нинг мавжудлигини кўрсатдик, бунда q *тўлиқмас бўлинма* ва r-*қолдиқ* дейилади.

Энди (1)-тенгликни ҳар иккала томонини b га бўлиб,

$$\frac{a}{b} = q + \frac{r}{b} \qquad (2)$$

ни ҳосил қиламиз. Бу ерда $\frac{a}{b}$ нотўғри каср бўлиб, $\frac{r}{b}$ тўғри каср, q сон $\frac{a}{b}$ касрнинг бутун қисмидир. Демак,

$$q = \left[\frac{a}{b}\right] = E\left(\frac{a}{b}\right), \quad \frac{r}{b} = \left\{\frac{a}{b}\right\}.$$

Биз r=0 ҳолга алоҳида эътибор берамиз, бу ҳолда (1)-формуладан a=bq ёки $\frac{a}{b}$=q келиб чиқади. Бундай ҳолда a сон b га *бўлинади* (*қолдиқсиз бўлинади*), b сон a соннинг *бўлувчиси* ёки *кўпайтувчиси*; a сон эса b соннинг *карралиси* дейилади.

Агар a сон b сонга бўлинса, биз уни одатда b$|a$ каби ва бўлинмаса b$\nmid a$ каби белгилаймиз. Агар a сон b сонга бўлинса, айрим ҳолда $a \vdots$ b каби ҳам белгиланади.

2-§. БЎЛИНИШНИНГ ХОССАЛАРИ

Биз энди бўлинишнинг (яъни қолдиқсиз бўлинишни)нинг хоссаларини кўриб чиқамиз.

2-т е о р е м а. Агар a сон b сонга ва b сон c сонга бўлинса, у ҳолда a сон c сонга бўлинади. Яъни b$|a$ ва c|b лардан c$|a$ келиб чиқади.

И с б о т. Теорема шартига кўра $a=bq_1$ ва $b=cq_2$, бундан кўпайтиришнинг ассоциатив қонунга асосан

$$a=bq_1=(cq_2)q_1=c(q_2q_1)=cq.$$

2-теоремадан бўлинишнинг транзитивлик қонуни келиб чиқади.

3-т е о р е м а. Агар $a_1, a_2 \ldots, a_n$ сонлар с га бўлинса ва $x_1, x_2, \ldots, x_n$ ихтиёрий бутун сонлар бўлса, у ҳолда $a_1x_1+a_2x_2+\ldots a_nx_n$ сон с га бўлинади.

И с б о т. Теорема шартига кўра

$$a_1=b_1c,\ a_2=b_2c,\ldots\ a_n=b_nc.$$

кўпайтиришнинг қўшишга нисбатан дистрибутивлик қонуни асосида

$$a_1x_1+a_2x_2+\ldots+a_nx_n=(b_1x_1+b_2x_2+\ldots+a_nx_n)c.$$

4-т е о р е м а. Агар a сон b сонга бўлинса, у ҳолда умуман, $\pm a$ сон $\pm b$ сонга бўлинади, хусусий ҳолда $|a|$ сон $|b|$ сонга бўлинади.

И с б о т. $a=bq=(-b)(-q)$, $-a=b(-q)=(-b)q$

5-т е о р е м а. Ҳар бир сон ўзига бўлинади.

И с б о т. $a=a\cdot 1$

6-т е о р е м а. ± 1 ҳар қандай сонни бўлади, ± 1 дан бошқа шу хусусиятга эга бўлган сон йўқ.

И с б о т. $a=1\cdot a=(-1)(-a)$. Агар x ҳар бир соннинг бўлувчиси бўлса, у ҳолда 1 x га бўлинади, аммо 1 фақат ± 1 га бўлинади. Шунинг учун ҳам, $x=\pm 1$.

7-т е о р е м а. 0 ҳар қандай сонга бўлинади, 0 дан фарқли шу хоссага эга бўлган бошқа сон йўқ.

И с б о т. $0=a\cdot 0$, агар $a\neq 0$ бўлса, у ҳолда у $|a|+1$га бўлина олмайди

И з о ҳ. 4-теорема бўлиниш масалаларида фақат мусбат сонлар билан чегараланишга имкон беради. Масалан, сонларнинг бўлувчилари деб биз уларнинг фақат мусбат бўлувчиларини назарда тутамиз.

3-§. ЭНГ КИЧИК УМУМИЙ КАРРАЛИ

Фараз қилайлик a_1, a_2, ... a_n – берилган (бутун, ...уй бут) сонлар бўлсин, уларнинг кўпайтмаси $a_1 \cdot a_2 \cdots a_n$ бу ...сонларни ҳар бирига бўлинади, яъни уларнинг *умумий карралиси* бўлади. Бунга ўхшаш умумий карралилар чексиз ...ди, чунки ихтиёрий бутун к учун $ka_1 \cdot a_2 \cdots a_n$ берилган ...сонларнинг умумий карралиси бўлади. Демак, бу сонларнинг ...ш кичик мусбат умумий карралиси мавжуд, уни m=[a_1, a_2,..., a_n] орқали белгилаймиз, у шу сонларнинг *энг кичик умумий карралиси* (ЭКУК) дейилади. Равшанки m≤ $a_1 \cdot a_2$ a_n.

8-т е о р е м а. Берилган a_1, a_2, ...a_n сонларнинг ЭКУК шу сонларнинг бошқа ихтиёрий карралисининг бўлувчиси бўлади.

И с б о т. Фараз қилайлик m_1 сон a_1, a_2,... a_n сонларнинг бошқа бирор умумий карралиси бўлсин; m_1 ни m га бўламиз, унда 1-теоремага кўра

$$m_1 = mq + r, \quad 0 \le r < m.$$

Бундан 3-теоремага кўра $r=m_1-mq$ ҳам a_1, a_2, ... a_n сонларнинг умумий карралиси бўлади. Лекин r<m бўлиб, m энг кичик умумий каррали; демак, r=0 ва $m|m_1$. Теорема исботланди.

Н а т и ж а. Агар с сон a_1, a_2,..... a_n сонларнинг ҳар бирига бўлинса, у ҳолда с бу сонларнинг энг кичик умумий карралисига ҳам бўлинади.

4-§. ЭНГ КАТТА УМУМИЙ БЎЛУВЧИ

Ихтиёрий n та a_1, a_2,..., a_n сонлар 1 га тенг бўлган умумий бўлувчига эга. Агар бу сонлар 1 дан бошқа умумий бўлувчига эга бўлмаса, бундай сонлар *ўзаро туб сонлар* дейилади. Агар a_1, a_2,..., a_n сонларнинг ихтиёрий иккитаси

ўзаро туб бўлса, у ҳолда улар *жуфт-жуфт ўзаро туб сонлар* дейилади. Мисол 8, 12, 25 сонлар ўзаро туб, аммо жуфт-жуфт ўзаро туб эмас, чунки (8, 12, 25)=1, (8, 12)=4; 5, 7, 46 сонлар эса жуфт-жуфт ўзаро туб, чунки (5, 7)=(5, 46)=(7, 46)=1. Берилган сонлар 1 дан бошқа умумий бўлувчиларга эга бўлиши ҳам мумкин. Ҳар ҳолда умумий бўлувчиларнинг сони чеклидир, чунки бу бўлувчиларнинг ҳар бири (абсолют қиймати билан) берилган сонларнинг энг кичигидан катта эмас. Фараз қилайлик d_1, d_2, d_3.....d_n берилган сонларнинг барча бўлувчилари бўлиб,

$$d=[d_1, d_2, d_3\ldots]$$

бўлсин. Берилган $a_1, a_2, \ldots, a_n$ сонларнинг ҳар бири d_1, d_2, d_3...ларнинг умумий карралиси, демак, 8-теоремага кўра d га ҳам бўлинади. Шундай қилиб, d ҳам берилган сонларнинг умумий бўлувчиси, яъни $\{d_1, d_2, d_3\ldots\}$ тўпламга киради. Шу билан бирга равшанки, у бу бўлувчиларнинг энг каттаси, чунки у уларнинг ҳар бирига бўлинади. У қуйидаги ча белгиланади:

$$d=(a_1, a_2, \ldots, a_n)$$

ва шу сонларнинг энг *катта умумий бўлувчиси* (ЭКУБ) дейилади. Шундай қилиб биз, қуйидагини исботладик.

9-т е о р е м а. Берилган сонларнинг энг катта умумий бўлувчиси мавжуд ва у бошқа умумий бўлувчиларга бўлинади.

10-т е о р е м а. d сони $a_1, a_2, \ldots, a_n$ сонларнинг ЭКУБ бўлиши учун $\frac{a_1}{d}, \frac{a_2}{d}, \ldots \frac{a_n}{d}$ бўлинмаларнинг ўзаро туб бўлиши зарур ва кифоядир.

И с б о т (*зарурийлиги*). Тескарисини фараз қиламиз: d=($a_1, a_2, \ldots, a_n$) бўлиб, $\frac{a_1}{d}, \frac{a_2}{d}, \ldots \frac{a_n}{d}$ лар умумий бўлувчи с(>1)га эга бўлсин. У ҳолда, демак, $\frac{a_1}{dc}, \frac{a_2}{dc}, \ldots \frac{a_n}{dc}$ бутун

сонлар, яъни $a_1, a_2, \ldots, a_n$ лар умумий бўлувчи dc>d га эга, бу эса d нинг ЭКУБ лигини рад этади.

Кифоялиги. Фараз қилайлик $\frac{a_1}{d}, \frac{a_2}{d}, \ldots \frac{a_n}{d}$ ўзаро туб сонлар бўлиб, d эса ЭКУБ бўлмасин, у ҳолда 9-теоремага кўра $(a_1, a_2, \ldots, a_n)$ сон dc (c>1) кўринишга эга бўлади. Лекин у ҳолда $\frac{a_1}{dc} = \frac{a_1}{d}:c$, $\frac{a_2}{dc} = \frac{a_2}{d}:c$, $\frac{a_n}{dc} = \frac{a_n}{d}:c$, яъни c (>1) сон $\frac{a_1}{d}, \frac{a_2}{d}, \ldots \frac{a_n}{d}$ сонларнинг умумий бўлувчиси бўлиб чиқади, бу эса фаразимизга, яъни уларнинг ўзаро тублигига зиддир. Теорема тўла исботланди.

11-т е о р е м а. Агар d=$(a_1, a_2, \ldots, a_n)$ бўлса, у ҳолда $(a_1c, a_2c \ldots\ldots a_nc)$=dc ва шунингдек, k сони $a_1, a_2, \ldots, a_n$ сонларнинг бирор умумий бўлувчиси бўлса, у ҳолда

$$(\frac{a_1}{k}, \frac{a_2}{k}, \ldots \frac{a_n}{k}) = \frac{d}{k}$$

бўлади.

И с б о т. Бу тасдиқ 10 теорема ва

$$\frac{a_1}{d} = \frac{a_1c}{dc}, \ldots, \frac{a_n}{d} = \frac{a_nc}{dc}$$

$$\frac{a_1}{d} = \frac{a_1:k}{d:k}, \ldots, \frac{a_n}{d} = \frac{a_n:k}{d:k}$$

тенгликлардан келиб чиқади.

5-§. БЎЛИНИШ ҲАҚИДАГИ КЕЙИНГИ ТЕОРЕМАЛАР

12-т е о р е м а. Агар (a, c)=1 бўлиб, ab кўпайтма c га бўлинса, у ҳолда b сон c га бўлинади.

И с б о т. Олдинги теоремага кўра $(a, c)=1$ ни иккала томонини b га кўпайтириб, қуйидагига эга бўламиз: $(ab, bc)=b$. Теорема шартига кўра $c|ab$ ва bc сон c га каррали бўлганлиги учун $c\backslash bc$. У ҳолда 11-теоремага кўра $c\backslash(ab, bc)$. Лекин $(ab, bc)=b$. Демак, $c\backslash b$.

Биз энди иккита a ва b сонларнинг ЭКУК ва ЭКУБ лари орасидаги муносабатни кўриб чиқамиз. Фараз қилайлик M сон a ва b сонларнинг бирор умумий карралиси бўлсин. Умумий карралини таърифига асосан $a\backslash M$ ва $b\backslash M$. Бундан

$$M=ak \qquad (3)$$

келиб чиқади. Ўз навбатида бундан $b|ak$ деган хулосага келамиз. Энди $d=(a,b)$ ни қарайлик, бундан 10-теоремага кўра $a=a_1d$, $b=b_1d$ ва $(a_1, b_1)=1$ келиб чиқади. (3)-тенглик ва $b\backslash M$ дан қуйидагилар ҳосил бўлади:

$$b\backslash ak \Rightarrow b_1d\backslash a_1kd \Rightarrow b_1|a_1k.$$

Лекин $(a_1, b_1)=1$ бўлгани учун, 12-теоремага кўра $b_1|k$ деган хулосага келамиз. Демак,

$$k=b_1t=\frac{b}{d}t$$ буни (3)-га қўйсак

$$M=\frac{ab}{d}t$$

ҳосил бўлади. Бундан $t=1$ бўлганда

$$m=\frac{ab}{d}$$

келиб чиқади. Шундай қилиб, биз қуйидагига эга бўлдик.

13-т е о р е м а. Иккита a ва b сонларнинг кўпайтмаси шу сонларнинг ЭКУК ва ЭКУБ ни кўпайтмасига тенг $ab=(a,b)[a,b]$; a ва b сонларга бўлинадиган ҳар бир M сон уларнинг ЭКУК га ҳам бўлинади:

$$M=mt=\frac{ab}{d}t.$$

1-х у л о с а. Ўзаро туб сонларнинг ЭКУКи шу сонларнинг кўпайтмасига тенг, яъни

$$[a, b]= ab, (a, b)=1.$$

2-х у л о с а. Бутун k сон учун $[ak, bk]=k[a, b]$.

3-х у л о с а. Агар $k|a$ ва $k|b$ бўлса, у ҳолда

$$\left[\frac{a}{k}, \frac{b}{k}\right] = \frac{[a,b]}{k}.$$

Ихтиёрий n та $a_1, a_2, \ldots, a_n$ сонларнинг ЭКУК ва ЭКУБ ни топиш ҳар доим иккита сонларнинг кетма-кет ЭКУК ва ЭКУБни топишга келтирилади. Биз буни учта a, b, c сонлар учун кўрсатамиз.

14-т е о р е м а. Ихтиёрий a, b, c натурал сонлар учун $[a, b, c]=[[a, b], c]$ тенглик ўринли бўлади.

И с б о т. Айтайлик $[a, b, c]=m$, $[a, b]=m_1$ $[m_1, c]=m_2$ бўлсин. Буларга асосан $a|m_1$, $b|m_1$. Бу муносабатлардан 2-теоремага кўра $a\backslash m_2$, $b\backslash m_2$, $c\backslash m_2$, яъни m_2 сон a, b, c сонларнинг умумий карралиси экан, шунинг учун

$$m \mid m_2 \qquad (4)$$

деган хулосага келамиз. Бошқа томондан, $a|m$, $b|m$ ва $m_1|m$ бўлгани учун

$$m|m_2 \qquad (5)$$

муносабат ўринлидир. (4) ва (5)-га кўра $m_2=m$, яъни $[a, b, c]=[[a, b], c]$.

15-т е о р е м а. Ихтиёрий a, b, c натурал сонлар учун $(a, b, c)=((a,b), c)$ тенглик ўринлидир.

И с б о т. Ушбу $(a, b)=d_1$, $(d_1,c)=d$ белгилашларни киритамиз. 2-теоремага кўра a ва b сонлар d га бўлинади, яъни d сон a, b, c лар учун умумий бўлувчи. Фараз қилайлик d^1 сон a, b, c сонларнинг бошқа бирор умумий бўлувчиси бўлсин. У ҳолда 9-теоремага кўра d_1 сон d^1 га бўлинади. Демак (яна 9-теоремага кўра) d сони d^1 га бўлинади, d сони a, b, c сонлар учун ЭКУБ. Бошқача қилиб айтганда $d=(a, b, c)=((a, b), c)$.

Мисол: $d=(65, 104, 156)=((65, 104),156)=(13, 156)=13$. Буни қуйидагича текширамиз: $(65, 104, 156)=(5\cdot13; 8\cdot13; 12\cdot13)=(3, 8, 12)\cdot13=13$.

1-БОБ УЧУН МАШҚЛАР

1. Агар (a, n)=1, n\ad-bc ва n\a-b бўлса, у ҳолда n\c-d.
2. Агар (a, b)=1 бўлса, у ҳолда (a^3-b^3,$(a-b)^3$) a-b ёки 3(a-b) экан,лигини кўрсатинг.
3. Агар (a, b)=1 бўлса, у ҳолда (a ± b, ab)=1.
4. Агар a, b, c жуфт-жуфт ўзаро туб бўлса, у ҳолда (ab+bc+ca, abc)=1.
5. Фараз қилайлик (n, a) =d, n=dq, (q,d)=d_1, q=d_1q_1 (q_1,c)=d_2. У ҳолда (n, abc)= =$d_1 \cdot d_2 \cdot d_3$.
6. Агар (a, b, c)=1 бўлса, у ҳолда (a, b, c)=(a, b) · (a,c).
7. Ушбу (a,b)=(a+b, [a,b]) тенгликни кўрсатинг.
8. Ушбу (a, b, c)^2\(ab, bc, ca) ни кўрсатинг.
9. Агар (a,b)=1 бўлиб a ва b ларнинг жуфт-тоқлиги ҳар хил бўлса, у ҳолда ($(a+b)^n$, $(a-b)^n$)=1.
10. Фараз қилайлик a, b, x, y бутун сонлар, a ва b ларнинг жуфт-тоқлиги ҳар хил бўлиб, d=ax_0+by_0 сон ax+by кўринишдаги сонларнинг мусбатлари орасида энг кичиги бўлсин. У ҳолда d=(a, b). Бундан фойдаланиб, 9-теорема ва 11-теорема исботлансин.
11. a бутун сони 23 га бўлинганида 29 чала бўлинма ҳосил бўлади. Бўлинувчи a нинг энг катта қиймати топилсин.
12. Бўлинувчи 457 га, бўлинма эса 28 га тенг. Бўлинувчи b ни ва r қолдиқни топинг.
13. n-натурал сон бўлса, n(n^2+5) ни 6 га бўлинишини кўрсатинг.
14. Агар касрнинг сурати иккита тоқ сонлар квадратиларининг айирмасига, махражи эса шу сонлар квадратларининг йиғиндисига тенг бўлса, бундай касрни ҳар доим иккига қисқартириш мумкинлигини, лекин 4 га қисқартириш мумкин эмаслигини кўрсатинг.
15. Евклид алгоритмидан фойдаланиб қуйидаги сонларнинг ЭКУБини топинг:
    а) 1001, 6253; б) 1517, 2257; в) 2737, 9163 ва 9639;

1411, 4641 ва 2257.

16. $d=(a, b)$ ни ва $d=ax+by$ тенгликни қаноатлантирадиган x ва y сонларни топинг:

а) $a=1445$, $b=629$, б) $a=903$, $b=731$,

в) $a=1786$, $b=705$, г) $a=4543$, $b=885$,

д) $a=6919$, $b=1443$.

17. Қуйидаги сонлар жуфтини ЭКУКи топилсин.

а) 279 ва 372 б) 178 ва 381 в) 318 ва 477

г) 758 ва 1137 д) 360 ва 504.

18. $(a, b)=24$, $[a, b]=2496$ берилган, a ва b сонлар топилсин.

19. Икки соннинг йиғиндиси 589 га, улар ЭКУКининг шу сонлар ЭКУБига нисбати 90 га тенг. Шу сонлар топилсин.

20. Агар икки соннинг ҳар бирини шу сонлар ЭКУБига бўлишдан ҳосил бўлган бўлинмалар йиғиндиси 27 га ва уларнинг ЭКУКи 2693 га тенглиги маълум бўлса, шу икки сон топилсин.

21. Ихтиёрий a, b, c натурал сонлар учун

$$[a,b,c]=\frac{abc(a,b,c)}{(a,b)(a,c)(b,c)}$$

тенгликнинг ўринли эканлигини исботланг.

1-бобга доир тарихий маълумот

1. Сон- математиканинг асосий тушунчаларидан бири. Сон тушунчаси энг содда кўринишда ибтидоий жамоа даврида вужудга келган, инсоният фаолият доирасининг кенгайиши ва математик билимларнинг ривожланиши билан такомиллашган. Предметларни санашга бўлган эҳтиёж туфайли *натурал сонлар*, кейинчалик *чексиз натурал сонлар қатори* (1,2,3,4,...) тушунчаси келиб чиқди.

2. Натурал сонлар қаторининг чексизлигини тафаккур ўстириш сон тушунчасининг ривожланишида муҳим қадам эди. *Натурал* ва *туб* сонлар қаторларининг чексизлиги ва етарлича

катта сонларни номлаш, белгилаш масалалари мил.ав.3-асрдаёқ юнон математиклари Евклид («Негизлар») ва Архимед («Қум заррачаларини ҳисоблаш») асарларида муҳокама қилинган.

Сон устидаги тўрт амал қоидаларини ўрганиш билан *арифметика* шуғулланади. Натурал сонлар қаторидаги чуқур қонуниятларни ўрганиш ҳозиргача тугалланмаган. Сон тушунчасининг такомилланиши *каср сон* тушунчасини киритиш билан бошланди. Каср сон бирор миқдорни ўлчаш, яъни бу миқдорни бошқа бир миқдор -ўлчов билан таққослаш натижасида келиб чиқади. Сон тушунчасининг ривожланишида ўрта аср Яқин ва Ўрта Шарқ мамлакатлари олимлари ҳам катта ҳисса қўшдилар. Европада манфий сонларни француз математиги Р.Декарт (Rene' Descartes, латинча номи Cartesius, 1596-1650) киритди. Барча бутун, каср (мусбат ва манфий) сонлар тўплами нол билан бирга *рационал сонлар* дейилади. Узлуксиз равишда ўзгарадиган миқдорларни ўрганиш учун *иррационал сонлар* тушунчаси киритилган. 18-19 асрларда алгебраик тенгламалар назариясининг ривожланиши *комплекс сонлар* тушунчасига олиб келди. Комплекс сонлар устидаги барча амаллар сақланган ҳолда комплекс сонлар тўпламини ортиқ кенгайтириш мумкин эмас. Сон тушунчасини ва унинг хоссаларини немис математикалари Г.Кантор (Georg Cantor, 1845-1918), Р.Дедекинд (Richard Dedekind, 1831-1916), К.Вейерштрасс (Karl Weierstrass Theodor Wilgelm, 1815-1897) ва италиялик математик Жузеппе Пеано (1858-1932) ўз ишларида тўла исботлаб бердилар.

2. Евклид (мил.ав.3 аср) – қадимги юнон математиги. Евклид ҳаёти ҳақида аниқ маълумот йўқ, у Искандария (Александрия) да Птоломей 1 подшолиги даврида (мил.ав.305-283) яшаб ижод этган. Унинг асосий математик асари «Негизлар». Унда Евклид Юнонистонда тўпланган бой математик материални мантиқий системага солган. Проклнинг ёзилишича Птоломей «геометрияда «Негизлар»

ıён қилинганга кўра қисқароқ йўл йўқми деб Евклиддан
ган экан. Евклид унга «геометрияда шоҳона йўл йўқ» деб
ıб берибди. «Негизлар» нинг математика тараққиётида
ı катта. «Негизлар»13 китобдан иборат бўлиб, VII,-VIII, -
китобларида бутун сонларга асосланган назарий
ıметика баён қилинган. «Негизлар» да натурал сонлар,
жуфт, туб сонлар ҳамда рационал ва иррационал сонлар
қилинган.

3. 3-теорема «Негизлар» нинг V-китобида

2-БОБ. ТУБ СОНЛАР

6-§. ТУБ СОНЛАР ВА УЛАРНИНГ АЙРИМ ХОССАЛАРИ

Ҳар бир n натурал сон ҳеч бўлмаганда иккита бўлувчиларга эга: 1 ва n. Шундай n натурал сонлар мавжудки, улар 1 ва n дан бошқа бўлувчиларга эга эмас.

1-т а ъ р и ф. p натурал сон *туб* дейилади, агар p > 1 ва у 1 ва узидан бошқа натурал бўлувчиларга эга бўлмаса.

Одатда туб сонлар p ва q лар билан белгиланади, туб сонларнинг дастлабки 20 таси қуйидагилардан иборат:

2, 3, 5, 7, 11, 13, 15, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71.

2-т а ъ р и ф. n > 1 натурал сон *таркибли* дейилади агар у 1 ва n дан фарқли ҳеч бўлмаганда битта натурал бўлувчига эга бўлса.

Бу таърифга кўра 2 дан бошқа барча n=2k (k >1) жуфт сонлар таркиблидир, чунки улар 2 га бўлинади ва 1< 2 < n.

Бу таърифлардан кўрамизки 1 сон туб ҳам эмас, таркибли ҳам эмас.

16-т е о р е м а. Ҳар бир n >1 натурал соннинг 1 дан фарқли энг кичик бўлувчиси p туб сондир.

И с б о т. Ҳақиқатан, акс ҳолда p бирор q (1<q<p) бўлувчига эга бўлиб, q/p ва p/n. Бундан q/n ва q<p келиб чиқади. Бу эса p нинг энг кичик бўлувчи эканлигига зиддир.

17-т е о р е м а. Ҳар қандай n натурал сон берилган p туб сонга ёки бўлинади ёки у билан ўзаро тубдир.

И с б о т. Агар p туб сон бўлиб, n ихтиёрий натурал сон бўлса, у ҳолда n ва p сонларнинг энг катта умумий бўлувчиси ёки p га ёки 1га тенг, чунки p бошқа бўлувчиларга эга эмас.

18-т е о р е м а. Агар $a\,b$ кўпайтма бирор p туб сонга бўлинса, у ҳолда кўпайтувчилардан камида биттаси p га бўлинади. Теореманинг исботи 12-теоремадан келиб чиқади.

Математик индукциядан фойдаланиб, бу теоремани кўпайтувчиларнинг сони иккитадан ортиқ бўлганда ҳам кўллаш мумкин.

Н а т и ж а. Агар бир неча сонларнинг кўпайтмаси p туб сонга бўлиниб, унинг барча кўпайтувчилари туб сонлардан иборат бўлса, кўпайтувчиларнинг бири p га тенгдир.

7-§. АРИФМЕТИКАНИНГ АСОСИЙ ТЕОРЕМАСИ

19- т е о р е м а. Ҳар бир $1<n$ натурал сон туб сон ёки туб сонлар кўпайтмаси шаклида ёзилади, агар бу кўпайтмада кўпайтувчиларнинг ўрни эътиборга олинмаса, у ҳолда бу кўпайтма ягона бўлади.

И с б о т. Ихтиёрий $1<n$ учун ушбу

$$n = p_1 \cdot p_2 \cdots p_s \qquad (6)$$

кўпайтманинг мавжудлиги ва ягоналигини кўрсатамиз, бунда $p_1, p_2, \ldots, p_s$ – туб сонлар.

3- т а ъ р и ф. Ихтиёрий $1<n$ натурал сонни (6)-кўринишда ёзиш бу *сонни туб сонлар кўпайтмасига ёйиш* дейилади.

Т е о р е м а н и н г и с б о т и. 16–теоремага кўра ихтиёрий n натурал соннинг 1 дан катта энг кичик натурал бўлувчиси туб сон бўлади. Демак,

$$n = p_1 \, n_1 \qquad (7)$$

тенглик ўринлидир. Агар (7)- да n_1 туб сон бўлса, у ҳолда теорема исбот бўлади. Агар n таркибли сон , p_2 эса унинг туб бўлувчиси бўлса, у ҳолда $n_1 = p_2 n_2$ ва $n = p_1 p_2 n_2$ ҳосил бўлади. Агар n_2 туб сон бўлса, у ҳолда теорема исбот бўлади. Мабодо n_2 таркибли сон бўлса, бу жараённи $n_s=1$ бўлгунича давом эттирамиз, унда биз қуйидагиларни ҳосил қиламиз:

$$n = p_1 n_1,$$

$$n_1 = p_2\, n_2,$$
$$n_2 = p_3\, n_3,$$
$$\cdots\cdots$$
$$n_{s-1} = p_s\, n_s.$$

Бу тенгликларни ҳадлаб кўпайтириб, $n_1 \cdot n_2 \cdots n_{s-1} \cdot n_s (n_s = 1)$ кўпайтмага қисқартирсак, (6)- ёйилма $n = p_1 p_2 \ldots p_s$ ҳосил бўлади. Энди (6)- ёйилмани ягоналигини исбот қиламиз. Фараз қилайлик n сони (6) – дан бошқа

$$n = q_1 q_2 \ldots q_t \qquad (8)$$

ёйилмага ҳам эга бўлсин. (6)- ва (8)- ларни чап томонларининг тенглигидан

$$p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_t \qquad (9)$$

ҳосил бўлади. Бу тенгликнинг чап томонидаги ҳар бир p_i (i = 1, 2, .., s) туб сон бўлиб, унинг ўнг томонини бўлади. Лекин барча q_j (j = 1, 2, …, t) лар ҳам туб сон. 18- теореманинг натижасига кўра p_i ларнинг бирортаси q_ℓ га ва q_j ларнинг бирортаси p_m га тенг бўлиши керак. Демак, (8) ва (9) – ёйилмаларнинг ҳар бири тенг сондаги туб кўпайтувчилардан иборат. Агар улардаги бирор p туб сон ёйилманинг маълум томонида иккинчи томондагига нисбатан кўпроқ қатнашган бўлса, у ҳолда (9)- ёйилмани ҳар иккала томонини p га бир неча марта қисқартириб, унинг бир томонида
p мавжуд, иккинчи томонида эса p қатнашмаган ҳолга келамиз. Бунинг бўлиши мумкин эмас. Демак, s =t ва (6)- ёйилма ягона экан.

Юқоридаги (6)- ёйилмада баъзи бир кўпайтувчилар ўзаро тенг бўлиши ҳам мумкин. Фараз қилайлик (6)- да p_1 туб сон α_1 марта, p_2 туб сон α_2 марта, ва ҳ. к. p_k туб сон α_k марта қатнашсин. У ҳолда (6)- ёйилма

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots . p_k^{\alpha_k}$$

кўринишда ёзилади. Бу кўриниш n соннинг туб сонлар бўйича ***каноник ёйилмаси*** дейилади.

Каноник ёйилманинг бир тадбиқини кўрамиз.

20- т е о р е м а. Фараз қилайлик n нинг каноник ёйилмаси $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ бўлсин. У ҳолда n нинг барча бўлувчилари

$$d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} \qquad (10)$$

кўринишдаги сонлардан иборат, бунда

$$0 \le \beta_1 \le \alpha_1,\ 0 \le \beta_2 \le \alpha_2, \ldots\ldots,\ 0 \le \beta_k \le \alpha_k.$$

И с б о т. Ҳақиқатан, фараз қилайлик n сон d га бўлинсин. У ҳолда n=dq бўлади; демак, n нинг каноник ёйилмасида d нинг барча туб бўлувчилари мавжуд бўлиб, уларнинг даражалари d нинг каноник ёйилмасидаги даражаларидан кичик бўлмайди. Шунинг учун, d бўлувчи (10)-кўринишга эга. Аксинча, n нинг (10)-кўринишдаги ҳар қандай d га бўлиниши равшан.

М и с о л. $N = 380 = 2^2 \cdot 5 \cdot 19$ нинг барча бўлувчиларини топиш учун $d = 2^{\beta_1} 5^{\beta_2} 19^{\beta_3}$ ифодада β_1, β_2, β_3 ларга мос равишда қуйидаги қийматларни бериш керак: β_1=0, 1, 2; β_2=0, 1, β_3=0, 1. У ҳолда 380 нинг барча бўлувчилари ҳосил бўлади: 1, 2, 4, 5, 10, 19, 20, 38, 76, 95, 190, 380.

8-§. ТУБ СОНЛАР ТЎПЛАМИНИНГ ЧЕКСИЗЛИГИ

21-т е о р е м а. Туб сонлар тўплами чексиздир. Бу теореманинг бир неча исботи мавжуд. Буларнинг энг биринчисини Евклид берган.

Е в к л и д и с б о т и. Фараз қилайлик туб сонларнинг сони чекли бўлиб, уларнинг охиргиси p бўлсин. 2 дан бошлаб p гача бўлган барча туб сонларнинг кўпайтмасини олиб, устига 1 қўшамиз:

$$P = (2 \cdot 3 \cdot 5 \ldots p) + 1$$

P сони 2 га ҳам, 3 га ҳам ва ҳ.к. p га ҳам бўлинмайди, чунки биринчи қўшилувчи бу сонларнинг барчасига бўлиниб, иккинчиси бўлинмайди (у 1 га тенг). Демак, ёки P нинг ўзи туб сон ёки унинг q туб бўлувчиси p дан катта. Хуллас, шундай туб сон мавжудки, у ихтиёрий p туб сондан катта.

туб бўлувчиси $\sqrt{n}$ дан ошмайди.

И с б о т. Агар n= n_1 n_2 бўлса, у ҳолда n_1, n_2 сонларнинг бири $\sqrt{n}$ дан катта, иккинчиси эса $\sqrt{n}$ дан кичик, фақат n аниқ квадрат бўлгандагина $n_1 = n_2 = \sqrt{n}$. Хусусий ҳолда n нинг туб бўлувчиси ҳам $\sqrt{n}$ дан ошмайди.

Энди Эратосфен «ғалвири» ни кўриб чиқамиз. Агар N дан катта бўлмаган барча туб сонларни топиш керак бўлса, биз иккидан бошлаб, N гача бўлган барча натурал сонларни ёзиб чиқамиз, ҳосил бўлган жадвалда иккидан кейин ҳар бир иккинчисини, учдан кейин ҳар бир учинчисини, бешдан кейин ҳар бир бешинчисини, 7 дан кейин ҳар бир еттинчисини ва ҳ.к. бу жараённи $\sqrt{N}$ дан ошмайдиган р туб сонгача давом эттириб, р га бўлинадиган сонларни ўчирамиз. Ўчирилмай қолган сонлар N дан ошмайдиган туб сонлар бўлади, чунки биз N дан ошмайдиган барча каррали сонларни ўчириб ташладик. Бу усул Эратосфен «ғалвири» дейилади.

И з о ҳ. 2 ни (ягона жуфт туб сон) сақлаб, N дан ошмайдиган барча тоқ сонларни ёзиш керак. Кейин юқорида айтганимиздек 3 дан кейин ҳар бир учинчиси, 5 дан кейин ҳар бир бешинчиси ўчирилади ва ҳ.к.

М и с о л. N=120 бўлсин, у ҳолда $7 < \sqrt{120}$, $11 > \sqrt{120}$ бўлади. 2 дан 120 гача бўлган интервалдаги туб сонларни топиш учун 2 ва 119 гача бўлган барча тоқ сонларни ёзамиз. Кейин юқоридагидек 3, 5 ва 7 га каррали бўлганларини ўчириб, қуйидагини ҳосил қиламиз (ўчирилган сонларнинг таги чизилган):

2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119.

Бундан кўрамизки ≤ 120 бўлган туб сонларнинг сони 30 та экан.

ТУБ КЎПАЙТУВЧИЛАРГА АЖРАТИШ

Қуйидаги масалани қараймиз: n!=1·2···n ни бўладиган p нинг энг юқори даражаси p^{α}, яъни $p^{\alpha}|n!$ ва $p^{\alpha+1}\nmid n!$ шартларни қаноатлантирадиган α топилсин.

Бу масалани ечишдан олдин қуйидаги леммани исбот қилиш керак.

Лемма. Агар n, a ва b натурал сонлар бўлса, у ҳолда қуйидаги формула ўринлидир:

$$\left[\frac{n}{ab}\right]=\left[\frac{1}{b}\left[\frac{n}{a}\right]\right].$$

Исбот. Фараз қилайлик $n=aq+r$, $q=\left[\frac{n}{a}\right]$, $0\le r<a$, яъни $q=bq_1+r_1$ бўлсин. Айтайлик $q=bq_1+r_1$, $q_1=\left[\frac{q}{b}\right]$, $0\le r_1\le b-1$ бўлсин. Энди унинг бу қийматини n нинг ифодасига қўйиб, қуйидагига эга бўламиз:

$$n=a(bq_1+r_1)+r=(ab)q_1+(ar_1+r)$$

Бундан $0\le ar_1+r\le a(b-1)+a-1=ab-1<ab$. Демак, n ни ab га бўлганда ҳосил бўладиган тўлиқсиз бўлинма q_1 бўлиб, ar_1+r қолдиқдир. Шундай қилиб, бир томондан $q_1=\left[\frac{n}{ab}\right]$, иккинчи томондан эса $\left[\frac{1}{a}\left[\frac{n}{b}\right]\right]$дир. Кўриниб турибдики, лемма $a=b$ бўлганда ҳам ўринлидир.

Фараз қилайлик p берилган туб сон бўлсин. Агар p>n бўлса, у ҳолда кўриниб турибдики, $p\nmid n!$ яъни α=0 бўлади. Агар p<n бўлса, у ҳолда n! таркибига p, 2p, 3p,... $\left[\frac{n}{p}\right]p$

кўпайтувчилар қатнашади. Бу кўпайтувчилар кўпайтмаси

$$p\cdot 2p\cdot 3p\cdots\left[\frac{n}{p}\right]p=\left[\frac{n}{p}\right]!\,p^{\left[\frac{n}{p}\right]}$$

га тенг. Демак n! нинг таркибига $p^{\left[\frac{n}{p}\right]}$ ва $\left[\frac{n}{p}\right]!$,

таркибидаги p^{α_1} киради. Худди шу мулоҳазаларга $\left[\frac{n}{p}\right]!$ нинг p га бўлинадиган кўпайтувчиларнинг кўпайт қуйидагидан иборат:

$$p\cdot 2p\cdot 3p\cdots\left[\frac{1}{p}\left[\frac{n}{p}\right]\right]p=\left[\frac{n}{p^2}\right]!\,p^{\left[\frac{n}{p^2}\right]},$$

чунки леммага кўра

$$\left[\frac{1}{p}\left[\frac{n}{p}\right]\right]=\left[\frac{n}{p^2}\right].$$

Энди шу мулоҳазаларни $\left[\frac{n}{p^2}\right]!$ га қўллаймиз; унинг бўлинадиган кўпайтувчиларининг кўпайтмаси

$$p\cdot 2p\cdot 3p\cdots\left[\frac{1}{p}\left[\frac{n}{p^2}\right]\right]p=\left[\frac{n}{p^3}\right]!\,p^{\left[\frac{n}{p^3}\right]}$$

дан иборат, чунки

$$\left[\frac{1}{p}\left[\frac{n}{p^2}\right]\right]=\left[\frac{n}{p^3}\right]$$

ва ҳ.к. бу жараённи шундай β кўрсатгичгача д эттирамизки, унинг учун $p^{\beta+1}>n$ бўлсин.

24-т е о р е м а. n! га кўпайтувчи бўлиб кирадиган p энг юқори даражаси қуйидагидан иборат:

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots+\left[\frac{n}{p^k}\right],$$

...ми p^k n, лекин $p^{k+1}>n$. Агар p>n бўлса, у ҳолда n! p га ...ммайди.

Ис т и ж а. Агар n! нинг каноник ёйилмаси

$$n! = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_3^{\alpha_3}$$

...ми, у ҳолда

$$\alpha_i = \left[\frac{n}{p_i}\right]+\left[\frac{n}{p_i^2}\right]+\ldots+\left[\frac{n}{p_i^{k_i}}\right],\ i=1, 2,\ldots, s$$

...ўлади

М и с о л. 3 нинг 57! ни бўладиган энг юқори даражаси 3^{α} ...топилсин.

Ечиш. $\alpha=\frac{57}{3}+\left[\frac{57}{9}\right]+\left[\frac{57}{27}\right]=19+6+2=27$

2-БОБ УЧУН МАШҚЛАР.

1. 2.1-теорема асосида синов йўли билан 437, 509, 811, 1849, 953, 1079, 10519, 17357, 2027 сонларнинг қайсилари туб ва қайсилари таркиблилиги аниқлансин; таркиблилари туб сонлар кўпайтмасига ёйилсин (ж:509, 811, 953, 2027 – туб сонлар)
2. Эратосфен ғалвири 2 дан 500 гача оралиқда қўлланилсин.
3. $P=(2\cdot3\cdot5\ldots p)\pm1$ сонларнинг қийматлари p=5, 7, 11, 13 бўлганда топилсин; уларнинг қайсилари туб ва қайсилари таркиблилиги аниқлансин, таркиблилари туб сонлар кўпайтмасига ёйилсин. (ж: $2\cdot3\cdot5\cdot7-1=209=11\cdot19$; $2\cdot3\cdot5\cdot7\cdot11\cdot13+1=30031=59\cdot509$ сонлар таркибли; қолганлари туб сонлар)
4. 2 дан 500 гача бўлган натурал сонлар оралиғидаги туб сонларнинг нечтаси 4n+1 кўринишга, нечтаси 4n+3 кўринишга, нечтаси 3n+1 кўринишга ва нечтаси 3n+2

кўринишга эга? (ж: улардан 40, 50,. 45, 50 таси м равишда 4n+1, 4n+3, 3n+1 ва 3n+2 кўринишга эга).

5. 100! нинг туб сонлар бўйича каноник ёйилмасини топи
6. 3,7,11 ва 23 туб сонларнинг 250! сон бўлинадиган э юқори даражаларини топинг.
7. 7520! соннинг каноник ёйилмасида 3 сон қайси дараж кўрсатгичи билан қатнашади.
8. 7520! сон бўлинадиган энг катта туб сон нечага тенг.
9. 2640 ва 2680 сонлари орасида жойлашган қайси сонлар ту эканлигини текширинг.
10. 1300 ва 1350 орасидаги ҳамма туб сонларни топинг.
11. Берилган сонларни туб кўпайтувчиларга ёйинг:

а) 3551; б) 6497; в) 1817; г)2407.

12. 90 дан ошмайдиган туб сонлар жадвалини тузинг.
13. Қуйидаги сонларни туб кўпайтувчиларга ажратиш йўли билан уларнинг ЭКУБи ва ЭКУКини топинг:

а) 360 ва 504; б) 187 ва 533;

в) 9163, 2737 ва 9639; г) 374, 1599 ва 9061.

2-бобга доир тарихий маълумот

1. 16- ва 18-теоремалар бошқа кўринишда «Негизлар» нинг V-китобида келтирган.

2. 19-теорема ҳам ўз мазмуни билан қадимдан маълум, лекин асоссиз равишда, ўз-ўзидан равшан деб қаралган. Бу теоремани аниқ таърифлаб, исботи билан биринчи марта немис математиги К.Гаусс (Gauss Karl Friedrich, 1777-1865) берган эди.

3. 21-теорема «Негизлар» нинг IX-китобида баён қилинган.

4. 22-теоремадаги айниятнинг ўнг томонидаги қатор *Риман дзета-функцияси* деб аталувчи $\zeta(s)$ аналитик функцияни аниқлайди:

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad s=\sigma+it.$$

Бу қатор s-комплекс текисликнинг $\sigma\geq 1+\delta,\delta>0$ ярим қисоатлантирадиган ихтиёрий чекли соҳасида яқинлашади. $\sigma>1$ бўлганда бу функция *Эйлер кўпайтмаси* кўринишда аниқланади

$$\zeta(s)=\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1},$$

бунда p барча туб сонлар қийматини қабул қилади. Кейин бу функцияни немис математиги П.Дирихле (Peter Gustav Lejeune Dirichlet, 1805-1859) ва, хусусан, рус математиги П.Л.Чебишев (Пафнутий Львович Чебышев, 1821-1894) туб сонлар тақсимоти қонунини текшириш муносабати билан ишлатди. Аммо $\zeta(s)$ нинг муҳим хоссалари, уни комплекс ўзгарувчи $s=\sigma+it$ нинг функцияси деб қарагандан кейин, очилди. Буни биринчи бўлиб немис математиги Б.Риман (Bernhard Rieman, 1826-1866, Сочинения, пер.с немец.М.-Л.1948) $\zeta(s)$ нинг муҳим хоссаларини ўрганди ва «Риман гипотезаси» деб аталувчи машҳур гипотезани ўртага ташлади. Бу гепотезага кўра $\zeta(s)$ нинг барча комплекс илдизлари $\sigma=\frac{1}{2}\left(s=\frac{1}{2}+it\right)$ тўғри чизиқда ётади. Бу гипотеза ҳозиргача исбот қилинмаган. Агар бу гепотеза исбот қилинса туб сонларнинг асимптотик қонунига, умуман сонлар назариясининг кўп масалаларига ойдинлик киритилар эди. Дзета-функция ва унинг тадбиқлари ҳақида китобнинг охирида келтирилган [19, 23, 24, 27, 34, 36, 37, 39, 40, 42, 44] адабиётлардан қараш мумкин.

5. Эратосфен (мил.ав.276-194 й.) – буюк, юнон олими Искандариядаги машҳур кутубхонанинг бош кутубхоначиси бўлиб ишлаган. Бу кутубхонада тарихчиларнинг

таъкидлашича 100 000 дан 700 000 гача турли китоблар ва қўлёзмалар бўлган.

Эратосфен, кўпроқ математик сифатида эмас, географ ва астроном сифатида машҳур. У Искандария ва Ассуан орасидаги меридианни ўлчаш асосида Ер куррасининг радиусини етарлича аниқ қийматини топган (6311 км. Аслида Ернинг қутбий радиуси – 6356,777 км, экваториал радиуси-6378,160 км.)

6. 23-теоремани биринчи бўлиб аталиялик математик Фибоначчи (Леонардо Пизанский, 1170-1228) кўрсатган эди. У n соннинг $\leq \sqrt{n}$ бўлган сонларга бўлинишини текшириш етарлилигини кўрсатган.

7. Француз математиги А.Лежандр (Анриен Мари, 1753-1833) ўз замоннасигача сонлар назариясида йиғилган маълумотларни изчиллик билан, тўла равишда ўзининг «Сонлар назарияси» (Theorie de nombres, 4 ed. Paris, 1855) китобида келтирилган.

24- теорема Лежандр китобининг 1808 йилда чоп этилган иккинчи нашрида учрайди.

Сонлар назарияси сонларни уларнинг тузулиши, ички алоқалари нуқтаи назаридан ўрганади, бир системадаги сонларни, ўзининг хоссалари билан соддароқ бўлган бошқа сонлар системаси орқали ифодалаш мумкинлигини текширади.

Натурал сонлар тушунчаси ва уларни умумлаштиришни қатъий мантиқий асослаш ҳамда улар билан боғлиқ бўлган амаллар назарияси арифметика асосларида қаралади. Арифметикани фан сифатида сонлар назарияси билан бир деб ҳисоблашади. Сонлар назариясини олий арифметика ҳам дейишади.

2. *Сонлар назариясининг асосий бўлимлари.* Сонлар назариясида вужудга келган масала ва муаммоларни, асосан, тўрт гуруҳга бўлиш мумкин.

1) *Диофант (ёки аниқмас) тенгламаларини ечиш*, яъни номаълумларнинг сони тенгламаларни сонидан катта бўлган

бутун коэффицентли алгебраик тенглама ёки бундай тенгламалар системасини бутун сонларда ечиш

2) *Диофант яқинлашишлари.* Сонлар назариясининг бу бўлимида ҳақиқий сонларни рационал сонлар билан яқинлашишлари, ҳар хил кўринишдаги тенгсизликларни бутун сонларда ечиш, масалан, α-иррационал сон бўлганда $|\alpha x - y| < \frac{1}{x}$ тенгсизликни қаноатлантирадиган бутун x ва y сонларни топиш масалалари киради. Диофант яқинлашишларига *трансцендент* сонлар назарияси ҳам киради; бу бўлимда ҳар хил иррационал сонлар синфларининг арифметик табиатини текшириб, уларни трансцендент сонларга ёки алгебраик сонларга мансублиги аниқланади.

3) *Туб сонларнинг натурал сонлар қаторида ёки бошқа сонли кетма-кетликлардаги тақсимотига оид масалалар.* Бу бўлимда натурал сонлар қаторида туб сонлар қандай жойлашган, n-туб сонни қандай топиш мумкин, кетма-кет жойлашган иккита туб сонлар орасида масофани топиш ва шунга ўхшаш масалалар қаралади.

4) *Аддитив муаммолар.* Бу муаммолар бутун сонларни махсус кўринишдаги қўшилувчиларга ёйишга тегишлидир.

Юқоридаги масалаларни тадқиқот қилиш жараёнида сонлар назариясида турли хил методлар яратилган бўлиб, бу методлар сонлар назариясининг йўналишларини ажратиш учун асос бўла олади.

Методлар асосан 5 та йўналишларга бўлинади.

I. *Сонлар назариясининг элементар методлари.* Элементар методларга шундай методлар киради, уларда асосан элементар математика ҳамда дифференцал ва интеграл ҳисобининг элементлари қўлланилади. Биринчи навбатда элементар методларга қуйидагилар киради: таққосламалар назариясининг методлари, уни буюк немис математиги К.Гаусс (1777-1855) яратган; узлуксиз касрлар методлари, уни француз математиги Ж.Лагранж (1736-1813)

3-БОБ. ЕВКЛИД АЛГОРИТМИ ВА УЗЛУКСИЗ КАСРЛАР

11-§. ЕВКЛИД АЛГОРИТМИ

Амалиётда иккита a ва b сонларнинг, туб сонлардаги ёйилмаларига боғлиқ бўлмаган равишда, ЭКУБ ни топиш катта аҳамиятга эга. Бундай усул мавжуд ва у кетма-кет бўлиш ёки Е в к л и д а л г о р и т м и деб номланади.

Фараз қилайлик a сон b сонга бўлинмасин. У ҳолда бўлиш ҳақидаги теоремага кўра

$$\left.\begin{aligned} a &= bq_1 + r_2, \\ b &= r_2q_2 + r_3, \\ r_2 &= r_3q_3 + q_4, \\ &\cdots\cdots\cdots\cdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \\ r_{n-1} &= r_nq_n \end{aligned}\right\} \qquad (12)$$

бунда r_2, r_3, ..., r_n ушбу $b > r_2 > \ldots r_{n-1} > r_n > 0$ тенгсизликларни қаноатлантиради. Натурал сонлар қуйидан чегараланган, шунинг учун ҳам бирор n дан бошлаб $r_{n+1}=0$ бўлади.

Қуйидаги икки тасдиқнинг тўғрилигини:

1) a ва b сонлар r_n га бўлиниши;
2) a ва b сонларнинг исталган умумий бўлувчисига r_n нинг бўлинишини кўрсатамиз.

1) тасдиқни исботлаш учун (12)-тенгликларга охиргисидан биринчисигача бўлган тартибда мурожаат қиламиз. Охирги тенгликдан r_{n-1} нинг, r_n га бўлиниши, ундан олдингисидан

$$r_{n-2} = r_{n-1}q_{n-1} + r_n = r_n \cdot q_n \cdot q_{n-1} + r_n = r_n(q_n \cdot q_{n-1} + 1)$$

натижага кўра, r_{n-2} нинг ҳам r_n га бўлиниши ва ҳ.к. шу тарзда давом эттирилса, иккинчи ва биринчи тенгликлардан a ҳамда b сонларнинг r_n га бўлиниши келиб чиқади.

2) тасдиқни исботлашда (12)-тенгликлардан энди (1)-тенгликларга нисбатан тескари тартибда фойдаланамиз. Бу тенгликларнинг биринчисидан 3-теоремага кўра a ва b сонларнинг ихтиёрий умумий бўлувчисига r_2 ҳам бўлиниши, иккинчисига кўра b ва r_2 ларнинг умумий бўлувчисига r_3 нинг бўлиниши ва ҳ.к. охиргисидан битта олдингисига кўра r_{n-2} ва r_{n-1} ларнинг умумий бўлувчисига r_n нинг бўлиниши келиб чиқади.

Демак, r_n охирги қолдиқ a ва b сонларнинг умумий бўлувчиси бўлиб, қолган барча умумий бўлувчиларга бўлинади.9-теоремага кўра бундай бўлувчи a ва b сонларнинг ЭКУБ идир. Шундай қилиб, Евклид алгоритмини биз қуйидаги қоида тарзида таърифлашимиз мумкин.

Қ о и д а. Иккита соннинг ЭКУБ ини топиш учун, уларнинг каттасини кичигига бўлиш, сўнгра, кичик сонни биринчи қолдиққа бўлиш, ундан кейин биринчи қолдиқни иккинчисига, иккинчисини учинчи қолдиққа ва ҳ.к. бундай бўлишни қолдиқ нолга айлангунча давом эттириш керак. Охирги нолдан фарқли қолдиқ берилган сонларнинг ЭКУБ и бўлади.

Мисол: $a=100971, b=32409$ сонлар берилган. Қуйидагиларни ҳосил қиламиз:

$$100971 = 32409 \cdot 3 + 3744,$$
$$32409 = 3744 \cdot 8 + 2457,$$
$$3744 = 2457 \cdot 1 + 1287,$$
$$2457 = 1287 \cdot 1 + 1170,$$
$$1287 = 1170 \cdot 1 + 117,$$

$$1170 = 117 \cdot 10.$$

шундай қилиб, (100971, 32409)=117.

13-теоремага асосан бу иккита соннинг ЭКУКини қуйидагича топамиз:

$$[100971,\ 32409] = \frac{100971 \cdot 32409}{117} = 27968967.$$

12-§. УЗЛУКСИЗ КАСРЛАР

10-§ даги (12)-тенгликларни биринчисини ҳар иккала томонини b га, иккинчисини r_2 ва ҳ.к. охиргисини r_n га бўлиб, қуйидагиларни ҳосил қиламиз:

$$\frac{a}{b} = q_1 + \frac{r_2}{b},$$

$$\frac{b}{r_2} = q_2 + \frac{r_2}{r_3},$$

.....

$$\frac{r_{n-2}}{r_{n-2}} = q_{n-1} + \frac{r_n}{r_{n-1}},$$

$$\frac{r_{n-1}}{r_n} = q_n,$$

бундан

$$\frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_2}{r_3}}} + q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{r_4}{r_3}}} = \ldots$$

Шундай қилиб, $\frac{a}{b}$ ни ушбу кўринишда ёзиш мумкин:

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}} \qquad (13)$$

шоҳида $q_1, +\frac{1}{q_2}, +\frac{1}{q_3}, \ldots$ буғинлардан тузилган (13)-ифоданинг ўнг томони *узлуксиз* (ёки *занжирли*) *каср* дейилиб, қисқача

$$\frac{a}{b} = (q_1, q_2, \ldots, q_n)$$

каби ёзилади; $q_1, q_2, \ldots q_n$ лар узлуксиз касрнинг *тўлиқсиз бўлинмалари* ёки *ёйилманинг элементлари* деб номланади.

Хулоса қилиб айтганда, $\frac{a}{b}$ нотўғри касрни узлуксиз касрга ёйдик. Агар $\frac{a}{b}$ тўғри каср бўлса, у ҳолда қуйидаги ёйилмага эга бўламиз:

$$\frac{a}{b} = \frac{1}{\frac{a}{b}} = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_n}}} = (0, q_1, q_2, \ldots q_n)$$

(қавсларда биринчи ўринда албатта 0 ёзиш керак). Ниҳоят, агар манфий каср берилган бўлса, уни ҳар доим қуйидагича тасвирлаш мумкин:

$$-k + \frac{a}{b},$$

бунда, $k > 0$ - бутун сон ва, $\frac{a}{b}$ - тўғри мусбат каср. Шундай қилиб, бундан олдинги белгилашларга ўхшаш

$$-k + \frac{a}{b} = -k + (0, q_1, q_2, ..., q_n)$$

га келамиз, бунда, биринчисидан истисно равишда, қолган барча буғинлар мусбат. Оқибат натижада, қуйидаги теорема исботланди.

24-т е о р е м а. Ҳар қандай рационал сонни ягона равишда узлуксиз касрга ёйиш мумкин бўлиб, унинг барча тўлиқсиз бўлинмалари бутун сон ва иккинчисидан бошлаб, мусбат (биринчиси ё>0 ёки <0 ёинки =0) ҳамда охиргиси бирдан каттадир.

1-и з о ҳ. Ҳар қандай бутун сонни бир бўғинли узлуксиз касрдек қараш мумкин. Масалан, $5 = (5); \frac{1}{a}$ кўринишдаги касрни икки бўғинли узлуксиз касрдек қараш мумкин: $\frac{1}{a} = (0; a)$.

2-и з о ҳ. Агар энг сўнгги q_n тўлиқсиз бўлинмага ҳеч қандай шарт қўйилган бўлмаса, у ҳолда рационал соннинг узлуксиз касрга ёйилмаси иккита ҳар хил кўринишга эга бўлади: биринчиси $q_n > 1$ бўлганда $(q_1, q_2, ..., q_n)$ бўлиб, иккинчиси $(q_1, q_2, ..., q_n - 1, 1)$. Охиргисида буғинлар сони биттага ортиқ ва, энг сўнгги тўлиқсиз бўлинма 1 га тенг.

М и с о л: (1-§ га қ.)

$$\frac{100971}{32409} = 3 + \cfrac{1}{8 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{10}}}}} = (3,8,1,1,1,10).$$

1.6. МУНОСИБ КАСРЛАР ВА УЛАРНИНГ ХОССАЛАРИ

Биз ихтиёрий рационал сонни чекли узлуксиз касрга ёйиш мумкинлигини кўриб чиқдик. Энди чекли узлуксиз касрга қандай рационал сонни белгилашини кўриб чиқамиз. Узлуксиз касрлар назариясида қуйидаги касрлар катта аҳамиятга эга:

$$\delta_1 = q_1, \delta_2 = q_1 + \frac{1}{q_2}, \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, \ldots$$

ёки

$$\delta_1 = (q_1), \delta_2 = (q_1, q_2), \delta_3 = (q_1, q_2, q_3), \ldots$$

Булар берилган узлуксиз касрни *муносиб касрлари* дейилади. Равшанки,

$$\frac{a}{b} = (q_1, q_2, \ldots, q_n) = \delta_n.$$

δ_k муносиб касрнинг тартиби k га тенг деб ҳисобланади.

Муносиб касрни ҳисоблашдан олдин шуни таъкидлаш керакки δ_k дан δ_{k+1} га ўтиш учун δ_k да q_k ни $q_k + \frac{1}{q_{k+1}}$ га алмаштириш лозим.

Шуни ҳам шартлашиш керакки δ_k ни ҳисоблаш жараёнида ҳосил бўлган сурат ва махражни мос равишда P_k ва Q_k орқали белгилаймиз ва кейинчалик қулай бўлиш учун $P_0 = 1$ ва $Q_0 = 0$ деб оламиз. Белгилашларга кўра

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1},$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_1 q_2 + 1}{q_2} = \frac{q_2 q_1 + 1}{q_2 \cdot 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{(q_2 + \frac{1}{q_3})P_1 + P_0}{(q_2 + \frac{1}{q_3})Q_1 + Q_0} = \frac{q_3(q_2 P_1 + P_0) + P_1}{q_3(q_2 Q_1 + Q_0) + Q_1} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3} \ldots$$

ларни ёзамиз.

Бу ердан кўринадики, δ_2 дан δ_3 га ўтиш қонуняти δ_k дан δ_{k+1} га ўтишда сақланади. Шунинг учун ҳам математик индукция принципига асосан ихтиёрий k $(2 \le k \le n)$ учун

$$\delta_k = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}} \ldots \qquad (14)$$

Бу ерда

$$P_k = q_k P_{k-1} + P_{k-2}, Q_k = q_k Q_{k-1} + Q_{k-2}. \qquad (15)$$

Кейинги мулоҳазаларда δ_k муносиб каср ҳақида гапирганда унинг охирги кўриниши $\frac{P_k}{Q_k}$ ни тушунамиз. (15)-рекуррент формула δ_k ларни топиш учун хизмат қилади, амалда ҳисоблашлар қуйидаги тарзда бажарилади:

		q_1	q_2	...	q_k	...	q_n
P_k	$P_0 = 1$	$P_1 = q_1$	P_2	...	P_k	...	P_n
Q_k	$Q_0 = 0$	$Q_1 = 1$	Q_2	...	Q_k	...	Q_n

М и с о л. (3, 8, 1, 1, 1, 10) узлуксиз касрнинг муносиб касрларини топинг.

	0	1	2	3	4	5	6
q_k		3	8	1	1	1	10
P_k	1	3	8·3+1 =25	25·1+3= 28	1·28+25 =53	1·53+28=81	10·81+53= 863
Q_k	0	1	8·1+0 =8	8·1+1=9	1·9+8=1 7	1·17+9=26	10·26+17= 277

Шундай қилиб, берилган узлуксиз касрнинг муносиб касрлари қуйидагилардан иборат:

$$\delta_1 = \frac{3}{1}, \delta_2 = \frac{25}{8}, \delta_3 = \frac{28}{9}, \delta_4 = \frac{53}{17}, \delta_5 = \frac{81}{26}, \delta_6 = \frac{863}{277}$$

Энди муносиб касрларнинг айрим хоссаларини кўриб чиқамиз.

1. Фараз қилайлик $\Delta_k = P_k Q_{k-1} - P_{k-1} Q_k$ бўлсин, (15)-формулалардан фойдаланиб, Δ_k ни қуйидагича ёзамиз:

$$\Delta_k = P_k Q_{k-1} - P_{k-1} Q_k = (q_k P_{k-1} + P_{k-2}) Q_{k-1} - P_{k-1}(q_k Q_{k-1} + Q_{k-2}) = -(P_{k-1} Q_{k-2} - P_{k-2} Q_{k-1}) = -\Delta_{k-1}$$

бундан кўрамизки барча Δ_k ларнинг абсолют қийматлари тенг, ишоралари эса навбатма-навбат алмашиниб туради. Бундан ташқари

$$\Delta_1 = P_1 Q_0 - P_0 Q_1 = q_1 \cdot 0 - 1 \cdot 1 = -1.$$

бўлганидан барча $k(1 < k < n)$ учун

$$\Delta_k = P_k Q_{k-1} - P_{k-1} Q_k = (-1)^k \qquad (16)$$

ни ҳосил қиламиз.

Охирги формула $(P_k, Q_k) = 1$ лигини кўрсатади. Ҳақиқатан, агар биз $(P_k, Q_k) = d > 1$ деб фараз қилсак, унда зиддиятга учраймиз, чунки у ҳолда 16-формуладан $(-1)^k$ ҳам d га бўлинади деган хулоса чиқар эди.

Шундай қилиб,

26-т е о р е м а. Барча $k - 1,2,\ldots,n$ учун қуйидаги тенглик ўринлидир:

$$P_kQ_{k-1} - P_{k-1}Q_k = (-1)^k.$$

27-т е о р е м а. Ихтиёрий муносиб касрнинг сурати ва махражи ўзаро туб сонлардир.

28-т е о р е м а. Барча $k = 1,2,\ldots,n$ учун

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_kQ_{k-1}},$$
$$\left|\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}}\right| = \frac{1}{Q_kQ_{k-1}}. \qquad (17)$$

И с б о т. Исботи 25-теоремадан келиб чиқади.

Энди фараз қилайлик α бутун бўлмаган ихтиёрий ҳақиқий сон бўлсин, $q_1 = [\alpha]$ деб олиб, α учун

$$\alpha = q_1 + \frac{1}{\alpha_2}, \alpha_2 > 1 \qquad (18)$$

ифодани ёза оламиз. Шунга ўхшаш бутун бўлмаган $\alpha_2,\ldots,\alpha_{n-1}$ лар учун қуйидагиларга эга бўламиз:

$$\left.\begin{aligned}
&\alpha_2 = q_2 + \frac{1}{\alpha_3}, \alpha_3 > 1,\\
&\cdots\cdots\cdots\cdots\\
&\alpha_{n-2} = q_{n-2} + \frac{1}{\alpha_{n-1}}, \alpha_{n-1} > 1,\\
&\alpha_{n-1} = q_{n-1} + \frac{1}{\alpha_n}, \alpha_n > 1.
\end{aligned}\right\} \qquad (19)$$

Булардан (13)-га ўхшаш α учун ушбу

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{\alpha_n}}}} = (q_1, q_2, \ldots, q_{n-1}, \alpha_n) \qquad (20)$$

ушлуксиз каср кўринишдаги ёйилмани ҳосил қиламиз. Равшанки, агар α иррационал сон бўлса, у ҳолда α_n ҳам иррационал сон бўлади. Фараз қилайлик $n \geq 2$ ва δ_n муносиб каср α га тенг бўлмасин; δ_{n-1} ва δ_n ларнинг ифодалари α нинг (20)-ифодасидан осонлик билан ҳосил бўлади, δ_{n-1} ни ҳосил қилиш учун $\frac{1}{\alpha_n}$ ни нол билан δ_n ни ҳосил қилиш учун эса $\frac{1}{\alpha_n}$ ни $\frac{1}{q_n}$ билан алмаштириш керак. $\alpha_{n-1}, \alpha_{n-2}, ..., \alpha_2, \alpha$ лар учун келтирилган (18) ва (19) тенгликлардан кўрамизки:

Биринчи алмаштиришдан	Иккинчи алмаштиришдан
α_{n-1} камаяди,	α_{n-1} ортади,
α_{n-2} ортади,	α_{n-2} камаяди,
α_{n-3} камаяди,	α_{n-3} ортади

ва ниҳоят, бу алмаштиришларни биридан α камаяди ва иккинчисидан α ортади. Айтилганлардан шундай хулосага келамизки δ_{n-1} ва δ_n ларнинг бири α дан кичик, иккинчиси эса α дан катта, демак, α сон δ_{n-1} ва δ_n ларнинг орасида жойлашган.

28-т е о р е м а. Ушбу тенгсизлик ўринлидир

$$|\alpha - \delta_{n-1}| \leq \frac{1}{Q_n Q_{n-1}}.$$

И с б о т. Ҳақиқатан, агар $\delta_n = \alpha$ бўлса, у ҳолда бу муносабат (тенглик аломати билан (17)-дан келиб чиқади; δ_n муносиб каср α га тенг бўлмаса, у ҳолда бу муносабат тенгсизлик аломати билан (17)- ва (20)-дан келиб чиқади).

14-§. ЧЕКСИЗ УЗЛУКСИЗ КАСРЛАР ВА УЛАРНИНГ ТАДБИҚЛАРИ

Агар α сон иррационал бўлса, у ҳолда (18) ва (19) лардан аниқланувчи барча α_n лар ҳам иррационал бўлади ва биз $[\alpha_n]=q_n,[\alpha_{n+1}]=q_{n+1},\ldots$ деб белгилаб олиб, (13)-чекли ёйилма ўрнига ушбу

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots}} = (q_1, q_2, q_3, \ldots) \qquad (22)$$

ёйилмани ҳосил қиламиз.

Равшанки, α иррационал сон бўлганда бу жараён ҳеч қачон тугамайди ва биз *чексиз узлуксиз касрга* эга бўламиз.

М и с о л: $\sqrt{56}$ нинг узлуксиз касрга ёйилмасини топинг. Қуйидагиларни топамиз

$$\sqrt{56} = 7 + \frac{1}{\alpha_1}, \alpha_1 > 1;$$

$$\alpha_1 = \frac{1}{\sqrt{56}-7} = \frac{\sqrt{56}+7}{7} = 2 + \frac{1}{\alpha_2}, \alpha_2 > 1;$$

$$\alpha_2 = \frac{7}{\sqrt{56}-7} = \sqrt{56}+7 = 14 + \frac{1}{\alpha_3}, \alpha_3 > 1;$$

$$\alpha_3 = \frac{1}{\sqrt{56}-7} = \alpha_1; \alpha_4 = \alpha_2, \alpha_5 = \alpha_3 = \alpha_1, \ldots$$

Шундай қилиб, биз қуйидаги даврий касрни ҳосил қилдик:

$$\sqrt{56} = (7,2,14,\ldots) = (7,(2,14)).$$

Узлуксиз касрларни алгебраик ва трансцендент тенгламаларни ечишга қўллаш мумкин. Энди биз узлуксиз касрларни календар (тақвим) тузишдаги тадбиқини қараб чиқамиз:

Астрономиядан маълумки, бир тропик йил, яъни Ер Қуёш атрофида бир марта айланиб чиқиш вақти 365, 24220... «ўртача» кеча-кундуз (сутка) бошқача айтганда 365 кун, 5 соат, 48 минут, 46 секундга тенг. Кўриниб турибдики йилнинг кеча-кундузга нисбатан бундай мураккаб нисбатда бўлиши амалий ҳаётда ўта ноқулай, албатта уни, аниқлиги кам бўлса ҳам, соддароқ нисбат билан алмаштириш керак. Бунинг учун $\alpha = 365{,}24220...$ сонни узлуксиз касрга ёямиз:

$$\alpha = 365 + \frac{1}{\alpha_1}, \alpha_1 > 1;$$

$$\alpha_1 = \frac{1}{0{,}24220} = 4{,}1288191... = 4 + \frac{1}{\alpha_2}, \alpha_2 > 1;$$

$$\alpha_2 = \frac{1}{0{,}1288191} = 7{,}7628239... = 7 + \frac{1}{\alpha_3}, \alpha_3 > 1;$$

$$\alpha_3 = \frac{1}{0{,}7628239} = 1{,}3109185... = 1 + \frac{1}{\alpha_4}, \alpha_4 > 1;$$

$$\alpha_4 = \frac{1}{0{,}3109185} = 3{,}2162769... = 3 + \frac{1}{\alpha_5}, \alpha_5 > 1;$$

$$\alpha_5 = \frac{1}{0{,}2162769} = 4{,}6237023... = 4 + \frac{1}{\alpha_6}, \alpha_6 > 1.$$

Шундай қилиб, қуйидаги чексиз узлуксиз каср ёйилмасини ҳосил қилдик:

$$365{,}24220... = 365 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \ddots}}}}} = (365,4,7,1,3,4...).$$

Энди қуйидаги

		365	4	7	1	3	4	...
P_q	1	365	1461	10592	12033	46751		...
Q_k	0	1	4	29	33	128		...

жадвални тузиб, муносиб касрларни ҳосил қиламиз:

$$\delta_1 = 365; \delta_2 = 365\frac{1}{4}; \delta_3 = 365\frac{7}{29}; \delta_4 = 365\frac{8}{33}; \delta_5 = 365\frac{31}{128},...$$

Равшанки

$$\alpha - \delta_1 = 0{,}24220; \alpha - \delta_2 = -0{,}0078; \alpha - \delta_3 = 0{,}00082; \alpha - \delta_4 = -0{,}00022; \alpha - \delta_5 = 0{,}00012.$$

Демак, муносиб касрлар борган сари α нинг берилган қийматига яқинлашиб боради. Йилнинг узунлиги сифатида $\delta_2 = 365\frac{1}{4}$ қадимий халқлар (мисрликлар, бобиллар, хитойлар) га маълум эди, лекин улар мунтазам равишда қабиса йилларини ишлатмас эдилар.

Милоддан олдин 238 йилнинг 7-мартида Птоломей III Эвергеннинг Декрети чиқди. Бу Декретда кўрсатилишича, ҳар бир тўртинчи йил 365 эмас, 366 кеча-кундуз (сутка) дан иборат бўлиши керак эди. Аммо Декрет 40 йилдан кейин тамоман эсдан чиқиб кетди; қарийб икки асрдан кейин – милоддан аввал 46-йилда Рим консули Юлий Цезар Миср астрономи Сосиген маслаҳати билан уни қайтадан тиклаб, ҳар тўрт йилда феврал ойида 1 кун киритиб қўйди. Бу эса

ёки с т и л ёки Юлий тақвими (календари) деб аталади. Юлий тақвими тропик йилдан 11 минут 14 секунд (ёки 0,25 -0,24220...=0,0078 кун) ортиқ бўлиб, 400 йилда тахминан 3 кунга кечикилади, 16-асрга келиб бу фарқ 10 кунга етди. Натитжада христиан байрамлари ва баҳорги тенг кунлик 21 мартдан 11 мартга келиб қолди. Бу хатони тузатиш учун Рим папаси Григорий XIII 1582 йил 24 февралда италиялик математик А.Л.Лилио лойиҳаси бўйича ислоҳот ўтказди.

Григорий тақвимида йилнинг узунлиги $365\frac{7}{29}$ ва $365\frac{8}{33}$ дан катта, унинг хатолиги ҳам катта. Григорий тақвимининг Юлий тақвимидан фарқи шундан иборатки, унда ҳар бир юзинчи йил қабиса (высокосный) бўлмай, фақат юзликларнинг сони 4 га бўлинадиган юзинчи йиллар қабисадир. Шундай қилиб, 1700, 1800, 1900-йиллар қабиса йили бўлмай, 1600 ва 2000 йиллар қабиса йилидир.

Католик мамлакатларида 1 март 1582 йилдан Григорий тақвимига ўтишди, шу вақтгача ортиб қолган 10 кеча-кундуз 5-октябрдан 14-октябргача ўчириб ташланди, яъни 5 октябр ўрнида 15-октябр деб ҳисоблашди.

Энг аниқ тақвимни Эронда 1079 йилда буюк шоир, математик, астроном Умар Хайём киритди. У 33 йиллик циклни киритди, унда етти марта қабиса йили 4 нчи йил бўлиб, саккизинчиси 4 йил эмас, 5 йил ҳисобланади.

Шундай қилиб, ҳар 33 йилда ҳосил бўладиган $33\cdot0,24220...=8$ йил тузатилади, яъни ҳар бир йилнинг узунлиги $365\frac{8}{33}$ кеча-кундуздир. Бу эса δ_4 тўртинчи муносиб касрнинг ўзгинасидир.

Энг ажабланарли жойи шундаки Умар Хайём даврида узлуксиз касрлар математикага киритилмаган эди, у $365\frac{8}{33}$

сонни қандай қилиб топди экан? Бу Хайёмнинг буюклигининг яна бир далолатидир.

3-БОБ УЧУН МАШҚЛАР.

1. Евклид алгоритмини қўллаб, (6188, 4709) ни топинг (ж.17).
2. Евклид алгоритмини қўллаб, (23113, 54259, 42137, 52519) ни топинг (ж.19).
3. Қуйидаги сонларнинг энг кичик умумий карралисини топинг: 1)843, 491; 2) 514, 818, 1293 (ж.1) 413913; 2) 271820118).
4. Евклид алгоритмини қўллаб, берилган a ва b сонларнинг энг катта умумий бўлувчиси d ни ва уни d=a x+by кўринишда тасвирлашни амалга оширадиган x ва y ларни топинг: 1) a =624, b=891; 2) a =449, b=1243.
5. Кетма-кет бўлиш жараёнида (11-§) ҳосил бўлган r_n қолдиқлар $r_{n+2} < \frac{1}{2} r_n (n = 1,2,...)$ тенгсизликни қаноатлантиришини кўрсатинг. Бундан фойдаланиб, Эвклид алгоритмида мумкин бўлган бўлишлар сонини чамаловчи баҳони топинг.
6. Қуйидаги 1)$\frac{3621}{2769}$,2)$\frac{6165}{7809}$ касрларни узлуксиз касрга ёйиш ёрдамида қисқартиринг. (ж.1)$\frac{17}{13}$,2)$\frac{15}{19}$.)
7. Қуйидаги 1)$\frac{571}{359}$,2)$\frac{385}{648}$,3)$\frac{5831}{4237}$4)$\frac{2415}{1995}$,5)$\frac{736894}{520379}$ сонларни узлуксиз касрларга ёйинг ва мос равишдаги муносиб касрларни топинг.

Маҳражи Q_k дан ошмайдиган барча рационал сонлар орасида α ҳақиқий сонни энг аниқ тасвирловчи каср $\frac{P_k}{Q_k}$ муносиб касрдан иборатлигини исботланг.

Муносиб касрлар учун ушбу $\frac{P_{k+2}}{Q_{k+2}} - \frac{P_k}{Q_k} = \frac{(-1)^k q_{k+1}}{Q_k Q_{k+2}}$ формулани исботланг.

10. 15 § даги муносабатлардан фойдаланиб $\frac{P_n}{Q_n}$ нинг $q_0, Q_1, Q_2, ..., Q_n$ лар орқали ошкор кўринишни топинг.

11. Барча натурал n лар учун $\frac{n^4 + 3n^2 + 1}{n^3 + 2n}$ ни қисқармас касрлигини кўрсатинг (кўрсатма: муносиб касрнинг хоссасига асосан).

12. Ушбу $\sqrt{a^4 + 2a}$ ифодани даврий чексиз узлуксиз касрга ёйинг. (ж. $(a^2, a, 2a^2, 2a^2)$).

13. $\sqrt{11}$ сонга махражи 60 дан ортмайдиган энг яхши рационал яқинлашишни топинг ва хатосини баҳоланг.

14. Қуйидаги $1)\sqrt{5}, 2)\sqrt{7}, 3)\sqrt{13}, 4)\sqrt{41}, 5)\sqrt{59}$ квадрат илдизларни узлуксиз касрларга ёйиб, 0,0001 аниқликда ҳисобланг.

15. $1)\pi = 3{,}141592653507..., 2)\ e = 2{,}718281828459045...$ сонларнинг узлуксиз касрга ёйилмасининг дастлабки бешта муносиб касрлари топилсин.

16. Узлуксиз каср ёрдамида $3x^2-7x-3=0$ тенгламанинг иккала илдизи 0,0001 аниқликда топилсин.
(Ж. $x_1=((2,1,2))\approx 2{,}7032; x_2=(-1,1,1,(1,2,2))=-0{,}3699$).

17. Қуйидаги касрларни узлуксиз касрларга ёйинг ва уларнинг муносиб касрларини топинг:

а) $\frac{137}{143}$, б) $\frac{521}{143}$, в) $\frac{247}{74}$, г) $\frac{313}{57}$, д) $\frac{77}{187}$.

3-бобга доир тарихий маълумот

1. Инглиз математиги Э. Д.Бут ўзини «Сонли методлар» (Andrew D.Booth, D. Sc. Numerical methods, second edition, London, Butterworts Scientific publication, 1957) китобининг кириш қисмида «Ҳисоблаш методларини системага солганлиги учун биринчи араб математиги Муҳаммад Ибн-Мусо ал-Хоразмийдан миннатдормиз» деб ёзган эди.

Ҳозирги вақтда а л г о р и т м деб *маълум бир типга оид ҳамма масалаларни ечишда қўлланиладиган барча амаллар системасининг муайян тартибда бажарилиши ҳақидаги аниқ қоидага* айтилади.

Ал-Хоразмий "Ҳинд саноғи тўғрисида" ги (қ.[54]) ги арифметик рисоласида ўнлик саноқ системасини ва бу системада тўрт арифметик амалларнинг бажариш қоидаларини биринчи бўлиб баён қилган. Бу рисола 12-асрда латин тилига таржима қилинган ва у Осиёда ҳам Европада ҳам ўнлик саноқ системасини қўлланилишига ва тарқалишига пойдевор бўлган.

Европада бундай қоидалар ал-Хоразмий номи билан аталиб «Algorizmi» дейилган. Ал-Хоразмий рисоласининг биринчи сўзлари: Қола ал-Хоразмий сўзлари латин тилига «Dixit Algorizmi» (Дедики ал-Хоразмий) деб таржима қилинган. Бунда ал-Хоразмий бузилиб, Algorizmi деб ёзилган. Кейинчалик у Algorithmi ва Algorithmus кўринишларни олиб, охирида фанда ҳар қандай регуляр ҳисоблаш жараёнини билдирадиган «алгоритм» сўзига айланган.

2. Ал-Хоразмийнинг «Китоб ал-мухтасар фи ҳисоб ал-жабр ва-муқобала» («Тиклаш ва қарама-қарши қўйиш ҳақида қисқача китоб») номли алгебраик рисоласида биринчи марта

алгебра математиканинг мустақил бўлими сифатида ажралади. Унда алгебраик миқдорлар устида амаллар алмашириш қоидалари, 1-, 2-даражали алгебраик тенгламаларни ечиш усуллари ва бундай тенгламаларга келадиган турли амалий масалалар, жумладан меросни бўлиш масаласи ажралган.

Рисола латинчага таржима қилинганда «вал-муқобала» сўзлари тушиб қолдирилган ва «algebra» номи билан жаҳонга тарқалган. (Шунинг учун бўлса керак ўрта асрларда Европа давлатларида синган қўл-оёқни тиклайдиган табиб (костоправ) ни алгебрист деб аташган).

3. Абу Абдулло Муҳаммад ибн-Мусо ал-Хоразмий (780, Хива – 850, Боғдод) ёшлигиданоқ илм-фанга қизиққан. Ўша даврда катта илмий ва маданий марказ ҳисобланган Халифатнинг пойтахти – Боғдодга таклиф қилинган. Аввал халифа ал-Маъмун (813-833), сўнгра Мутасим (833-842) ва ал-Восиқ (842-847) саройларида ишлаган. У Шарқнинг биринчи академияси – Бағдоддаги «Байтул ҳикмат» («Донолар уйи») да фаол иш олиб борган. Биринчи халифанинг хукмронлигида у «Донолар уйи» нинг кутубхонасини бошқарган. Бу ерда унинг раҳбарлигида арблар ва бошқа халқлар билан бир қаторда Аҳмад Фарғоний, *Аҳмад ибн Марвазий* каби Ўрта Осиёлик олимлар тадқиқот олиб боришган. Хоразмий ўз ижодиётида Ўрта Осиёнинг Исломдан олдинги ўзига хос илмий меросига, кўпни Ҳиндистон ва Яқин Шарқнинг эллинистик давлатларидаги илмий ғояларга таяниб ишлади.

Хоразмийнинг бизгача етиб келган илмий ишлари, шу даврда Яқин ва Ўрта Шарқда халқаро тил вазифасини бажарган, а р а б т и л и д а ёзилган.

Шунинг учун ҳам Яқин ва Ўрта Шарқдаги олимларни Европада араб олимлари деб билишган. Инглиз математиги Д.Бут ал-Хоразмийни араб математиги ва Европада ҳинд рақамлари 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 ларни араб рақамлари дейишига ҳам сабаб шу. (Совет иттифоқи даврида илмий

мақолалар рус тилида ёзилганлиги ва фамилиялар руслашган формада ёзилганлиги учун нафақат россиялик олимларни, балки бошқа республикадаги олимларни ҳам Узоқ Хорижда рус олимлари деб аташар эди).

4. 16-асрдаёқ узлуксиз касрлар математикага кира бошлади, у италиялик математик Бомбелли (Рафаэле, 1530-1572) ишларида учрайди. Бошқа бир италиялик математик Катальди (Cataldi P.A. 1626 йилда ўлган) 1613 йилда узлуксиз касрларни (13)-кўринишда тасвирлаган, фақат «+» ўрнига «et» ёзган. Ньюберглик математик Швентер (Schwenter, 1585-1636) узлуксиз касрларни (13)-кўринишда ёза бошлади. 31-бетдаги схемани қўллади, муносиб касрларни ҳосил қилиш қонуниятини топди.

27- ва 29-теоремалар нидерланд математиги, физиги ва механиги Гюйгенс (Хейгенс Христиан, 1629-1695) га маълум эди, у бу теоремаларни тишли қилдираклар назариясига қўллади. Немис математиги, астрономи ва физиги Ламберт (Johan Heinrich, 1728-1777) 1766 йилда узлуксиз касрлар ёрдамида e ва π сонларнинг иррационаллигини исботлади.

5. Француз математиги, механиги Лагранж (Lagrange Jozeph-Louis, 1736-1813) ва Л.Эйлерлар чекли ва чексиз узлуксиз касрларнинг асосий хоссаларини ўрганишди, ҳар хил тадбиқларини топишди. Улар a_n элементлари функцияларидан иборат булган узлуксиз касрларни ўрганишди. Рус математиклари П.Л.Чебишев (Пафнутий Львович, 1821-1922) элементлари кўпҳадлардан иборат узлуксиз касрларни *ортогонал кўпҳадларни* ўрганишга қўллади.

6. Леонард Эйлер (Leonard Euler, 1707-1783) Швейцариянинг Базел шаҳрида пастор (руҳоний) оиласида туғилган. Дастлабки маълумотини отасидан олган, сўнгра Базел университетида ўқиди (1720-1724), у ерда И.Бернулли лекцияларини тинглади. 1727 йилда Петербург Фанлар Академиясининг таклифига биноан Петербургга келди. У Петербургдаги ҳаётнинг биринчи 14 йиллик даврида 80 дан

ортиқ асар ёзиб, 50 тасини нашр қилдирди. 1741 йилда Эйлер Пруссия Қироли Фридрих II таклифи билан Берлин Фанлар Академиясига келди. Берлиндаги 25 йиллик ҳаёти даврида 400 га яқин асар (катта монографиялар билан) тайёрлади.

1766 йилда Эйлер ўз оиласи билан Петербургга қайтиб келди ва катта ёшлиги ҳамда кўр бўлиб қолишига қарамай, умрининг охиригача 400 га яқин асарларни нашрга тайёрлади.

Эйлер ижодининг муҳим хусусияти унинг ўта унумдорлиги бўлиб, Эйлер ҳаётлигида унинг ишларидан 550 га яқин китоб ва мақолалари нашр қилинган. Эйлер ишларининг умумий сони қарийб 850 та. Швейцариянинг табиий-илмий жамияти Эйлернинг Тўла асарлар тўпламини 1909 йилдан бери чоп эта бошлаб, 1975 йилда тугатди, у 72 жилддан иборат. Эйлернинг билим доираси ниҳоятда кенг бўлиб, ўз давридаги математика, механика, эластиклик назарияси, физика, оптика, мусиқа назарияси, машиналар назарияси, баллистика, денгиз фани ва бошқаларни ўз ичига олган. Эйлер асарларининг қарийб 60% математикага, қолган 40% унинг тадбиқларига оид.

Чебишевнинг таъкидлашича сонлар назариясининг умумий қисмини ташкил этувчи барча тадқиқотлар Эйлердан бошланган, у сонлар назариясига бағишлаб 100 дан ортиқ асар ёзган. Буюк француз математиги П.С.Лаплас (de Laplace, Пьер Симон, 1749-1827) "Эйлер 18-асрни 2-ярмидаги барча математикларнинг устози эди" деб ёзади. Йирик математиклар П.С.Лаплас, Ж.Л.Лагранж (Logrange Жозеф Луи, 1736-1813), Г.Монж (Monge Гаспар, 1746-1818), А.М.Лежандр, О.Коши (Cauchy Огюстен Луи, 1789-1857), М.В.Остроградский (Михаил Васиьевич, 1801-1862) ва б. ўз изланишларини бевосита унинг асарлари асосида бошлаганлар.

4-БОБ. АРИФМЕТИК ФУНКЦИЯЛАР ВА ТУБ СОНЛАРНИНГ ТАҚСИМОТ ҚОНУНИ

Арифметик функцияларни назарий-сонли функциялар ҳам дейишади.

Т а ъ р и ф. Аниқлаш соҳаси натурал сонлар тўплами ёки бутун рационал сонлар тўплами ва ҳ. к. дан иборат бўлган ҳақиқий ёки комплекс қийматларни қабул қиладиган функция *арифметик функция* дейилади.

Бу арифметик функцияларнинг кенг маънодаги таърифидир. Одатда арифметик функция деб бирор арифметик хоссага эга бўлган, таърифда келтирилган турдаги функцияга айтилади. Кенг қўлланиладиган арифметик функциялар анъанавий белгилашга эга. Масалан, $\varphi(n)$ - Эйлер функцияси, $d(n)$ ёки $\tau(n)$ – n-натурал соннинг бўлувчилари сони, $\mu(n)$ - Мебиус функцияси, $\Lambda(n)$ - Мангольд функцияси, $\sigma(n)$ ёки $s(n)$ - n натурал соннинг бўлувчилари йиғиндиси.

Арифметик функциялар тўпламига юқорида кўрилган $[x]$ - соннинг бутун қисми ва $\{x\}$- соннинг каср қисмини ҳам киритишади, бу ерда x-ихтиёрий ҳақиқий сон.

Бошқа арифметик функциялар бирор шартни қаноатлантирадиган сонларнинг қанчалигини белгилайди. Масалан, $\pi(x)$ - функция, x дан ошмайдиган туб сонларнинг қанчалигини, $\pi(x, q, \ell)$ эса махражи q га, биринчи ҳади ℓ га тенг бўлган арифметик прогрессиядаги туб сонларнинг қанчалигини белгилайдиган функция.

15-§. МУЛТИПЛИКАТИВ ФУНКЦИЯЛАР

5-т а ъ р и ф. Барча бутун сонлар тўпламида аниқланган ва қуйидаги икки:

1) ихтиёрий ўзаро туб m ва n натурал сонлар учун

$$f(mn)=f(m)\,f(n) \qquad (23)$$

тенглик ўринли;

2) f(m) айнан нолга тенг эмас,

шартни қаноатлантирувчи f(n)-арифметик функция ***мултипликатив функция*** дейилади.

6 - т а ъ р и ф. Агар (23)-тенглик ихтиёрий иккита m ва n натурал сонлар учун бажарилса, арифметик функция ***тўла мултипликатив функция*** дейилади.

Равшанки, тўла мултипликатив функция мултипликатив функция бўлади, акси умуман олганда нотўғри.

1-м и с о л. $f(n)=n^s$, s ихтиёрий комплекс сон, тўла мултипликатив функциядир, чунки

$$f(mn)=(mn)^s=m^s n^s=f(m)\,f(n).$$

Мултипликатив функциялар қуйидаги хоссаларга эга.

30-т е о р е м а. Агар f(n) мултипликатив функция бўлса, у ҳолда f(1)=1.

И с б о т. Ҳақиқатан, таърифга кўра, f(n) айнан нолга тенг эмас, яъни шундай a сон топиладики, $f(a)\neq 0$. У ҳолда $f(a)=f(1\cdot a)=f(1)\,f(a)$ га кўра f(1)=1 бўлади.

31-т е о р е м а. Агар $f_1(n)$ ва $f_2(n)$ иккита мултипликатив функция бўлса, уларнинг кўпайтмаси $F(n)=f_1(n)\,f_2(n)$ ҳам мултипликатив функциядир.

И с б о т. Ҳақиқатан $f_1(n)$ ва $f_2(n)$ мултипликатив функциялар бўлгани учун

$$F(1)=f_1(1)f_2(1)=1,$$

яъни F(n) айнан нолга тенг эмас. Иккинчи томондан,

$$F(mn)=f_1(mn)f_2(mn)=f_1(m)\cdot f_1(n)\cdot f_2(m)\cdot f_2(n)=$$
$$=f_1(m)f_2(m)f_1(n)\,f_2(n)=F(m)F(n).$$

Теорема исботланди.

32-т е о р е м а. Фараз қилайлик, f(n) мултипликатив функция ва $n=p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$ ифода n соннинг каноник ёйилмаси бўлсин. У ҳолда n нинг барча бўлувчилари бўйича

тузилган йиғинди $\sum_{d/n}$ символ билан белгиланса, ушбу айният

$$\sum_{d/n} f(d) = [1 + f(p_1) + f(p_1^2) + ... + f(p_1^{a_1})]... \quad (24)$$
$$...[1 + f(p_k) + f(p_k^2) + ... + f(p_k^{a_k})]$$

ўринлидир (n=1 бўлганда, айниятнинг ўнг томони 1 га тенг деб ҳисобланади).

И с б о т. Ўнг томондаги қавслари очиб чиқсак,

$$f(p_1^{\beta_1})f(p_2^{\beta_2})...f(p_k^{\beta_k}) = f(p_1^{\beta_1}p_2^{\beta_2}...p_k^{\beta_k}),$$
$$0 \le \beta_1 \le a_1, 0 \le \beta_2 \le a_2, ...,0 \le \beta_k \le a_k$$

кўринишдаги қўшилувчиларнинг йиғиндиси ҳосил бўлади, шу билан бирга, бундай қўшилувчилардан ҳеч қайсиси тушиб қолмайди ва йиғиндида фақатгина бир марта қатнашади. Равшанки, бу йиғинди (24)-тенгликни чап томонини айнан ўзини ифодалайди (24-теоремага кўра).

Энди (24)-тенгликнинг хусусий ҳолини кўриб чиқамиз. $F(n)=n^s$ бўлсин, у ҳолда

$$\sum_{d/n} d^s = (1 + p_1^s + p_1^{2s} + ... p_1^{a_1 s})...(1 + p_k^s + p_k^{2s} + ... p_k^{a_k s}). \quad (25)$$

Бу айниятдан сонлар назарияси учун иккита муҳим формулани ҳосил қиламиз.

1.Натурал сон бўлувчиларининг йиғиндиси. s=1 бўлганда (25)-айниятнинг чап томонидан n соннинг барча бўлувчилари йиғиндиси

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} ... \frac{p_k^{a_k+1} - 1}{p_k - 1}$$

ҳосил бўлади.

Мисол.

$$\sigma(15120)=\sigma(2^4\cdot 3^3\cdot 5\cdot 7)=\frac{2^{4+1}-1}{2-1}\cdot\frac{3^{3+1}-1}{3-1}\cdot\frac{5^{1+1}-1}{5-1}\cdot\frac{7^{1+1}-1}{7-1}=$$
$$=31\cdot 40\cdot 6\cdot 8=59520.$$

2. Натурал соннинг бўлувчилари сони. s=0 бўлганда (25)-нинг чап томони n натурал соннинг барча бўлувчиларининг сони τ(n) ни ифодалайди.. Бундан қуйидаги формулани ҳосил қиламиз:

$$\tau(n)=(a_1+1)(a_2+1)...(a_k+1).$$

Мисол.

τ(15120)=(4+1)(3+1)(1+1)(1+1)=80.

16-§ МИЁБИУС ФУНКЦИЯСИ

Арифметик функцияларнинг яна бири Миёбиус функцияси μ(n) бўлиб, қуйидагича аниқланади:

$$\mu(n)=\begin{cases}1, & агар \quad m=1 \quad булса,\\ 0, & агар \quad n=p^2m \quad булса,\\ (-1)^k, & агар \quad n=p_1p_2...p_k \quad булса.\end{cases}$$

Мисоллар. Равшанки,

μ (2)=-1, μ (3)=-1, μ (4)=0, μ (5)=-1, μ (6)=1, μ (7)=-1, μ (8) 0, μ (9)=0, μ (10)=1, μ (11)=-1.

33-т е о р е м а. Фараз қилайлик, f(n) мултипликатив функция, $n=p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ эса n нинг каноник ёйилмаси бўлсин. У ҳолда

$$\sum_{d/n}\mu(d)f(d)=[1-f(p_1)][1-f(p_2)]...[1-f(p_k)]$$

тенглик ўринлидир (n=1 бўлганда ўнг томон 1 га тенг деб ҳисобланади).

И с б о т. $\mu(n)$ нинг мултипликативлиги равшан. Демак, 30-теоремага кўра $F(n)$ $\mu(n)I(n)$ функция ҳам мултипликатив ва $F(p^\alpha)$ 0 лигини ҳисобга олсак, теореманинг тасдиғи (31)-теоремадан келиб чиқади.

Хусусий ҳолда $I(n)$ 1 деб олсак, қуйидаги келиб чиқади:

$$\sum_{d/n}\mu(d)=\begin{cases}0, & агар \quad n>1 \quad булса,\\ 1, & агар \quad m=1 \quad булса.\end{cases} \tag{26}$$

Агар $f(d)=\dfrac{1}{d}$ деб олсак, у ҳолда

$$\sum_{d/n}\frac{\mu(d)}{d}=\begin{cases}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k}), & агар \quad n>1 \quad булса,\\ 1, & агар \quad n=1 \quad булса\end{cases} \tag{27}$$

Энди тадбиқлар учун муҳим бўлган қуйидаги теоремани келтирамиз.

34-т е о р е м а. Фараз қилайлик бутун мусбат

$$\delta=\delta_1, \delta_2, \ldots, \delta_k$$

сонларга исталган ҳақиқий ёки комплекс

$$f=f_1, f_2, \ldots, f_k$$

сонлар мос қўйилган бўлсин. У ҳолда S^* символ билан δ нинг 1 га тенг қийматларига мос келадиган f лар йиғиндиси ва S_d символ билан δ нинг d га бўлинадиган қийматларига мос келадиган f лар йиғиндиси белгиланса, у ҳолда

$$S^*=\sum\mu(d)S_d$$

тенгликка ўринлидир, бунда d сон δ нинг қийматларидан ақалли биттаси бўлинадиган бутун мусбат қийматларни қабул қилади.

И с б о т. Ҳақиқатан, (26)-тенгликдан фойдаланиб, S^* ни қуйидагича ёзиш мумкин:

$$S^*=f_1\sum_{d/\delta_1}\mu(d)+f_2\sum_{d/\delta_2}\mu(d)+\ldots+f_k\sum_{d/\delta_k}\mu(d).$$

Энди d бир хил қийматларга эга бўлган ҳадларни ёзиб, μ(d) ни қавслардан чиқарсак, қавслар ичида фақат оддий f лар йиғиндиси қоладики, уларга мос δ лар d га бўлинади, бу эса S_d нинг ўзидир.

17-§ ЭЙЛЕР ФУНКЦИЯСИ

7-т а ъ р и ф. Берилган n натурал сондан ошмайдиган ва n билан ўзаро туб бўлган натурал сонларнинг нечталигини ифодаловчи функция *Эйлер функцияси* деб аталиб, φ(n) каби белгиланади.

35-т е о р е м а. Фараз қилайлик $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ n нинг каноник ёйилмаси бўлсин. У ҳолда

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right) \qquad (28)$$

ёки

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_{21}^{a_2} - p_2^{\alpha_2-1})\dots(p_k^{\alpha_k} - p_k^{\alpha_k-1}) \qquad (29)$$

бўлади. Хусусий ҳолда

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}, \quad \varphi(p) = p-1. \qquad (30)$$

И с б о т. Биз бу ерда 34-теоремани қўллаймиз ва δ ҳамда f сонларни қуйидагича аниқлаймиз: m сон 0, 1, …, n-1 қатордаги қийматларни қабул қилсин, m нинг ҳар бир қийматига δ =(m, n) ва f=1 сонларни мос қўямиз.

У ҳолда S* йиғинди δ =(m, n) нинг 1 га тенг қийматлари сонига, яъни φ (n) га тенг. S_d эса δ =(m, n) нинг d га бўлинадиган қийматлари сонига тенг бўлади. Лекин d сон n нинг бўлувчиси бўлгандагина (m, n) сон d га бўлинади. Бу шарт бажарилганда, S_d йиғинди n нинг d га бўлинувчи

қийматлари сонини ифодалайди, яъни $\frac{n}{d}$ га тенг бўлади. У ҳолда қуйидагига эга бўламиз:

$$\varphi(n)=\sum_{d/n}\mu(d)\frac{n}{d}.$$

Бу ва (27)-дан (28)-формула келиб чиқади. (29) ва (30)-формулаларнинг ҳосил бўлиши равшан.

М и с о л л а р.

$\varphi(72)=72(1-\frac{1}{2})(1-\frac{1}{3})=24,$

$\varphi(125)=5^3-5^2=125-25=100,$

$\varphi(7)=7-1=6$

36-т е о р е м а. $\varphi(n)$ мултипликатив функциядир.

И с б о т. Ҳақиқатан $(m,n)=1$ бўлса, (35)-теоремадан

$$\varphi(m,n)=\varphi(m)\,\varphi(n)$$

келиб чиқади.

М и с о л.

$$\varphi(875)=\varphi(125)\,\varphi(7)=100\cdot 6=600.$$

Ниҳоят,

37-т е о р е м а. Қуйидаги

$$\sum_{d/n}\varphi(d)=n$$

Гаусс формуласи ўринлидир.

И с б о т. (24)-айниятда $f(n)=\varphi(n)$ деб оламиз ва (29)-формулани қўллаймиз, натижада

$$\sum_{d/n}\varphi(d)=[1+\varphi(p_1)+\varphi(p_1^{\alpha_1})+\ldots+(p^{\alpha})]\ldots[1+\varphi(p_k)+\varphi(p_k^2)+\ldots+\varphi(p_k^{\alpha_k})]=$$

$$=[1+(p_1-1)+(p_1^2-p_1)+\ldots+(p_1^{\alpha_1}-p_1^{\alpha_1-1})]\ldots[1+(p_k-1)+(p_k^2-p_k)+\ldots+(p_k^{\alpha_k}-p_k^{\alpha_k-1})]$$

ифодага келамиз.

Катта қавслардаги ўхшаш ҳадларни йиғсак,

$$p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}=n$$

ҳосил бўлади.

М и с о л. $n=36$ деб олсак, қуйидаги ҳосил бўлади:

$\varphi(1)+ \varphi(2)+ \varphi(3)+ \varphi(4)+ \varphi(6)+ \varphi(9)+ \varphi(12)+ \varphi(18)+ \varphi(36)= =1+1+2+2+2+6+4+6+12=36.$

18-§ ТУБ СОНЛАРНИНГ ТАҚСИМОТ ҚОНУНИ

Биз 21-теоремада натурал сонлар қаторида туб сонларнинг сони чексиз кўплигини кўрган эдик. Туб сонларнинг натурал сонлар қаторида қандай жойланишини ўрганиш сонлар назариясининг муҳим масалаларидан биридир. Қуйида 1 дан 100 гача, 101 дан 200 гача ва ҳ.к. 901 дан 1000 гача ҳамда 1001 дан 2000 гача ва ҳ.к., 9001 дан 10000 гача бўлган натурал сонлар орасидаги туб сонларнинг нечталиги келтирилган.

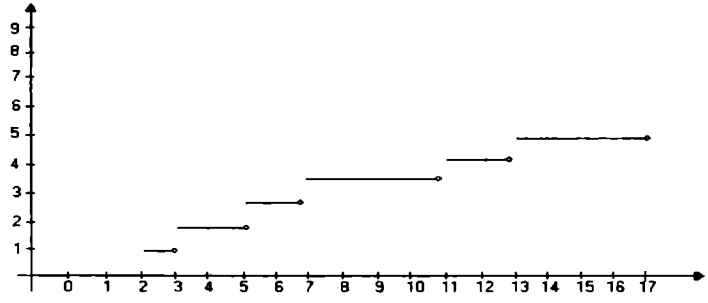
...дан	...гача	Туб сонлар (та)
1	100	26
101	200	21
201	300	16
301	400	16
401	500	17
501	600	14
601	700	16
701	800	14
801	900	15
901	1000	14
1001	2000	168
2001	3000	127
3001	4000	120
4001	5000	119
5001	6000	114
6001	7000	117
7001	8000	107
8001	9000	110
9001	10000	112

Бу жадвалга кўра туб сонлар турли 100 ва 1000 ликлар орасида турлича жойлашган. Иккита натурал сонлар орасида жойлашган туб сонлар сонини бирор аналитик усул билан ифодалаш, яъни уларнинг сонини ифодаловчи формулани топиш масаласи билан жуда кўп математиклар шуғулланишади. Жумладан, Лагранж, Гаусс ва Чебишев чуқур тадқиқотлар олиб боришган.

Одатга кўра, $\pi(x)$ орқали x ҳақиқий сондан ошмайдиган туб сонларнинг сонини белгилашади. Бу белгилашда Евклид теоремасини қуйидагича ифодалаш мумкин:

$$\pi(x) \xrightarrow[x\to\infty]{} \infty \quad \textit{ёки} \quad \lim_{x\to\infty} \pi(x) = \infty .$$

Биринчи чизмада $\pi(x)$ функциянинг графиги келтирилган. $\pi(2)=1$, $\pi(3)=\pi(4)=2$, $\pi(5)=\pi(6)=3$, $\pi(7)=\pi(8)=\pi(9)=\pi(10)=4$, $\pi(11)=\pi(12)=5$, $\pi(13)=6$ ва ҳ.к. зинапоянинг чап чети $\pi(x)$ графигига



1-чизма

тегишли бўлиб, ўнг чети унга тегишли эмас. Бир туб сондан иккинчисига ўтишда $\pi(x)$ нинг қиймати бирга ортади; унинг ҳар бир x учун қийматини бу бирларни x дан ортмайдиган

барча туб сонлар учун қўшиб чиқиш билан ҳосил қилинади. Шунинг учун ҳам $\pi(x)$ ни қуйидагича ёзиш мумкин:

$$\pi(x)=\sum_{p\le x}1.$$

Лежандр туб сонлар жадвалини текшириш натижасида 1808 йилда $\pi(x)$ ни тақрибий ҳисоблаш учун империк формулани эълон қилди (ўша вақтда туб сонлар жадвали 400000 гача бўлган сонлар учун тузилган эди).

Лежандр исботсиз тасдиқланган эдики, етарлича катта x лар учун

$$\pi(x)\approx\frac{x}{\ln x-B}$$

бўлиб, бунда B=1,08366.

Гаусс, Лежандрга боғлиқсиз равишда, натурал қаторнинг ҳар бир мингта сони орасидаги туб сонларнинг сонини ҳисоблаб, қуйидаги фаразни олға сурди:

$$\pi(x)\approx\int_2^x\frac{dt}{\ln t}$$

Лопитал қоидасини қўллаб, кўрсатиш мумкинки,

$$\lim_{x\to\infty}\left(\int_2^x\frac{dt}{\ln t}:\frac{x}{\ln x}\right)=1. \qquad (31)$$

М а ш қ. (31)-тенглик исботлансин.

Лежандр ва Гаусс фаразиялари $\pi(x)$ учун бир хил асимптотик баҳога олиб келади:

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\ln x}}=1 \quad \textit{ва} \quad \lim_{x\to\infty}\frac{\pi(x)}{\int_2^x\frac{dt}{\ln t}}=1$$

Ёки мос равишда

$$\pi(x)\sim\frac{x}{\ln x} \text{ ва } \pi(x)\sim\int_2^x\frac{dt}{\ln t}. \qquad (32)$$

Бу тенгликлар *туб сонлар тақсимотининг асимптоик қонуни деб аталувчи қонунни* ифодалайди, бу қонун ҳақиқатан ҳам ўринлидир. Аммо буни назарий жиҳатдан асослаш учун Лежандрнинг ҳам, Гауснинг ҳам кучлари етмади. (32)-муносабатлар ва ундан ҳам кучли тасдиқларни исботлаш кейинги авлоддаги буюк математикларнинг изланишлари натижасида амалга оширилди.

П.Л.Чебишев 1852 йилда «Туб сонлар ҳақида» номли рисоласида $\pi(x)$ функцияси учун

$$0{,}92129\frac{x}{\ln x} < \pi(x) < 1{,}0555\frac{x}{\ln x} \qquad (33)$$

тенгсизликларни келтириб чиқарди. Бу тенгсизликлар *Чебишев тенгсизликлари* дейилади. Чебишевнинг туб сонлар тақсимотига оид буюк натижалари унинг замондошларида катта таассурот қолдирди.

Сильвестер 1881 йилда «Сонлар назарияси соҳасида янада янги муваффақиятга эришиш учун ақл-заковати бўйича Чебишев оддий одамлардан қандай юқори турган бўлса, Чебишевдан шундай даражада юқори турадиган одам туғилишини кутиш лозим» деган эди.

1909 йилда Э.Ландау ўзининг туб сонлар тақсимотига бағишланган махсус асарида Чебишев тўғрисида шундай ёзади:

«Евклиддан сўнг туб сонлар ҳақида муаммони ечиш учун тўғри йўл танлаган ва муҳим муваффақиятларни қўлга киритган одам Чебишев эди».

Аммо П.Л.Чебишевнинг ютуқлари туб сонлар тақсимотининг асимптотик қонунини исботлаш учун, яъни

$$\lim_{x\to\infty}(\pi(x):\frac{x}{\ln x})$$

нинг мавжудлигини кўрсатиш учун етарли эмас эди. Агар лимит мавжуд бўлса, бу лимит 1 га тенг бўлишини у кўрсатган эди.

1859 йилда Б.Риман бу муаммони ҳал этишда комплекс аргументли $\zeta_v(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$ $(\mathrm{Re}\, s=\sigma>1)$ функция ёрдамида туб сонларнинг тақсимоти учун муҳим натижаларни олиш мумкинлигини айтган эди. Ҳозирги вақтда ζ (s) *Риманнинг дзета-функцияси* деб аталади. Бу функцияни Эйлер ва Чебишев s нинг ҳақиқий қийматлари учун ўрганишган эдилар. Риман ζ(s) (s=σ+it) нинг барча илдизлари $\sigma=\frac{1}{2}$ тўғри чизиқда ётади, деб айтган эди. *Риманнинг гипотезаси* деб аталадиган бу тасдиқ ҳозиргача исбот ҳам, инкор ҳам қилинмаган. Агар бу гипотеза исбот қилинса, туб сонларнинг тақсимоти учун кўп ажойиб теоремалар келиб чиқар эди. Риман ўзининг методи бўйича бирорта арифметик натижани қўлга киритмаган. Аммо 1896 йилда Ж.Адамар ва Валле-Пусен бир-бирига боғлиқсиз равишда Риман методидан фойдаланиб,

$$\lim_{x\to\infty}(\pi(x):\frac{x}{\ln x})$$

нинг мавжудлигини исбот қилишди.

Туб сонлар тақсимотининг элементар (комплекс ўзгарувчи функциялардан фойдаланмасдан) исботини 1949 йилда даниялик математик А.Сельберг ва венгриялик математик Р.Эрдеш кўрсатишди. Бу исбот бошқа математиклар томонидан соддалаштирилди. Энг содда исботни А.Г.Постников ва Н.П.Романов биргаликда топганлар.

19-§ ТУБ СОНЛАРГА ОИД АЙРИМ МУАММОЛАР

1. Биринчи навбатда қуйидаги масалани қарайлик: шундай чегараларни топиш керакки, улар орасида ҳеч бўлмаганда битта туб сон жойлашган бўлсин. 1845 йилда Бертран шундай фаразни айтган эди: агар $2a>7$ бўлса, у ҳолда a ва $2a-2$ орасида ҳеч бўлмаганда битта туб сон мавжуд. Бу фаразни Чебишев 1852 йилда исбот қилди. Бошқа фаразлар ҳам ўртага ташланган эди. Масалан, Дебов фарази: n^2 ва $(n+2)^2$ орасидаги туб сонларнинг сони иккитадан кам эмас.

Гаусс кўрсатган эдики, сонларнинг 26379-юзталигида бирорта ҳам туб сон йўқ, 27050-юзталигида эса 17 туб сон бор, яъни 3-юзталигидагидан ҳам кўп. Умуман айтганда, шундай етарлича катта оралиқлар топиладики, унда бирорта ҳам туб сон ётмайди. Масалан, $N=n!=1\cdot 2\cdot 3\cdots n$ бўлсин, у ҳолда n қанча катта бўлмасин, $N+2$, $N+3$, ..., $N+n$ сонларнинг барчаси таркибли бўлади.

Ягона қўшни туб сонлар 2 ва 3 дир, чунки бошқа қўшни сонларнинг бири жуфт. Лекин p ва $p+2$ кўринишдаги (қўшни тоқ сонлар) нинг ҳар иккаласи туб бўлиши мумкин. Масалан, 3,5; 5,7; 11,13; 17,19; 29,31; 41,43; 59,61; 71,73; 101,103. Бундай сонлар жуфтлиги «*эгиз туб сонлар*» дейилади. Жуда катта «эгиз»лар ҳам топилган, масалан, 109619, 109621; 10009871, 10009873; 1000061087, 1000061089 эгиз туб сонларнинг сони чеклими ёки чексизми маълум эмас. 1919 йилда В.Брун қуйидаги теоремани исбот қилди.

38-т е о р е м а. Агар эгиз туб сонларнинг сони чексиз бўлса, p ва $p+2$ эгиз туб сонлар бўйича олинган $\sum\left(\frac{1}{p}+\frac{1}{p+2}\right)$ чексиз қатор яқинлашади.

Маълумки, барча туб сонлар бўйича олинган $\sum \frac{1}{p}$ чексиз қатор узоқлашади.

2. $M_n=2^n-1$ кўринишдаги туб сонлар *Мерсенн сонлари* дейилади. Бундай сонларни XVII асрда француз математиги Мерсенн қараган эди. Агар n=ab тоқ таркибли сон ва $3\le b\le n$ бўлса, у ҳолда 2^n-1 ҳам таркибли сон бўлади:

$$2^{a\,b}-1=(2^a-1)(2^{a\,(b-1)}+2^{a\,(b-2)}+\ldots 2^a+1)$$

Ихтиёрий $n=2k\ge 4$ жуфт сон учун $2^n-1=(2^k+1)(2^k-1)$ таркибли сондир. Шундай қилиб, $M_n=2^n-1$ фақат n=p туб сон бўлганда туб сон бўлиши мумкин. Масалан, p=2, 3, 5, 7, 13, 17, 19 бўлганда, Мерсенннинг қуйидаги туб сонларига эга бўламиз: $M_1=3$, $M_3=7$, $M_5=31$, $M_7=127$, $M_{13}=8191$, $M_{17}=131071$ ва $M_{19}=524287$, лекин p=11, 23, 29 бўлганда, M_p таркибли сондир. Катта p лар учун M_p нинг туб ёки таркиблилигини аниқлаш катта ҳисоблашларни талаб қилади. Кўрсатилганки, M_{31} (Эйлер, 1750 й), M_{61} (Первушин, 1883 й), M_{89} ва M_{107} (Поуэрс, 1907 ва 1914 йиллар) – туб сондир. 1952 йилгача маълум бўлган энг катта Мерсеннинг сони 39 рақамдан иборат ушбу $M_{127}=170141183460469231731687303715884105727$ сондир.

ЭҲМ ларни қўллаш натижасида 1952 йилда p=521, p=607, p=2203 ва p=2281 бўлганда M_p нинг тублиги кўрсатилган эди. 1957 йилда M_{3217} соннинг тублиги кўрсатилган. Бу соннинг рақамлари сони 969 та.

Ҳозирги вақтда энг катта Мерсеннинг туб сони M_{44497} бўлиб, унинг рақамлари 13390 тадан кўпдир. Мерсеннинг туб сонлари чексиз кўпми? Бу масала ҳозиргача ечилмаган.

3.Одатда *Ферма сонлари* деб аталувчи $F_n=2^n+1$ кўринишдаги сонлар фақат $n=2^k$ бўлгандагина туб сон бўлиши мумкин. Ҳақиқатан, агар n сон бирор $1<a$ тоқ кўпаювчига эга бўлса, у ҳолда

$$2^n+1=2^{\frac{n}{a}}+1=(2^{\frac{n}{a}}+1)(2^{\frac{n}{a}(a-1)}+\ldots+2^{\frac{n}{a}}+1)$$

бўлиб, n≥3 ва $a \geq 3$ бўлганлиги учун, ҳар иккала кўпайтувчи ҳам >1. Демак, F_n таркибли сон. Ферма барча F_{2^k} сонлар туб сонлар деган фаразни ўртага ташлади ва уни k=0, 1, 2, 3, 4 учун текшириб кўрди, ҳақиқатан бу қийматларда 3, 5, 17, 257, 65537 туб сонлар ҳосил бўлади. Навбатдаги F_{2^5} сон $2^{2^5}+1=2^{32}+1$ шунча ҳам катта эдики, Ферма унинг тублигини ҳам, таркиблилигининг ҳам кўрсата олмади.

1739 йилда Эйлер бу соннинг таркиблилигини исботлаб, Ферма фаразининг нотўғрилигини кўрсатди. Эйлер $2^{2^k}+1$ кўринишдаги сонларнинг бўлувчиларга ажратишни умумий усулини топди ва бу сонларнинг бўлувчилари $2^{(k+1)t}+1$ кўринишга эгалигини исбот қилди.

Ҳозирги вақтда k=5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 18, 23, 36, 38, 73 қийматларда F_{2^k} сонларнинг тарикблилиги маълум.

Маълумки, Ферма сонлари циркул ва чизғич ёрдамида мунтазам кўп бурчакни ясаш масаласи билан боғлиқ. Гаусс шуни исбот қилган эдики, циркул ва чизғич ёрдамида мунтазам кўпбурчакни чизиш мумкин бўлиши учун, унинг томонлари сони $n=2^{\alpha} p_1 \cdot p_2 \cdot \ldots \cdot p_S$ га тенг бўлиб, бунда p_i туб сонлар $2^{2^k}+1$ кўринишга эга бўлиши зарур ва кифоядир; n нинг дастлабки 1000 қийматлари орасида бу шартни қаноатлантирадиганлари 54 та.

4.Ферма фарази, яъни $2^{2^k}+1$ кўринишдаги барча сонлар туб деган даъво инкор қилингандан кейин, табиий равишда, k нинг барча қийматларида туб сонларни берадиган бошқа f(k) функцияларни қуриш масаласи қўйилди.

Эйлер ушбу $f(x)=x^2-x+41$ кўпҳадни кўрсатди, унда x=0,1,…,40 қийматларни қабул қилганда f(x) нинг қийматлари фақат туб сонлар, x=41 ва x=42 бўлганда эса бу кўпҳаднинг қийматлари $f(41)=41^2$, $f(42)=41\cdot 43$ таркибли сонлардир. Яна қуйидаги функциялар топилган: $f(x)=x^2-$

x<17 (x=0, 1, ...,15 қийматларда f(x) нинг қийматлари туб сонлар), $f(x)=2x^2+29$ x=0,1,...,28 қийматларда f(x) нинг қийматлари туб сонлар). Осонлик билан кўриш мумкинки, умуман бутун коэффициентли кўпҳад аргументнинг барча натурал қийматларида фақат туб қийматларни қабул қилиши мумкин эмас.

39-т е о р е м а. Ихтиёрий бутун коэффициентли кўпҳад аргументнинг бирор натурал қийматида таркибли сон бўлган қийматни қабул қилади.

И с б о т. Фараз қилайлик $f(x)= a_0x^n + a_1x^{n-1}+ a_n$ бўлсин, бунда барча a_i бутун сонлар. Фараз қилайлик, k нинг бирор қийматида f(k)=p бўлсин, бунда p - туб сон. Маълумки, n-даражали кўпҳад бир хил қийматни энг кўпи билан n– та нуқтада қабул қилади; демак, шундай $1 < t$ бутун сон топиладики, $f(k+pt)\neq p$.

Энди f(k+pt) ни pt нинг даражалари бўйича ёямиз:

$$f(k+pt)=f(k)+A_1pt+A_2(pt)^2+\dots A_n(pt)^n, \qquad (34)$$

бунда барча A_i– бутун сонлар, f(k)=p- бўлганлиги учун (34) дан $p \mid f(k+pt)$ келиб чиқади, яъни f(k+pt) таркибли сон.

39-теоремада f(x) функциянинг кўпҳадлиги муҳим роль ўйнайди. Аргументнинг барча натурал қийматларида фақат туб қийматларни қабул қиладиган баъзи функцияларнинг кўриниши маълум. Масалан, шундай α мавжуд бўлиб, барча $1\le x$ қийматларда $f(x)=[\alpha^{3^x}]$–нинг қабул қиладиган қийматлари туб сонлардан иборат бўлишини 1947 йилда Милс кўрсатган эди.

5.Эйлер-Голдбах муаммоси ҳақида қисқача тўхталиб ўтамиз. Петербург фанлар Академиясининг академиги Христиан Голдбах 1742 йил 7 июнда Леонард Эйлерга қуйидаги хатни ёзганди: «Менинг фикримча, ҳар бир тоқ сон (7 дан бошлаб) учта туб сонларнинг йиғиндисидан иборат». 1742 йил 30 июнда Эйлер қуйидагича жавоб берди: "Ҳар бир

жуфт сон (4 дан бошлаб) иккита туб сонларнинг йиғиндисига тенг, буни мен тўла чин теорема деб биламан, лекин мен уни исбот қилолмайман."

Булар ҳозирги вақтда *Эйлер ва Голдбахнинг бинар ва тернар муаммолари* дейилади. Бу муаммоларни ечишга сонлар назарияси соҳасидаги йирик мутахассислар шуғулланишган. Тернар муаммони етарлича катта сонлар учун 1937 йилда академик И.М.Виноградов ечди.

40-т е о р е м а (Виноградов). Шундай доимий N_0 сон топиладики, N_0 дан катта бўлган барча тоқ сонларни учта туб сонлар йиғиндиси шаклида тасвирлаш мумкин.

Шундай қилиб, етарлича катта N_0 сонлар учун тернар муаммо ечилган. Бинар муаммо ҳозир ҳам муаммолигича турибди.

6. Биз юқорида туб сонларнинг натурал сонлар қаторида тақсимланишини кўриб чиқдик. Энди натурал сонлар қаторининг чексиз кетма-кетлиги бўлган арифметик прогрессияда туб сонларнинг тақсимоти ҳақида қисқача тўхталиб ўтамиз.

Масалан, айирмаси 8 га тенг бўлган

$$5, 13, 21, 29, 37, 45, 53, 61, 77, 85, 93, 101, \ldots \qquad (35)$$

прогрессияни олайлик. Бу прогрессиянинг бошида нисбатан кўп туб сонлар учрайди (уларнинг таги чизилган). Бу прогрессияда туб сонлар чексиз тўпламни ташкил этадими ёки бирор жойдан бошлаб туб сонлар учрамай қоладими?

1837 йилда Лежен Дирихле фақат (35)-прогрессияда эмас, балки айирмаси билан биринчи ҳади ўзаро туб бўлган ихтиёрий прогрессияда туб сонлар чексиз кўплигини кўрсатди.

41-т е о р е м а (Дирихле). Агар $(k, l)=1$ бўлса, у ҳолда

$$l, l+k, l+2k, l+3k, \ldots \qquad (36)$$

прогрессияда чексиз кўп туб сонлар мавжуд.

Теоремадаги (k, l)=1 шарт муҳим, чунки агар (k, l) d>1 бўлса, у ҳолда (36)-прогрессиянинг барча ҳадлари d га бўлинади ва прогрессияда энг кўпи билан битта туб сон мавжуд бўлиши мумкин. Бу теоремани исботиз қабул қиламиз. Теоремани Дирихле берган исботи аналитик функцияларнинг нозик методларини билишни талаб қилади.

Хусусий ҳолларда Дирихле теоремасини элементар йўл билан исбот қилиш мумкин. Биз қуйида шундай теоремаларни иккитасини келтирамиз.

42-т е о р е м а. 4n+3 кўринишдаги прогрессияларда туб сонлар чексиз кўп.

И с б о т. Тоқ туб сонларни 4 га бўлганда қолдиқ 1 ёки 3 га тенг. 4m+1 кўринишдаги сонларнинг кўпайтмаси яна 4m+1 кўринишга эга. Фараз қилайлик 4m+3 кўринишдаги туб сонлар $p_1, p_2, p_3, \ldots, p_k$ бўлсин. Энди $p=4p_1 \cdot p_2 \cdot p_3 \cdots p_k-1$ сонни кўрайлик, бу сон 4m+3 кўринишдаги туб сон ёки 4m+3 кўринишдаги q туб бўлувчига эга ва q туб сон $p_1, p_2, \ldots, p_k$ туб сонларнинг бирортасига ҳам тенг эмас. Шундай қилиб, 4n+3 та кўринишдаги туб сонларнинг сони k та деган фаразимиз нотўғри экан.

43-т е о р е м а. 6m+5 кўринишдаги прогрессияда туб сонлар чексиз кўп.

И с б о т. 3 дан катта туб сонлар 6m+1 ёки 6m+5 кўринишга эга; 6m+1 кўринишдаги туб сонларнинг кўпайтмаси яна 6m+1 кўринишдаги сон бўлади. Фараз қилайлик, 6m+5 кўринишдаги туб сонларнинг сони k та бўлиб,улар $p_1, p_2, p_3, \ldots, p_k$ лардан иборат бўлсин.Равшанки,$6p_1 \cdot p_2 \cdot p_3 \cdots p_k-1$ сон ёки 6m+5 кўринишдаги туб сон ёки 6m+5 кўринишдаги q туб бўлувчига эга. Демак, бизнинг фаразимиз нотўғри, яъни 6m+5 кўринишдаги туб сонларнинг сони чексиз.

4-БОБ УЧУН МАШҚЛАР.

1. 1)τ(6004) ва 2)s (6004) топилсин. (Ж.: 1) 8; 2) 1200).
2. Барча a=1, 2, …, 100 сонлар учун μ(a) функция қийматларининг жадвалини тузинг.
3. 34-теорема асосида a=1, 2, …, 50 сонлар учун φ(a) функция қийматларининг жадвалини тузинг.
4. 1) φ(5040) ва 2) φ (1248000) ни топинг.
5. Фараз қилайлик, N=p^{α} q^{β} бўлсин, бунда p ва q≠p туб сонлар. N^2 сон 15 та ҳар хил бўлувчиларга эга. N^3 ни бўлувчилари сони нечта? N^k ники-чи? (Ж.: 1)28).
6. $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ сонни бўлувчиларининг m-даражалари йиғиндиси топилсин.
7. Ушбу $\varphi(m^k) = m^{k-1}\varphi(m)$ тенгликни исботланг.
8. Агар n сони 2m+1 та бўлувчига эга бўлса, у ҳолда бу сонни m усул билан иккита сонлар кўпайтмаси шаклида тасвирлаш мумкин.
9. Барча кўпайтувчиларнинг кўпайтмаси 5832 га тенг бўлган сонни топинг.
10. Шундай сонни топингки, уни бўлувчиларининг кўпайтмаси $3^{30}\cdot 5^{40}$ бўлсин.
11. φ (7^n) = 705894, n ни топинг. (Ж.: n=7)
12. x ни φ (2x)= φ (3x) шартдан топинг (Ж.: x=2; 4 (mod 6)).
13. p туб соннинг n! га кирадиган даражаси $\frac{n}{p-1}$ дан ошмаслигини кўрсатинг.
14. $\varphi(n) = 100$ бўлганда n нинг 5^{α} кўринишини топинг.
15. $\varphi(n) = 600$ бўлса, n нинг $3^{\alpha}5^{\beta}$ кўринишини топинг.
16. 301, 302... , 504 сонлар орасида нечта 24 билан ўзаро туб бўлган сонлар бор?

4-бобга доир тарихий маълумот

1. Мёбиус (Möbius August Ferdinand, 1790-1868) – немис математиги, Гауснинг шогирди, асосий ишлари геометрияга бағишланган. Бир томонли сиртларни кўрсатган. Улардан бири Мёбиус варағи (лист Мебнуса, Möbius band).

2. Бу ва кейинги боблардаги материалларнинг кўп қисми буюк математик К.Ф.Гаусс (1777-1855) номи билан боғлиқ. Гаусс 1777 йилда Брауншвейг (Германия) да туғиган. Умрининг кўп қисмини Гётингенда ўтказган, у ерда у 1795-1798 йилларда студент, 1807 йилдан бошлаб умрининг охиригача Гётинген университетининг профессори ва Гётинген астрономик абсерваториясининг директори бўлган. Гаусс 15 ёшлигидан бошлаб сонлар назарияси соҳасида ишлаган, бу соҳада ўзидан олдин ўтган математикларга маълум бўлган муҳим натижаларни мустақил равишда топди, кейинчалик у ўта муҳим натижаларни кашф этди.

Гаусс сонлар назарияси ва олий алгебрадан биринчи йирик асари «Disquisitions arithmeticae» («Арифметик тадқиқотлар») ни 1796 йилдан бошлаб ёза бошлади. Бу асарнинг кўп қисми унинг студентлик йилларида ёзилган. Бу асар фақат 1801 йилда латин тилида тўла чопдан чиқди. Бу асар сонлар назарияси ва олий алгебранинг кейинги равнақини олдиндан белгилаб қўйди. Гаусс бу асарнинг биринчи қисмида *таққослама* тушунчасини киритди. Бу тушунчани аслида унча аниқ бўлмаган равишда Гауссдан олдинги кўп математиклар ишлатишган. Лекин фақат Гаусс таққосламани тўғри аниқлаб, унинг назариясини систематик равишда ривожлантирди. Гауснинг бу асарда келтирган натижалари, хусусан ўзароликнинг квадратик қонуни сонлар назариясининг кейинги ривожи учун асос бўлди. Ўзаролик қонунни биринчи бўлиб тўла исботини Гаусс 19 ёшда берган. Ўзаролик қонунни *Гаусс қонуни* ҳам дейишади, кейинчалик Гаусс бу қонунни яна олтита бошқа исботини берди. 19-асрда

ўзаролик қонуннинг 50 дан ортиқ исботи эълон қилинган эди Гаусс кейинги йилларда математиканинг турли йўналишлари билан шуғулланиб, жумладан, дифференциал геометрия, эҳтимоллар назарияси, чексиз қаторлар ва потенциаллар назариясида муҳим натижаларга эришди. Ҳар қандай алгебраик тенгламани камида битта илдизи борлигини исботлади. У ноевклид геометриянинг асосчиларидан бири. Физика, назарий астрономия, геодезия ва магнетизм соҳаларида ҳам тадқиқотлар олиб бориб, муҳим натижаларни қўлга киритган.

Гауссни ҳақли равишда *математиканинг қироли* дейишади.

1908 йилдан бошлаб Гёттинген Фанлар Академияси Гауснинг 11 жилдлик асарлар тўпламини нашрдан чиқарди. Гауснинг «Disquisitions arithmetikae» асари Гаусс вафотининг 100 йиллиги муносабати билан рус тилига таржима қилиниб, 1959 йилда Москвада нашр қилинди (қ. [20]).

3. 34-, 35-, 36-теоремалар Гауссни «Disquisitions arithmetikae» асарининг биринчи бўлимида келтирилган бўлиб, фақат бизнинг белгилашлар Гауссникидан бир оз фарқ қилади.

4. 37-теорема Гауснинг асарида бор.

5. Биз 19-§ да «эгиз туб сонлар», «Ферма туб сонлари» ва «Мерсенн туб сонлари» нинг чеклими ёки чексизми ҳозиргача номаълумлигини айтиб ўтган эдик. Биз бу ерда сонлар назарияси тарихида узоқ муддат математикларни эътиборини ўзига тортган иккита масала тўғрисида тўхтамоқчимиз.

m сон *мукаммал сон* дейилади, агар у ўзидан фарқли бўлган бўлувчиларининг йиғиндисига тенг бўлса. Масалан, 6=1+2+3, 28=1+2+4+7+14. Мукаммал сонлар Евклиднинг «Негизлар»и да учрайди. Унда тўртта мукаммал сон берилган. «Негизлар» да Евклид кўрсатган эдики, агар p ва 2^p-1 сонлар туб бўлса, у ҳолда

$$n=2^{p-1}(2^p-1)$$

мукаммал сон бўлади. 18-асрда Л.Эйлер кўрсатдики, агар n тоқ мукаммал бўлса, у ҳолда 2^p-1 туб бўлади. Ҳозирги вақтда 47 та жуфт мукаммал сонлар маълум, уларнинг энг каттаси $2^{44496}(2^{44497}-1)$ бўлиб, 1962 йилда ЭҲМ ёрдамида топилган. Ҳозирги вақтда $[1, 10^{50}]$ оралиқда тоқ мукаммал соннинг мавжуд эмаслиги аниқланган.

6. Иккита m ва n *сонлар дўст сонлар дейилади*, агар уларнинг ҳар қайсиси иккинчисининг бўлувчилари йиғиндисига тенг бўлса. Масалан, 220=1+2+4+71+142 ва 284=1+2+4+5+10+11+20+22+44+55+110.

Дўст сонларни дастлаб Пифагор (мил.ав.тахм.570-500 йиллар) киритган. Пифагорчилар дўст сонлар илоҳий кудратга эга деб, катта эътибор беришар эди. Шарқ математиклари ҳам дўст сонлар билан шуғулланишган. Булар қуйидагилардир:

- 9 асрда Боғдодда ишлаган Собит ибн Қурра ўзининг "Дўст сонларни осон йўл билан топиш ҳақидаги рисола" сида биринчи бўлиб сонларни дўст бўлиш мезонини беради.
- 13-асрда яшаган тожик математиги Маҳмуд бин-ал-Вусудий 1228 йилда ёзган "Лубоб ал-ҳисоб" ("Ҳисоб мағизи") асарида Собит ибн Қорра усулидан фарқли равишда дўст сонларни аниқлаш мезонини беради.
- Улуғбекнинг шогирди, самарқандлик математик Ғиёсиддин Жамшид ал-Коший "Арифметика калити" номли асарида дўст сонлар билан шуғулланиб, уларнинг дўст бўлиш мезонини келтиради.

-Шерозлик математик ва астроном Маҳмуд ибн Маъсуд Қутбиддин Шерозий (1236-1311) ўзининг "Дурра ат-тож" ("Тож дури") номли энциклопедик асарида дўст сонларни ўрганган. Маълумки, 17-асргача математик асарлар формуласиз, сўз билан ёзилар эди. Юқорида номлари келтирилган олимлар кўрсатган мезонларни ҳозирги замон символикаси билан ёзганда улар бир хил бўлади ёки маълум

алмаштириш бажариб, уларни бир хил кўринишга келтириш мумкин. Масалан, Маҳмуд ал-Вусудий мезонини қуйидагича баён қилиш мумкин:

Агар

$$p = 3 \cdot 2^{k-1} - 1,\ q = 3 \cdot 2^{k-1} - 1,\ r = 9 \cdot 2^{2k-1} - 1$$

сонларнинг ҳар бири туб бўлса, у ҳолда дўст сонларнинг биринчиси $m=2^k pq$ ва иккинчиси $n=2^k r$ бўлади. У шу мезон ёрдамида 17296 ва 18416 сонларнинг дўстлигини кўрсатган ($k=4$ га тўғри келади). Бу дўст сонларнинг француз математиклари П.Ферма ва Р.Декарт 17-асрда қайта топишди. Л.Эйлер қарийиб 60 жуфт дўст сонларни топди. ЭҲМлар уларни бир неча юзтасини топишга имкон берди. Ҳозиргача уларнинг сони чеклими ёки чексизми номаълум.

7. Франциялик физик Марен Мерсенн (Mersenne M., 1558-1648) ўзининг «Cogita physico mathematica» асарида

$$M_n = 2^n - 1 \quad (n = 2, 3...)$$

сонларни қараган эди. У бу сонларни n нинг 2, 3, 5, 7 қийматларида M_n =3, 7, 31, 127 сонларнинг тублигини кўриб, n нинг барча n=p туб қийматларида M_p туб сон бўлади деган фаразни айтган. Кейинчалик маълум бўлдики n=p туб бўлганда ҳам M_p нинг аксарияти таркибли бўлар экан. Масалан, $2300<p<3300$ оралиқдаги туб сон учун M_p таркибли сон бўлиб чиқди. Мерсенн сонлари жуда тез ўсиб боради. Шунинг учун ҳам ҳар гал навбатдаги Мерсенн сонини топгандан кейин, бу охиргиси бўлса керак деб ўйлашади. 1964 йилда Гиллис M_{11213} сонни топгандан кейин, уни охиргиси деб ўйлашади. Буни рақамларнинг сонини аниқлаймиз. Умуман, $M_p=2^p-1$ сонни рақамларинг сонини аниқлаш ўрнига бу масалани

$$M_p+1=2^p$$

сон учун қараймиз. Бу ҳар иккала сонни рақамларининг миқдори тенг, чунки $M_p+1=2^p$ сонни рақамларнинг миқдори биттага ортиқ бўлиши учун бу сон 0 рақам билан тугаши

керак. Лекин бундай бўлиши 2 нинг бирор даражаси учун мумкин эмас, ҳақиқатан 2 нинг даражалари

$$2, 4, 8, 16, 32, 64, 128, 256,\ldots$$

Равшанки, бу сонларнинг охирги рақами

$$2, 4, 6, 8$$

иборат. Айтилганлардан сўнг $n=2^p$ ни рақамларининг миқдорини аниқлаш учун буни логарифмлаймиз: $\lg n=\lg 2^p=p\lg 2$. Логарифмик жадвалдан $\lg 2$ нинг тақрибий қиймати $\lg 2=0{,}30103$ ни топамиз. Бундан $\ln n=11213\cdot 0{,}30103=3375{,}4493$.

Бу соннинг характеристикаси 3375 бўлганлиги учун шундай хулосага келамизки 2^{11213} (демак, M_{1213} ҳам) 3376 та рақамга эга.

Бу сон Иллинойс университетида топилгани учун Иллинойс университетининг Математика факультети ўзларининг ютуқлари билан шунча ҳам мағрур бўлиб, барчани ҳайратда қолдириш мақсадида бу сонни ўзларининг почта штемпелига акс эттириб, ҳар бир жўнатиладиган хатнинг конвертида M_{1213} соннинг тасвири тушурилган эди.

1971 йилда топилган M_{19937} Мерсенн сонининг рақамлар миқдори 6002 та. Охирги хабарларга кўра ҳозиргача топилган Мерсеннинг охирги сони M_{44497} бўлиб, рақамларининг сони 13395 та.

8. 1788 йилда Лежандр (36)-арифметик прогрессияда чексиз кўп туб сонлар мавжуд бўлиши ҳақидаги фикрни айтган эди. Г.В.Лейбниц $6d\pm 1$ кўринишдаги, Л.Эйлер эса $30d\pm 1$, $30d\pm 7$, $30d\pm 11$, $30d\pm 13$ кўринишдаги арифметик прогрессияларда чексиз кўп туб сонлар мавжудлигини исбот қилишди.

Умумий ҳолда бу теоремани буюк немис математиги Л.Дирихле (Peter Gustav Lejeune Dirichlet, 1805-1859) 1837 йилда d айирма туб сон бўлгандаги ҳолини исбот қилган эди. Фақат 1840 йили уни тўла равишда исбот қилди. Дирихле математиканинг деярли барча соҳаларида йирик кашфиётлар қилган. Дирихле номини абадийлаштириш учун юқоридаги

теореманинг ўзи ҳам кифоя эди. Дирихле исботини тушуниш анча оғир. Дирихле исботини бошқа немис математиги Ландау (Эдмунд Георг Герман, 1877-1938) анчагина соддалаштирди.

Дирихле теоремасининг элементар исботини 1949 йилда норвегиялик математик Атле Селберг берди. 1956 йилда Москвалик математик Гельфонд (Александр Осипович, 1906-1968) Дирихле теоремасининг А.Селберг методига нисбатан соддароқ элементар методини кўрсатди.

5 - БОБ. ТАҚҚОСЛАМАЛАР

20-§. АСОСИЙ ТУШУНЧАЛАР

Фараз қилайлик m натурал сон бўлсин, бу сон билан биргаликда унга каррали бўлган барча mt (t-ихтиёрий бутун сон) сонларни қараймиз. Бу карраликларнинг тўплами алгебрада модул деб аталади.

8-т а ъ р и ф. Агар иккита a ва b бутун сонларнинг айирмаси m га бўлинса (ёки m модулга тегишли бўлса), у ҳолда улар ўзаро m модул бўйича *таққосланувчи сонлар* дейилади ва қуйидагича ёзилади.

$$a \equiv b(\text{mod } m). \qquad (37)$$

Бу таърифдан кўрамизки a ва b сонларни m га бўлганда бир хил қолдиқ қолади. Шунингдек, $a = b+mt$ тенглик ўринли бўлади, бунда t-бутун сон.Агар a сон b сон билан m модул бўйича таққосланмаса, у ҳолда $a \equiv b(\text{mod } m)$ деб ёзилади.

21-§. ТАҚҚОСЛАМАЛАРНИНГ, ТЕНГЛИК ХОССАЛАРИГА ЎХШАШ ХОССАЛАЛАРИ.

44-т е о р е м а. Таққослама учун қуйидаги учта асосий қонун бажарилади:

1. *Симметрия қонуни*: Агар $a \equiv b(\text{mod } m)$ бўлса, у ҳолда $b \equiv a (\text{mod } m)$;
2. *Транзитивлик қонуни*: Агар $a \equiv b(\text{mod } m)$, $b \equiv c(\text{mod } m)$ бўлса, у ҳолда $a \equiv c(\text{mod } m)$ бўлади;
3. *Рефлексивлик қонуни*: $a \equiv a \ (\text{mod } m)$;

И с б о т. 1. Агар a -b айирма m га бўлинса, у ҳолда b-a айирма ҳам m га бўлинади, демак, $a \equiv b(\text{mod } m)$ дан $b \equiv a$ (mod m) келиб чиқади.

2. Агар a ва b ва b с айирмалар m га бўлинса, у ҳолда a-b+b-c a-c ҳам m га бўлинади, яъни a≡b(mod m), b≡c(mod m) дан a≡c(mod m) келиб чиқади.

3. a-a 0 ҳар қандай m натурал сонга бўлинади, демак, a≡a (mod m).

Теорема исботланди.

45-т е о р е м а. Бир хил модулли таққосламаларни ҳадлаб қўшиш мумкин.

И с б о т: Ҳақиқатдан,

a_1≡b_1(mod m), a_2≡b_2(mod m), …, a_k≡b_k(mod m)

бўлса, уларни

a_1=b_1+mt_1, a_2=b_2+mt_2, …, a_k=b_k+mt_k (37^1)

каби ёзиш мумкин. Бу тенгликларни ҳадлаб қўшиб,

a_1+a_2+…+a_k=b_1+b_2+…b_k+m(t_1+t_2+…+t_k) (38)

ёки

a_1+a_2+…+a_k=b_1+b_2+…b_k+mt

тенгликларга эга бўламиз. Бундан

a_1+a_2+…+a_k=b_1+b_2+…b_k(mod m) (39)

келиб чиқади.

1-н а т и ж а. Таққосламанинг ҳар иккала томонини бир хил натурал сонга кўпайтириш мумкин. Ҳақиқатдан (39) тенгликда a_1=a_2=…=a_k=a ва b_1=b_2=…=b_k=b деб олсак, натижа келиб чиқади.

2- н а т и ж а. Таққосламанинг бир қисмидаги сонни иккинчи қисмига қарама-қарши ишора билан ўтказиш мумкин.

Ҳақиқатдан a+b≡c (mod m) таққослама берилган бўлса, унга -b≡-b(mod m) таққосламани қўшсак, a≡c-b(mod m) таққослама ҳосил бўлади.

3-н а т и ж а: Таққосламани ҳар бир қисмига модулга каррали сонни қўшиш мумкин. Ҳақиқатдан, a≡b(mod m) таққосламани, кўриниб турган, mk≡0 (mod m) таққослама билан қўшсак, a+mk≡b(mod m) ни ҳосил қиламиз.

46-т е о р е м а. Бир хил модулли таққосламаларни ҳадлаб кўпайтириш мумкин.

И с б о т: Ҳақиқатдан, (37^1)-тенгликларни ҳадлаб кўпайтирсак,

$$a_1 a_2 \dots a_k = b_1 b_2 \dots b_k + mN \qquad (40)$$

тенгликка эга бўламиз, бунда

$$N = b_2 b_3 \dots b_k t_1 + b_1 b_3 \dots b_k t_2 + \dots b_1 b_2 \dots b_{k-1} t_k,$$

(40)-дан

$$a_1 a_2 \dots a_k = b_1 b_2 \dots b_k \pmod m \qquad (40^1)$$

келиб чиқади.

1-н а т и ж а. $a \equiv b \pmod m$ таққосламанинг ҳар иккала томонини бирор k натурал даражага кўтариш мумкин:

$$a^k \equiv b^k \pmod m.$$

Ҳақиқатдан, (40^1)-тенгликда $a_1 = a_2 = \dots = a_k = a$, $b_1 = b_2 = \dots = b_k = b$ деб олиш кифоядир.

47-т е о р е м а. Агар бир вақтда $a_i \equiv b_i \pmod m$ $(i = \overline{0, n})$ ва $x \equiv y \pmod m$ таққосламалар ўринли бўлса, у ҳолда

$$a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv b_0 x^n + b_1 x^{n-1} + \dots + b_n \pmod m$$

таққослама ўринли бўлади.

И с б о т: $x \equiv y \pmod m$ таққосламага 46-теореманинг 1-натижасини қўл-ласак,

$$x^k \equiv y^k \pmod m \qquad (k = 0,1,..,n)$$

келиб чиқади. Бу таққосламани, 46-теоремага асосан, $a_{n-k} \equiv b_{n-k} \pmod m$ $(k = 0,1,2,...n)$ таққослама билан кўпайтириб,

$$a_{n-k} x^k \equiv b_{n-k} y^k \pmod m \quad (k = 0,1,2,\dots n)$$

ларни ҳосил қиламиз. Буларни, 46-теоремага асосан, қўшиб чиқсак, теореманинг тасдиғи келиб чиқади.

48-т е о р е м а. Агар $a \equiv b \pmod m$ таққосламада d сони a ва b ларнинг умумий бўлувчиси бўлиб, $(d,m) = 1$ у ҳолда таққосламанинг ҳар иккала томонини d га бўлиш мумкин.

И с б о т: Ҳақиқатдан, $a \equiv b \pmod m$, $a = a_1 d$, $b = b_1 d$ муносабатлардан кўрамизки, $a - b = (a_1 - b_1)d$ айирма m га

бўлинади. Лекин (d,m)=1, шунинг учун a_1-b_1 айирма m га бўлинади, яъни $a_1 \equiv b_1 \pmod m$.

22-§.ТАҚҚОСЛАМАЛАРНИНГ КЕЙИНГИ ХОССАЛАРИ

49-т е о р е м а. а) таққосламани иккала қисмини ва модулини бир хил бутун сонга кўпайтириш мумкин. б) таққосламани иккала қисми ва модули умумий кўпайтувчига эга бўлса, таққосламанинг иккала қисми ва модулини умумий кўпайтувчига бўлиш мумкин.

И с б от: а) Ҳақиқатдан, $a \equiv b \pmod m$ дан

$$a = b+mt,\ ak = bk+mkt$$

келиб чиқади. Демак, $a \cdot k \equiv b \cdot k \pmod m$.

б)Энди фараз қилайлик $a \equiv b \pmod m$, $a = a_1 d$, $b = b_1 d$, $m = m_1 d$ бўлсин. У ҳолда

$$a = b+mt,\ a_1 d = b_1 d + m_1 dt,\ a_1 = b_1 + m_1 t$$

тенликлар ҳосил бўлади, бундан $a_1 \equiv b_1 \pmod{m_1}$ келиб чиқади.

50-т е о р е м а. Агар таққослама бир неча модул бўйича ўринли бўлса, у ҳолда бу таққослама шу модулларнинг энг кичик умумий каррали бўйича ҳам ўринли бўлади.

И с б о т. Ҳақиқатдан, фараз қилайлик

$$a \equiv b \pmod{m_1},\ a \equiv b \pmod{m_2},\ \ldots,\ a \equiv b \pmod{m_k}$$

бўлсин, у ҳолда a-b айирма барча $m_1, m_2, \ldots, m_k$ модулларга бўлинади. Демак, бу айирма шу модулларнинг энг кичик умумий каррали $m=[m_1, m_2, \ldots, m_k]$ га ҳам бўлинади, яъни $a \equiv b \pmod m$.

51-т е о р е м а. Агар таққослама бирор m модул бўйича ўринли бўлса, у ҳолда таққослама шу модулнинг ихтиёрий бўлувчиси бўйича ҳам ўринли бўлади.

И с б о т. Ҳақиқатдан, $a \equiv b \pmod m$ ёки a-b=mt бўлиб, $m=m_1 d$ бўлса, у ҳолда a-b=$m_1$dt бўлади. Бундан эса a-b=m_1(dt) ёки $b \equiv a \pmod{m_1}$ келиб чиқади.

52-т е о р е м а. Агар $a \equiv b \pmod m$ бўлса, у ҳолда $(a, m)=(b, m)$ бўлади.

И с б о т. Ҳақиқатдан, $a \equiv b \pmod m$ дан $a=b+mt$ ёки $a-mt=b$ тенгликлар келиб чиқади. Фараз қилайлик $(a, m)=d$ ва $(b,m)=d_1$ бўлсин. Айтайлик, $a=da_1$ ва $m=dm_1$ бўлсин. Энди $a_1d-m_1dt=b$ тенгликнинг чап қисми d га бўлинади. Демак, b ҳам d га бўлинади. Бунда d сон b ва m соннинг умумий бўлувчиси эканлиги келиб чиқади. Иккинчи томондан $(b,m)=d_1$ бўлганлиги учун

$$d \mid d_1. \qquad (41)$$

Шартга кўра $b=b_1d_1$, $m=m_2d_1$, булардан фойдаланиб кўрамизки $a=b_1d_1+m_2d_1t$. Бундан $d_1 \mid a$ ҳамда d_1 сон a ва m сонларнинг умумий бўлувчиси эканлиги келиб чиқади. Иккинчи томондан $(a,m)=d$ бўлганлиги учун

$$d_1 \mid d \qquad (42)$$

бўлади. (41) ва (42)- тенликлардан $d_1=d$, яъни

$$(a,m)=(b,m)$$

ҳосил бўлади.

23-§. ЧЕГИРМАЛАРНИНГ ТЎЛА СИСТЕМАСИ

Ҳар бир бутун сон m модул бўйича m га бўлиш натижасида келиб чиқадиган ўзининг қолдиғи билан таққосланади. Сонни m га бўлиш натижасида қуйидаги қолдиқларнинг бири ҳосил бўлади: 0,1,2,...,m-1. Бу қолдиқларнинг ихтиёрий иккитаси m модул бўйича таққосланмайди. Бошқача қилиб айтганда барча бутун сонлар m та синфларга бўлинади.

9-т а ъ р и ф. m га бўлинганда бир хил қолдиқ берадиган сонлар тўплами m *модул бўйича чегирмалар синфи* дейилади.

Чегирмалар синфини

$$C_0, C_1, \ldots, C_{m-1}$$

каби белгилаймиз.

C_r синфнинг элементлари mq+r кўринишга эга бўлиб, q га ҳар хил бутун қийматлар бериш натижасида бу элементларни ҳосил қилиш мумкин. Масалан, m=7 бўлганда r=3 қолдиқ ҳосил қиладиган сонлар 7q+3 кўринишга эга ва q=0, ±1, ±2,... десак {...,-18, -11, -4, 3, 10, 17, 24,...} синф ҳосил бўлади.

Равшанки, иккита сон m модул бўйича таққосланувчи бўлиши учун улар шу модул бўйича битта синфда ётиши лозим ва аксинча.

10-т а ъ р и ф. Чегирмалар синфининг ихтиёрий элементи шу синфнинг *чегирмаси* дейилади.

11-т а ъ р и ф. m модул бўйича тузилган ҳар бир чегирмалар синфидан ихтиёрий равишда биттадан чегирма олиб тузилган чегирмалар тўплами m модул бўйича *чегирмаларнинг тўла системаси* дейилади. Масалан, m=5 модул бўйича 5q, 5q+1, 5q+2, 5q+3, 5q+4 синфлар ҳосил бўлади. Буларнинг ҳар биридан биттадан олиб тузилган {5, 16, 112, -2, -16} сонлар тўплами 5 модул бўйича чегирмаларнинг тўла системаси бўлади.

q=0 қийматда ҳосил бўладиган ва демак, r қолдиққа тенг чегирма *манфий бўлмаган энг кичик чегирма* дейилади.

Абсалют қиймати энг кичик бўлган ρ чегирма *абсалют энг кичик чегирма* дейилади.

Равшанки, $r < \frac{m}{2}$ қийматда ρ=r ва $r > \frac{m}{2}$ қийматда ρ=r-m бўлади; ниҳоят, m - жуфт ва $r = \frac{m}{2}$ бўлса, $\frac{m}{2}$ ва $\frac{m}{2} - m = -\frac{m}{2}$ сонларнинг исталганини ρ деб қабул қилиш мумкин.

Одатда чегирмаларнинг тўла системаси сифатида 0,1,...,m-1 дан иборат манфий бўлмаган энг кичик чегирмалар олинади, шунингдек, абсолют энг кичик

чегирмалар ҳам ишлатилади. Юқорида айтилганга асосан абсолют энг кичик чегирмалар: m тоқ бўлганда

$$-\frac{m-1}{2},\ldots,-1,0,1,\ldots\frac{m-1}{2}$$

қатор билан, m жуфт бўлганда эса

$$-\frac{m}{2}+1,\ldots-1,0,1,\ldots\frac{m}{2},$$

$$-\frac{m}{2},\ldots-1,0,1,\ldots\frac{m}{2}-1$$

қаторларнинг бири билан тасвирланади.

53-т е о р е м а. Ҳеч қайси иккитаси m модул бўйича ўзаро таққосланмайдиган m та ҳар қандай бутун сонлар чегирмаларнинг шу m модул бўйича тўла системасини ташкил этади.

И с б о т. Ҳақиқатдан, бу сонлар ўзаро таққосланмаганлиги учун улар ҳар хил синфларга тегишли бўлади, шу билан бирга уларнинг сони m синфларнинг сонига тенг бўлганлиги сабабли, ҳар бир синфга бу сонларнинг биттасигина киради.

54-т е о р е м а. Агар $(a,m)=1$ бўлиб, x сон m модул бўйича тўла системани ташкил этувчи чегирмаларга тенг қийматларни қабул қилса, b ҳар қандай бутун сон бўлганда ҳам $ax+b$ сонлар яна чегирмаларнинг m модул бўйича тўла системасини ташкил этади.

И с б о т. Ҳақиқатдан, x сонлар нечта бўлса, $ax+b$ сонлар ҳам шунча, яъни m тадир. Энди 53-теоремага кўра, m модул бўйича ўзаро таққосланмайдиган иккита x_1 ва x_2 сонга мос келадиган ax_1+b ва ax_2+b сонларнинг m модул бўйича таққосланмаслигини кўрсатиш кифоядир. Тескарисини фараз қилсак, $ax_1+b\equiv ax_2+b$ таққосламага келамиз, бундан $ax_1\equiv ax_2 \pmod m$ ва $(a,m)=1$ лигини ҳисобга олсак $x_1\equiv x_2 \pmod m$ келиб чиқади. Бу эса x_1, x_2 сонлар ўзаро таққосланмайди деганимизга зиддир.

24-§. ЧЕГИРМАЛАРНИНГ КЕЛТИРИЛГАН СИСТЕМАСИ

52-теоремага кўра, m модул бўйича ўзаро таққосланувчи сонлар m модул билан бир хил энг катта умумий бўлувчига эга. Хусусан, мана шу умумий бўлувчи бирга тенг бўлган ҳол, демак, модул билан ўзаро туб бўлган сонлар аҳамиятлидир.

13-т а ъ р и ф. m модул билан ўзаро туб бўлган барча чегирмалар синфларидан биттадан элемент олиб тузилган тўплам *чегирмаларнинг m модул бўйича келтирилган системаси* дейилади.

Чегирмаларнинг келтирилган системасини шу чегирмаларни тўла системасининг модул билан ўзаро туб бўлган сонларидан тузиш мумкин. Одатда чегирмаларнинг келтирилган системаси манфий бўлмаган энг кичик чегирмалар системаси 0,1,2,...m-1 дан ажратиш йўли билан тузилади. Бу сонлар орасида m билан ўзаро туб бўлган сонларнинг сони $\varphi(m)$ та. Шунинг учун келтирилган системадаги сонларнинг сони, шунингдек, модул билан ўзаро туб сонлардан тузилган синфлар сони $\varphi(m)$ тадир.

М и с о л. 30 модул бўйича чегирмаларнинг келтирилган системаси қуйидагилардан иборат:

1, 7, 11, 13, 17, 19, 23, 29.

55-т е о р е м а. m модул бўйича ўзаро таққосланмайдиган ва шу модул билан ўзаро туб бўлган ҳар қандай $\varphi(m)$ та сон чегирмаларнинг m модул бўйича келтирилган системасини ташкил этади.

И с б о т. Ҳақиқатдан, бу сонлар берилган модул бўйича ўзаро таққосланмайдиган ва у билан туб бўлгани сабабли модул билан ўзаро туб сонлардан ташкил этилган ҳар хил синфларга киради; m модул билан ўзаро туб сонлар $\varphi(m)$ та, яъни айтилган кўринишдаги синфлар сонига тенг бўлгани учун, бундай ҳар бир синфга юқоридаги сонларнинг биттасигина киради.

56-т е о р е м а. Агар ax ифодада x ўзгарувчи m модул бўйича чегирмаларнинг келтирилган сиситемасини ташкил этса ва (a,m)=1 бўлса, у ҳолда ax ҳам m модул бўйича чегирмаларнинг келтирилган системасини ташкил этади.

И с б о т. Ҳақиқатдан, x сонлар нечта бўлса, ax сонлар ҳам шунча, яъни φ(m) тадир. Энди 55-теоремага кўра, ax сонларнинг m модул бўйича ўзаро таққосланмаслигини ва модул бўйича ўзаро тубилигини кўрсатиш етарлидир. Бу тасдиқларнинг биринчиси 54-теоремада умумийроқ кўринишдаги ax+b сонлар учун исбот қилинган эди. Иккинчи қисми эса (a,m)=1 ва (x,m)=1 дан келиб чиқади.

М и с о л. a=7, m=18 бўлсин. У ҳолда (7, 18)=1 бўлиб, m модул бўйича чегирмаларнинг келтирилган системаси x=1,5,7,11,13,17 дан иборат; 5x ни m=18 модул бўйича чегирмаларини топамиз:

7·1≡7(mod 18), 7·5≡17(mod 18), 7·7≡13(mod 18), 7·11≡5(mod 18), 7·13≡1(mod 18), 7·17≡11(mod 18).

Демак, 7x ни 18 га бўлгандаги қолдиқлар {7,17,13,5,1,11} бўлар экан. Бу система {7,17,13,5,1,11} системадан сонларнинг турган ўрни билан бир-биридан фарқ қилар экан.

25-§. ЭЙЛЕР ВА ФЕРМА ТЕОРЕМАЛАРИ

57-т е о р е м а (*Эйлер теоремаси*). Агар m>1 ва (a,m)=1 бўлса, у ҳолда

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

таққослама ўринлидир.

И с б о т. Ҳақиқатан, агар x миқдор m модул бўйича келтирилган системани ташкил этувчи манфий бўлмаган энг кичик чегирмаларга тенг қийматларни қабул қилса, яъни

$$x=r_1, r_2, \ldots, r_t, \qquad t=\varphi(m)$$

бўлса, у ҳолда 56-теоремага кўра ax сонларнинг r_1', r_2', ..., r_t' дан иборат манфий бўлмаган энг кичик чегирмалари ҳам шу

системани (лекин, умуман айтганда, бошқа тартибда) ташкил этади.

Қуйидаги

$$a r_1 \equiv r_1' \pmod m,$$
$$a r_2 \equiv r_2' \pmod m,$$
$$\dots\dots\dots\dots$$
$$a r_t \equiv r_t' \pmod m,$$

таққосламаларни ҳадлаб кўпайтирсак,

$$a^t r_1 r_2 \dots r_t \equiv r_1' r_2' \dots r_t' \pmod m$$

ҳосил бўлади, бунинг иккала томонини модул билан ўзаро туб бўлган $r_1 r_2 \dots r_t \equiv r_1' r_2' r_t'$ кўпайтмага қисқартирсак,

$$a^t \equiv 1 \pmod m$$

таққосламани ҳосил қиламиз. Лекин $t=\varphi(m)$ бўлганлиги учун

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

М и с о л. $m=16$, $a=9$ бўлсин, у ҳолда $(16,9)=1$ бўлиб, $9^{\varphi(16)} \equiv 1 \pmod{16}$ бўлади.

Текшириб кўрамиз: $\varphi(16)=\varphi(2^4)=2^4-2^3=8$,

$9^2=81\equiv 1 \pmod{16}$, $9^8=(9^2)^4\equiv 1 \pmod{16}$.

Агар теоремада $m=p$ туб сон бўлса, у ҳолда $\varphi(p)=p-1$ бўлиб, қуйидагига эга бўламиз.

58-т е о р е м а *(Ферма теоремаси).* Агар p туб сон бўлиб, a сон p га бўлинмаса, у ҳолда

$$a^{p-1} \equiv 1 \pmod p$$

таққослама бажарилади.

М и с о л. $a=16$ ва $p=11$ бўлсин, у ҳолда $\varphi(11)=10$ ва $16^{10} \equiv 1 \pmod{11}$.

Текширамиз: $16\equiv 5 \pmod{11}$, $16^2\equiv 3 \pmod{11}$, $16^{10}\equiv 3^5 \pmod{11} = 243 \pmod{11} \equiv 1 \pmod{11}$.

Ферма теоремасини қулайроқ, кўринишга келтириш мумкин. бу таққосламани иккала томонини a га кўпайтириб,

$$a^p \equiv a \pmod p$$

таққосламани ҳосил қиламиз; бу таққослама ихтиёрий бутун a сон учун тўғридир, чунки у, p га бўлинувчи a лар учун ҳам ўринлидир.

И з о ҳ. $a^{n-1}\equiv 1 \pmod n$ таққослама бажарилганда ҳар доим ҳам n туб сон бўлавермайди. Масалан, $2^{341-1}\equiv 1 \pmod{341}$ Ҳақиқатан,

$$2^{10}=1024=3\cdot 341+1\equiv 1 \pmod{341},$$

шунинг учун

$$2^{340}=(2^{10})^{34}\equiv 1 \pmod{341},$$

лекин $341=31\cdot 11$ таркибли сон.

26-§. ЭЙЛЕР ВА ФЕРМА ТЕОРЕМАЛАРИНИНГ ТАДБИҚЛАРИ

Эйлер ва Ферма теоремаларининг тадбиқлари кўпдир. Биз бу ерда даражаларни берилган сонга бўлганда ҳосил бўладиган қолдиғини ҳисобаймиз.

1-м и с о л. 2^{80} ни 13 га бўлганда ҳосил бўладиган қолдиқ топилсин. Ферма теоремасига кўра $2^{12}\equiv 1 \pmod{13}$, шунинг учун $2^{72}=(2^{12})^6\equiv 1 \pmod{13}$, $2^8=256=19\cdot 13+9\equiv 9 \pmod{13}$.

Демак, $2^{80}\equiv 9 \pmod{13}$.

Шундай қилиб, 2^{80} ни 13 га бўлганда 9 қолдиқ қолади.

2-м и с о л. 319^{261} ни 15 га бўлганда ҳосил бўладиган қолдиқ топилсин.

Е ч и ш. $319\equiv 4 \pmod{15}$, $319^{261}\equiv 4^{261} \pmod{15}$. Эйлер теоремасига кўра $2^{\varphi(15)}=2^8=4^4\equiv 1 \pmod{15}$, иккинчи томондан $261=4\cdot 65+1$. Шунинг учун, $4^{261}=(4^4)^{65}\cdot 4\equiv 4 \pmod{15}$.

Демак, изланаётган қолдиқ 4 га тенг.

3-м и с о л. 3^{60} ни 83 га бўлганда ҳосил бўладиган қолдиқни топинг.

Е ч и ш. Ферма теоремаси бу ҳол учун ўтмайди, чунки $\varphi(83)=82>60$. Шунинг учун шундай 3^k ни топиш керакки k

нинг мумкин қадар катта қийматларида 83 га бўлганда иложи борича кичикроқ қолдиқ қолсин. Равшанки.

$3^4=81\equiv -2(\text{mod } 83)$; $3^{60}=3^{4\cdot 15}\equiv(-2)^{15}(\text{mod } 83)$

$2^5=512=83\cdot 6+14\equiv 14(\text{mod } 83)$,

$2^{15}=2^{5\cdot 3}\equiv 14^3(\text{mod } 83)=14\cdot 196\equiv 14\cdot 30 \ (\text{mod } 83)=$ $420=83\cdot 5+5\equiv 5(\text{mod } 83)$.

Демак, $3^{60}\equiv -5(\text{mod } 83)\equiv 78 \ (\text{mod } 83)$. Қидирилаётган қолдиқ 78 га тенг экан.

5 - БОБ УЧУН МАШҚЛАР

1. Қуйидаги –21,8,17,-38,121,87,-62,224,225 сонларнинг 11 модул бўйича манфий бўлмаган энг кичик мусбат ва абсолют энг кичик чегирмаларини топинг. Бу сонларнинг қайсилари 13 модул бўйича таққосланади.
2. 100 нинг 2,3,5,7,11,51,99,331 модуллар бўйича манфий бўлмаган энг кичик ва абсолют энг кичик чегирмалари топилсин.
3. 2^{999} ва 3^{999} сонларнинг иккита охирги рақамларини топинг.
4. Ушбу $4365^{47}\cdot 7937^{73}$ соннинг 8 модул бўйича чегирмаси топилсин.
5. $7^{100}+11^{100}$ соннинг 13 га бўлганда ҳосил бўлган қолдиғини топинг.
6. 84^{399} сонни 9 га бўлганда ҳосил бўлган қолдиқ топилсин.
7. 65^{17} ни 7 га ва 6^{592} ни 11 га бўлганда ҳосил бўлган қолдиқлар топилсин.
8. k нинг қайси қийматларида 85^k нинг 9 модул бўйича энг кичик чегирмаси 1 га тенг бўлади.
9. $2^{11\cdot 31}\equiv 2(\text{mod } 11\cdot 31)$ эканлигини кўрсатинг.
10. Агар $a^{100}\equiv 2(\text{mod } 73)$ ва $a^{101}\equiv 69(\text{mod } 73)$ бўлса, a ни 73 га бўлганда қолдиғини топинг.

5-бобга доир тарихий маълумот

1. 47-теорема Гауссннинг «Арифметик тадқиқотлар» ида бор.

2. Диофант (Diophantos)-қадимги Юнонистоннинг буюк математиги Искандария (Александрия) да яшаган ва ишлаган. Унинг қачон туғилгани ва ўлгани номаълум. Математика тарихчилари уни 3- ёки 4-асрда яшаган деб тахмин қилишади. Унинг ҳаёти ҳақидаги маълумот Диофант ўлгандан кейин кўп вақт ўтмасдан шеърий формада ёзилган бир арифметик масала туфайли етиб келган. Бу масалани ечиб билиш мумкинки Диофант 84 ёшида ўлган. Диофант «Арифметика», «Поризмлар» ва «Кўпбурчакли сонлар» номли асарлар ёзган, асарларнинг кўп қисми бизгача етиб келмаган. «Арифметика» асари 13 китобдан иборат бўлиб, бизгача олтитаси етиб келган. Бу етиб келган китобларда шундай масалалар қаралганки, улар даражаси 4 дан ошмайдиган ноаниқ (номаълумларнинг сони тенгламалар сонидан кўп) тенгламаларга келади. Диофант бундай тенгламаларни фақат рационал ва мусбат ечимини топиш методини берган. У фақат мусбат ва рационал ечимини кўрсатган. У ўз олдида тенгламани барча ечимларини топишни мақсад қилиб қўймайди, тенглама чексиз кўп ечимга эга бўлса ҳам, битта ечимини топиш билан қаноатланади. Ечишнинг умумий методини бермаган.

Диофантнинг «Арифметика» асари П.Ферма, Л.Эйлер ва К.Гауссннинг тадқиқотлари учун таянч нуқта бўлган.

3. П.Ферма (Pierre de Fermat, 1601-1665) француз математиги, касби ҳуқуқшунос (юрист) 1631 йилдан Тулузада парламент маслаҳатчиси бўлиб ишлаган. Қатор машҳур асарларнинг муаллифи Ферма сонлар назариясига оид натижаларини Диофант «Арифметика» сининг ҳошиясида ёзган. Ферма, одатда исботини ёзмасдан, фақат қўллаган методи ҳақида қисқача кўрсатмалар берган. Ферма

ҳаётлигида унинг ишлари мактублари ва шахсий алоқалари орқали бошқа олимларга маълум бўлган. У М.Мерсенн билан дўст бўлган ва унга ўз ишларини сақлашга бериб қўйган. У Б.Паскал, Ж.Робервал, Р.Декарт, П.Гассенди, Ф.Б.Кавальери, Э.Торичелли, Х.Гюйгенс ва бошқа олимлар билан ёзишиб турган. Ферма ишларининг кўп қисми унинг вафотидан сўнг унинг ўғли Самуил Ферма (1630-1690) томонидан 1679 йилда «Opera varia» («Ҳар хил математик масалалар» номи билан) нашр эттирилган.

Ферма математиканинг турли соҳаларида ишлаган. У сонлар назариясининг асосчиларидан бири ҳисобланади. Сонлар назариясида Ферманинг номини олган иккита теорема бор. Биринчиси 25-§ даги 28-теорема (*Ферманинг кичик теоремаси*). Иккинчиси (*Ферманинг буюк теоремаси, Ферманинг машҳур теоремаси, Ферманинг охирги теоремаси)* қуйидаги тасдиқдан иборат: n иккидан катта ва бутун сон бўлганда $x^n+y^n=z^n$ (*Диофант тенгламаси)* нолдан фарқли бутун x, y, z сонларда ечимга эга эмас. Бу тасдиғни Ферма 1630 йилда Диофантни «Арифметика» асарининг ҳошиясида қуйидагича ёзган эди: «Кубни иккита кубга, биквадратни икита биквадратга, умуман, квадратдан катта ҳеч қандай даражани шу кўрсатгичга эга бўлган иккита даражага ажратиш мумкин эмас». Кейин у қўшиб қўйган эди: «Мен буни ҳақиқатан ажойиб исботини топдим, лекин бунинг учун бу ҳошиялар жуда кичик». Ферманинг қоғозларида бу теоремани n=4 бўлган ҳолининг исботини топишган. n=3 бўлганда бу теоремани Л.Эйлер (1770 й.) исботлади, n=5 бўлганда Л.Дирихле ва А.Лежандр (1825 й.), n=7 бўлганда Г.Ламе (1839 й.) исботлади. Немис математиги Э.Куммер (Эрнст Эдуард, 1810-1893) алгебраик сонлар назариясида *идеал* тушунчасини киритиб, 100 дан ошмайдиган барча n=p туб сонлар учун Ферманинг буюк теоремасини исбот қилди. Ферманинг буюк теоремасини содда таърифланишига қарамасдан, унинг тўлиқ исботи

Диофант тенгламалари назариясида янги ва чуқур методлар яратишни талаб қилса керак.

Математика соҳасида мутахассис бўлмаган кишилар орасида бу теоремани исбот қилишга бўлган ўринсиз уринишлар ўз вақтида бундай исбот учун катта халқаро мукофот таъсис этилиши билан боғлиқ бўлган. Бу мукофот Биринчи жаҳон уруши охиридаёқ (1914-1918) бекор қилинган.

4. 58-теорема Ферманинг 1640 йилда Френикл де Бесси (Frenicle de Bessy, 1602-1675) га ёзган хатида баён қилинган эди. Ба хатда Ферма мазкур теореманинг исботини топганман дейилган, лекин исботнинг ўзи йўқ эди. Ферма теоремасининг маълум исботларидан биринчисини Г.Лейбниц (Leibniz Gotfried Wilhelm, 1646-1716) берган эди. Лейбницнинг исботи

$$(a_1 + a_2 + ... + a_n)^p \equiv a_1^p + ... + a_n^p \pmod{p}$$

таққосламага асосланган.

Эйлер Ферма теоремасини бир неча исботини берди, улардан бирнчиси 1736 йилда эди. 1760 йилда эса Эйлер Ферма теоремасини умумлаштириб, 57-теоремани исбот қилди. Шуни айтиш керакки Ферма ва Эйлернинг терминлари ва белгилашлари ҳозирги замонникидан тубдан фарқ қилади. Биз келтирган исботни 1806 йилда Дж.Айвори (Ivory J., 1765-1842) Ферма теоремаси учун берган исботнинг бевосита умумлашгани бўлиб, ҳозирги замонда аксарият дарсликларда келтирилади (қ.мас., [4], [7]).

5. Такомил сонлар билан буюк аллома Ибн Сино (Абу Али Ибн Сино, 980-1037) ҳам шуғулланган. У 1030-1035 йилларда форс-тожик тилида ёзилган энциклопедик асари «Донишнома» фалсафа, мантиқ физика ва математикага бағишланган бўлиб, унда мукаммал сонлар ҳам ўрганилган.

6-БОБ. БИР НОМАЪЛУМЛИ ТАҚҚОСЛАМАЛАР

27-§. АСОСИЙ ТУШУНЧАЛАР

Фараз қилайлик

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$$

бутун коэффицентли, a_0 бош коэффициенти m га бўлинмайдиган n-даражали кўпҳад бўлсин.

14-т а ъ р и ф. Агар x номаълум бутун сон

$$f(x) = 0 \pmod m \qquad (43)$$

шартни қаноатлантирса, у ҳолда (43)-муносабат *бир номаълумли n-даражали таққослама* дейилади.

Таққосламани ечиш уни қаноатлантирадиган барча x ларни топишни билдиради. Лекин, агар x_1 сон $f(x_1) = 0 \pmod m$ ни қаноатлантирса, у ҳолда (47-теорамага кўра) шу таққосламани x_1 билан m модул бўйича таққосланувчи, яъни $x = x_1 \pmod m$ шартга бўйсунувчи, ҳар қандай x сон ҳам қаноатлантиради. Шундай сонларнинг барчасидан тузилган синф *битта ечим* деб ҳисобланади.

15-т а ъ р и ф. *(43)-таққосламани m модул бўйича тўла системанинг нечта чегирмаси қаноатлантирса, бу таққослама шунча ечимга эга* дейилади.

1-м и с о л. Ушбу

$$2x^2+3x+1=0 \pmod 5$$

таққосламанинг ечимлари топилсин.

Е ч и ш. Ҳисоблашни соддалаштириш учун 5 модул бўйича абсолют қиймати билан энг кичик чегирмаларни оламиз: 0; ±1; ±2. Текшириш кўрсатадики, фақат x=-1 ва x=2 чегирмалар таққосламани қаноатлантиради. Шунинг учун, таққослама иккита $x=2 \pmod 5$ ва $x=4 \pmod 5$ ечимга эга.

2-м и с о л. Ушбу

$$x^3+2x+1=0 \pmod 3$$

ққослама ечилсин.

Е ч и ш. 3 модул бўйича 0,1,2 чегирмаларни текшириб кўсак, уларнинг бирортаси ҳам қаноатлантирмайди. Демак, у таққослама ечимга эга эмас.

16-т а ъ р и ф. Агар таққосламани ҳар қандай бутун ни қаноатлантирса, бундай таққослама *айний* дейилади.

Айний таққослмага Ферма теормасидан келиб чиқадиган

$$x^p - x = (\mathrm{mod}\ p)$$

ққослама мисол бўла олади. Бу таққослама барча бутун х ларни қаноатлантиради.

28-§. БИРИНЧИ ДАРАЖАЛИ ТАҚҚОСЛАМАЛАР

Биринчи даражали бир номаълумли таққосламанинг умумий кўриниши қуйидагидан иборат:

$$ax \equiv b\ (\mathrm{mod}\ m) \qquad (44)$$

1. Бу таққосламанинг ечмини топишда икки ҳол $(a, m) = 1$ ва $(a, m) = d > 1$ бўлиши мумкин. Биз аввал $(a, m) = 1$ ҳолни кўриб чиқамиз. 27-§ га асосан 44- таққослама ечимларининг сони тўла системадаги, уни қаноатлантирувчи чегирмаларнинг сонига тенг. Лекин (54 – теоремага кўра) х сон m модул бўйича тўла системанинг чегирмаларига тенг қийматларни қабул қилади. Демак, х нинг тўла системадан олинган фақат битта қийматида ax сон b билан таққосланади. Шундай қилиб, $(a, m) = 1$ бўлганда (44)-таққослама ягона ечимга эга.

2. Энди $(a, m) = d > 1$ бўлсин. Агар $ax - b = my$ деб олсак (яъни $ax - b$ сон m га бўлинади), у ҳолда b сон d га бўлинмаса (44)-таққослама ечимга эга бўлмайди. Фараз қилайлик b сон d га бўлинсин: $b = b_1 d_1$; яна $a = a_1 d$; $m = m_1 d$ деб белгилайлик. У ҳолда (d га бўлиш натижасида) (44) – таққослама

$$a_1 x_1 \equiv b_1 (\mathrm{mod}\ m_1) \qquad (45)$$

таққосламага тенг кучли бўлади, бу ерда эса $(a_1, m_1) = 1$

бўлиб, (45) – таққослама ягона ечимга эга бўлади: $x \equiv x_0 \pmod{m_1}$ ёки $x=x_0+km_1$, бунда k-ихтиёрий бутун сон. (45)-таққосламанинг ҳар иккала томонини d га кўпайтириб кўрамизки барча $x=x_0+km_1$ сонлар (45)-таққосламани $k=0,1,2,\ldots, d-1$ бўлганда қаноатлантиради. Равшанки $к=0,1,2\ldots, d-1$ бўлганда ҳосил бўладиган

$$x_0, x_0+m_1, x_0+2m_1, \ldots, x_0+(d-1)m_1 \qquad (46)$$

ечимлар m модул бўйича ҳар хил синфларда ётади, k нинг бошқа қийматларидаги $x_0+к\ m_1 = x_0+к\frac{m}{d}$ ечимларнинг барчаси m модул бўйича (46)-сонлар билан таққосланади. Демак, биз бу ҳолда d та ечимга эга бўламиз. Шундай қилиб, қуйидаги теоремани исбот қилдик.

59-т е о р е м а. Фараз қилайлик $(a,m)=d$ бўлсин. Агар b сон d га бўлинмаса $ax \equiv b \pmod{m}$ таққослама ечимга эга эмас. Агар, b сон d га бўлинса, у ҳолда таққослама d та ечимга эга бўлади.

29-§. БИР НОМАЪЛУМЛИ БИРИНЧИ ДАРАЖАЛИ ТАҚҚОСЛАМАНИНГ ЕЧИМИНИ ТОПИШ

Биз (44)- таққосламани ечишни бир неча усулларини кўриб чиқамиз.

1. *Синаш усули.* Бу усул шундан иборатки (44)-таққосламадаги x ўрнига m модул бўйича барча чегирмаларни қўйиб, текшириб чиқамиз. Буларнинг қайси бири (44)- таққосламани қаноатлантирса, ўша чегирма қатнашган синф ечим ҳисобланади. Биз юқоридаги мисолларни синаш усулида ечган эдик.

2. *Коэффицентларни ўзгартириш усули.* Бу ўзгартиришлар қуйидагидан иборат: коэффицентларни абсолют энг кичик чегирма билан алмаштириш, b ни модул билан таққосланувчи шундай сон билан алмаштириш

керакки, натижада ўнг томонда ҳосил бўлган сон a га бўлинсин ва ҳ.к.

1-м и с о л. $11x\equiv 3 \pmod{25}$ таққосламани ечинг.

Е ч и ш. $11x\equiv 3-25 \pmod{25}$, $11x\equiv -22 \pmod{25}$, $x\equiv -2 \pmod{25}$.

2-м и с о л. $83x\equiv 13 \pmod{22}$ таққосламани ечинг.

Е ч и ш. $83x\equiv 13 \pmod{22}$, $88x-5x\equiv 13+22 \pmod{22}$, $-5x\equiv 35 \pmod{22}$,

$x\equiv -7 \pmod{22}$.

3. *Эйлер методидан фойдаланиш усули.* Маълумки, $(a,m) = 1$ бўлганда $a^{\varphi(m)} \equiv 1 \pmod{m}$ таққослама ўринли бўлади. Бу таққосламанинг ҳар иккала томонини b га кўпайтирамиз:

$$a^{\varphi(m)}b \equiv b \pmod{m}.$$

буни a $x\equiv b \pmod{m}$ таққослама билан солиштириб, ечим учун

$$x \equiv a^{\varphi(m)-1}b \pmod{m}$$

га эга бўламиз.

Ечимни тайёр формула шаклида топган бўлсак ҳам, масала тўлиқ ечилиши учун $a^{\varphi(m)-1}b$ нинг модул бўйича энг кичик манфий бўлмаган ёки абсолют қиймати билан энг кичик чегирмани топиш керак.

3-м и с о л. $11x\equiv 13 \pmod{24}$ таққослама ечилсин. Бунда $(11, 24)=1$, $\varphi(24)=8$. Демак, $x\equiv 11^7 \cdot 13 \pmod{24}$. Модули билан энг кичик чегирмани топамиз:

$11^2=121\equiv 1 \pmod{24}$, $11^6\equiv 1 \pmod{24}$, $x\equiv 11^7 \cdot 13 = 11 \cdot 13 \pmod{24} \equiv$

$\equiv 143 \pmod{24} \equiv -1 \pmod{24}$.

Ечим $x\equiv 23 \pmod{24}$.

4. *Узлуксиз касрлардан фойдаланиш усули.* Таққосламанинг модули катта бўлса, бу усул анча афзалдир.

Фараз қилайлик $(a,\ m)=1$ бўлсин, у ҳолда $\frac{m}{a}$ ни узлуксиз касрга ёямиз:

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}}.$$

Бизга $\frac{P_k}{Q_k}$ муносиб касрларнинг иккита охиргиси $\frac{P_{n-1}}{Q_{n-1}}$ ва $\frac{P_n}{Q_n} = \frac{m}{a}$ керак бўлади. Узлуксиз касрларнинг (26-теорема) хоссасига кўра

$$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^n,$$

бундан

$$mQ_{n-1} - aP_{n-1} = (-1)^n,$$

$$aP_{n-1} \equiv (-1)^{n-1} (\mathrm{mod}\ m),$$

$$a[(-1)^{n-1}P_{n-1}b] \equiv b(\mathrm{mod}\, m).$$

Шундай қилиб, таққосланинг биз қидираётган ечими

$$x \equiv (-1)^{n-1}P_{n-1}b(\mathrm{mod}\, m).$$

бўлади.

М и с о л. $259x \equiv 147 \pmod{749}$ таққослама ечилсин.

Е ч и ш. Бунда (259, 749)=7 ва, шунингдек, 147 ҳам 7 га бўлинади. Шунинг учун, таққослама 7 та ечимга эга. Таққосланинг ҳар иккала томонини ва модулини 7 га қисқартириб, қуйидаги

$$37x \equiv 21 \pmod{107}$$

га эга бўламиз. Энди $\frac{107}{37}$ ни узлуксиз касрга ёйиб, P_{n-1} топамиз. Бунинг учун кетма-кет бўлишни қўллаймиз:

$107=37\cdot2+33,\quad 37=33\cdot1+4,$
$33=4\cdot8+1$
$4=1\cdot4$

Демак, $q_1=2$, $q_2=1$, $q_3=8$, $q_4=4$.

12-§ келтирилган жадвални тузамиз:

q_k		2	1	8	4
P_k	1	2	3	26	107

Демак, $P_{n-1}=P_3=26$. Бундан

$x \equiv(-1)^3 26\cdot21 (\text{mod } 107)=-546(\text{mod } 107) \equiv -11 (\text{mod } 107)$

ёки

$x \equiv -11(\text{mod } 107)$.

Бундан кўрамизки, берилган таққосламанинг ечимлари қуйидагича бўлади:

$x \equiv -11, -11+107; -11+2\cdot107; -11+3\cdot107; -11+4\cdot107; -11+5\cdot107; -11+6\cdot107(\text{mod } 749)$, яъни $x \equiv -11, 96; 203; 310; 417; 524; 631 (\text{mod } 749)$.

30-§. БИРИНЧИ ДАРАЖАЛИ ТАҚҚОСЛАМАЛАР СИСТЕМАСИ

Умумий ҳолда бундай система қуйидагидан иборат:

$A_1x \equiv B_1 (\text{mod } m_1)$, $A_2x \equiv B_2 (\text{mod } m_2)$,... $A_kx \equiv B_k (\text{mod } m_k)$.

Бу системани ечиш системани барчасини қаноатлантирадиган x нинг бутун қийматларини топиш демакдир. Равшанки, бундай сонларнинг мавжудлиги учун ҳар бир таққослама ечимининг мавжудлиги зарурдир (лекин кифоя эмас).

Шунинг учун, модуллар жуфт-жуфт ўзаро туб бўлган энг содда

$x \equiv b_1 (\text{mod } m_1)\ x \equiv b_2 (\text{mod } m_2),\ldots\ x \equiv b_k (\text{mod } m_k)$ (47)

системани ечимини топиш билан қаноатланамиз.

60-т е о р е м а. Фараз қилайлик M_t *ва* M_t^1 сонлар $M=m_1 m_2 \dots m_k=M_t m_t$, $M_t \cdot M_t^1 \equiv 1 \pmod{m_t}$, $t=1,2,\dots,k$ шартлар билан аниқланган ва

$$x_0 = M_1 M_1^1 b_1 + M_2 M_2^1 b_2 + \dots + M_k M_k^1 b_k$$

бўлсин. У ҳолда x нинг (47)-системани қаноатлантирувчи қийматлари

$$x \equiv x_0 \pmod{m_1 m_2 \dots m_k} \equiv x_0 \pmod{M} \qquad (48)$$

таққосламадан аниқланади.

И с б о т. Равшанки, M_t дан фарқли барча M_j лар m_t га бўлинганлиги туфайли $t=1,2,\dots,k$ қийматларнинг ҳар бирида

$$x_0 \equiv M_t M_t^1 b_t \equiv b_t \pmod{m_t}$$

таққослама ўринли бўлади. Демак, (47)-системани қаноатлантиради. Бундан эса (47)-системанинг

$$x \equiv x_0 \pmod{m_1}, \; x \equiv x_0 \pmod{m_2}, \dots x \equiv x_0 \pmod{m_k} \qquad (49)$$

система билан тенг кучлилиги (яъни (47)- ва (49)-системаларни x нинг бир хил (48)-қийматлари қаноатлантириши) бевосита келиб чиқади. (49)- системани эса 50- ва 51- теоремаларга асосан) x нинг фақат (48)-таққосламани ўринлатувчи қиймати қаноатлантиради.

М и с о л. Ушбу

$$x \equiv b_1 \pmod{6}, \; x \equiv b_2 \pmod{7}, \; x \equiv b_3 \pmod{11}$$ система ечилсин.

Е ч и ш. Бунда $M=6\cdot7\cdot11=462$, $M_1=7\cdot11=77$, $M_2=6\cdot11=66$, $M_3=6\cdot7=42$ шу билан бирга $77 M_1' \equiv 1 \pmod 6$, $66 M_2' \equiv 1 \pmod 7$, $42 M_3' \equiv 1 \pmod{11}$ ёки

$$-M_1' \equiv 1 \pmod 6, \; 3M_2' \equiv 1 \pmod 7, \; -2M_3' \equiv 1 \pmod{11}$$

ёинки

$$M_1' \equiv 5 \pmod 6, M_2' \equiv 5 \pmod 7, M_3' \equiv 5 \pmod{11}.$$

Демак,

$x \equiv 77 \cdot 5b_1 + 66 \cdot 5b_2 + 42 \cdot 5b_3 = 385b_1 + 330b_2 + 210b_3.$

Натижада х нинг системани қаноатлантирувчи қийматларини

$x \equiv 385b_1 + 330b_2 + 210b_3 (\mathrm{mod}\, 462)$ кўринишда

ифодалаш мумкин. Шундай қилиб, бундан х нинг

$x \equiv 2(\mathrm{mod}\, 6), x \equiv 3(\mathrm{mod}\, 7), x \equiv 5(\mathrm{mod}\, 11)$ системани

қаноатлантирадиган қийматлари

$x \equiv 385 \cdot 2 + 330 \cdot 3 + 2105 (\mathrm{mod}\, 462) \equiv 38 (\mathrm{mod}\, 462)$ эканлиги келиб чиқади.

31-§. ТУБ МОДУЛ БЎЙИЧА ИХТИЁРИЙ ДАРАЖАЛИ ТАҚҚОСЛАМАЛАР

Туб модул бўйича таққослама энг содда бўлсада, энг муҳим ҳамдир, чунки таркибли модулли таққосламанинг ечиш масаласини туб модулли таққосламани ечишга келтириш мумкин. Шунинг учун n – даражали таққосламани ечишни биз туб модуллисидан бошлаймиз. Фараз қилайлик p-туб сон бўлиб,

$$f(x) \equiv 0(\mathrm{mod}\, p);\ \mathrm{f(x)} = \mathrm{a}_0 x^n + \mathrm{a}_0 x^{n-1} + \ldots + \mathrm{a}_n \qquad (50)$$

таққослама берилган бўлсин.

61-т е о р е м а. n – даражали $p(p \le n)$ туб модулли таққослама даражаси p-1 дан ошмайдиган таққосламага тенг кучлидир.

И с б о т. Ҳаққатан, f(x) ни x^p-x га бўлганда

$$f(x) \equiv (x^p - x)\mathrm{Q(x)} + \mathrm{R(x)}$$

ҳосил бўлади, бунда R(x) нинг даражаси p-1 дан ошмайди. Ферма теоремасига кўра x^p-x ≡0(mod p), шунинг учун f(x) ≡R(x)(mod p) бўлиб, бундан теореманинг тасдиғи келиб чиқади.

И з о ҳ. Бу теоремани амалда қўллаш учун f(x) ни x^p-x га бўлиб, ўтирмасдан x^m ни х нинг даражаси p-1 дан ошмайдиганига келтириш учун қуйидагича иш тутиш

мумкин: m ни p-1 га бўлиб, r қолдиқни 1 дан p-1 гача ораликда оламиз (одатда қолдиқ 0 дан p-2 гача олинади, биз бу ерда 0 ни ўрнига p-1 ни оламиз) , яъни m=(p-1)k+r, $1 \le r \le p-1$. Энди ушбу айний

$$x \equiv x^p \pmod p$$

таққосламанинг ҳар иккала томонини кетма кет x^{r-1}, $x^{(p-1)\cdot 1+r-1}$,..., $x^{(p-1)(k-1)+(r-1)}$ ларга кўпайтириб, қуйидагиларни ҳосил қиламиз:

$$x^r \equiv x^{(p-1)\cdot 1+r} \equiv x^{(p-1)\cdot 2+r} \equiv \ldots = x^{(p-1)(k-1)+r} \equiv x^{(p-1)k+r} \pmod p .$$

Шуни таъкидлаш керакки бу ерда r=0 ни олиш мумкин эмас, чунки у ҳолда x^{r-1} га кўпайтириш x^{-1} га кўпайтиришни билдирар эди.

Шундай қилиб,

$$x^m = x^{(p-1)k+r} \equiv x^r \pmod p, 1 \le r \le p-1 \qquad (51)$$

таққосламага эга бўлдик.

Шунинг билан бирга биз теореманинг янги исботини ҳам ҳосил қилдик.

М и с о л. $x^9+ 3x^7+ x^6-3x^5 +x^3+x+1\equiv 0 \pmod 5$ таққослама даражаси 4 дан ошмайдиган таққосламага келтирилсин.

Е ч и ш. (51) дан фойдаланиб қуйидагига эга бўламиз:

$$x+ 3x^3+ x^2-3x +x^3+x+1\equiv 0 \pmod 5$$

ёки,

$$4x^3+ x^2- x+1\equiv 0 \pmod 5.$$

62-т е о р е м а. Агар (50)- таққослама n дан ортиқ ечимга эга бўлса, у ҳолда f(x) нинг барча коэффицентлари p га бўлинади.

И с б о т. Фараз қилайлик (50)-таққослама ҳеч бўлмаганда n+1 та ечимга эга бўлсин. Бу ечимларнинг чегирмаларини $x_1, x_2, \ldots, x_n, x_{n+1}$ орқали белгилаймиз ва f(x) ни қуйидагича ёзиб оламиз:

$$\begin{aligned} f(x) &= a_0(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n)+ \\ &+ A(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})+ \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &+ A_{n-2}(x-x_1)(x-x_2)+ \\ &+ A_{n-1}(x-x_1)+ \\ &+ A_n. \end{aligned} \qquad (52)$$

Бу ифоданинг ўнг томонидаги қавсларни кўпайтириб, f(x) ни кўпҳад шаклида ёзиб, ҳосил бўлган коэффицентларни $a_0, a_1, \ldots, a_n$ ларга тенглаштириш натижасида келиб чиқадиган чизиқли алгебраик тенгламалар системасидан $A_0, A_1, \ldots, A_n$ коэффицентларни аниқлаймиз.

Энди (52)-да $x=x_1$ ни қўямиз, натижада $A_n=f(x_1)$ ни ҳосил қиламиз. $p|f(x_1)$ бўлганлиги учун $p|A_n$. Кейин $x=x_2$ ни қўямиз, натижада $A_{n-1}(x_1 - x_2)= A_n-f(x_2)$ келиб чиқади, бунинг ўнг томони ҳам p га бўлинади, лекин $x_2 - x_1$ сон p га бўлинмайди, бундан эса $p| A_{n-1}$ деган хулосага келамиз. Бу жараённи давом эттириб, $x= x_{n+1}$ ни қўямиз, натижада

$$f(x_{n+1}) = a_0(x_{n+1}-x_1)(x_{n+1}-x_2)\ldots(x_{n+1}-x_n)$$

га эга бўламиз, бундан эса a_0 коэффицент p га бўлинади деган хулосага келамиз; $a_0, a_1, \ldots, a_n$ лар $A_0, A_1, \ldots, A_n$ сонларнинг алгебраик йиғиндиси бўлганлиги учун улар ҳам p га бўлинади.

Э с л а т м а. Таркибли модулли таққослама учун (62)-теорема ўринли эмас. Масалан, $x^2 + x + 6 \equiv 0(\mathrm{mod}\,6)$ таққослама $x \equiv 0,2,3,5\ (\mathrm{mod}6)$ лардан иборат тўртта ечимга эга.

63 – т е о р е м а. (Вилсон теоремаси). p туб бўлганда

$$(p-1)!+1 \equiv 0(\mathrm{mod}\,p) \qquad (53)$$

таққослама ўринлидир.

И с б о т. p = 2 бўлганда теореманинг тўғрилиги равшан; p>2 қийматлар учун

$$(x-1)(x-2)\ldots[x-(p-1)]-(x^{p-1}-1) \equiv 0(\mathrm{mod}\,p)$$

таққосламани кўриб чиқайлик. Бу таққосламанинг даражаси p-2 дан ошмайди ва Ферма теоремасига кўра чегирмалари 1,2,...p-1 сонлардан иборат (p-1) та ечимга эга. Демак, 62-теоремага кўра бу таққосламанинг барча коэффицентлари, жумладан озод ҳад ҳам p га бўлинади, бу ҳад (53)-таққосламанинг чап томонидаги сондир. Теорема исботланди.

Мисол. $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6+1=721\equiv 0(\mathrm{mod}\,7)$.

32-§. ТАРКИБЛИ МОДУЛЛИ ИХТИЁРИЙ ДАРАЖАЛИ ТАҚҚОСЛАМАЛАР

Бу параграфда таркибли модулли таққосламани ечишга келтириш мумукинлигини кўрсатамиз. Аввал ушбу теоремани исбот қиламиз.

64-т е о р е м а. Агар $m_1, m_2, ..., m_k$ жуфт-жуфт ўзаро туб сонлар бўлса, у ҳолда

$$f(x)\equiv 0(\mathrm{mod}\ \ m_1\cdot m_2\cdots m_k) \qquad (54)$$

таққослама

$$f(x)\equiv 0(\mathrm{mod}\, m_1), f(x)\equiv 0(\mathrm{mod}\, m_2),..., f(x)\equiv 0(\mathrm{mod}\, m_k) \qquad (55)$$

таққосламалар системаси билан тенг кучли бўлади. Шу билан бирга, (55)-системадаги таққосламаларнинг мос модуллар бўйича ечимларининг сонини $N_1, N_2, ..., N_k$ деб ва (54)-таққослама ечимларининг сонини N деб белгиласак, у ҳолда

$$N = N_1\cdot N_2\cdots N_k$$

бўлади.

И с б о т. 51-теоремага кўра, агар таққослама $M = m_1\cdot m_2\cdots m_k$ модул бўйича ўринли бўлса, у ҳолда унинг ҳар бир бўлувчиси m_j бўйича ҳам ўринли бўлади. Бундан кўринадики (54)-таққосламани қаноатлантирадиган ечим

(55)-таққосламани ҳам қаноатлантиради. Аксинча, 50-теоремага кўра, агар таққослама $m_1, m_2, ..., m_k$ модуллар бўйича ўринли бўлса, у ҳолда таққослама ЭКУК $[m_1, m_2, ..., m_k]$ бўйича ҳам ўринли бўлади; $(m_i, m_j) = 1$ бўлганлиги сабабли, уларнинг $M = m_1 \cdot m_2 \cdots m_k$ кўпайтмаси бўйича ҳам ўринли бўлади. Шундай қилиб, (54)-таққослама билан (55)-таққосламалар системаси тенг кучли экан. Шу билан теоремани биринчи тасдиғи исботланди.

Теореманинг иккинчи тасдиғини исбот қилишдан олдин шуни таъкидлаб ўтиш керакки, агар (55)-системасининг бирорта таққосламаси ечимга эга бўлмаса, у ҳолда система тўлалигича ечимга эга бўлмайди, демак, (54)-таққослама ҳам ечимга эга бўлмайди.

Фараз қилайлик b_1 (55)-системадаги 1-таққосламанинг битта ечимининг чегирмаси бўлсин, яъни $x \equiv b_1 (\mathrm{mod}\, m_1)$, b_2 (55)-системадаги 2-таққосламани битта ечимининг чегирмаси бўлсин, яъни $x \equiv b_2 (\mathrm{mod}\, m_2)$ ва х.к. b_k k-таққосламани битта ечимининг чегирмаси бўлсин, яъни $x \equiv b_k (\mathrm{mod}\, m_k)$. У ҳолда (55)-система ягона

$$x \equiv x_0 = M_1 \cdot M_1' b_1 + M_2 \cdot M_2' b_2 + ... + M_k \cdot M_k' b_k (\mathrm{mod}\, M)$$

ечимга эга, бу ечим, шунингдек, (55)-системани ва (54)-таққосламанинг ечими бўлади. Лекин (55)-системанинг 1-таққосламаси N_1, 2-таққосламаси N_2 ва ҳ.к., k-таққослама N_k ечимга эга. Демак, $N_1 \cdot N_2 \cdots N_k$ та (55)-кўринишдаги система ҳосил бўлади, буларга шунча x_0 мос келади. Бу $N = N_1 \cdot N_2 \cdots N_k$ та сонларга (55)-системанинг бир-биридан фарқли ечимлари мос келишини кўрсатиш учун бу чегирмалар M модул бўйича хар хил синфларда ётишини кўрсатиш зарурдир. Охирги тасдиқнинг ўринли эканлигини кўрсатиш учун биз битта таққослама ечимининг чегирмасини

бошқаси билан алмаштирганда, масалан, b_1 ни b_1' га алмаштирганда ҳосил бўлган x_0 ва x_0' сонлар ҳар хил синфларда ётишини кўсатамиз.

Равшанки, масалан $M_1 \cdot M_1' b_1$ ва $M_1 \cdot M_1' b_1'$ сонлар M модул бўйича таққосланадими ёки таққосламайдими, шунга қараб x_0 ва x_0' ларнинг ифодасида қолган қўшилувчилар бир хил. Фараз қилайлик

$$M_1 \cdot M_1' b_1 \equiv M_1 \cdot M_1' b_1' (\mathrm{mod}\, M),$$

таққослама ўринли бўлсин, у ҳолда $M_1 M_1' b_1 = M_1 M_1' b_1' (\mathrm{mod}\, m_1)$ ҳам ўринли бўлади. Бундан $M_1 M_1' = 1(\mathrm{mod}\, m_1)$ бўлганлиги учун $b_1 \equiv b_1' (\mathrm{mod}\, m_1)$ таққослама ўринлидир, лекин бу мумкин эмас, чунки b_1 ни b_1' сонлар m_1 модул бўйича ҳар хил синфларда ётади. Шундай қилиб, барча сонлар M модул бўйича таққосланмайди. Демак, $N = N_1 \cdot N_2 \cdot \ldots \cdot N_k$.

М и с о л. Ушбу $f(x) = x^4 - 6x^3 + 5x^2 + 9 \equiv 0(\mathrm{mod}\, 21)$ (56)

таққослама ечилсин.

Е ч и ш. (56) –таққосламани $f(x) = 0(\mathrm{mod}\, 3), f(x) = 0(\mathrm{mod}\, 7)$ таққосламалар системаси билан алмаштирамиз. Осонлик билан кўриш мумкинки, 1-таққослама 3 та ечимга эга: x=0; 1; 2 (mod 3), 2- таққослама эса битта ечимга эга: x=-1 (mod 7).

Энди ушбу $x = b_1 (\mathrm{mod}\, 3), \quad x = b_2 (\mathrm{mod}\, 7)$ системани ечамиз. Бу ерда M=3·7=7·3 бўлганидан M_1=7, M_2=3, шунинг учун

$$7M_1^{|} \equiv 1(\mathrm{mod}\,3), \quad M_1^{|} \equiv 1(\mathrm{mod}\,3);$$

$$3M_2^{|} \equiv 1(\mathrm{mod}\,7), \quad M_2^{|} \equiv 5(\mathrm{mod}\,7);$$

$$x_0 = 7\cdot 1\cdot b_1 + 3\cdot 5\cdot b_2 = 7b_1 + 15b_2.$$

Шундай қилиб, (56)-таққослама қуйидаги ечимларга ега

$$x_1 = 7\cdot 0 + 15\cdot(-1) = -15(\mathrm{mod}\,21) \equiv 6(\mathrm{mod}\,21);$$

$$x_2 = 7\cdot 1 - 15 = -8(\mathrm{mod}\,21) \equiv 13(\mathrm{mod}\,21);$$

$$x_3 = 7\cdot 2 - 15 = -1(\mathrm{mod}\,21) \equiv 20(\mathrm{mod}\,21);$$

Энди фараз қилайлик $M = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ бўлиб, бунда $p_1, p_2, \ldots, p_k$ туб сонлар бўлсин. 64-теоремага асосан $f(x) \equiv 0(\mathrm{mod}\,M)$ таққосламани текшириш ва ечиш

$$f(x) \equiv 0(\mathrm{mod}\,p^{\alpha}) \qquad (57)$$

кўринишдаги таққосламани текшириш ва ечишга келтирилади.

(57)-таққосламани бевосита синаш усули билан ечиш р ва α унча катта бўлмаганда ҳам ноқулай, чунки p^{α} катта сон булиб кетиши мумкин. Хайриятки (57)-таққосламани

$$f(x) \equiv 0(\mathrm{mod}\,p) \qquad (58)$$

таққосламага келтириб ечиш мумкин.

Ҳақиқатан, (57)-таққосламани қаноатлантирувчи ҳар бир x_1 албатта (58)- таққосламани қаноатлантириши керак ($p^{\alpha}|f(x_1)$ бўлса, $p|f(x_1)$ бўлади), шунинг учун ҳам (57)-таққосламани қаноатлантирувчи сонларни (58)-таққосламани қаноатлантирадиган сонлар орасидан қидириш керак. Бу ишни биз босқичма-босқич бажарамиз. Аввал (58)-таққосламадан кейин модули p^2 бўлган, кейин p^3 ,..., бўлган таққосламаларни ечамиз.

Фараз қилайлик (56)-таққосламанинг бирор ечими

$$x \equiv x_1(\mathrm{mod}\,p) \qquad (59)$$

бўлсин. У ҳолда $x=x_1+pt_1$ бўлиб, бунда t_1 –ихтиёрий бутун сон; х нинг бу қийматини

$$f(x) \equiv 0(\mathrm{mod}\, p^2) \qquad (60)$$

таққосламага қўйиб, чап томонини Тейлор формуласи бўйича ёйсак:

$$f(x_1 + pt_1) = f(x_1) + pt_1 f'(x_1) + \frac{(pt_1)^2}{2!} f''(x_1) + \ldots + \frac{(pt_1)^k}{k!} f^{(k)}(x_1)$$

келиб чиқади, бунда $\frac{1}{k!} f^{(k)}(x_1)$ маълумки, бутун сон. Бу ёйилмада дастлабки иккита ҳаддан ташқари қолган барчаси p^2 га бўлинади. Шунинг учун ҳам p^2 модул бўйича (58)-таққослама

$$f(x_1) + pt_1 \cdot f'(x_1) \equiv 0(\mathrm{mod}\, p^2)$$

таққосламага тенг кучлидир. Бундан $p|f(x_1)$ бўлгани учун

$$\frac{f(x_1)}{p} + t_1 \cdot f'(x_1) \equiv 0(\mathrm{mod}\, p)$$

ёки

$$f(x_1)t \equiv -\frac{f'(x_1)}{p}(\mathrm{mod}\, p) \qquad (61)$$

таққосламага эга бўламиз. Биз $f'(x_1)$ нинг p га бўлинмайдиган ҳоли учун кенгроқ тўхталиб ўтамиз. (61)-таққосламанинг ечими

$$t_1 \equiv t'(\mathrm{mod}\ p), t_1 = t' + pt_2, t_2 = 0, \pm 1, \pm 2 \ldots$$

бўлади. Бу ҳолда (60)-таққосламанинг ечими

$$x = x_1 + p(t' + pt_2) = x_1 + pt' + p^2 t_2.$$

бўлади.

Бу формула $t_2=0$ бўлганда (60)-таққосламани битта ечимини беради, уни x_2 деб белгилаймиз.

У ҳолда

$$x = x_2 + p^2 t_2, t_2 = 0, \pm 1, \pm 2 \ldots$$

ёки

$$x \equiv x_2 (\mathrm{mod}\, p^2)$$

ечимни ҳосил қиламиз. Бу қийматни

$$f(x) \equiv 0 (\mathrm{mod}\, p^3)$$

таққосламага қўйсак,

$$f(x_2 + p^2 t_2) \equiv 0 (\mathrm{mod}\, p^3),$$

$$\frac{f(x_2)}{p^2} + f'(x_2) t_2 \equiv 0 (\mathrm{mod}\, p) \qquad (62)$$

келиб чиқади. Бунда

$$x_2 \equiv x_1 (\mathrm{mod}\, p\ )$$

эканлигидан

$$f'(x_2) \equiv f'(x_1) (\mathrm{mod}\, p\ )$$

бўлади. Лекин $f'(x_1)$ сон p га бўлинмайди, демак, $f'(x_2)$ ҳам p га бўлинмайди. Шунинг учун (62)-таққослама битта

$$t_2 = t_2' (\mathrm{mod}\ \ p),$$

$$t_2 = t_2' + p t_3,\ \ t_3 = 0, \mp 1, \pm 2, \ldots$$

ечимга эга; x нинг ифодаси эса

$$x = x_2 + p^2 t_2' + p^3 t_3 = x_3 + p^3 t_3$$

кўринишни олади. Шу тарзда, (58)-таққосламани ҳар бир берилган ечимига асосланиб, (57)-таққосламанинг ўша ечим билан таққосланувчи ечимини топамиз. Шундай қилиб, (58)-таққосламанинг ҳар бир $x \equiv x_1 (\mathrm{mod}\, p)$ ечими, $f'(x_1)$ сон p га бўлинмаган ҳолда (57)-таққосламанинг битта

$$x = x_\alpha + p^\alpha t_\alpha,$$

$$x = x_\alpha (\mathrm{mod}\ \ p^\alpha)$$

ечимини беради.

М и с о л. Ушбу

$$f(x) \equiv (\mathrm{mod}\,27), f(x) = 3x^4 + 7x + 5$$

таққослама ечилсин.

Е ч и ш. Равшанки, f(x)≡0(mod 3) битта x≡1(mod 3) ечимга эга.

Бу ерда $f'(x) = 12x^3 + 7$, демак, f'(1)=19 ≡ 0(mod 3), биз қаралаётган ҳолга тўғри келади. Юқоридаги усулни қўллаб, қуйидагиларни ҳосил қиламиз:

$$x = 1 + 3t_1;$$

$$f(1) + 3t_1 f'(1) \equiv 0(\mathrm{mod}\,9),\ 15 + 3t_1 \cdot 19 \equiv 0(\mathrm{mod}\,9),$$

$$19t_1 + 5 \equiv (\mathrm{mod}\,3),\ t_1 \equiv 1(\mathrm{mod}\,3),\ t_1 \equiv 1 + 3t_2,$$

$$x = 4 + 9t_2;$$

$$f(4) + 9t_2 \cdot f'(4) \equiv 0(\mathrm{mod}\,27),\ 801 + 9t_2 775 \equiv 0\,(\mathrm{mod}\,27),$$

$$89 + t_2 \cdot 775 \equiv 0\,(\mathrm{mod}\,3),\ 2 + t_2 = 0\,(\mathrm{mod}\,3),\ t_2 \equiv 1\,(\mathrm{mod}\,3),$$

$$x = 13 + 27t_3$$

ёки

$$x \equiv 13\,(\mathrm{mod}\,27)..$$

Агар (61) – таққосламада $f'(x_1)$ сон p га бўлиниб, ўнг томони p га бўлинмаса, у ҳолда бу таққослама ечимга эга эмас, шунингдек, (58)– таққослама ҳам ечимга эга эмас.

Ниҳоят, $f(x_1)$ сон p га бўлинсин ва шу билан бирга ўнг томони ҳам p га бўлинсин, у ҳолда (61) – таққослама айний бўлиб, барча бутун t_1 сонлар
уни қаноатлантиради. Шундай қилиб, (60) – таққосламани (59) – формула билан топиладиган барча сонлар қаноаталнтиради, бу сонлар (58) – таққосламани қаноатлантирадиган сонлар. Лекин бу сонлар p^2 модул бўйича битта синфда ётмасдан p та синфда ётади, шунинг

учун (60) – таққослама p та ечимга эга. Бу ечимлардан умумий усулга кўра p^3 модул бўйича таққосламани қаноатлантирадиганларини танлаб оламиз ва ҳ.к.

33-§. ЧИЗИҚЛИ ДИОФАНТ ТЕНГЛАМАЛАРИНИ ЕЧИШ

Биз энди чизиқли Диофант (ноаниқ) тенгламаларини ечиш усулини кўриб чиқамиз.

14-т а ъ р и ф. n номаълумли 1- даражали Диофант тенгламаси деб ушбу кўринишдаги

$$a_1x_1+a_2x_2+\ldots+a_nx_n=b \qquad (63)$$

тенгламага айтилади, бунда барча коэффициентлар, озод ҳад ва номаълумлар бутун сонлар ва ҳеч бўлмаганда бирорта $a_i\neq 0$.

15-т а ъ р и ф. (63)-*Диофант тенгламасининг ечими* деб, уни қаноатлантирадиган $(x_1^0,x_2^0,\ldots,x_n^0)$ бутун сонлар мажмуасига айтилади.

65-т е о р е м а. Агар a_1, a_2,... a_n жуфт-жуфт ўзаро туб бўлишса, у ҳолда

$$a_1x_1+a_2x_2+\ldots+a_nx_n=1 \qquad (64)$$

тенглама бутун сонларда ечимга эга.

И с б о т. Ушбу

$$a_1x_1+a_2x_2+\ldots+a_nx_n=b \qquad (63)$$

тенглама ечимга эга бўладиган мусбат бутун b сонларнинг тўпламини M орқали белгилаймиз. Равшанки, M тўплам бўш эмас, берилган a_1, a_2,..., a_n лар учун бутун $x_1,x_2,\ldots,x_n$ ларни танлаш мумкинки, $a_1x_1+a_2x_2+\ldots+a_nx_n$ мусбат бўлсин. M тўпламда энг кичик бутун мусбат сон мавжуд, биз уни d ($d\in M$) билан белгилаймиз. Энди $x_1^1,x_2^1\ldots,x_n^1$ орқали

$$a_1x_1^1+a_2x_2^1+\ldots+a_nx_n^1=d$$

тенгламани қаноатлантирадиган бутун сонларни белгилаймиз. Фараз қилайлик $a_1=dq+r$ бўлсин, бунда $0\leq r<d$, у ҳолда

$r = a_1 - (a_1x_1^1 + a_2x_2^1 + a_nx_n^1)q = a_1(1 - qx_1^1) + a_2(-qx_2^1) + ..a_n(-qx_n).$

Демак, биз шундай

$x_1 = 1 - qx_1^1,\ x_2 = -qx_2^1,\ldots,\ x_n = -qx_n^1$ бутун

қийматларни танладикки, улар учун

$$a_1x_1+a_2x_2+\ldots+a_nx_n=r,$$

лекин $0\le r<d$, d эса M тўпламининг энг кичик элементи. Бундан келиб чиқадики, r мусбат бўлиши мумкин эмас, r=0, $a_1=dq_1$, яъни $d|a_1$. Шунга ухшаш $d|a_2,\ldots, d|a_n$.

Бундан кўрамизки, d сон $a_1, a_2,\ldots, a_n$ сонларнинг умумий бўлувчиси, лекин $(a_1, a_2,\ldots, a_n)=1$ бўлганлиги учун d|1, d=1, $1\in M$, яъни (64) – тенглама бутун сонларда ечимга эга.

66- т е о р е м а. Фараз қилайлик d (63) – тенгламанинг коэффициентлари $a_1, a_2,\ldots, a_n$ ларнинг энг катта умумий бўлувчиси бўлсин. У ҳолда (63) – тенглама ечимга эга бўлиши учун d|b шарти зарур ва кифоядир. Бундай тенглама ечимларининг сони ёки нолга ёки чексизга тенг.

И с б о т. Кетма-кет теореманинг ҳар учала тасдиғини исбот қиламиз.

1)Фараз қилайлик d|b бўлсин. У ҳолда $\frac{a_1}{d}x_1 + \frac{a_2}{d}x_2 + \ldots\frac{a_n}{d}x_n = 1,$ бунда $(\frac{a_1}{d}, \frac{a_2}{d}, \ldots\frac{a_n}{d}) = 1$, теңглама учун (65-теоремага кўра) шундай $c_1, c_2,\ldots c_n$ бутун сонлар мавжудки, улар учун

$$\frac{a_1}{d}c_1 + \frac{a_2}{d}c_2 + \ldots\frac{a_n}{d}c_n = 1,$$

у ҳолда

$$a_1(c_1\frac{b}{d}) + a_2(c_2\frac{b}{d}) + \ldots a_n(c_n\frac{b}{d}) = b,$$

яъни $(c_1\frac{b}{d}, c_2\frac{b}{d}\ldots c_n\frac{b}{d})$ мажмуа (63)-тенгламанинг ечими.

2) Фараз қилайлик d†b бўлсин. Уҳолда (63)-тенгламанинг чап томони ихтиёрий бутун $x_1, x_2, \ldots x_n$ лар учун d га бўлинади, ўнг томони эса d га бўлинмайди, бундай бўлиши мумкин эмас.

3) Агар $(x_1^1, x_2^1 \ldots, x_n^1)$ бутун сонлар мажмуаси (63)-тенгламани қаноатлантирса, у ҳолда t=0, ±1, ±2,... учун, масалан,

$$(x_1^1 + a_2 t, x_2^1 - a_1 t, x_3^1, \ldots x_n^1)$$

мажмуалар ҳам (63) – тенгламани қаноатлантиради. Шундай қилиб, (63)-тенглама ё умуман ечимга эга эмас ёки чексиз кўп ечимга эга.

1-м и с о л. $15x_1-12x_2+21x_3=50$ Диофант тенгламаси ечимга эга эмас, чунки d=3 ва 3†50.

2-м и с о л. $3x_1-5x_2+7x_3-25x_4=120$ Диофант тенгламаси чексиз кўп ечимга эга, чунки бу ерда d=1.

67-т е о р е м а. Агар x_0 сон $ax \equiv c \pmod b$ таққосламани қаноатлантирса, у ҳолда $(x_0, \frac{c-ax_0}{b})$ мажмуа

$$ax+by=c \qquad (65)$$

Диофант тенгламасининг ечими бўлади.

И с б о т. $ax_0 \equiv c \pmod b$ дан $\frac{c-ax_0}{b}$ нинг бутун сонлиги келиб чиқади, бевосита текшириш кўрсатдики

$$ax_0 + b(\frac{c-ax_0}{b}) = c.$$

68-т е о р е м а. Фараз қилайлик a ва b нолдан фарқли бўлиб, $d=(a,b)$, d|c ва (x_0, y_0) мажмуа

$$ax+by=c \qquad (66)$$

Диофант тенгламасининг бирор ечими бўлсин. У ҳолда (65)-тенгламанинг барча ечимлари (x^1, y^1) мажмуалар тўплами билан устма-уст тушади, бунда

$$x^1 = x_0 - \frac{b}{d}t,\ y^1 = y_0 + \frac{b}{d}t$$

t эса ихтиёрий бутун сон.

И с б о т. Фараз қилайлик (x^1, y^1) (65)-тенгламанинг бирор ихтиёрий ечими бўлсин, яъни

$$ax^1 + by^1 = c$$

шартга кўра x_0, y_0 сонлар (66)-тенгламани қаноатлантиради, яъни

$$ax_0 + by_0 = c$$

Охирги иккита тенгликдан

$$\frac{a}{d}(x_0 - x^1) = \frac{b}{d}(y^1 - y_0)$$

келиб чиқади, бунда $\frac{a}{d}$ ва $\frac{b}{d}$ бутун сонлар. У ҳолда $\frac{a}{d} \mid \frac{b}{d}(y^1 - y_0)$, шу билан бирга $(\frac{a}{d}, \frac{b}{d}) = 1$. Шунинг учун (12-теоремага кўра) $\frac{a}{d} \mid (y^1 - y_0)$. Демак,

$$y^1 - y_0 = \frac{a}{d}t, y^1 = y_0 + \frac{a}{d}t.$$

бунда t- ихтиёрий бутун сон. y^1нинг топилган қийматини (65)-га қўйиб,

$$ax^1 = c - b(y_0 + \frac{a}{d})t = ax_0 - \frac{ab}{d}t,$$

ни бундан эса $x^1 = x_0 - \frac{b}{d}t$ ни ҳосил қиламиз. Шундай қилиб, (65)-тенгламанинг ихтиёрий ечими

$$x^1 = x_0 - \frac{b}{d}t,\ y^1 = y_0 + \frac{a}{d}t \qquad (67)$$

дан иборат, бунда t- ихтиёрий бутун сон.

Тескари тасдиқ ҳам ўринли. Ўрнига қўйиш йўли билан кўрсатиш мумкинки (67) ифода (66)- тенгламани қаноатлантиради.

М и с о л. 36x-22y=12 тенглама ечилсин.

Е ч и ш. Бу ерда (36, 22)=2, 2|12. Ушбу $36x \equiv 12 \pmod{22}$ таққослама учун қуйидагига эга бўламиз:

$$18x=6 \pmod{11},\ 3x=1 \pmod{11},\ x_0=4.$$

Демак $36 \cdot 4 - 22y_0 = 12,\ y_0 = 6.$ шундай қилиб, ихтиёрий ечим қуйидаги кўринишга эга:

$$x=4+11t,\ y=6+18t$$

Энди (63) – кўринишдаги тенгламани ечишнинг бошқа усулини мисолларда кўрамиз.

М и с о л. 28x-5y=11 Диофант тенгламаси ечилсин.

Е ч и ш. Тенглама коэффициентларини уларнинг энг кичиги 5 га бўламиз ва тўлиқмас бўлинмаларни (агар қолдиқсиз бўлинса, тўлиқ бўлинмани) оламиз ва қуйидаги белгилашни киритамиз

$$5x-y=u. \qquad (68)$$

Буни 5 га кўпайтириб, берилган тенгламадан айирамиз:

$$3x=11-5u$$

Бундан $x = \dfrac{11-5u}{3}$. Бу ифода бутун сон бўлиши учун u=1+3t бўлиши керак. Демак, x=2-5t. Буни тенгламага қўйиб, y=9-28t ни ҳосил қиламиз. Шундай қилиб, умумий ечим ушбу кўринишга эга

$$x=2-5t,\ y=9-28t.$$

М и с о л. Қуйидаги

$$27x+22y-6z=5 \qquad (69)$$

Диофант тенгламасининг умумий ечими топилсин.

Е ч и ш. Тенгламани чап томонидаги коэффициентларни уларнинг энг кичиги, яъни 6 га бўламиз, тўлиқмас бўлинмаларни оламиз ва қуйидаги белгилашни киритамиз

$$4x+3y-z=u. \qquad (70)$$

Бу тенгликни ҳар иккала томонини 6 га кўпайтириб, (69)-тенгламадан айирамиз

$$3x+4y=5-6u \text{ ёки } 3x+4y+6y=5.$$

Охирги x,y,u номаълумли тенглама берилган тенгламага ўхшайди, лекин бунда энг катта коэффицент 6 га тенг, бу эса берилган тенгламада энг кичик коэффицент эди. Охирги тенгламани чап томонини 3 га бўлиб, тўлиқмас бўлинмаларни (агар бўлинса бўлинмани) оламиз ва қуйидаги белгилашни киритамиз

$$x+y+2u=v$$

буни 3 га кўпайтириб, олдингисидан айирсак

$$y=5-3v$$

ҳосил бўлади, кейин олдинги тенгламадан x ни топамиз

$$x=-5-2u+4v.$$

Энди x ва y нинг ифодасини (70)-га қўйиб, z ни ҳосил қиламиз $z=-5-9u+7v$.

Шундай қилиб, (69)-тенгламанинг умумий ечими

$$x=-5-2u+4v,\ y=5-3v,\ z=-5-9u+7v$$

бунда u ва v – ихтиёрий бутун сонлар.

6-БОБ УЧУН МАШҚЛАР.

1. Ушбу таққосламалар ечилсин:

1) $221x \equiv 111 (\mathrm{mod}\, 360)$, 2) $29x+16 \equiv 0 (\mathrm{mod}\, 136)$.

2. Ушбу таққосламалар системаларини ечинг:

1) $3x \equiv 5 (\mathrm{mod}\, 13), 4x \equiv 6 (\mathrm{mod}\, 11)$;

2) $x \equiv 5 (\mathrm{mod}\, 12), x \equiv 7 (\mathrm{mod}\, 15)$;

3) $x \equiv a (\mathrm{mod}\, 3), x \equiv b (\mathrm{mod}\, 5), x \equiv c (\mathrm{mod}\, 7)$.

3. 13 га бўлганда 5, 17 га бўлганда эса 7 қолдиқ ҳосил бўладиган барча бутун сонларни топинг.

4. Шундай сонни топиш керакки уни 3,5 ва 7 га бўлганда мос равишда 2,3 ва 2 қолдиқларни берсин (Дзин-Киу-Цао (1220-1290) масаласи).

5. Шундай сонларни топиш керакки уларни 2,5,7,9 га бўлганда мос равишда 1,2,3,4 қолдиқларни беришсин.

6. 18 модул бўйича шундай биринчи даражали таққосламаларни топиш керакки, улар қуйидаги шартларнинг бирини қаноатлантирсин:

1) битта ечимга эга; 2) 2,3 ва 6 та ечимларга эга; 3)18 модул бўйича 18 та ечимга эга бўлиши мумкинми? 15 та ечимга эга бўлиши мумкинми?

7. Қуйидаги таққосламалар нечита ечимга эга:

1) $12x^7+5x^5-3x^4\equiv 0(\mathrm{mod}\,7)$ 2) $16x^6-4x^4+3x^2+3x-1\equiv 0(\mathrm{mod}\,4)$.

8. Қуйидаги таққосламаларнинг ечимлари топилсин:

1) $x^2\equiv 3(\mathrm{mod}\,37)$ (ж: ± 15);

2) $x^2\equiv 569(\mathrm{mod}\,769)$ (ж: ± 177);

3) $x^3-x^2-2x\equiv 0(\mathrm{mod}\,5)$ (ж: 0;2);

4) $x^3-3x+1\equiv 0(\mathrm{mod}\,2)$;

5) $x^5\equiv 121(\mathrm{mod}\,75)$, (ж: 5;47;400;485;592);

6) $x^7+x^6+2x^5-3x^4-4x^3+2x^2+3x+2\equiv 0(\mathrm{mod}\,11)$ (ж: -1,-3,3);

7) $2^x\equiv x^2(\mathrm{mod}\,7),(x>0)$ (ж: $x\equiv 2;4;6;10;15(\mathrm{mod}\,21)$);

8) $x^3\equiv 31(\mathrm{mod}\,37)$, (ж: 6,8,23);

9) $x^7\equiv 100(\mathrm{mod}\,607)$, (ж: 335)

10) $x^{12}\equiv 7(\mathrm{mod}\,19)$.

9. Фараз қилайлик $(a_0,m)=1$ бўлсин. Бош коэффиценти 1 га тенг бўлган шундай n- даражали таққосламани топиш керакки у

$$a_0x^n+a_1x^{n-1}+\ldots+a_n\equiv 0(\mathrm{mod}\,m)$$

таққосламага тенг кучли бўлсин.

10.Ушбу $f(x)\equiv 0(\mathrm{mod}\,p); f(x)=x^n+a_1x^{n-1}+\ldots+a_n, n\le p$ таққослама n та ечимга эга бўлиши учун x^p-x ни f(x) га

бўлганда ҳосил бўлган қолдиқнинг барча коэффицентлари p га бўлиниши зарур ва кифоялигини исбот қилинг.

11.Ушбу

$$x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+$$
$$x^6+x^5+x^4+x^3+x^2+4x\equiv 0(\mathrm{mod}\,5)$$

таққослама даражаси 5дан кичик бўлган қандай таққосламага тенг кучли?

12.Ушбу $14x^5-25x^4+35x^3+15x^2-19x+5$ кўпҳадни 7 модул бўйича энг содда кўринишга келтиринг.

13.Ушбу чизиқли Диофант тенгламаларининг ечимлари топилсин:

1)17x+35y=1, 4) 284x-186y=114,
2)112x-67y=36, 5) 35x+113y=211,
3)89x+115y=145, 6) 126x+131y=2.

14. Ушбу 24335x-3588y=1 тенгламанинг энг кичик мусбат сонлардан иборат бўлган ечимини топинг. (ж. x=2807, y=19038)

15. Ушбу Диофант тенгламаларини ечинг:

1) 23x-5y+80z=101,
2) 430x-13y+8z=189,
3) 14x+21y+19z=412.

16. Ушбу уч номаълумли Диофант тенгламаси 15x+6y+20z=a ечилсин
(ж. x=a -6t_1-14t_2, y=a -5t_1-15t_2, z=-a -6t_1+15t_2).

17. Қуйидаги Диофант тенгламалари системасини ечинг:

1) $\left.\begin{matrix}3x-2y+4z+2t=19,\\ 5x+6y-2z+3t=19;\end{matrix}\right\}$ (Ж := 11+16z-18y, t = 26-26z+28y),

2) $\left.\begin{matrix}x+4y+5z=272,\\ 3x+9y+8z=656;\end{matrix}\right\}$, 3) $\left.\begin{matrix}4x+3y+2z+8v=36,\\ 3x-4y+7z+5v=12.\end{matrix}\right\}$.

18. Қуйидаги кўпҳадларни (синаш усули билан 7 модул бўйича ечимини топинг) 7 модул бўйича кўпайтувчиларга ажратинг:

1)$3x^4+x^2+5x-2$, 2) x^3+5x^2-2x-3, 3) x^4-x^2+x+1.

19. Ушбу таққосламаларни синаш методи билан ечинг:
а) 3x ≡ 1 (mod 7), б) 5x ≡-2 (mod 11),
в) 4x ≡ 7 (mod 17), г) 7x ≡ 5 (mod 8),
д) 15x ≡ 25 (mod 35), е) 15x ≡ 11 (mod 36),
ж) 11x ≡ 15 (mod 36), з) 13x ≡ 1 (mod 15),
и) 21x ≡ 4 (mod 35), к) 4x ≡ 21 (mod 35).

20. Қуйидаги таққосламаларни коэффицентларни алмаштириш усули билан ечинг:
а) 5x ≡ 7 (mod 8), б) 5x ≡ 3 (mod 11),
в) 7x ≡ 6 (mod 15), г) 7x ≡ 5 (mod 24),
д) 17x ≡ 25 (mod 28), е) 19x ≡ 12 (mod 35),
ж) 16x ≡ 19 (mod 31).

21. Ушбу таққосламаларни Эйлер теоремаси ёрдамида ечинг:
а) 3x ≡ 7 (mod 11), б) 17x ≡ 25 (mod 28), в) 27x – 7 (mod 58).

22. Ушбу таққосламаларни узлуксиз касрлардан фойдаланиб ечинг:
а) 67x ≡ 64 (mod 183), б) 89x ≡ 86 (mod 241),
в) 213x ≡ 137 (mod 316), г) 111x ≡ 81 (mod 447),
д) 186x ≡ 374 (mod 422), е) 129x ≡ 321 (mod 471).

23. Ушбу системаларни ечинг:
а) $x \equiv 19 \pmod{24}$, $x \equiv 10 \pmod{10}$
б) $x \equiv 23 \pmod{35}$, $x \equiv 13 \pmod{20}$
в) $x \equiv 12 \pmod{24}$, $x \equiv 3 \pmod{33}$
г) $x \equiv 6 \pmod{15}$, $x \equiv 18 \pmod{21}$, $x \equiv 3 \pmod{12}$
д) $x \equiv 13 \pmod{15}$, $x \equiv 6 \pmod{35}$, $x \equiv 26 \pmod{45}$
е) $x \equiv 19 \pmod{22}$, $x \equiv 8 \pmod{33}$, $x \equiv 14 \pmod{21}$
ж) $x \equiv 1 \pmod{3}$, $x \equiv 4 \pmod{5}$, $x \equiv 2 \pmod{7}$,
$x \equiv 9 \pmod{11}$, $x \equiv 3 \pmod{13}$.

24. Қуйидаги ситемалар ечимларининг умумий кўринишини топинг:
а) $x \equiv в_1 \pmod{8}$, $x \equiv в_2 \pmod{9}$, $x \equiv в_3 \pmod{13}$
б) $x \equiv в_1 \pmod{25}$, $x \equiv в_2 \pmod{27}$, $x \equiv в_3 \pmod{59}$.

6-бобга доир тарихий маълумот

1. Астрономия муаммоларидан келиб чиққан (айрим осмон ҳодисаларини даврий равишда такрорланишини аниқлаш) 1 – даражали 2 ва 3 номаълумли тенгламаларни ечишни ҳинд астрономлари ва математиклари Ариабхата (476 йилда туғилган), Брахмагупта (588-660) ва Бхаскара (1114-1178) қарашган.

2. 1-даражали тенгламалар системасига келадиган масалалар эрамизни бошида яшаган хитой математиги Сун Тзуннинг арифметикага оид китобида ҳам қаралган. Сун Тзунникида ва ундан кейин ўтган бир қатор хитой, Ўрта ва Яқин Шарқ ҳамда Европа олимларининг асарларида масала қуйидагича қўйилган: шундай сонни топингки уни маълум сонларга бўлганда маълум қолдиқларни берсин. Бундай системани ечиш учун Сун Тзун берган усул, аслида 60-теоремада келтирган усул билан тенг кучлидир. Шунинг учун 60-теоремани «*қолдиқлар ҳиқидаги хитой теоремаси*» ҳам дейишади. Сун Тзуннинг иши Европада 1852 йилда маълум бўлган. Хитой математикларининг ишидан бехабар ҳолда бундай масалаларни ечиш усулини ҳинд математиги Брахмагупта ҳам берган.

3. Италиялик математик Леонардо Пизанский (Leonardo Pisano, 1170-1228) тахаллуси Фибоначчи (Fibonacci) Шарқ мамлакатлари бўйлаб сафар қилиб, у ерлардаги олимлар билан танишади ва бу ердаги билимлар билан Европаликларни таништиради. Унинг асосий асарлари «Liber Abaci» (1202) (чизиқли ва квадрат тенгламаларни ечиш тўғрисида) ва «Practica Geometriae» (1220) (алгебрани геометрияга тадбиқи бўйича). Бу асарларда Шарқ мамлакатларида арифметика, алгебра ва геометрияда эришган муваффақиятлар келтирган. «Liber Abaci» да қуйидаги масала ҳам қаралган: 7 га бўлинадиган шундай N сонни топингки уни 2,3,4,5 ва 6 га бўлганда 1 қолдиқ берсин.

4. Француз математиги Баше де Мезириак (Bachet de Meziriac, 1587-1638) 1624 йилда чоп этилган «Problems plaisans et delectables que se font par la nombres» («Сонларга асосланган қизиқарли ва ёқимли масалалар») номли оммабоб китобида $ax+by=c$ тенгламани ечишни келтирган. Бу китоб кўпчиликни сонлар назариясига қизиқтириб, сонлар назариясининг ривожланишига катта ҳисса қўшади.

Баше де Мезириак шоир сифатида ҳам машҳур, бир неча тилларда шеърлар ёзган. 1621 йилда Диофант асарини ўзининг коментарийлари билан чопдан чиқарган.

5. Баше де Мезириакдан кейин 17- ва 18-асрларда $ax+by=c$ тенгламани ечишнинг ҳар хил қоидаларини Л.Эйлер, француз математиги М.Ролл (Rolle Michel, 1652-1719) ва бошқа математиклар беришган.

6. 62-теоремага тенг кучли бўлган теоремани 1768 йилда Лагранж исбот қилган. 62-теорема сал бошқача формада Гауснинг «Арифметик тадқиқотлари» да бор. Гаусс бу теореманинг исботини индукция методи билан олиб боради. Бу асарда кўп номаълумли чизиқли таққосламалар ҳам қаралган.

7. Инглиз математиги Варинг (Waring Эдуард, 1734-1798) 1770 йилда чоп қилдирган "Meditationes Algebraicae" («Алгебраик мулоҳазалар») асарида 63-теоремани исботсиз келтириб, бу теоремани Дж.Вилсон (Wilson J. 1741-1793) га тегишли деб ёзади. Вилсон теоремасининг биринчи исботини Лагранж берган. Гаусс бу теоремани таркибли модуллар учун ҳам умумлаштирган.

8. Биз 33-§ да чизиқли Диофант тенгламаларга доир мисоллар ечганимизда тенглама коэффицентларини уларнинг энг кичигига бўлиб, бўлинмаларини олиш жараёнини қўллаган эдик. Бу методни умумий ҳолда Лагранж ишлаб чиққан.

9. Немис математиклари Фробениус (Frobenius, Фардинанд Георг, 1849-1917) ва Стейниц (Steinez, Вилгейм, 1836-1900) чизиқли таққосламаларни тўла текширишган.

Стейниц-математик, шахмат назариётчиси, шахмат бўйича биринчи жаҳон чемпиони (1886-1894). У Прагада туғилиб, Венада ўқиб, Англия ва Америкада яшаган.

7-БОБ. ИККИНЧИ ДАРАЖАЛИ ТАҚҚОСЛАМАЛАР

34-§. ИККИНЧИ ДАРАЖАЛИ ТАҚҚОСЛАМАНИ ИККИ ҲАДЛИГА КЕЛТИРИШ

Умумий кўринишдаги

$$ax^2 + bx + c \equiv 0 (\mathrm{mod}\, m) \qquad (71)$$

таққосламани икки ҳадлига келтирамиз. (71)-таққосламани иккала томонини ва модулини $4a$ га кўпайтирамиз

$$4a^2x^2 + 4abx + 4ac \equiv 0 (\mathrm{mod}\, 4am). \qquad (72)$$

Бу ерда (72)-таққослама (71)-таққослама билан тенг кучли бўлиши учун модулини ҳам $4a$ га кўпайтирдик. Ҳақиқатан, агар бу ишни қилмасак, у ҳолда $(4a, m) = d > 1$ бўлганда (72)-таққосламадан (71)-таққосламага ўтаолмас эдик, чунки (48-теорема) таққосламанинг иккала томонини фақат модул билан ўзаро туб кўпайтувчига қисқартириш мумкин. Равшанки, $4a$ ва m ўзаро туб бўлганда модулни $4a$ га кўпайтирмасдан (71)-га тенг кучли таққослама ҳосил қилиш мумкин. (72)-таққосламани ушбу кўринишга

$$(2ax + b)^2 \equiv b^2 - 4ac (\mathrm{mod}\, 4am)$$

ёки

$$D^2 = b^2 - 4ac, y = ax + b \text{ деб олсак}$$

$$y^2 \equiv D (\mathrm{mod}\, 4am) \qquad (73)$$

кўринишга келтириш мумкин. Аксинча, агар (73)-таққосламанинг y ечимини топсак, у ҳолда (71)-таққосламанинг ечими учун $x = \dfrac{y - b}{2a}$ га эга бўламиз; агар $y - b$ сон $2a$ га бўлинса, у ҳолда (71)-таққосламанинг x ечимини топамиз (бу шарт ҳар доим ҳам бажарилмайди).

Шундай қилиб, (73)-таққосламанинг y ечимлари орасида шундайлари бўлиши мумкинки, уларга (71)-таққосламанинг x ечими мос келади. Лекин шундай y ҳам учрайдики, уларга x ечим мос келмайди; шундай ҳол ҳам бўлиши мумкинки, $4am$ модул бўйича ҳар хил синфларда ётувчи y ларга m модул бўйича битта синфда ётувчи x мос келиши мумкин. Шундай бўлсада, (73)-таққосламанинг барча ечимларини текшириб, биз албатта (71)-таққосламанинг барча x ечимларини топамиз, чунки (71)-таққосламанинг ҳар бир x ечимига (73)-таққосламанинг y ечими учраши шарт. Агар (71)- таққосламанинг умуман ечими бўлмаса, у ҳолда (73)-таққосламанинг ҳам ечими бўлмайди.

Шундай қилиб, қуйидаги теорема исботланди.

69-т е о р е м а. Умумий кўринишдаги иккинчи даражали (71)-таққосламани ҳар доим (73)-кўринишдаги икки ҳадли таққосламага келтириш мумкин.

М и с о л. Ушбу $3x^2 - 16x + 12 \equiv 0 (\mathrm{mod}\, 36)$ таққослама ечилсин.

Е ч и ш. Таққосламанинг ҳар иккала томони ва модулини 3 га кўпайтирамиз, натижада

$$9x^2 - 48x + 36 \equiv 0 (\mathrm{mod}\, 108)$$

ёки

$$(3x - 8)^2 \equiv 28 (\mathrm{mod}\, 108)$$

ҳосил бўлади. Агар $y = 3x - 8$ деб олсак, у ҳолда

$$y^2 \equiv 28 (\mathrm{mod}\, 108)$$

келиб чиқади. Бу таққослама қуйидаги таққосламалар системасига тенг кучлидир:

$$y^2 \equiv 28 (\mathrm{mod}\, 4), \qquad y^2 \equiv 28 (\mathrm{mod}\, 27),$$

ёки

$$y^2 \equiv 0 (\mathrm{mod}\, 4), \qquad y^2 \equiv 1 (\mathrm{mod}\, 27).$$

Равшанки, биринчи таққосламанинг ечимлари $y \equiv 0(\mathrm{mod}\,4),\ y \equiv 2(\mathrm{mod}\,4)$; иккинчиси эса $y \equiv 1(\mathrm{mod}\,27),\ y \equiv -1(\mathrm{mod}\,27)$.

Бу ечимларнинг комбинацияларини олиб, қуйидаги таққосламалар системасини ҳосил қиламиз:

$$\left.\begin{matrix} y \equiv 0(\mathrm{mod}\,4), \\ y \equiv 1(\mathrm{mod}\,27) \end{matrix}\right\},\quad \left.\begin{matrix} y \equiv 0(\mathrm{mod}\,4), \\ y \equiv -1(\mathrm{mod}\,27) \end{matrix}\right\},\quad \left.\begin{matrix} y \equiv 2(\mathrm{mod}\,4), \\ y \equiv 1(\mathrm{mod}\,27) \end{matrix}\right\},\quad \left.\begin{matrix} y \equiv 2(\mathrm{mod}\,4), \\ y \equiv -1(\mathrm{mod}\,27) \end{matrix}\right\}$$

Бу системаларнинг умумий кўриниши

$$y \equiv b_1(\mathrm{mod}\,4),\ y \equiv b_2(\mathrm{mod}\,27)$$

дан иборат. Бу системага 60-теоремани қўллаб, умумий ечим учун

$$y \equiv 27 \cdot 3b_1 + 4 \cdot 7b_2 \equiv 81b_1 + 28b_2(\mathrm{mod}\,28)$$

ни ҳосил қиламиз. Бунга $b_1 = 0;2$ ва $b_2 = 1;-1$ ларни қўйиб, қуйидаги 4 та ечимга эга бўламиз: $y \equiv \pm 26;\pm 28(\mathrm{mod}\,108)$. Бу қийматларни ҳар бирини $3x - 8 = y$ формулага қўйиб, x ни ҳисоблаймиз. Лекин $y = 26$ ва $y = -28$ қийматлар x учун каср қийматларни беради, шунинг учун улар бизга тўғри келмайди. Қолган иккита $y = -26$ ва $y = 28$ ечимлар x учун 36 модул бўйича бир-биридан фарқли $x = -6$ ва $x = 12$ иккита ечимни беради. Демак, берилган таққослама иккита ечимга эга.

35-§. ИККИ ҲАДЛИ ТАҚҚОСЛАМАЛАР, ЧЕГИРМА ВА НОЧЕГИРМАЛАР ҲАҚИДА УМУМИЙ ТЕОРЕМАЛАР

Бундан кейин $n(n > 1)$-даражали таққосламалардан энг соддаларини, яъни

$$x^n \equiv a(\mathrm{mod}m),\ (a,m) = 1. \qquad (74)$$

кўринишдаги икки ҳадли таққосламаларнигина кўриб чиқамиз.

18-т а ъ р и ф. Агар (74)-таққослама ечимга эга бўлса, a сон m модул бўйича $n-$*даражали чегирма* акс ҳолда m модул бўйича $n-$*даражали ночегирма* деб айтилади. Хусусий ҳолда, $n=2$ бўлганда чегирма ва ночегирма – *квадратик*, $n=3$ бўлганда – *кубик*, $n=4$ бўлганда – *биквадратик чегирма* ёки *ночегирма* деб аталади.

Биз $n=2$ бўлган ҳолни кенгроқ текширамиз. Биринчи навбатда p тоқ $(p>2)$ туб модул бўйича олинган

$$x^2 \equiv a(\mathrm{mod}\, p),(a,p)=1 \qquad (75)$$

икки ҳадли таққосламани кўриб чиқамиз.

70-т е о р е м а. Агар a сон p модул бўйича квадратик чегирма бўлса, у ҳолда (75)-таққослама иккита ечимга эга бўлади.

И с б о т. Ҳақиқатан, a квадратик чегирма бўлса, у ҳолда (75)-таққослама энг камида битта $x\equiv x_1(\mathrm{mod}\, p)$ ечимга эга. Лекин $(-x_1)^2=x_1^2$ бўлганлиги туфайли, бу таққослама иккинчи $x\equiv -x_1(\mathrm{mod}\, p)$ ечимга ҳам эга. Иккинчи ечим биринчисидан фарқли, чунки акс ҳолда $x_1\equiv -x_1(\mathrm{mod}\, p)$ таққосламадан $2x_1\equiv 0(\mathrm{mod}\, p)$ га келамиз. Бундай бўлиши мумкин эмас, чунки $(2,p)=(x_1,p)=1$. (75)-таққослама 2-даражали туб модулли бўлганлиги учун (62-теорема) унинг ечими иккитадан ошмайди.

Туб модулли (75)-таққосламани кичик модуллар учун синаш усули билан ечиш мақсадга мувофиқдир. Бунинг учун p модул бўйича чегирмаларнинг келитирилган

$$\pm 1,\pm 2,\ldots,\pm\frac{p-1}{2} \qquad (76)$$

системасидаги ҳар бир чегирмани кетма-кет (75)-га қўйиб ўтирмасдан фақат $1,2,\ldots,\frac{p-1}{2}$ ларни текшириб кўриш кифоя. Бу ҳолда чап томонда

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \qquad (77)$$

сонлар ҳосил бўлади.

71-т е о р е м а. (77)-қатордаги сонларнинг ҳар бири p модул бўйича турли синфларда ётади.

И с б о т. Тескарисини фараз қилайлик, яъни $1 \le k < l \le \frac{p-1}{2}$ бўлганда $k^2 \equiv l^2 \pmod p$ бўлсин. У ҳолда

$k^2 - l^2 \equiv 0 \pmod p, (k+l)(k-l) \equiv 0 \pmod p,$

$0 < k+l < p, o < l-k < p$ бўлганлиги учун охирги таққослама бажарилмайди. Фаразимиз нотўғри экан.

Н а т и ж а. Ҳар қандай p туб модул бўйича тузилган чегирмалар системасидаги сонларнинг $\frac{p-1}{2}$ таси квадратик чегирма ва $\frac{p-1}{2}$ таси квадратик ночегирма бўлади.

Ҳақиқатан, (77)-қаторда квадратик чегирмалар ёзилган, уларнинг сони $\frac{p-1}{2}$ та, айнан шунчаси квадратик ночегирмадир.

М и с о л. 19 модул бўйича энг кичик квадратик чегирмалар топилсин.

Е ч и ш. Уларнинг сони $\frac{19-1}{2} = 9$. Уларни 19 модул бўйича қуйидагича ҳисоблаб топамиз:

$$1^2 \equiv 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 16,\ 5^2 = 25 \equiv 6,\ 6^2 = 36 \equiv 17,\ 7^2 = 49 \equiv 11,\ 8^2 = 64 \equiv 7,$$
$$9^2 = 81 \equiv 5 \pmod{19}.$$

Шундай қилиб, 19 модул бўйича энг кичик квадратик чегирмалар қуйидагидан иборат:

1, 4, 5, 6, 7, 9, 11, 16, 17.

Бундан кўрамизки 19 модул бўйича квадратик ночегирмалар қуйидагилардир:

2, 3, 8, 10, 12, 13, 14, 15, 18.

72-т е о р е м а (Эйлер мезони). Агар a сон р модул бўйича квадратик чегирма бўлса, у ҳолда

$$a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p) \qquad (78)$$

таққослама ўринли бўлади, a сон р модул бўйича ночегирма бўлганда эса

$$a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p) \qquad (79)$$

таққослама ўринли бўлади.

И с б о т. Ферма теоремасига кўра

$$a^{p-1} \equiv 1(\mathrm{mod}\, p), \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0(\mathrm{mod}\, p).$$

иккинчи таққосламанинг чап томонидаги кўпайтувчилардан биттасигина р га бўлинади. Бу иккита кўпайтувчилар бир вақтда р га бўлинмайди, акс ҳолда уларнинг айирмаси 2 ҳам р га бўлинган бўлар эди, лекин р тоқ туб сон бўлганлиги учун (2, р)=1.

Шу сабабли (78)- ва (79)-таққосламаларнинг биттасигина бажарилади. Ҳақиқатан, бундай ҳолда ҳар бир a квадратик чегирма учун х нинг (х, р)=1 шартни қаноатлантирадиган шундай қиймати мавжудки, бу қиймат учун

$$a \equiv x^2(\mathrm{mod}\, p) \qquad (80)$$

таққослама бажарилади. Бундан эса $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}}(\mathrm{mod}\, p)$ ёки $a^{\frac{p-1}{2}} \equiv x^{p-1}(\mathrm{mod}\, p) \equiv 1(\mathrm{mod}\, p)$ келиб чиқади, демак, a сон (78)-таққосламани қаноатлантиради. Шу билан бирга, (78)-таққосламанинг барча ечимлари квадратик чегирмалардан

иборат, чунки таққослама $\frac{p-1}{2}$ даражали бўлганлиги учун, $\frac{p-1}{2}$ дан ортиқ ечимга эга бўлмайди.

Шунинг учун квадратик ночегирмалар (79)-таққосламани қаноатлантиради.

36-§. ЛЕЖАНДР СИМВОЛИ ВА УНИНГ ХОССАЛАРИ

Берилган a сон квадратик чегирма бўлишими ёки бўлмаслигини р нинг катта қийматлари учун Эйлер мезони билан текшириш катта қийинчилик туғдиради. Бундай ҳолда Лежандр $\left(\frac{a}{p}\right)$ символидан фойдаланиш анча қулайдир.

19-т а ъ р и ф. Қуйидаги

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{агар } a \text{ сон р туб модул бўйича квадратик чегирма бўлса;}\\ -1, & \text{агар } a \text{ сон р туб модул бўйича квадратик ночегирма бўлса}\end{cases}$$

шартларни қаноатлантирувчи $\left(\frac{a}{p}\right)$ символ *Лежандр символи* дейилади; a Лежандр символининг *сурати*, р эса *махражи* дейилади.

М и с о л. $\left(\frac{5}{17}\right)=-1$ чунки Эйлер мезонига кўра

$5^{\frac{17-1}{2}}=5^8\equiv -1(\mathrm{mod}17);\left(\frac{7}{19}\right)=1,$

чунки $7^{\frac{19-1}{2}}=7^9\equiv 1(\mathrm{mod}19).$

Эйлер мезони ва Лежандр символидан қуйидаги тенглик келиб чиқади:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p). \qquad (81)$$

Биз энди Лежандр символининг асосий хоссаларини кўриб чиқамиз, бу хоссалар символнинг ўзини тез ҳисоблашга ва

$$x^2 \equiv a(\mathrm{mod}\, p)$$

таққосламанинг ечими мавжуд ёки мавжуд эмаслигини аниқлашга ёрдам беради.

1-х о с с а. Агар $a \equiv a_1(\mathrm{mod}\, p)$ бўлса, у ҳолда $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$ тенглик ўринли.

И с б о т. Ҳақиқатан, бир синфнинг элементлари берилган модул бўйича ё квадратик чегирма ёки квадратик ночегирма бўлади. Бундан хоссанинг тўғрилиги келиб чиқади.

2-х о с с а. $\left(\frac{1}{p}\right) = 1$

И с б о т. Ҳақиқатан, $x^2 \equiv 1(\mathrm{mod}\, p)$ таққослама доимо $x = \pm 1(\mathrm{mod}\, p)$ ечимга эга.

3-х о с с а. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

И с б о т. Ҳақиқатан, a=-1 бўлганда (81)-таққосламадан

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} (\mathrm{mod}\, p)$$

келиб чиқади. Бу таққосламанинг чап ва ўнг томонида абсолют қиймати бирга тенг бўлган миқдорлар турибди. Агар улар тенг бўлса бундай миқдорлар p>2 модул бўйича таққосланувчи бўлади.

Н а т и ж а. p=4m+1шаклдаги туб сонлар учун –1 квадратик чегирма, p=4m+3 кўринишдаги туб сонлар учун квадратик ночегирма бўлади.

Ҳақиқатан

$$\left(\frac{-1}{4m+1}\right)=(-1)^{2m}=1,\ \left(\frac{-1}{4m+3}\right)=(-1)^{2m+1}=-1.$$

4-х о с с а.

$$\left(\frac{a_1\cdot a_2\cdots a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right).$$

И с б о т. Ҳақиқатан, (81)-таққосламага асосан қуйидагиларни ёза оламиз:

$$\left(\frac{a_1\cdot a_2\cdots a_n}{p}\right)=(a_1\cdot a_2\cdots a_n)^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}\cdot a_2^{\frac{p-1}{2}}\cdots a_n^{\frac{p-1}{2}}\equiv\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)(\mathrm{mod}\ p);$$

$\left(\frac{a_1\cdot a_2\cdots a_n}{p}\right)$ ва $\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$ кўпайтманинг абсолют миқдори 1 га тенг. Юқорида биз таъкидлаганимиздек, бундай миқдорларнинг иккаласи p>2 модул бўйича таққосланувчи бўлиши учун улар тенг бўлиши керак. Шу билан хосса исботланди.

Гаусс, Эйлер мезонидан фарқли бўлган, берилган a сон p туб модул бўйича квадратик чегирма ёки ночегирмалигини аниқлайдиган мезонини ўрнатди.

73-т е о р е м а (*Гаусс мезони*). Ихтиёрий a, (a, p)=1 учун қуйидаги тенглик ўринлидир:

$$\left(\frac{a}{p}\right)=(-1)^t,$$

бунда t

$$a, 2a, \ldots, \frac{p-1}{2}a \qquad (82)$$

қатордаги сонларнинг p модул бўйича абсолют қиймати билан энг кичик чегирмаси манфий бўлганларининг сони.

И с б о т. Равшанки, (82)-қатордаги ҳар бир сон p модул бўйича чегирмаларнинг келтирилган системаси

$$-\frac{p-1}{2},\ldots,-2,-1,1,2,\ldots,\frac{p-1}{2} \qquad (83)$$

дан олинган фақат биттагина сон билан таққосланади. Демак, (82)-дан ҳир бир $s\cdot a$ сонга (83) дан $(-1)^{t_s}\cdot r_s$ сонни мос қўямиз, яъни $sa \equiv (-1)^{t_s} r_s (\mathrm{mod}\, p)$; бунда $1 \le r_s \le \frac{p-1}{2}$ ва t_s 0 ёки 1 га тенг, шу билан бирга, фақат sa нинг p бўйича абсолют қиймати билан энг кичик чегирмаси манфий бўлсагина $t_s=1$.

Агар шу сонлардан иккитаси sa ва ℓa ни олсак, у ҳолда уларга мос келадиган r_s ва r_ℓ сонлар бир-биридан фарқли бўлади. Ҳақиқатан, агар $r_s = r_\ell$, яъни $sa \equiv (-1)^{t_s}\cdot r_s (\mathrm{mod}\, p)$, $la \equiv (-1)^{t_s}\cdot r_s$ бўлса, у ҳолда $sa \equiv \pm la (\mathrm{mod}\, p), p \mid (s \mp l)a$. Бу ерда $1 \le s,l \le \frac{p-1}{2}, s \ne l$ бўлганлиги учун $0 < |s \pm l| \le p-1$, бундан p†(s±ℓ). Демак, p| a. Бу эса теорема шартига зиддир.

Шундай қилиб, агар s ўзгарувчи 1,2,…,p_1 (қулайлик учун $\frac{p-1}{2} = p_1$ деб олдик) қатордан ҳар хил қийматларни қабул қилса, у ҳолда r_s ҳам 1,2,…,p_1 қатордан ҳар хил қийматларни қабул қилади. Демак, 1,2,…,p_1 ва $r_1, r_2, \ldots r_{p_1}$ қаторлардаги сонлар фақат қаторларда жойлашиш тартиби билан фарқ қилиши мумкин. Демак,

$$R = r_1 \cdot r_2 \cdots r_{p_1} = 1\cdot 2 \cdots p_1,\ (R,p) = 1.$$

Энди

$$1 \cdot a \equiv (-1)^{t_1} r_1 (\mathrm{mod}\, p),$$

$$2 \cdot a \equiv (-1)^{t_2} r_2 (\mathrm{mod}\, p),$$

.....

$$p_1 \cdot a \equiv (-1)^{t_{p_1}} r_{p_1} (\mathrm{mod}\, p)$$

таққосламаларни кўпайтириб ва p модул билан ўзаро туб бўлган R га қисқартириб, қуйидагини ҳосил қиламиз

$$a^{p_1} \equiv (-1)^{t_1+t_2+\ldots+t_{p_1}} (\mathrm{mod}\, p).$$

Эйлер мезони

$$a^{p_1} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p)$$

дан фойдалансак

$$\left(\frac{a}{p}\right) \equiv (-1)^{t_1+t_2+\ldots+t_{p_1}} (\mathrm{mod}\, p).$$

келиб чиқади, бундан эса

$$\left(\frac{a}{p}\right) \equiv (-1)^{t_1+t_2+\ldots+t_{p_1}} = (-1)^t \qquad (84)$$

ҳосил бўлади, бунда t сон 1 га тенг бўлган t_i ларнинг сони, яъни (83)-қатордаги сонларнинг p модул бўйича абсолют қиймати билан энг кичик чегирмаларнинг манфийларининг сони.

Гаусс мезонининг топилган ифодасини ихчамроқ кўринишга келтирамиз. Равшанки,

$$\left[\frac{2ax}{p}\right] = \left[2\left[\frac{ax}{p}\right] + 2\left\{\frac{ax}{p}\right\}\right] = 2\left[\frac{ax}{p}\right] + \left[2\left\{\frac{ax}{p}\right\}\right].$$

Бу сон a x нинг манфий бўлмаган энг кичик чегирмаси $\frac{1}{2}p$ дан кичик ёки катта бўлишига қараб жуфт ёки тоқ бўлади, яъни (84) да t_x=0 бўлган ҳолда жуфт сонни, t_x=1 бўлган ҳолда тоқ сонни ифодалайди. Бундан

$$(-1)^{r_x} = (-1)^{\left[\frac{2ax}{p}\right]}$$

тенглик ўринли эканлиги кўриниб турибди, шунинг учун, (84)-дан қуйидагини ҳосил қиламиз:

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{2ax}{p}\right]}..$$

Энди a ни тоқ деб фараз қилиб (демак, a +p -жуфт), бу ифодани яна соддалаштирамиз:

$$\left(\frac{2a}{p}\right)=\left(\frac{2a+2p}{p}\right)=\left(\frac{4\cdot\frac{a+p}{2}}{p}\right)=\left(\frac{2^2}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right)=\left(\frac{\frac{a+p}{2}}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]}=$$

$$=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\sum_{x=1}^{p_1}x}.$$

Маълумки, $\sum_{x=1}^{p_1} x = \frac{p_1(p_1+1)}{2} = \frac{1}{2}\frac{p-1}{2}\cdot\frac{p+1}{2} = \frac{p^2-1}{8}$,

шунинг учун ҳам

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}}.. \qquad (85)$$

Бундан a =1 бўлганда Лежандр символининг яна бир хоссасини ҳосил қиламиз

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.. \qquad (86)$$

Натижада қуйидаги теорема келиб чиқади.

74-т е о р е м а.

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ агар } p\equiv 1(\text{mod}8) \text{ ёки } p\equiv 7(\text{mod}8) \text{ бўлса,} \\ -1, \text{ агар } p\equiv 3(\text{mod}8) \text{ ёки } p\equiv 5(\text{mod}8) \text{ бўлса.} \end{cases}$$

И с б о т. Ҳақиқатан, ҳар қандай туб сонни 8m+r аклида ёзиш мумкин, бунда қолдиқ r 1, 3, 5, 7 сонлардан ирига тенг;

$$\frac{p^2-1}{8}=\frac{(8m+r)^2-1}{8}=8m^2+2mr+\frac{r^2-1}{8}$$

йлганлиги учун $\frac{p^2-1}{8}$ сон r=1 ва r=7 қийматларда жуфт; 3 ва r=5 тоқ қийматларда тоқдир. Теорема исботланди.

Бу теоремани бошқача таърифлаш ҳам мумкин.

75-т е о р е м а. 2 сони 8m+1 ва 8m+7 кўринишдаги туб онлар учун квадратик чегирма бўлиб, 8m+3 ва 8m+5 йринишдаги туб сонлар учун эса квадратик ночегирмадир.

6-х о с с а (*квадратик чегирмаларнинг ўзаролик онуни*). Агар p ва q иккита ҳар хил тоқ туб сонлар бўлса, у олда

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \qquad (87)$$

И с б о т. (85) ва (86)-дан қуйидагини ҳосил қиламиз

$$\left(\frac{q}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{qx}{p}\right]}. \qquad (88)$$

Шунга ўхшаш, $\frac{q-1}{2}=q_1$ деб олсак

$$\left(\frac{p}{q}\right)=(-1)^{\sum_{y=1}^{q_1}\left[\frac{py}{q}\right]}. \qquad (89)$$

осил бўлади.

Энди qx ва py ифодаларда x ва y нинг ҳар бири устақил равишда

$$x=1,2,\ldots,p_1, y=1,2,\ldots,q_1$$

қийматларни қабул қилганда ҳосил бўладиган p_1q_1 та (x, y) сонлар жуфтлигини қарайлик. Бунда ҳеч қачон qx=py бўла олмайди, чунки акс ҳолда бу тенгликдан py нинг q га бўлиниши келиб чиқади, бу эса (p, q)=(y, q)=1 шартга кўра (0<y<q бўлганлиги сабабли) мумкин эмас. Шунинг учун, **qx<py ни қаноатлантирувчи сонлар жуфтликларини** S_1 та деб, **py<qx ни қаноатлантирувчи сонлар жуфтликларини** S_2 та деб фараз қилиб, $S_1+S_2=p_1q_1$ дейиш мумкин; $x<\frac{p}{q}y$ тенгсизликни қаноатлантирувчи сонлар жуфтликларининг миқдори S_1 та эканлиги равшандир. Бунда берилган y учун $x=1,2,...,\left[\frac{p}{q}y\right]$ деб олиш мумкин. ($\frac{p}{q}y\le\frac{p}{q}q_1<\frac{p}{2}$ бўлганлиги учун $\left[\frac{p}{q}y\right]\le p_1$). Демак,

$$S_1=\sum_{y=1}^{q_1}\left[\frac{p}{q}y\right].$$

Шунга ўхшаш йўл билан

$$S_2=\sum_{x=1}^{p_1}\left[\frac{q}{p}y\right]$$

ни ҳосил қиламиз. Энди (88) ва (89) дан

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{S_1+S_2}=(-1)^{p_1q_1}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

тенгликнинг ўринлилиги ва бундан хоссанинг тўғрилиги келиб чиқади.

1-и з о ҳ. Агар p ва q нинг иккаласи ҳам 4m+3 кўринишда бўлса, $\frac{p-1}{2}\cdot\frac{q-1}{2}$ сон тоқ бўлади; агар бу сонларнинг ақалли биттаси 4m+1 кўринишда бўлса

$\frac{p-1}{2}\cdot\frac{q-1}{2}$ сон жуфт бўлади. Буларга асосан айтилган хоссани қуйидагича таърифлаш мумкин. Агар p ва q сонларнинг иккаласи ҳам 4m+3 кўринишда бўлса

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right);$$

агар p ва q сонлардан ақалли биттаси 4m+1 кўринишда бўлса

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$$

тенглик ўринлидир.

М и с о л л а р. 1) $x^2\equiv 520(\mathrm{mod}\,631)$ таққослама ечимга эгами?

Е ч и ш. Модул 631 туб сон. Лежандр символининг хоссаларини қўллаб, қуйидагиларни топамиз:

$$\left(\frac{520}{631}\right)=\left(\frac{4}{631}\right)\left(\frac{130}{631}\right)=\left(\frac{2}{631}\right)\left(\frac{65}{631}\right)=\left(\frac{65}{631}\right)=\left(\frac{5}{631}\right)\left(\frac{17}{631}\right)=\left(\frac{631}{5}\right)\left(\frac{631}{17}\right)=$$

$$=\left(\frac{1}{5}\right)\left(\frac{2}{17}\right)=1$$

Таққослама ечимга эга.

2) $x^2\equiv 34(\mathrm{mod}\,113)$ таққослама ечимга эгами?

Е ч и ш. 113- туб сон, қуйидагиларни ҳосил қиламиз:

$$\left(\frac{34}{113}\right)=\left(\frac{2}{113}\right)\left(\frac{17}{113}\right)=\left(\frac{17}{113}\right)=\left(\frac{113}{17}\right)=\left(\frac{11}{17}\right)=\left(\frac{17}{11}\right)=\left(\frac{6}{11}\right)=\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)=-\left(\frac{3}{11}\right)=-\left(\frac{11}{3}\right)$$

$$=\left(\frac{2}{3}\right)=-1.$$

Таққослама ечимга эга эмас.

37-§. ЯКОБИ СИМВОЛИ ВА УНИНГ ХОССАЛАРИ

Лежандр символини ҳисоблашда суратни туб кўпайтувчиларга ажратиш энг катта қийинчилик туғдиради, сурат етарлича катта бўлган ҳолда кўпайтувчиларга ажратиш масаласи амалда бажарилмай қолиши мумкин.

Кўпайтувчиларга ажратишдан қутилиш учун махраж тоқ таркибли сон бўлган ҳолда *Лежандр символ Якоби символи* дейилади.

20-т а ъ р и ф. Фараз қилайлик $P= p_1 p_2 \cdots p_s$, бунда p_i тоқ туб сонлар бўлиб, уларнинг орасида тенглари ҳам бўлиши мумкин. ***Якоби символи*** $\left(\frac{a}{P}\right)$ қуйидаги

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right)$$

тенглик билан аниқланади, бунда $\left(\frac{a}{p_i}\right)$ $(i=1,...,s)$ - Лежандр символлари.

Таърифга кўра Лежандр символи $\left(\frac{a}{p}\right)$ Якоби символининг хусусий ҳоли бўлиб, ундан P=p бўлганда келиб чиқади. Шундай қилиб, туб модул P=p учун $x^2 \equiv a(\mathrm{mod}\, p)$ таққослама ечимга эга бўлса Якоби символи +1 га, агар ечимга эга бўлмаса –1 га тенг. Шу билан бирга, Якоби символи $\left(\frac{a}{P}\right)$ таркибий модул учун $x^2 \equiv a(\mathrm{mod}\, P)$ таққослама ечимга эга бўлмаса ҳам +1 га тенг бўлиши мумкин.

Масалан, $x^2 \equiv 2(\mathrm{mod}15)$ таққослама ечимга эга эмас, лекин Якоби символи

$$\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)(-1)^3=+1.$$

Якоби символининг хоссалари Лежандр символининг хоссаларига ўхшаш. Бу хоссаларни ўрганишда ҳар гал

таъкидланмасдан, Р орқали ихтиёрий тоқ сонни белгилаб, $\left(\frac{a}{P}\right)$ Якоби символида (a, Р)=1 деб оламиз.

1-х о с с а. Агар $a \equiv a_1 (\mathrm{mod}\, P)$ бўлса, у ҳолда $\left(\frac{a}{P}\right)=\left(\frac{a_1}{P}\right)$.

И с б о т. Ҳақиқатан, Якоби сомволининг таърифига ва Лежандр символининг 1-хоссасига кўра

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right)=\left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\cdots\left(\frac{a_1}{p_s}\right)=\left(\frac{a_1}{P}\right),$$

чунки a сон Р модул бўйича a_1 билан таққосланувчи бўлса, у ҳолда у Р соннинг бўлувчилари $p_1, p_2, \ldots, p_s$ модуллар билан ҳам таққосланувчи бўлади.

2-х о с с а. $\left(\frac{1}{P}\right)=1$.

И с б о т. Ҳақиқатан,

$$\left(\frac{1}{P}\right)=\left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_s}\right)=1.$$

3-х о с с а. $\left(\frac{1}{P}\right)=(-1)^{\frac{P-1}{8}}$.

И с б о т. Лежандр символининг 3-хоссасига кўра

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_s}\right)=(-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots+\frac{p_s-1}{2}}. \qquad (90)$$

Лекин

$$\frac{P-1}{2}=\frac{p_1p_2\cdots p_s-1}{2}=\frac{\left(1+2\cdot\frac{p_1-1}{2}\right)\left(1+2\cdot\frac{p_2-1}{2}\right)\cdots\left(1+2\cdot\frac{p_s-1}{2}\right)-1}{2}= \qquad (91)$$

$$=\frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots+\frac{p_s-1}{2}+2N$$

(90) ва (91) дан

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{8}}$$

келиб чиқади.

4-х о с с а. $\left(\frac{a_1a_2\cdots a_n}{P}\right)=\left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)\cdots\left(\frac{a_n}{P}\right)$.

И с б о т. Ҳақиқатан,

$$\left(\frac{a_1a_2\cdots a_n}{P}\right)=\left(\frac{a_1a_2\cdots a_n}{p_1}\right)\cdots\left(\frac{a_1a_2\cdots a_n}{p_s}\right)=\left(\frac{a_1}{p_1}\right)\left(\frac{a_2}{p_1}\right)\cdots\left(\frac{a_n}{p_1}\right)\cdots\left(\frac{a_1}{p_s}\right)\left(\frac{a_2}{p_s}\right)\cdots\left(\frac{a_n}{p_s}\right)=$$
$$=\left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)\cdots\left(\frac{a_n}{P}\right)$$

Хусусий ҳолда

$$\left(\frac{ab^2}{P}\right)=\left(\frac{a}{P}\right)$$

5-х о с с а.

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

И с б о т. Ҳақиқатан, Якоби символининг таърифи ва Лежандр символининг 5-хоссасидан

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_s}\right)=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_s^2-1}{8}} \qquad (92)$$

Лекин

$$\frac{P^2-1}{8}=\frac{p_1^2p_2^2\cdots p_s^2-1}{8}=\frac{\left(1+8\cdot\frac{p_1^2-1}{8}\right)\left(1+8\cdot\frac{p_2^2-1}{8}\right)\cdots\left(1+8\cdot\frac{p_s^2-1}{8}\right)-1}{8}= \qquad (93)$$
$$=\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_s^2-1}{8}+2N.$$

Энди 5-хосса (92) ва (93) дан келиб чиқади.

75-т е о р е м а (*Квадратик чегирмаларнинг ўзаролик қонуни*). Фараз қилайлик P ва Q ўзаро туб ва тоқ сонлар бўлсин. У ҳолда

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right) \tag{94}$$

И с б о т. Фараз қилайлик $Q=q_1 q_2 \cdots q_r$ бўлиб, q_i туб сонлар (улар орасида тенглари ҳам бўлиши мумкин) бўлсин. У ҳолда Якоби символининг таърифи ва Лежандр символининг 4-хоссасига кўра

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\cdots\left(\frac{Q}{p_s}\right)=\prod_{k=1}^{s}\prod_{m=1}^{r}\left(\frac{q_m}{p_k}\right)=(-1)^{\sum_{k=1}^{s}\sum_{m=1}^{r}\frac{p_k-1}{2}\cdot\frac{q_m-1}{2}}\prod_{k=1}^{s}\prod_{m=1}^{r}\left(\frac{p_k}{q_m}\right)= \tag{95}$$

$$=(-1)^{\left(\sum_{k=1}^{s}\frac{p_k-1}{2}\right)\left(\sum_{m=1}^{r}\frac{q_m-1}{2}\right)}\cdot\left(\frac{P}{Q}\right)$$

Биз 3-хоссанинг исботи жараёнида

$$\frac{P-1}{2}=\sum_{k=1}^{s}\frac{p_k-1}{2}+2N,\quad \frac{Q-1}{2}=\sum_{m=1}^{r}\frac{q_m-1}{2}+2N_1 \tag{96}$$

тангликларни ўринли бўлишини кўрган эдик. (95) ва (96) тенгликлардан (94) келиб чиқади. Туб модуллар учун Якоби символининг хоссаларидан фойдаланиб, Лежандр символини тезроқ ҳисоблаш мумкин.

М и с о л. Ушбу $x^2\equiv 261 \pmod{443}$ таққослама ечимга эгами?

Е ч и ш. Бунда 443 туб сон, $\left(\frac{261}{443}\right)$ Лежандр символини Якоби символининг хоссаларидан фойдаланиб ҳисоблаймиз:

$$\left(\frac{261}{443}\right)=\left(\frac{443}{261}\right)=\left(\frac{182}{261}\right)=\left(\frac{2}{261}\right)\left(\frac{91}{261}\right)=-\left(\frac{91}{261}\right)=-\left(\frac{261}{91}\right)=-\left(\frac{79}{91}\right)=\left(\frac{91}{79}\right)=\left(\frac{12}{79}\right)=\left(\frac{2^2}{79}\right)\left(\frac{3}{79}\right)=$$

$$=\left(\frac{3}{79}\right)=-\left(\frac{79}{3}\right)=-\left(\frac{1}{3}\right)=1.$$

Таққослама иккита ечимга эга.

38-§. ТАРКИБЛИЙ МОДУЛ БЎЙИЧА ИККИНЧИ ДАРАЖАЛИ ТАҚҚОСЛАМАЛАР

Икки ҳадли иккинчи даражали таркибли модулли

$$x^2 \equiv a(\mathrm{mod}\, m),\ m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ (a,m) = 1$$

таққосламаларни текшириш ва ечиш 32-§ даги умумий кўрсатмаларга асосан бажарилади.

Биз ишни

$$x^2 \equiv a(\mathrm{mod}\ p^{\alpha}), a > 0, (a,p) = 1 \qquad (97)$$

таққосламадан бошлаймиз, бунда р-туб сон. Агар $f(x) = x^2 - a$ деб олсак, у ҳолда $f'(x) = 2x$ бўлади. Агар

$$x^2 \equiv a(\mathrm{mod}\ p\ ) \qquad (98)$$

таққосламанинг ечими $x \equiv x_1(\mathrm{mod}\, p)$ бўлса, у ҳолда (a, р)=1 бўлганлиги учун (x_1, р)=1 бўлади, шунингдек, р-тоқ бўлганлиги учун ($2x_1$, р)=1, яъни $f'(x_1)$ сон р га бўлинмайди. Шунинг учун ҳам (97)-таққосламани ечимини қидиришда, 32-§ даги мулоҳазаларни қўллаш мумкин. Бу мулоҳазалардан (98)-таққосламанинг ҳар бир ечими (97)-таққосламанинг бир ечимини бериши келиб чиқади. Шундай қилиб, биз қуйидаги теоремани исботладик.

76-т е о р е м а. a соннинг р модул бўйича квадратик чегирма ёки ночегирмалигига қараб, (98)-таққосламанинг иккита ечими мавжуд ёки битта ҳам ечими мавжуд эмас.

Энди

$$x^2 \equiv a(\mathrm{mod}\, 2^{\alpha}), (a,2) = 1 \qquad (99)$$

таққосламани қараймиз. $f'(x_1)=2x_1$. Демак, 32-§ даги мулоҳазалардан фойдаланиб бўлмайди. Шунинг учун биз бошқача йўл тутишимиз керак. Агар (99)-таққослама ечимга

а бўлса, у ҳолда $(a, 2)=1$ га кўра $(x, 2)=1$ бўлади, яъни =2k+1- тоқ, демак, $x^2-1=4k^2+4k=4k(k+1)$ сон 8 га ўлинади. Шунинг учун (99)-таққосламани

$$\left(x^2-1\right)+1\equiv a(\mathrm{mod}\,2^\alpha)$$

ўринишга келтириб, унинг ечимга эга бўлиши учун уйидаги

$\alpha=2$ да $a\equiv 1(\mathrm{mod}\,4)$; $\alpha\geq 3$ да $a\equiv 1(\mathrm{mod}\,8)$ (100)

шартларнинг бажарилиши зарурлигига ишонч ҳосил қиламиз.

Бу шартлар бузилмаган ҳолларда (99)-таққосламанинг ечимларини топиш билан шуғулланамиз. Юқорида айтилганлардан шундай хулосага келамиз: $\alpha\leq 3$ бўлса таққосламани барча тоқ сонлар қаноатлантиради. Шунинг учун $x^2\equiv a(\mathrm{mod}\,2)$ таққослама битта $x\equiv 1(\mathrm{mod}\,2)$ ечимга; $x^2\equiv a(\mathrm{mod}\,4)$ таққослама иккита $x\equiv 1;3(\mathrm{mod}\,4)$ ечимларга ва $x^2\equiv a(\mathrm{mod}\,8)$ таққослама тўртта $x\equiv 1,3,5,7(\mathrm{mod}\,8)$ ечимларга эга.

Биз α=4,5,... бўлган ҳолларда барча тоқ сонларни иккита

$$x=\pm(1+4t_3) \qquad (101)$$

$\left(1+4t_3\equiv 1(\mathrm{mod}\,4);-1-4t_3\equiv -1\equiv 3(\mathrm{mod}\,4)\right)$ арифметик прогрессия кўринишида ёзамиз. Энди (101)-сонларнинг қайси бири $x^2\equiv a(\mathrm{mod}16)$ таққосламани қаноатлантиришини кўриб чиқамиз:

$$(1+4t_3)^2\equiv a(\mathrm{mod}\,16), t_3'\equiv\frac{a-1}{8}(\mathrm{mod}2), t_3=t_3'+2t_4, x=\pm\left(1+4t_3'+8t_4'\right)=\pm(x_4+8t_4).$$

Бу сонлар орасидан $x^2\equiv a(\mathrm{mod}\,32)$ таққосламани қаноатлантирадиганла-рини топамиз:

$$(x_4+8t_4)^2\equiv a(\mathrm{mod}32), t_4'=\frac{a-x_4^2}{16x_4}(\mathrm{mod}2); t_4=t_4'+2t_5, x=\pm(x_4+8t_4'+16t_5)=\pm(x_5+16t_5)$$

ва ҳ.к. Бу жараённи давом эттириб, $\alpha>3$ учун x нинг (99)-таққосламани қаноатлантирувчи қийматлари

$$x = \pm\left(x_\alpha + 2^{\alpha-1} t_\alpha\right)$$

кўринишга эга эканлигига ишонч ҳосил қиламиз. x нинг бу қийматлари (99) таққосламанинг тўртта ҳар хил

$$x \equiv x_\alpha; x_\alpha + 2^{\alpha-1}; -x_\alpha; -x_\alpha - 2^{\alpha-1} (\mathrm{mod}\, 2^\alpha)$$

ечимларини ташкил этади. 4 модул бўйича бу ечимларнинг дастлабки иккитаси 1 билан, кейинги иккитаси эса -1 билан таққосланади. Шундай қилиб биз қуйидаги теоремани исботладик.

77-т е о р е м а. Ушбу

$$x^2 \equiv a(\mathrm{mod}\, 2^\alpha), (a,2) = 1$$

таққосламанинг ечилиши учун зарурий шартлар қуйидагилардан иборат: $\alpha = 2$ қийматда $a \equiv 1(\mathrm{mod}\, 4)$ бўлиб, $\alpha \geq 3$ қийматларда эса $a \equiv 1(\mathrm{mod}\, 8)$. Бу шартлар бажарилса, $\alpha = 1$ қийматда ечимлар сони битта, $\alpha = 2$ қийматда иккита, $\alpha \geq 3$ қийматда эса тўртта бўлади.

М и с о л. Ушбу

$$x^2 \equiv 105(\mathrm{mod}\, 128) \qquad (102)$$

таққосламанинг ечимлари топилсин.

Е ч и ш. Бу ерда $105 \equiv 1(\mathrm{mod}\, 8)$ ва $\alpha = 6$. Шунинг учун бу таққослама тўртта ечимга эга; x ни $x = \pm\left(1 + 4t_3\right)$ кўринишда ёзиб олиб, қуйидагиларни ҳосил қиламиз:

$(1+4t_3)^2 \equiv 105(\mathrm{mod}\, 16)$, $8t_3 \equiv 104(\mathrm{mod}\, 16)$, $t_3 \equiv 1(\mathrm{mod}\, 2)$, $t_3 = 1 + 2t_4$, $x = \pm(5 + 8t_4)$,
$(5+8t_4)^2 \equiv 105(\mathrm{mod}\, 32)$, $5 \cdot 16t_4 \equiv 80(\mathrm{mod}\, 32)$, $t_4 \equiv 1(\mathrm{mod}\, 2)$, $t_4 = 1 + 2t_5$, $x = \pm(13 + 16t_5)$,
$(13+16t_5)^2 \equiv 105(\mathrm{mod}\, 64)$, $13 \cdot 32t_5 \equiv 0(\mathrm{mod}\, 64)$, $t_5 \equiv 0(\mathrm{mod}\, 2)$, $t_5 = 2t_6$, $x = \pm(13 + 32t_6)$,
$(13+32t_6)^2 \equiv 105(\mathrm{mod}\, 128)$, $13 \cdot 64t_4 \equiv 64(\mathrm{mod}\, 128)$, $t_6 \equiv 1(\mathrm{mod}\, 2)$, $t_6 = 1 + 2t_7$,
$x = \pm(45 + 64t_7)(\mathrm{mod}\, 128)$.

Шунинг учун (102)-таққосламанинг ечимлари қуйидагилардан иборат:

$$x = \pm 45; \pm 109(\mathrm{mod}\, 128).$$

Юқорида зикр этилганлар ва 32-§ дан қуйидаги теорема келиб чиқади.

78-т е о р е м а. Қуйидаги таркибли модулли

$$x^2 \equiv a(\mathrm{mod}\, m), m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, (a,m) = 1$$

таққосланинг ечилиши учун зарурий шартлар қуйидагилардан иборат: $\alpha = 2$ қийматда $a \equiv 1(\mathrm{mod}\, 4)$ ва $\alpha \geq 3$ қийматларда $a \equiv 1(\mathrm{mod}\, 8)$ бўлиб,

$$\left(\frac{a}{p_1}\right) = 1, \left(\frac{a}{p_2}\right) = 1, \cdots, \left(\frac{a}{p_k}\right) = 1.$$

Бу шартлар бир вақтда бажарилса, $\alpha = 0$ ва $\alpha = 1$ қийматларда ечимлар сони 2^k та; $\alpha = 2$ қийматда 2^{k+1} та; $\alpha \geq 3$ қийматларда 2^{k+2} та бўлади.

М и с о л. Ушбу $x^2 \equiv 28(\mathrm{mod}\, 108)$ таққосланинг ечимлари топилсин.

Е ч и ш. Бу таққослама

$$x^2 \equiv 28(\mathrm{mod}\, 4) \equiv 28(\mathrm{mod}\, 2^2),$$

$$x^2 \equiv 28(\mathrm{mod}\, 27) \equiv 28(\mathrm{mod}\, 3^3)$$

ёки

$$x^2 \equiv 0(\mathrm{mod}\, 4), x^2 \equiv 1(\mathrm{mod}\, 27)$$

га тенг кучлидир, $\alpha = 2$ ва k=1 бўлганлиги учун таққослама $2^{k+1}=2^{1+1}=4$ та ечимга эга. Биринчи таққосланинг ечимлари: 0 ва 2, иккинчиси ҳам иккита ечимга эга: ±1.

Бу ечимларнинг мумкин бўлган тўртала комбинациясини оламиз: аввал x≡0(mod4), x≡1(mod27) ни оламиз, бундан x=4t ≡1(mod27), бунинг ечими t=7. Демак, x≡28(mod108). Бу берилган таққосланинг биринчи ечими. Равшанки, иккинчи ечим x≡-28(mod108) бўлади. Энди x≡2(mod4), x≡1(mod27) ларнинг комбинацияни оламиз. Бундан x=2+4t ≡ 1(mod27), 4t ≡ -1(mod27), t =-7, x=2-4·7 ≡-26(mod108). Бу учинчи ечим, равшанки, тўртинчи ечим x≡26(mod108). Шундай қилиб, биз тўртала x≡±26, ±28 (mod108) ечимларни топдик.

7-БОБ УЧУН МАШҚЛАР

1. Қуйидаги таққосламаларни икки ҳадли таққосламага келтиринг:

$1)2x^2-3x+5\equiv 0(\mathrm{mod}\,7)$, $2)5x^2-4x+6\equiv 0(\mathrm{mod}\,11)$,

$3)20x^2+21x+7\equiv 0(\mathrm{mod}\,13)$, $4)21x^2-3x+5\equiv 0(\mathrm{mod}\,10)$,

$5)19x^2-14x+9\equiv 0(\mathrm{mod}\,14)$.

2. Агар q натурал сон p туб сонга бўлинмаса у ҳолда $x^2\equiv q(\mathrm{mod}\,p)$ таққослама ё ечимга эга эмас ёки иккита ечими мавжуд.

3. 29 модул бўйича чегирмаларнинг келтирилган системаси орасида квадратик чегирмаларни кўрсатинг.

4. 31 модул бўйича чегирмаларнинг келтирилган системаси орасида квадратик чегирмаларни кўрсатинг.

5. Қуйидаги таққосламалар ечилсин:

$1)x^2\equiv 3(\mathrm{mod}\,311)$, $2)x^2\equiv 5(\mathrm{mod}\,271)$, $3)x^2\equiv 7(\mathrm{mod}\,349)$

6. Қуйидаги Лежандр символлари ҳисоблансин:

$1)\left(\frac{94}{109}\right)$, $2)\left(\frac{111}{271}\right)$, $3)\left(\frac{342}{677}\right)$, $4)\left(\frac{93}{131}\right)$, $5)\left(\frac{2116}{6269}\right)$.

7. Қуйидаги Лежандр ва Якоби символлари ҳисоблансин:

$1)\left(\frac{47}{125}\right)$, $2)\left(\frac{5610}{6649}\right)$, $3)\left(\frac{131}{283}\right)$, $4)\left(\frac{116}{397}\right)$, $5)\left(\frac{589}{1283}\right)$.

8. Лежандр символини ҳисоблаб, қуйидаги таққосламалар ечимларининг сонини аниқланг:

$1)x^2\equiv 2(\mathrm{mod}\,29)$, $2)x^2\equiv 3(\mathrm{mod}\,29)$, $3)x^2\equiv 3(\mathrm{mod}\,7)$.

9. Якоби символини ҳисоблаб ушбу таққосламалар ечимларининг сонини аниқланг:

$1)x^2\equiv 152(\mathrm{mod}\,557)$, $2)x^2\equiv 452(\mathrm{mod}\,557)$, $3)x^2\equiv 1234(\mathrm{mod}\,5981)$.

8-БОБ. БОШЛАНҒИЧ ИЛДИЗЛАР ВА ИНДЕКСЛАР

39-§ УМУМИЙ ТЕОРЕМАЛАР

Фараз қилайлик $(a,m)=1$ бўлсин, Эйлер теоремасига кўра $a^{\varphi(m)} \equiv 1 (\bmod m)$. Бу таққосламанинг ҳар иккала томонини n натурал даражага кўтариб, $a^{n\varphi(m)} \equiv 1 (\bmod m)$ ни ҳосил қиламиз. Бундан кўрамизки

$$a^{\gamma} \equiv 1 (\bmod m) \qquad (103)$$

таққосламани қаноатлантирадиган чексиз кўп γ натурал сонлар мавжуд.

21-т а ъ р и ф. Агар (103)-таққосламани қаноатлантирадиган γ ларнинг энг кичиги δ бўлса, у ҳолда a сон m модул бўйича δ *кўрсаткичга тегишли* дейилади.

79-т е о р е м а. Агар a сон m модул бўйича δ кўрсаткичга тегишли бўлса, у ҳолда $1 = a^0, a, \ldots, a^{\delta-1}$ сонлар m модул бўйича ўзаро таққосланмайдилар.

И с б о т. Агар $0 \le k < l < \delta$ ва $a^k \equiv a^l (\bmod m)$ бўлса, у ҳолда $a^{l-k} \equiv 1 (\bmod m)$ бўлади; $0 < l-k < \delta$ лиги равшан, бу эса δ нинг энг кичиклигига зиддир. Демак, k=ℓ. Шу билан теорема исботланди.

80-т е о р е м а. Агар a сон m модул бўйича δ кўрсаткичга тегишли бўлса, у ҳолда $a^{\gamma} \equiv a^{\gamma_1} (\bmod m)$ таққосламанинг бажарилиши учун $\gamma \equiv \gamma_1 (\bmod \delta)$ нинг бажарилиши зарур ва кифоядир. Хусусий ҳолда $\gamma_1 = 0$ бўлганда $a^{\gamma} \equiv 1 (\bmod \delta)$ нинг бажарилиши учун γ нинг δ га бўлиниши зарур ва кифоядир.

И с б о т. Фараз қилайлик r ва r_1 сонлар γ ва γ_1 сонларнинг δ модул бўйича манфий бўлмаган энг кичик чегирмалари бўлсин, у ҳолда шундай q ва q_1 сонлар топиладики $\gamma = \delta q + r$ ва $\gamma_1 = \delta q_1 + r_1$ тенгликлар ўринли бўлади. Бу ва $a^{\delta} \equiv 1 (\bmod m)$ таққосламадан қуйидагилар келиб чиқади:

$$a^{\gamma} \equiv (a^{\delta})^{q} a^{r} \equiv a^{r} (\bmod m), o \le r < \delta;$$

$$a^{\gamma_1} \equiv (a^{\delta})^{q_1} a^{r_1} \equiv a^{r_1} (\bmod m), o \le r_1 < \delta.$$

Демак, $a^{\gamma} \equiv a^{\gamma_1} (\bmod m)$ таққосламани бажарилиши учун $a^{r} \equiv a^{r_1} (\bmod m)$ таққосламанинг бажарилиши зарур ва етарлидир. Бундан (79-теоремага кўра) r=r_1. Шундай қилиб, $\gamma \equiv \gamma_1 (\bmod \delta)$ бажарилиши $a^{\gamma} \equiv a^{\gamma_1} (\bmod m)$ нинг бажарилиши учун зарур ва етарлидир. Хусусий ҳолда $\gamma_1 = 0$ бўлганда $\gamma \equiv 0 (\bmod \delta)$ ва $a^{\gamma} \equiv a^{0} = 1 (\bmod m)$ бўлади. Бошқача айтганда, γ нинг δ га бўлиниши $a^{\gamma} \equiv 1 (\bmod m)$ таққосламанинг бажарилиши учун зарур ва кифоядир.

Н а т и ж а. a соннинг m модул бўйича δ кўрсаткичи $\varphi(m)$ нинг бўлувчиси бўлади.

Ҳақиқатан, $a^{\varphi(m)} \equiv 1 (\bmod m)$ таққослама ва 80-теореманинг $\gamma_1 = 0$ ҳолидан натижа келиб чиқади.

Бўлувчиларнинг энг каттаси $\varphi(m)$ нинг ўзи бўлади.

22-т а ъ р и ф. Агар (a, m)=1 ва $\delta = \varphi(m)$ бўлса, у ҳолда a сон (агар бундай сонлар мавжуд бўлса) *m модул бўйича бошланғич илдиз* дейилади.

И з о ҳ. δ кўрсаткични топиш учун $a^0, a^1, \ldots a^{\varphi(m)}$ системадаги барча даражаларни 1 билан таққослаб чиқиш шарт эмас, бунинг ўрнига даража кўрсаткичига $\varphi(m)$ бўлинадиган даражаларни 1 билан таққослаш кифоя.

1-м и с о л. 19 модул бўйича 7 нинг даража кўрсаткичи топилсин.

Е ч и ш. $\varphi(19)=18$ нинг бўлувчилари 1, 2, 3, 6, 9, 18. Шунинг учун қуйидагиларга эга бўламиз: $7^1\equiv 7;\ 7^2\equiv 11;\ 7^3\equiv 1;\ 7^6\equiv 1;\ 7^9\equiv 1; 7^{18}\equiv 1(\mathrm{mod}19)$. Демак, 7 нинг19 модул бўйича даража кўрсаткичи $\delta=3$ бўлиб, 7 бошланғич илдиз эмас.

2-м и с о л. 17 модул бўйича 7 нинг даража кўрсаткичи топилсин.

Е ч и ш. $\varphi(17)=16$ бўлиб, нинг бўлувчилари 1, 2, 4, 8, 16, дан иборат. Қуйидагиларни топамиз: $7^1\equiv 7;\ 7^2\equiv -2;\ 7^4\equiv 4;\ 7^8\equiv -1;\ 7^{16}\equiv 1(\mathrm{mod}17)$. Демак, $\delta=\varphi(17)=16$ ва, шунинг учун, 7 сон 17 модул бўйича бошланғич илдиз.

81-т е о р е м а. Агар x сон m модул бўйича $a\,b$ кўрсаткичга тегишли бўлса, у ҳолда x^a шу модул бўйича b кўрсаткичга тегишли бўлади.

И с б о т. Фараз қилайлик x^a сон δ кўрсакичга тегишли бўлсин; $(x^a)^\delta\equiv 1(\mathrm{mod}\,m)$. Демак 80-теоремага кўра, $a\delta$ сон $a\,b$ га, яъни δ сон b га бўлинади, бундан $b\le\delta$. Иккинчи томондан $x^{ab}\equiv 1(\mathrm{mod}\,m)$ ёки $(x^a)^b\equiv 1(\mathrm{mod}\,m)$ таққослама ўринлидир. Бундан (80-теоремага кўра) b сон δ га бўлинади, яъни $\delta\le b$. Шундай қилиб, $\delta=b$ тенглик ўринлидир.

82-т е о р е м а. Агар (a, b)=1 бўлиб, x ва y сонлар m модул бўйича мос равишда a ва b кўрсаткичларга тегишли бўлса, у ҳолда xy сон $a\,b$ кўрсаткичга тегишли.

И с б о т. Фараз қилайлик ху сон δ кўрсаткичга тегишли бўлсин, у ҳолда $(xy)^\delta\equiv 1(\mathrm{mod}\,m)$. Бундан $x^{b\delta}\cdot y^{b\delta}\equiv 1\ (\mathrm{mod}\,m)$ келиб чиқади; $y^{b\delta}\equiv\left(y^b\right)^\delta\equiv 1\,(\mathrm{mod}\,m)$ бўлганлиги учун $x^{b\delta}\equiv 1\ (\mathrm{mod}\,m)$ ҳосил бўлади. Бундан (80-теоремага кўра) $b\delta$ нинг a га бўлиниши келиб чиқади. Лекин, (a, b)=1, δ сон a га бўлинади. Шунга ўхшаш

кўрсатиш мумкинки δ ҳам b га бўлинади; (a, b) 1 бўлганлиги учун δ сон ab га бўлинади, яъни $ab \le \delta$. Иккинчи томондан $x^a \equiv 1 (\mathrm{mod}\, m), y^b \equiv 1 (\mathrm{mod}\, m)$, бундан $x^{ab} \equiv 1 (\mathrm{mod}\, m), y^{ab} \equiv 1 (\mathrm{mod}\, m)$ ҳосил бўлади. Демак, $(xy)^{ab} \equiv 1 (\mathrm{mod}\, m)$. бундан (80-теоремага кўра) ab нинг δ га бўлинишини кўрамиз, яъни $\delta \le ab$. Шунинг учун $\delta = ab$.

40-§. БОШЛАНҒИЧ ИЛДИЗЛАРНИНГ МАВЖУДЛИГИ ВА УЛАРНИ ТОПИШ.

Энди биз қайси модуллар учун бошланғич илдизлар мавжуд деган масалани текширамиз. Аввал қуйидаги леммани исбот қиламиз.

Л е м м а. Агар

$a^{\lambda_1} \equiv 1 (\mathrm{mod}\, m_1), a^{\lambda_2} \equiv 1 (\mathrm{mod}\, m_2), \ldots, a^{\lambda_k} \equiv 1 (\mathrm{mod}\, m_k)$

таққосламалар ўринли бўлса, у ҳолда $a^{\mu} \equiv 1 (\mathrm{mod}\, m^*)$ таққослама ўринли бўлади, бунда $\mu = [\lambda_1, \lambda_2, \ldots, \lambda_k]$ ва $m^* = [m_1, m_2, \ldots, m_k]$.

И с б о т. Агар $a^{\lambda_i} \equiv 1 (\mathrm{mod}\, m_i)$ бўлса, у ҳолда ихтиёрий n бутун сон учун $a^{n\lambda_i} \equiv 1 (\mathrm{mod}\, m_i)$ таққослама ўринли, демак, барча $i=1, 2, \ldots, k$ учун $a^{\mu} \equiv 1 (\mathrm{mod}\, m_i)$ таққосламалар ўринли бўлади. Бундан (50 теоремага кўра) $a^{\mu} \equiv 1 (\mathrm{mod}\, m^*)$.

Фараз қилайлик $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots p_k^{\alpha_k}$ ифода m нинг каноник ёйилмаси бўлсин. Агар a сон m билан ўзаро туб бўлса, у ҳолда барча i=1, 2, …, k учун a сон $p_i^{\alpha_i}$ билан ўзаро туб бўлади. Фараз қилайлик a сон m модул бўйича λ_i

кўрсаткичга тегишли ва $\xi = [\lambda_1, \lambda_2, .., \lambda_k]$ бўлсин. У ҳолда леммага кўра

$$a^{\xi} \equiv 1 (\text{mod } m).$$

Агар a сон m модул бўйича бошланғич илдиз бўлса, у ҳолда $\xi = \varphi(m)$. Энди бир томондан (36-теоремага кўра) $\varphi(m) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})...\varphi(p_k^{\alpha_k})$, иккинчи томондан (80-теоремага кўра) $\lambda_1, \lambda_2, ..., \lambda_k$ мос равишда $\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), ..., \varphi(p_k^{\alpha_k})$ нинг бўлувчиси бўлади. Демак, $\lambda_1 \le \varphi(p_1^{\alpha_1}), \lambda_2 \le \varphi(p_2^{\alpha_2}), ..., \lambda_k \le \varphi(p_k^{\alpha_k})$. Агар бу муносабатларнинг бирортасида тенглик бажарилмаса, у ҳолда $\lambda_1 \cdot \lambda_2 \cdots \lambda_k < \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$ бўлади. Лекин $\xi \le \lambda_1 \cdot \lambda_2 \cdots \lambda_k$, шунинг учун $\xi < \varphi(m)$ бўлар эди. Демак, $\lambda_1 = \varphi(p_1^{\alpha_1}), \lambda_2 = \varphi(p_2^{\alpha_2}), ..., \lambda_k = \varphi(p_k^{\alpha_k})$ бўлиши, ва демак, a сони $p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_k^{\alpha_k}$ модулларнинг ҳар бири бўйича бошланғич илдиз бўлиши лозим. Бундан ташқари $\xi = \lambda_1 \cdot \lambda_2 \cdots \lambda_k$, яъни $\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), ..., \varphi(p_k^{\alpha_k})$ сонлар жуфт-жуфт ўзаро туб бўлиши лозим. Лекин иккита ҳар хил p ва q тоқ туб сонлар учун $\varphi(p^{\alpha}) = p^{\alpha-1}(p-1), \varphi(p^{\beta}) = p^{\beta-1}(p-1)$ сонлар жуфт-жуфт ўзаро туб эмас. Демак, m иккита ҳар хил тоқ бўлувчиларга эга бўлиши мумкин эмас, яъни m қуйидаги кўринишга эга бўлиши лозим: $m = 2^{\rho} \cdot p^{\alpha}$. Лекин $\varphi(2^{\rho}) = 2^{\rho-1}$ лигидан $\rho > 1$ бўлганда $2^{\rho-1}$ жуфт, демак, $\varphi(p^{\alpha})$ билан ўзаро туб эмас. Шундай қилиб, m модул бўйича бошланғич илдиз мавжуд бўлиши мумкин, агар у қуйидаги кўринишларга эга бўлса: $m = p^{\alpha}$ ёки $m = 2p^{\alpha}$ ёинки $m = 2^{\rho}$. Охирги ҳол учун $\rho = 1$ ёки $\rho = 2$ бўлиши керак.

Ҳақиқатан, фараз қилайлик $\rho > 2$ ва a-тоқ сон, яъни 2^ρ билан ўзаро туб бўлсин, демак, $a = 4k \pm 1$ кўринишга эга, бу ердан

$$a^{2^{\rho-2}} = 1 \pm 2^\rho k + 2^{\rho+1} N,$$

(бунда N-бирор бутун сон), ёки

$$a^{2^{\rho-2}} \equiv 1 (\mathrm{mod}\ 2^\rho)$$

келиб чиқади. Иккинчи томондан $\varphi(2^\rho) = 2^{\rho-1}$, яъни $2^{\rho-1} = \frac{1}{2}\varphi(2^\rho)$ ва 2^ρ билан ўзаро туб бўлган ҳар қандай a сон учун

$$a^{\frac{1}{2}\varphi(2^\rho)} \equiv 1 (\mathrm{mod}\ 2^\rho),$$

демак, $\rho \geq 3$ бўлганда 2^ρ модул бўйича бошланғич илдиз мавжуд эмас.

Шундай қилиб, биз қуйидаги теоремани исбот қилдик.

83-т е о р е м а. Фақат $m = 2, m = 4, m = p^\alpha$ ва $m = 2p^\alpha$ модуллар учун бошланғич илдизлар мвжуд бўлиши мумкин, бунда p-тоқ туб сон, α-натурал сон.

Энди бу теоремада кўрсатилган модуллар бўйича ҳақиқатан бошланғич илдизнинг мавжудлигини кўрсатамиз.

84-т е о р е м а. р модул бўйича бошланғич илдизлар мавжуд ва уларнинг сони $\varphi(p-1)$ та.

И с б о т. Фараз қилайлик р модул бўйича 1, 2, ..., р-1 қатордаги сонлар бир-биридан фарқли бўлган

$$\delta_1, \delta_2, \ldots \delta_r \quad (\delta_i \neq \delta_j) \qquad (104)$$

кўрсаткичларга тегишли бўлсин. Айтайлик τ сон $\delta_1, \delta_2, \ldots \delta_r$ кўрсаткичларнинг энг кичик умумий карралиси ва $\tau = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ унинг каноник ёйилмаси бўлсин. Б...

ёйилманинг $q_i^{\alpha_i}$ кўпайтувчиси (104)-қатордаги ҳеч бўлмаганда битта δ_j нинг бўлувчиси бўлади. Демак, $\delta_j = aq_i^{\alpha_i}$ танглик бажарилади. Фараз қилайлик ξ_j 1,2,..., $p-1$ сонларнинг бири ҳамда δ_j кўрсаткичга тегишли бўлсин. У ҳолда (81-теоремага кўра) $\eta_j = \xi_j^a$ сон $q_i^{\alpha_i}$ кўрсаткичга тегишли. Демак (82-теоремага кўра) $g = \eta_1\eta_2...\eta_k$ кўпайтма $\tau = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_k^{\alpha_k}$ кўрсаткичга тегишли. Шунинг учун 79-теореманинг натижасига кўра τ сон $p-1$ нинг бўлувчисидир, яъни $\tau \le p-1$. Лекин (104)-кўрсаткичлар τ нинг бўлувчиларини ифодаланганлиги учун, барча 1,2,...,р-1 сонлар (80-теоремага кўра) $x^\tau \equiv 1 (\mathrm{mod}\ p)$ таққосламани қаноатлантиради. Демак, (62-теоремага кўра) $p-1 \le \tau$. Шундай қилиб, $\tau = p-1$, яъни g бошланғич илдиз бўлади. Теорема исботланди.

И з о ҳ. р модул бўйича бошланғич илдизларнинг сони $\varphi(p-1)$ талигини биз 97-теоремада исбот қиламиз.

85-т е о р е м а. Фараз қилайлик р-туб сон бўлсин, у ҳолда p^α модул бўйича бошланғич илдизлар мавжуд. уларнинг сони $\varphi(\varphi(p^\alpha))$ бўлиб, р модул бўйича бошланғич илдизларнинг ҳар бири p^α модул бўйича $\varphi(p^{\alpha-1})$ бошланғич илдизларни беради. р модулни g бошланғич илдизининг ўзи, фақатгина $g^{p-1}-1$ сон p га бўлиниб, p^2 бўлинмаса, p^α модул бўйича бошланғич илдизни беради.

И с б о т. Фараз қилайлик a сон p модул бўйича δ кўрсатгичга тегишли бўлсин, демак, $a^\delta \equiv 1 (\mathrm{mod}\, p)$, яъни $a^\delta = 1 + pN$. Бундан

$$a^{\delta p^{\alpha-1}} = (1+pN)^{p^{\alpha-1}} = 1 + p^\alpha M$$

келиб чиқади, бунда M бутун сон, чунки $(1+pN)^{p^{\alpha-1}}$ нинг Ньютон биноми ёйилмасида, иккинчи ҳаддан бошлаб барчаси p^{α} га бўлинади. Шундай қилиб,

$$a^{\delta p^{\alpha-1}} \equiv 1 (\mathrm{mod}\, p^{\alpha}).$$

Лекин $\delta < p-1$ бўлганда $\delta p^{\alpha-1} < (p-1)p^{\alpha-1} = \varphi(p^{\alpha})$, яъни $\delta < p-1$ бўлса a сон p^{α} модул бўйича бошланғич илдиз бўлмайди. Демак, p^{α} модулнинг бошланғич илдизлари (агар улар мавжуд бўлса) р модул бўйича ҳам бошланғич илдиз бўлишлари шарт.

Фараз қилайлик g сон р модул бўйича бошланғич илдиз бўлсин, у ҳолда

$$g^{p-1} \equiv 1 (\mathrm{mod}\, p),$$

яъни $g^{p-1} = 1 + pN$, бунда N бутун сон. Аввал биз N сон p га бўлинмайдиган ҳолни кўриб чиқамиз, яъни $g^{p-1} - 1$ сон р га бўлиниб, p^2 га бўлинмасин. У ҳолда

$$g^{p(p-1)} = (1+Np)^{p} = 1 + Np^2 + N_1 p^3,$$

бунда N_1 сон (N га ўхшаб) p га бўлинмайди, чунки $(1+Np)^{p}$ нинг Ньютон формуласи бўйича ёйилмасида учинчи ҳаддан бошлаб p^3 га, тўртинчи ҳаддан бошлаб p^4 га бўлинади. Шундай қилиб,

$$g^{p(p-1)} = 1 + N_2 p^2,$$

бунда N_2 бутун сон бўлиб, p га бўлинмайди. Бу тенгликнинг ҳар иккала томонини p-даражага кўтариб, қуйидагини ҳосил қиламиз:

$$g^{p^2(p-1)} = (1+N_2 p^2)^{p} = 1 + N_2 p^3 + N_3 p^5,$$

бунда N_3 бутун сон, шундай қилиб

$$g^{p^2(p-1)} = 1 + N_4 p^3$$

бўлади, бунда N_4 бутун сон бўлиб, p га бўлинмайди ва ҳ.к. шу йўл билан математик индукция методини қўллаб, ушбу умумий формулани чиқарамиз:

$$g^{p^k(p-1)} = 1 + Mp^{k+1}$$

бунда M бутун сон бўлиб, p га бўлинмайди. Ёки

$$g^{p^k(p-1)} \equiv 1 (\mathrm{mod}\ p^{k+1}) \qquad (105)$$

бўлиб, $g^{p^k(p-1)} \equiv 1 (\mathrm{mod} p^l)$ агар $l > k+1$ бўлганда. Фараз қилайлик g сон p^α модул бўйича δ даража кўрсаткичга тегишли бўлсин, яъни $g^\delta \equiv 1 (\mathrm{mod}\, p^\alpha)$, демак, $g^\delta \equiv 1 (\mathrm{mod}\, p)$. Бундан келиб чиқадики, δ сон g нинг p модул бўйича даража кўрсаткичи, яъни $p-1$ га бўлинади. Иккинчи томондан Эйлер теоремасига кўра $g^{p^{\alpha-1}(p-1)} \equiv 1 (\mathrm{mod}\, p^\alpha)$, демак, $p^{\alpha-1}(p-1)$ сон δ га бўлинади. Шундай қилиб, δ қуйидаги кўринишга эга

$$\delta = p^t(p-1), \quad 0 \le t \le \alpha - 1.$$

Агар $t < \alpha - 1$ бўлса эди, у ҳолда

$$g^{p^t(p-1)} \equiv 1 (\mathrm{mod}\ p^\alpha)$$

га эга бўлар эдик, лекин (105)-формулага кўра бу мумкин эмас. Демак, $t = \alpha - 1$ ва g сон p^α модул бўйича бошланғич илдиз.

Энди $g^{p-1} - 1$ сон p^2 га бўлинадиган ҳолни кўриб чиқамиз. Фараз қилайлик $g^{p-1} - 1 = p^2 N$ ёки $g^{p-1} = 1 + p^2 N$ бўлсин, у ҳолда

$$g^{p^{\alpha-2}(p-1)} = (1 + p^2 N)^{p^{\alpha-2}} = 1 + p^\alpha M$$

тенгликка эга бўламиз, бунда M -бутун сон. Демак,

$$g^{p^{\alpha-2}(p-1)} \equiv 1 (\mathrm{mod}\ p^\alpha).$$

Яъни, g сон p^α модул бўйича бошланғич илдиз эмас, чунки у p^α модул бўйича $\le p^{\alpha-2}(p-1) < \varphi(p^\alpha)$ даража кўрсаткичга тегишли. Биз биламизки, агар g сон p модул бўйича бошланғич илдиз бўлса, у ҳолда g билан бир синфда ётувчи $f = g + kp$ (k -ихтиёрий бутун сон) чегирмаларнинг

барчаси p модул бўйича бошланғич илдиз бўлади, яъни улар р модул бўйича ўзаро таққосланади. Лекин p^{α} модул бўйича f ларнинг барчаси ҳам бир-бири билан таққосланмайди: $k = 0,1,\ldots, p^{\alpha-1} - 1$ учун $f = g + kp$ сонлар ўзаро таққосланмайди. k нинг бошқа бутун қийматларида юқоридаги қийматлари билан таққосланади, яъни f нинг p^{α} модул бўйича ўзаро таққосланмайдиган қийматлари $p^{\alpha-1}$ та. Бу қийматларнинг қайсилари p^{α} модул бўйича бошланғич илдиз бўлишини текширамиз. Бунинг учун, қайси ҳолларда $f^{p-1} - 1$ сон р га бўлиниб, p^2 га бўлинмаслигини текшириш керак.

Фараз қилайлик $g^{p-1} - 1 = Np$ бўлсин, у ҳолда

$$f^{p-1} - 1 = (g + kp)^{p-1} - 1 = (g^{p-1} - 1) + p(p-1)\ kg^{p-2} + Lp^2,$$

бунда L-бутун сон, ёки

$$f^{p-1} - 1 = Np + p(p-1)kg^{k-2} + Lp^2.$$

Бу тенгликни ҳар иккала томонини g (юқорида айтганимиздек g сон p га бўлинмайди) га кўпайтирамиз

$$(f^{p-1} - 1)g = Ngp + p(p-1)kg^{p-1} + L \cdot gp^2,$$

лекин $g^{p-1} = 1 + Np$, демак,

$$(f^{p-1} - 1)g = Ngp + p(p-1)k(Np+1) + Lp^2,$$

ёки

$$(f^{p-1} - 1)g = (Ng - k)p + Mp^2 \qquad (106)$$

бунда М-қандайдир бутун сон.

Бу ерда икки ҳолни фарқли равишда қараймиз:

1-ҳ о л. N сон р га бўлинмайди (яъни $g^{p-1} - 1$ сон p^2 га бўлинмайди). (106)-нинг ўнг томони p^2 га бўлинмаслиги учун u=Ng-k сон р га бўлинмаслиги керак. Фараз қилайлик u сон $p^{\alpha-1}$ дан кичик ва р га бўлинмайдиган қийматларни қабул қилсин, бундай қийматлар $\varphi(p^{\alpha-1})=p^{\alpha-2}(p-1)$ та. Бу

қийматлар учун k-нинг мос қийматларини топамиз k=Ng-u; уларни f=g+kp формулага қўямиз ва p^{α} модул бўйича бошланғич илдиз бўлувчи f нинг қийматларини аниқлаймиз, чунки f нинг бу қийматларида $f^{p-1}-1$ сонлар p^2 га бўлинмайди.

2-ҳ о л. Фараз қилайлик энди N сон p га бўлинадиган бўлсин (яъни $g^{p-1}-1$ сон p^2 га бўлинади); бу ҳолда агар k сони p га бўлинмаса, (10б) нинг ўнг томони p^2 га бўлинмайди. Демак,бу ерда биз k га p га бўлинмайдиган ва $p^{\alpha-1}$дан кичик бўлган барча $\varphi(p^{\alpha-1})$ қийматларни берамиз. Бунда f нинг мос қийматлари p^{α} модул бўйича бошланғич илдиз бўлади.

Шундай қилиб, ҳар иккала ҳолда ҳам, p модул бўйича ҳар қандай g бошланғич илдиз p^{α} модул бўйича таққосланмайдиган $\varphi(p^{\alpha-1})$ та бошланғич илдизни беради. p модул бўйича иккита ҳар хил g_1 ва g_2 бошланғич илдизлар p^{α} модул бўйича ҳар хил бошланғич илдизларни беради, чунки $f_1 = g_1 + k_1 p$ ва $f_2 = g_2 + k_2 p$ сонлар ҳатто p модул бўйича таққосланмайди. Шундай қилиб, p^{α} модул бўйича

$$\varphi(p-1)\varphi(p^{\alpha-1}) = \varphi(p^{\alpha-1}(p-1)) = \varphi(\varphi(p^{\alpha}))$$

ҳар хил (p^{α} модул бўйича таққосланмайдиган) бошланғич илдиз мавжуд. Ҳақиқатан, p модул бўйича бошланғич илдизларнинг сони $\varphi(p-1)$ та (84-теоремадан кейинги изоҳга қаранг, буни исботини биз кейинги параграфда келтирамиз) ва уларнинг ҳар бири p^{α} модул бўйича $\varphi(p^{\alpha-1})$ та бошланғич илдизларни беради, шу билан бирга $(p-1, p^{\alpha-1}) = 1$, шунинг учун 36-теоремани қўллаш мумкин. Шу билан теорема тўла исботланди.

1-м и с о л. 27 модул бўйича бошланғич илдизлар топилсин.

Е ч и ш. Бу ерда $p = 3, \alpha = 3, \varphi(27) = 3^2(3-1) = 18, \varphi(18) = 6.$ демак, 27 модул

бўйича 6 та бошланғич илдиз мавжуд. Шу билан бирга $\varphi(p-1)=\varphi(2)=1$ бўлганлиги учун 3 модул бўйича фақат битта бошланғич илдиз мавжуд, у 2 га тенг, $\varphi\left(p^{\alpha-1}\right)=\varphi(9)=6$. Демак, бу 2 бошланғич илдиз 27 модул бўйича 6 та бошланғич илдизларни бериши керак. $g^{\alpha-1}-1=2^2-1=3\cdot 1$ бўлганлиги учун $N=1$ ва y 3 га бўлинмайди, биз бу ерда 1-ҳолга дуч келдик; u га $\varphi(9)=6$ та 9 дан кичик ва у билан ўзаро туб 1, 2, 4, 5, 7, 8 қийматларни берамиз; k нинг қийматларини $k=Ng-u=2-u$ формуладан топамиз: $k=1,0,-2,-3,-5,-6$. Ниҳоят, f нинг қийматларини $f=g+kp=2+3k$ формуладан топамиз:

$$5;2;-4\equiv 23,-7\equiv 20;-13\equiv 14,-16\equiv 11(\mathrm{mod}\,27)$$

ёки

$$2,\ 5,\ 11,\ 14,\ 20,\ 23.$$

2-м и с ол. 49 модул бўйича бошланғич илдизлар топилсин.

Ечиш. Бу ерда $p=7,\alpha=2,\varphi(49)=7\cdot 6=42,\varphi(42)=\varphi(2\cdot 3\cdot 7)=12;$ демак, 12 та бошланғич илдизлар мавжуд; $p^{\alpha-1}=7,\varphi(7)=6$ бўлгани учун 7 модулнинг ҳар бир бошланғич илдизи 49 модулнинг 6 та бошланғич илдизини беради. 7 сон $\varphi(6)=2$ та бошланғич илдизга эга. Осонлик билан текшириб кўриш мумкинки, бу бошланғич илдизлар 3 ва 5 га тенг. Бу ерда $3^6-1=728=7\cdot 104$, N=104 сон 7 га бўлинмайди, яъни 1-ҳолга дуч келдик; k=Ng-u=312-u;u=1,2,3,4,5,6; демак, k=306,307,308,309,310,311 ёки 49 модул бўйича k=12,13,14,15,16,17; f=g+kp=3+7k. Бу ердан биз қуйидаги 6 та бошланғич илдизларни топамиз: $f_1=87\equiv 38, f_2=94\equiv 45$

$f_3=101\equiv 3, f_4=108\equiv 10, f_5=115\equiv 17, f_6=122\equiv 24(\mathrm{mod}\,49)$.

Энди 5 бошланғич илдиз учун $5^6-1=7\cdot 2232;2232$ сон 7 га бўлинмайди, яъни биз яна 1-ҳолга келдик; k=Ng-u=11160-u; u=1, 2, 3, 4, 5, 6; демак, k=11154, 11155, 11156,

11157, 11158, 11159 ёки 49 модул бўйича k=31,32,33,34,35,36; f=g+kp=5+7k. Бу ердан биз қолган 6 та бошланғич илдизларни топамиз:

$$f_7 = 222 \equiv 26, f_8 \equiv 33, f_9 \equiv 40, f_{10} \equiv 47, f_{11} \equiv 5, f_{12} \equiv 12. (\mathrm{mod} 49)$$

86-т е о р е м а. Фараз қилайлик $\alpha \geq 1$ ва g сони p^α модул бўйича бошланғич илдиз бўлсин, у ҳолда g ва $g + p^\alpha$ сонларнинг қайси бири тоқ бўлса, ўшаниси $2p^\alpha$ модул бўйича бошланғич илдиз бўлади. $2p^\alpha$ модул бўйича бошланғич илдизларнинг сони $\varphi(\varphi(2p^\alpha))$ та.

И с б о т. Агар a тоқ сон $a^\delta \equiv 1(\mathrm{mod}\, p^\alpha)$ таққосламани қаноатлантирса, у ҳолда $a^\delta \equiv 1(\mathrm{mod}\, 2)$ ни ҳам ва, демак, $a^\delta \equiv 1(\mathrm{mod}\, 2p^\alpha)$ таққосламани ҳам қаноатлантиради. Шунинг учун $\varphi(p^\alpha) = \varphi(2p^\alpha)$ бўлганлиги сабабли a сон p^α ва $2p^\alpha$ модуллардан бири бўйича бошланғич илдизни ифодалайди. Лекин p^α модул бўйича иккита g ва $g + p^\alpha$ бошланғич илдизлардан бири албатта тоқ бўлади. демак, у $2p^\alpha$ модул бўйича ҳам бошланғич илдиз бўлади. Энди p^α модулнинг ҳар бир тоқ бошланғич илдизи $2p^\alpha$ модул бўйича бошланғич илдиз эканлиги ва $\varphi(\varphi(p^\alpha)) = \varphi(\varphi(2p^\alpha))$ (чунки $\varphi(2) = 1$) тенгликдан теореманинг иккинчи тасдиғи ҳам келиб чиқади. Шу билан теорема исботланди.

3-м и с о л. 98 модул бўйича барча бошланғич илдизлар топилсин.

Е ч и ш. $98 = 2 \cdot 7^2$ бўлганлиги учун 2-мисол натижасидан ва 86-теоремадан фойдаланамиз. Биз кўрганимиздек, 49 модул бўйича бошланғич илдизлар қуйидагилардан иборат: 3,5,10,12,17,19,24,26,33,38,40,45. Буларнинг тоқларини қолдириб, жуфтларига 49 ни қўшамиз, натижада 98 модул бўйича қуйидаги

3, 5, 59, 61, 17, 19, 73, 75, 33, 87, 89, 45

ёки

3, 5, 17, 19, 33, 45, 59, 61, 73, 75, 87, 89

бошланғич илдизлар ҳосил бўлади.

Энди m=2 ва m=4 модулларни текшириш қолди.

1) m=2 бўлганда бу модул билан ўзаро туб бўлган сонларнинг биттагина синфи бор; унинг чегирмаси бир сонидир. Бирни 2 модул бўйича бошланғич илдиз деб қабул қилсак бўлади, чунки $\varphi(2)=1$, яъни $1^{\varphi(2)} \equiv 1(\mathrm{mod}\,2)$.

2) m=4 бўлганда бу модул билан ўзаро туб бўлган синфлар иккита, уларнинг чегирмалари 1 ва 3. Бу ерда $\varphi(4)=2$ ва $3^{\varphi(4)} \equiv 1(\mathrm{mod}\,4)$, демак, 3 сони 4 модул бўйича бошланғич илдиз ва у 4 модул бўйича ягонадир. Шу билан бирга $\varphi(\varphi(4))=\varphi(2)=1$, яъни бу ерда ҳам олдингиларига ўхшаб бошланғич илдизларнинг сони $\varphi(\varphi(4))$ тадир.

Шундай қилиб биз қуйидаги теоремани исбот қилдик.

87-т е о р е м а. m=2 ва m=4 модуллар учун бошланғич илдизлар мавжуд; m=2 учун ягона бошланғич илдиз 1 га тенг, m=4 учун ягона бошланғич илдиз 3 га тенг.

Энди $m=p^{\alpha}$ ва $m=2p^{\alpha}$ (p-тоқ туб сон, $\alpha \geq 1$) модуллар бўйича бошланғич илдизларни топиш учун яна бир умумий теоремани кўриб чиқамиз.

88-т е о р е м а. Фараз қилайлик $q_1, q_2, \ldots q_k$ сонлар $\varphi(m)$ нинг туб бўлувчилари бўлсин; m билан ўзаро туб бўлган g сон m модул бўйича бошланғич илдиз бўлиши учун g сон ушбу

$$g^{\frac{\varphi(m)}{q_1}} \equiv 1(\mathrm{mod}\,m), g^{\frac{\varphi(m)}{q_2}} \equiv 1(\mathrm{mod}\,m), \ldots, g^{\frac{\varphi(m)}{q_k}} \equiv 1(\mathrm{mod}\,m) \quad (107)$$

таққосламаларнинг ҳеч бирини қаноатлантирмаслиги зарур ва кифоядир.

И с б о т. *Зарурлиги.* Агар g бошланғич илдиз бўлса, у ҳолда у $\varphi(m)$ кўрсаткичга тегишли. Демак, (107) таққосламаларнинг ҳеч бирини қаноатлантирмайди.

Кифоялиги. Фараз қилайлик g (107) таққосламаларнинг ҳеч бирини қаноатнлантирмасин. Агар g сон δ кўрсатгичга тегишли ва $\delta < \varphi(m)$ бўлса, у ҳолда q орқали $\frac{\varphi(m)}{\delta}$ ни туб бўлувчиларнинг бирини белгилаб, $\frac{\varphi(m)}{\delta} = qt, \frac{\varphi(m)}{q} = \delta t, g^{\frac{\varphi(m)}{q}} \equiv g^{\delta t} \equiv 1 (\mathrm{mod}\, m)$ ларга эга бўламиз, бу эса бизнинг фаразимизга зид. Демак, $\delta = \varphi(m)$ ва g бошланғич илдиздир.

4-м и с о л. m=37 модул бўйича бошланғич илдизлар топилсин.

Е ч и ш. Бу ерда $\varphi(37) = 36 = 2^2 \cdot 3^2$; $\frac{36}{3} = 12$ ва $\frac{36}{2} = 18$. Демак, 37 га бўлинмйдиган g сон 37 модул бўйича бошланғич илдиз бўлиши учун

$$g^{12} \equiv 1 \ (\mathrm{mod} 37),\ g^{18} \equiv 1 \ (\mathrm{mod} 37)$$

таққосламаларнинг ҳеч бирини қаноатлатирмаслиги зарур ва кифоядир. Биз 2,3,4,5,6 сонларни 37 модул бўйича синаб кўрамиз. Ҳисоблашлар қулай бўлиши учун аввал 2^6, 3^6, 4^6, 5^6, 6^6 ни ҳисоблаб, кейин уларни квадратга ва кубга кўтарамиз:

$2^6 \equiv -10$, $3^6 \equiv -11$, $4^6 \equiv -11$, $5^6 \equiv 11$, $6^6 \equiv -1 (\mathrm{mod} 37)$;

$2^{12} \equiv -11$, $3^{12} \equiv 10$, $4^{12} \equiv 10$, $5^{12} \equiv 10$, $6^{12} \equiv 1 (\mathrm{mod} 37)$;

$2^{18} \equiv -1$, $3^{18} \equiv 1$, $4^{18} \equiv 1$, $5^{18} \equiv -1 (\mathrm{mod} 37)$.

Булардан кўринадики, 2 ва 5 сонлар 37 модул бўйича бошланғич илдиз бўлиб, 3,4, ва 6 бошланғич илдиз эмас, айнан шунга ўхшаш 7, 8,..., 36 сонларни синаб кўрамиз, натижада 37 модул бўйича қуйидаги 12 та бошланғич илдизни ҳосил қиламиз

2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35.

Энди 83-теоремани қуйидагича таърифлаш мумкин.

83*- т е о р е м а. Фақат m=2, m=4, $m=p^{\alpha}$ ва $m=2p^{\alpha}$ модуллар бўйича бошланғич илдизлар мавжуд.

41-§. ИНДЕКСЛАР ВА УЛАРНИНГ ХОССАЛАРИ.

Фараз қилайлик m 83* -теоремадаги модулларнинг бири, яъни $m=2,4,p^{\alpha},2p^{\alpha}$ ва, g сон m модул бўйича бошланғич илдиз бўлсин.

89-т е о р е м а. Агар γ сон $\varphi(m)$ модул бўйича энг кичик манфий бўлмаган $0,1,...,\varphi(m)-1$ чегирмаларнинг қийматини қабул қилса, у ҳолда g^{γ} сонлар m модул бўйича келтирилган чегирмалар системасидаги қийматларни қабул қилади.

И с б о т. Равшанки, g^{γ} сонлар $\varphi(m)$ та қийматларни қабул қилади, улар (79-теоремага кўра) m модул бўйича ўзаро таққосланмайди. Теорема исботланди.

Энди $(a,m)=1$ шартни қаноатлантирадиган a сонлар учун ўрта мактабдан маълум бўлган логарифм тушунчасига ўхшаш, *индекс* тушунчасини киритамиз. Бу ерда бошланғич илдиз логарифлар асосига ўхшаш маънога эга.

23-т а ъ р и ф. Агар

$$a \equiv g^{\gamma} (\mathrm{mod}\, m), \gamma \geq 0$$

бўлса, у ҳолда γ *сон* m *модул бўйича* a *соннинг* g *асосга кўра индекси* дейилади ва у

$$\gamma = ind_{g} a$$

каби белгиланади.

Агар g асос олдиндан берилган бўлса, у ҳолда, логарифмга ўхшаш, a нинг индекси $inda$ каби ёзилади. Юқоридагига асосан (a, m)=1 шартни қаноатлантирадиган a

лар $0,1,...,\varphi(m)-1$ сонлар орасида ягона γ' индексга эга; γ' ни топгандан кейин a нинг қолган барча индексларини кўрсатиш мумкин, 80-теоремага кўра, улар

$$\gamma \equiv \gamma' (\mathrm{mod}\, \varphi(m)) \qquad (108)$$

таққосламани қаноатлантирадиган барча манфий бўлмаган сонлар. Демак, m модул бўйича тузилган ва m билан ўзаро туб бўлган ҳар бир синфга (108) таққослама билан аниқланувчи индекслар тўплами мос келади ва аксинча.

Индекслар қуйидаги хоссаларга эга.

90-т е о р е м а. Ушбу

$$ind(ab..l) = inda + indb + ... + indl (\mathrm{mod}\, \varphi(m)) \qquad (109)$$

ва, хусусий ҳолда,

$$inda^n \equiv n\, inda (\mathrm{mod}\, \varphi(m)) \qquad (110)$$

таққосламалар ўринлидир.

И с б о т. Ҳақиқатан,

$$a \equiv g^{inda} (\mathrm{mod}\, m), b \equiv g^{indb} (\mathrm{mod}\, m), ..., l \equiv g^{indl} (\mathrm{mod}\, m)$$

таққосламаларни кўпайтириб, қуйидагини ҳосил қиламиз:

$$ab...l \equiv g^{inda+indb+..+indl} (\mathrm{mod} m).$$

Бундан индекс таърифига кўра

$$ind\,(ab...l) \equiv inda + indb + ... + indl\ (\mathrm{mod}\ \varphi(m))$$

келиб чиқади; (110)-таққослама эса (109) дан ҳосил бўлади.

91-т е о р е м а. m модул бўйича $\frac{b}{a} (\mathrm{mod}\, m)$ касрнинг индекси, яъни $ax \equiv b (\mathrm{mod}\, m)$ таққослама ечимининг индекси, хусусий ҳолда, агар b сон a га бўлинса оддий $\frac{b}{a}$ бўлинманинг индекси ($\varphi(m)$ модул бўйича) сурат ва махраж индексларининг а йирмаси билан таққосланади.

И с б о т. Бу ерда албатта a ва b лар m модул билан ўзаро туб деб фараз қилинади. Агар $ax \equiv b (\mathrm{mod}\, m)$ бўлса, у ҳолда $(x, m) = 1$ бўлади. 90-теоремага кўра

$inda + indx \equiv indb(\mathrm{mod}\,\varphi(m))$; демак,

$indx \equiv indb - inda(\mathrm{mod}\,m)$. Теорема исбот бўлди.

92-т е о р е м а. Бирнинг индекси нол билан, асос (яъни боланғич илдиз g) нинг ўзи бир билан, -1 (ёки $m-1$) нинг индекси эса $\frac{1}{2}\varphi(m)$ билан таққосланади. Бошқача қилиб айтганда

$$ind1 = 0(\mathrm{mod}\,\varphi(m)), indg \equiv 1(\mathrm{mod}\,\varphi(m)), ind(-1) = ind(m-1) = \frac{1}{2}\varphi(m)(\mathrm{mod}\,m).$$

И с б о т. Дастлабки иккита таққосламалар қуйидагилардан бевосита келиб чиқади:

$$g^0 \equiv 1(\mathrm{mod}\,m), g^1 \equiv g(\mathrm{mod}\,m).$$

Энди учинчисини бошланғич илдиз таърифидан ҳосил қиламиз: $g^{\varphi(m)} \equiv 1(\mathrm{mod}\,m)$ ёки

$$g^{\varphi(m)} - 1 = (g^{\frac{1}{2}\varphi(m)} - 1)(g^{\frac{1}{2}\varphi(m)} + 1) \equiv 0(\mathrm{mod}\,m).$$

Агар $m = p^\alpha$ бўлса, у ҳолда ҳар иккала кўпайтма бир вақтда p га бўлинмайди, чунки у вақтда уларнинг айирмаси 2 ҳам p га бўлинар эди. Демак, уларнинг фақат биттаси p^α га бўлинади. Лекин $g^{\frac{1}{2}\varphi(m)} - 1$ сон p^α га бўлинмайди, чунки p^α модул бўйича бошланғич илдиз g p^α модул бўйича $\varphi(m)$ кўрсаткичга тегишли. Демак,

$$g^{\frac{1}{2}\varphi(m)} + 1 \equiv 0(\mathrm{mod}\,p^\alpha)$$

ёки

$$g^{\frac{1}{2}\varphi(m)} \equiv -1(\mathrm{mod}\,p^\alpha),$$

бу эса

$$\frac{1}{2}\varphi(m) \equiv ind(-1)(\mathrm{mod}\,\varphi(m))$$

лигини кўрсатади.

Агар $m = 2p^{\alpha}$ бўлса, у ҳолда ҳам $g^{\frac{1}{2}\varphi(m)} + 1$ сон p^{α} га бўлинади ва жуфт, чунки g-тоқ, демак, бу ерда ҳам учинчи таққослама ўринли. $m = 4$ бўлганда бевосита текшириш мумкин

$$\frac{1}{2}\varphi(4) = 1,\ g = 3,\ 3^1 \equiv -1 (\mathrm{mod}\, 4).$$

Ниҳоят, агар $m = 2$ бўлса, у ҳолда учинчи таққослама бажарилмайди, чунки $\varphi(2) = 1$, ва $\frac{1}{2}\varphi(2)$ бутун эмас.

93-т е о р е м а. $m = 2$ дан бошқа ҳолларда, m модул бўйича бошланғич илдиз m модул бўйича квадратик ночегирмадир.

И с б о т. Агар a сон m модул бўйича квадратик чегирма бўлса, у ҳолда шундай x бутун сон топиладики $x^2 \equiv a (\mathrm{mod}\, m)$ $((a,m) = 1$ ва $(x,m) = 1)$ таққослама бажарилади. Охирги таққосламани ҳар иккала томонини $\frac{1}{2}\varphi(m)$ даражага кўтариб, қуйидагини ҳосил қиламиз:

$$x^{\varphi(m)} \equiv a^{\frac{1}{2}\varphi(m)} (\mathrm{mod}\, m).$$

Эйлер теоремасига кўра

$$x^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m),$$

демак,

$$x^{\frac{1}{2}\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

Шундай қилиб, a нинг даража кўрсатгичи m модул бўйича $\leq \frac{1}{2}\varphi(m)$, шунинг учун, у m модул бўйича бошланғич илдиз бўла олмайди.

Индекслар таққосламаларни ечишга кенг қўлланилади. Шу сабабли ҳар хил модуллар учун индекслар жадвалини шундай тузиш лозимки ҳар қандай берилган,

модул билан ўзаро туб бўлган сон учун индексларни топиш мумкин бўлсин ва аксинча берилган индексга кўра унга мос келадиган сонни топиш мумкин бўлсин. Индексларнинг бундай жадваллари $p<2000$ туб модуллар учун тузилган. Мазкур китобнинг охирида эса бу жадвалларнинг $p<100$ туб модуллар учун тузилган қисми келтирилган. Ҳар бир модул учун иккита жадвал мавжуд: уларнинг бири (I-Index ҳарфи остида) берилган сон учун унга мос келадиган индексни топишга хизмат қилади; иккинчи қисми (N-Numerus ҳарфи остида) берилган индекс учун унга мос келадиган сонни топишни таъминлайди.

Ҳар бир жадвал тўртбурчак шаклида тузилган бўлиб, унинг биринчи сатрида 0,1,2,...,9 рақамлар турибди; биринчи устунида эса 0,1,2,... рақамлар бор. Берилган соннинг индексини топиш учун, бу соннинг ўнлик хоналарини биринчи устундан ва бирлик хоналарини биринчи сатрдан топамиз. Бу ўнлик ва бирликдан йўналган сатр ва устуннинг кесишган жойида излнаётган индекс туради.

Шунга ўхшаш бурилган индексга кўра сон топилади. Бу жадвалларда мос равишда p ва $\varphi(p)=p-1$ модуллар бўйича сонларнинг манфий бўлмаган энг кичик чегирмалари (келтирилган система) ва уларнинг кичик индекслари (тўла система) кўрсатилган бўлади. Индекслар жадвалида ҳар бир p туб модул бўйича индекслар асоси бўлган g бошланғич илдиз кўрсатилади, g нинг даража кўрсаткичлари изланаётган индексларни беради. Бундан ташқари, жадвалда p модул бўйича барча бошланғич илдизлар ҳам келтирилган.

М и с о л. Биз 40-§ да 2 ва 5 сонлар $p=37$ модул бўйича бошланғич илдизлигини кўрсатган эдик; $g=2$ деб олиб индекслар жадвалини тузамиз (равшанки, $g=5$ деб олсак бу жадвал бошқача бўлади); $p=37$ модул бўйича 2 нинг даражалари қуйидаги кўринишга эга

$2^0 \equiv 1$ $2^7 \equiv 17$ $2^{14} \equiv 30$ $2^{21} \equiv 29$ $2^{28} \equiv 12$ $2^{35} \equiv 19$

$2^1 \equiv 2$ $2^8 \equiv 34$ $2^{15} \equiv 23$ $2^{22} \equiv 21$ $2^{29} \equiv 24$

$2^2 \equiv 4$ $2^9 \equiv 31$ $2^{16} \equiv 9$ $2^{23} \equiv 5$ $2^{30} \equiv 11$

$2^3 \equiv 8$ $2^{10} \equiv 25$ $2^{17} \equiv 18$ $2^{24} \equiv 10$ $2^{31} \equiv 22$

$2^4 \equiv 16$ $2^{11} \equiv 13$ $2^{18} \equiv 36$ $2^{25} \equiv 20$ $2^{32} \equiv 7$

$2^5 \equiv 32$ $2^{12} \equiv 26$ $2^{19} \equiv 35$ $2^{26} \equiv 3$ $2^{33} \equiv 14$

$2^6 \equiv 27$ $2^{13} \equiv 15$ $2^{20} \equiv 33$ $2^{27} \equiv 6$ $2^{34} \equiv 28$

Бу таққосламалар асосида юқорида айтилган жадваллар қуйидагича бўлади

I

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

N

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Бу жадвалдан масалан ind 27ни топиш учун 2-номерли сатри ва 7-номерли устунларнинг кесишган жойидан ind 27 ни, яъни ind 27=6 ни топамиз. Индекси 29 бўлган сонни 2-жадвалдан 2-сатр ва 9-устун кесишган катакда топамиз, яъни 29= ind 24.

Биз юқорида кўрдикки $m = p^\alpha$ ва $m = 2p^\alpha$ модуллар бўйича бошланғич илдизлар мавжуд. Бундай модуллар бўйича индекслар жадвалини тузиш мумкин. Чунки бундай

ҳолда ҳам g бошланғич илдизнинг даражалари m модул бўйича чегирмаларнинг келтирилган системасини ташкил этади.

42-§. ИНДЕКСЛАРНИНГ ТАҚҚОСЛАМАЛАРНИ ЕЧИШГА ҚЎЛЛАНИЛИШИ.

Индекслар жадвалининг қўлланилишини чизиқли тенгламани ечишдан бошлаймиз.

1-м и с о л. Ушбу $27x \equiv 56 (\mathrm{mod}\, 61)$ таққосламанинг ечими топилсин.

Е ч и ш. Бу таққосламанинг ҳар иккала томонини индекслаймиз, натижада индекслар орасидаги муносабатга ўтамиз:

$$ind\, 27 + indx \equiv ind\, 56 (\mathrm{mod}\ 60).$$

китобнинг охиридаги жадвалдан (I ҳарфи остидаги) ind 27=6, ind56=44 ларни топамиз, демак,

$$6 + indx \equiv 44 (\mathrm{mod}\ 60)$$

ёки

$$indx \equiv 38 (\mathrm{mod}\, 60).$$

ўнг томондаги жадвал (N ҳарфи остидаги) дан $x \equiv 45 (\mathrm{mod}\, 61)$ ни топамиз.

2-м и с о л. Ушбу $7x \equiv -12 (\mathrm{mod}\, 41)$ таққосламанинг ечими топилсин.

Е ч и ш. Биз аввал $-12 \equiv 29 (\mathrm{mod}\, 41)$ алмаштиришни бажарамиз, натижада

$$7x \equiv 29 (\mathrm{mod}\, 41)$$

бўлади. Индексларга ўтсак

$$ind\, 7 + indx \equiv ind\, 29 (\mathrm{mod}\, 40)$$

ёки

$$39 + indx \equiv 7 (\mathrm{mod}\, 40),$$

$$indx \equiv -32 \equiv 8 (\mathrm{mod}\, 40),$$

$$x \equiv 10 (\mathrm{mod}\, 41)$$

ҳосил бўлади.

Фараз қилайлик,

$$x^n \equiv a(\mathrm{mod}\, m) \qquad (111)$$

таққосламада $(n, \varphi(m)) = d$ бўлсин.

94-т е о р е м а. (111)-таққослама ечимга эга (демак, a сон m модул бўйича n-даражали чегирма) бўлиши учун $\mathrm{ind}\, a$ нинг d га бўлиниши зарур ва кифоядир. Агар таққослама ечимга эга бўлса, у ҳолда ечимларнинг сони d та бўлади.

И с б о т. Ҳақиқатан, (111)-таққосламани ҳар иккала томонини индекслаб, қуйидаги унга тенг кучли бўлган

$$n\ ind x \equiv ind a(\mathrm{mod}\, \varphi(m)) \qquad (112)$$

таққосламага эга бўламиз. 59-теоремага асосан (112)-таққослама ечимга эга бўлиши учун $\mathrm{ind}\, a$ нинг d га бўлиниши зарур ва кифоядир. Агар (112)-таққослама ечимга эга бўлса, у ҳолда indx нинг $\varphi(m)$ модул бўйича таққосланмайдиган d та қиймати мос келади. Шу билан теорема исботланди.

95-т е о р е м а. 94-теореманинг шартлари бажарилсин, у ҳолда m модул бўйича чегирмаларнинг келтирилган системасида d-даражали чегирмаларнинг сони $\dfrac{\varphi(m)}{d}$ га тенг.

И с б о т. m модул бўйича келтирилган система чегирмаларининг энг кичиклари бўлган $0,1,\ldots,\varphi(m)-1$ сонлар орасида $\dfrac{\varphi(m)}{d}$ таси d га каррали. Теорема исботланди.

И з о ҳ. 94-теоремадаги тасдиқларни

$$a_1 x^n \equiv b_1(\mathrm{mod}\, m) \qquad (113)$$

таққослама учун ҳам айтиш мумкин.

Бунинг учун (113)-таққосламани ҳар иккала томонини индекслаймиз

$$inda_1 + n\ indx \equiv indb_1 (\mathrm{mod}\,\varphi(m)).$$

Энди $inda = indb_1 - inda_1$ деб олиб, 94-теоремани қўллаймиз.

3-м и с о л. Ушбу

$$x^{16} \equiv 35(\mathrm{mod}\,37) \qquad (114)$$

таққослама учун (16, 36)=4 бўлиб, ind35=10 эса 4 га бўлинмайди. Шунинг учун (114)-таққослама ечимга эга эмас.

4-м и с о л. Ушбу

$$x^{22} \equiv 28(\mathrm{mod}\,37) \qquad (115)$$

таққослама учун (22, 36)=2 бўлиб, ind28=34 сон 2 га бўлинади. Шунинг учун (115)-таққослама ечилади ва унинг ечими 2 та. Бу ечимларни қуйидагича топамиз:

$$22indx \equiv 34(\mathrm{mod}\,36), \quad \text{ёки} \quad 11indx \equiv 17(\mathrm{mod}\,18),$$

бундан $indx \equiv 13(\mathrm{mod}\,18)$ ва indx нинг 36 модул бўйича таққосланмайдиган иккита ечимини аниқлаймиз

$$indx = 13;\ 31.$$

Индекслар жадвалидан (115)-таққослама учун қуйидаги иккита ечимни ҳосил қиламиз

$$x \equiv 15;\ 22(\mathrm{mod}\,37).$$

5-м и с о л. Ушбу

$$7x^5 \equiv 15(\mathrm{mod}\,37) \qquad (116)$$

таққосланинг ечимини топиш учун уни ҳар иккала томонини индекслаймиз

$$ind7 + 5indx \equiv ind15(\mathrm{mod}\,36),$$

бундан

$$5indx \equiv ind15 - ind7 \equiv 13 - 32 \equiv 17(\mathrm{mod}\,36)$$

келиб чиқади, бу ерда (5, 36)=1 бўлганлиги учун бу таққослама ягона

$$indx \equiv 25(\mathrm{mod}\,36)$$

ечимга эга. Бундан $x \equiv 20(\mathrm{mod}\,37)$ келиб чиқади.

6-м и с о л. Индекслари 3 га бўлинадиган

1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36 (117)

сонлар 37 модул бўйича энг кичик мусбат чегирмалар орасида кубик чегирмаларни ташкил этади. (117)-қатордаги сонлар $\frac{\varphi(m)}{d}=\frac{\varphi(37)}{3}=\frac{36}{3}=12$ тадир.

96-т е о р е м а. a нинг m модул билан δ кўрсатгичга тегишли бўлиши $(inda,\varphi(m))=\frac{\varphi(m)}{\delta}$ тенглик билан аниқланади; хусусий ҳолда, a нинг m модул бўйича бошланғич илдиз бўлиши $(inda,\varphi(m))=1$ шарт билан аниқланади.

И с б о т. Ҳақиқатан, δ сон $a^{\delta}\equiv 1(\mathrm{mod}\, m)$ шартни қаноатлантирувчи $\varphi(m)$ нинг энг кичик бўлувчиси бўлсин. Бу шарт эса қуйидаги:

$$\delta\ ind\ a\equiv 0(\mathrm{mod}\ \varphi(m))$$

ёки

$$ind\ a\equiv 0\left(\mathrm{mod}\frac{\varphi(m)}{\delta}\right).$$

га тенг кучлидир.

Демак, δ сон $\varphi(m)$ нинг шундай энг кичик бўлувчисики, бунда $\mathrm{ind}\,a$ сон $\frac{\varphi(m)}{\delta}$ га бўлинади. Шундай қилиб, $\frac{\varphi(m)}{\delta}$ сон $\varphi(m)$ нинг энг катта бўлувчиси ва шунинг билан бирга, $\mathrm{ind}\,a$ нинг ҳам бўлувчисидир. Демак, $\frac{\varphi(m)}{\delta}=(inda,\varphi(m))$. Хусусий ҳол $\delta=\varphi(m)$ бўлганда келиб чиқади. Теорема исботланди.

97-т е о р е м а. m модул бўйича келтирилган системада δ кўрсаткичга тегишли бўлган чегирмаларнинг

сони $\varphi(\delta)$; хусусий ҳолда, m модул бўйича бошланғич илдизларнинг сони $\varphi(\varphi(m))$ тадир.

И с б о т. m модул бўйича чегирмаларнинг келтирилган системасида энг кичиклари бўлган $0,1,...,\varphi(m)-1$ сонлар орасида $\frac{\varphi(m)}{\delta}$ га бўлинадиганлари $\frac{\varphi(m)}{\delta}t$ кўринишга эга, бу ерда $t=0,1,...,\delta-1$; $\left(\frac{\varphi(m)}{\delta}t,\varphi(m)\right)=\frac{\varphi(m)}{\delta}$ шарт $(t,\delta)=1$ шарт билан тенг кучли бўлиб, охирги шартни t нинг $\varphi(\delta)$ қиймати қаноатлантиради. Энди теореманинг исботи 96-теоремадан, хусусий ҳол эса $\delta=\varphi(m)$ бўлганда келиб чиқади.

И з о ҳ. Теореманинг хусусий ҳолидаги тасдиқни $m=2,4,p^{\alpha}$ *ва* $2p^{\alpha}$ $(\alpha>1)$ модуллар учун 85, 86, 87-теоремада ҳам келтирган эдик. Ҳозирги исбот у ердагидан фарқлидир.

7-м и с о л. 37 модул бўйича чегирмаларнинг келтирилган системасида 12 кўрсаткичга тегишли a сонлар $(inda,36)=\frac{36}{12}=3$ шартни қаноатлантирувчи сонлар ($\mathrm{ind}\,a$=3, 15, 21, 33), яъни a=8, 23, 29, 14 сонлардан иборат. Уларнинг сони $\varphi(\delta)=\varphi(12)=4$ та.

8-м и с о л. 37 модул бўйича чегирмаларнинг келтирилган системасида бошланғич илдизлар ($\mathrm{ind}\,a$, 36)=1 шартни қаноатлантирувчи ($\mathrm{ind}\,a$=1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35) a сонлардан, яъни

2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35 (118)

сонлардан иборат. (118)-қатордаги сонлар $\varphi(\varphi(\delta))=\varphi(36)=12$ тадир.

Биз 87-теоремада кўрдикки, $m=2$ ва $m=4$ модулар учун бошланғич илдизлар мавжуд ва 83-теоремада кўрган эдикки, $\alpha \geq 3$ бўлганда $m=2^{\alpha}$ модул бўйича бошанғич илдиз мавжуд эмас. Аниқроқ қилиб айтганда 2^{α} модул бўйича x тоқ соннинг тегишли бўлган даража кўрсаткичи $2^{\alpha-2}=\frac{1}{2}\varphi\left(2^{\alpha}\right)$ дан ошмайди.

Ҳақиқатан,

$$x=1+2t_0,$$

$$x^2=1+4t_0+4t_0^2=1+4t_0(t_0+1)=1+8t_1,$$

$$x^4=1+16t_2,$$

....

$$x^{2^{\alpha-2}}=1+2^{\alpha}t_{\alpha-2}\equiv 1(\mathrm{mod}\ 2^{\alpha}).$$

Таъкидлаймизки, 2^{α} модул бўйича $2^{\alpha-2}$ даражага тегишли бўлган сонлар мавжуд, масалан, 5 сони. Ҳақиқатан,

$$5=1+2^2,$$

$$5^2=1+2^3+2^4,$$

$$5^4=1+2^4+2^5U_2,$$

.....

$$5^{2^{\alpha-2}}=1+2^{\alpha}+2^{\alpha+1}U_{\alpha-2}.$$

Бу ердан кўринадики, $5^0,5^1,5^2,\ldots,5^{2^{\alpha-2}-1}$ сонлар бир-бири билан 2^{α} модул бўйича таққосланмайди.

Ушбу

$$5^0,5^1,\ldots,5^{2^{\alpha-2}-1}$$

$$-5^0,-5^1,\ldots,-5^{2^{\alpha-2}-1}$$

қаторлардаги сонлар 2^{α} модул бўйича келтирилган системани ташкил этади. Ҳақиқатан, бу сонлар

$2 \cdot 2^{\alpha-2} = \varphi(2^{\alpha})$; та ва ҳар бир алоҳида олинган қатордаги сонлар 2^{α} модул бўйича ўзаро таққосланмайди; биринчи қатордаги сонлар иккинчи қатордаги сонлар билан ўзаро таққосланмайди, чунки 5^{λ} сонлар $4k+1$ кўринишга, -5^{μ} сонлар эса $4m+3$ кўринишга эга, демак, улар ҳатто 4 модул бўйича ҳам таққосланмайди.

Шундай қилиб, қуйидаги теоремани исботладик.

98-т е о р е м а. Фараз қилайлик $\alpha = 0$ ёки $\alpha = 1$ бўлганда c=0, c_0=1 бўлиб, $\alpha \geq 2$ бўлганда эса $c = 2, c_0 = 2^{\alpha-2}$ бўлсин (демак, ҳар доим $cc_0 = \varphi(2^{\alpha})$) яна γ ва γ_0 сонлар бир-биридан мустасно равишда с ва c_0 модуллар бўйича манфий бўлмаган энг кичик

$$\gamma = 0,1,...,c-1;\ \gamma_0 = 0,1,...,c_0 - 1$$

чегирмаларга тенг қийматларни қабул қилсин. У ҳолда $(-1)^{\gamma} 5^{\gamma_0}$ сонлар 2^{α} модул бўйича келтирилган системанинг чегирмаларига тенг қийматларни қабул қилади.

Энди қуйидаги теоремани исбот қиламиз.

99-т е о р е м а. Ушбу

$$(-1)^{\gamma} 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma_0'} \pmod{2^{\alpha}} \qquad (118)$$

таққослама бажарилиши учун

$$\gamma \equiv \gamma' \pmod{c}, \gamma_0 \equiv \gamma_0' \pmod{c_0}$$

таққосламалар ўринли бўлиши зарур ва кифоядир.

И с б о т. Ҳақиқатан, $\alpha = 0$ ҳолда теорема ўз ўзидан равшан. Шунинг учун $\alpha > 0$ ҳолни кўрамиз. Фараз қилайлик с ва c_0 модуллар бўйича γ ва γ_0 сонларнинг энг кичик манфий бўлмаган чегирмалари r ва r_0 бўлсин, γ' ва γ_0' сонлар учун эса r' ва r_0' бўлсин. Юқорида айтганимиздек –1 сони с даража кўрсаткичга ва 5 сони c_0 даража кўрсаткичга тегишли. 80-теоремага кўра (118)-таққослама ўринли бўлиши

учун $(-1)^{\gamma} 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma_0'} (\mathrm{mod}\, 2^{\alpha})$ таққослама ўринли бўлиш зарур ва кифоядир, яъни 98-теоремага кўра $r = r'$ ва $r_0 = r_0'$ бўлиши зарур ва кифоядир. Шу билан теорема исботланди.

24-т а ъ р и ф. Агар

$$a \equiv (-1)^{\gamma} 5^{\gamma_0} (\mathrm{mod}\, 2^{\alpha})$$

бўлса, у ҳолда γ, γ_0 система 2^{α} *модул бўйича* a *соннинг индекслар сиситемаси* дейилади.

Фараз қилайлик m нинг каноник ёйилмаси $m = 2^{\alpha} p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ бўлиб, с ва c_0 сонлар 98-теоремада кўрсатилган қийматларни қабул қилсин ва g_t сон $p_t^{\alpha_t}$ модул бўйича энг кичик бошланғич илдиз бўлсин.

25-т а ъ р и ф. Агар

$$\left.\begin{aligned} &a \equiv (-1)^{\gamma} 5^{\gamma_0} (\mathrm{mod}\, 2^{\alpha}), \\ &a \equiv g_1^{\gamma_1} (\mathrm{mod}\, p_1^{\alpha_1}), \ldots, a \equiv g_k^{\gamma_k} (\mathrm{mod}\, p_k^{\alpha_k}) \end{aligned}\right\} \qquad (119)$$

таққосламалар бажарилса, у ҳолда $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_k$ система m *модул бўйича* a *соннинг индекслар системаси* дейилади.

Бу таърифдан γ, γ_0 система 2^{α} модул бўйича a нинг индекслар системаси $\gamma_1, \gamma_2, \ldots, \gamma_k$ эса $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$ модуллар бўйича a соннинг индекслари эканликлари келиб чиқади. Шунинг учун 23- ва 24-таърифларга кўра m модул билан ўзаро туб бўлган ҳар қандай a сон $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_k$ лардан тузилган $c \cdot c_0 \cdot c_1 \cdots c_k = \varphi(m)$ та чегирмалар орасида $\gamma', \gamma_0', \gamma_1', \ldots, \gamma_k'$ дан иборат ягона индекслар системасига эга. Шу билан бирга, юқоридаги $\varphi(m)$ та система $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_k$ ларнинг ҳар бири айрим-айрим $c, c_0, c_1, \ldots, c_k$ модуллар бўйича манфий бўлмаган энг кичик

чегирмаларга тенг қийматларни қабул қилиши натижасида ҳосил бўлади; a нинг барча индекслар системаси эса ушбу

$\gamma \equiv \gamma'(\mathrm{mod}\, c), \gamma_0 \equiv \gamma_0'(\mathrm{mod}\, c_0), \gamma_1 \equiv \gamma_1'(\mathrm{mod}\, p_1^{\alpha_1}), \ldots, \gamma_k \equiv \gamma_k'(\mathrm{mod}\, p_k^{\alpha_k})$

синфларнинг манфий бўлмаган сонларидан тузилган барча $\gamma_0, \gamma_1, \ldots, \gamma_k$ системалардан иборат. Берилган $\gamma_0, \gamma_1, \ldots, \gamma_k$ индекслар системасига эга бўлган a сонлар (119)-системани ечиш натижасида топилиши мумкин. Демак, улар сонларнинг m модул бўйича синфини ташкил этадилар.

8-БОБ УЧУН МАШҚЛАР

1. Куйидаги модуллар бўйича бошланғич илдизлар топилсин:
   1) 13, 2) 19, 3) 169, 4) 361, 5) 338, 6) 722.
2. Куйидаги модуллар бўйича келтирилган системалардаги сонларнинг қайси даража кўрсаткичларга тегишлилиги аниқлансин:
   1) 7, 2) 11, 3) 13.
3. 242 модул бўйича энг кичик бошланғич илдиз топилсин.
4. 29 модул бўйича индекслар жадвалини тузинг.
5. Индекслар жадвалидан фойдаланиб,
$1) x^{68} \equiv 83(\mathrm{mod}\, 97),\ 2) x^{55} \equiv 19(\mathrm{mod}\, 97), 3) x^{18} \equiv 40(\mathrm{mod}\, 97)$
таққосламаларнинг ечимлари сони аниқлансин.
6. Индекслар жадвалидан фойдаланиб,
$1) x^2 \equiv 61(\mathrm{mod}\, 67),\ 2) x^{33} \equiv 19(\mathrm{mod}\, 67),\ 3) x^{46} \equiv 14(\mathrm{mod}\, 67)$
таққосламаларни ечинг.
7. Индекслар жадвалидан фойдаланиб,
$1) 3x^{18} \equiv 31(\mathrm{mod}\, 37),\ 2) 5x^{12} \equiv 11(\mathrm{mod}\, 37), 3) 3x^{40} \equiv 31(\mathrm{mod}\, 37)$
таққосламалар ечилсин.
8. Индекслар жадвалидан фойдаланиб, 23 модул бўйича чегирмаларнинг келтирилган системаси орасида 1) квадратик чегирмаларни, 2) кубик чегирмаларни кўрсатинг.
9. 37 модул бўйича келтирилган чегирмалар орасида 1) 15-даражали чегирмаларни, 2) 8-даражали чегирмаларни кўрсатинг.

7- ва 8- бобларга доир тарихий маълумот

1. Эйлерни ҳақли равишда «даражали чегирмаларнинг яратувчиси» дейишлари бежиз эмас. Чунки даражали чегрималар назарияси Эйлернинг «Даражаларни бўлиш натижасида ҳосил бўладиган чегирмалар ҳақидаги теорема» номли мақоласи асосида келиб чиққан ва квадратик чегирмалар ҳақидаги «ўзаролик қонуни» ни ҳам Эйлер очган. Бу қонунни Гаусс «асосий теорема» («theorema fundamentale») деб айтган эди. Бу қонунни олдин Лежандр очган деб юришар эди. Ўзаролик қонунни эмперик равишда Эйлер 1772 йилда топган бўлиб, 1783 йилда чоп этилган 2 жилдлик «Аналитик асарлар» нинг 1-жилдида, исботсиз, яълон қилинган эди.

2. Ўзаролик қонунни биринчи тўла исботини Гаусс 1796 йилда 19 ёшида берган ва бошқа, иккинчи исботи билан 1801 йилда «Арифметик тадқиқотлар» да эълон қилинган. Кейинчалик Гаусс бу қонунни яна олтита исботини топган. Шунинг учун *«квадратик чегирмаларнинг ўзаролик қонуни»* ни *Гаусс қонуни* ҳам дейишади. 19-асрда ўзаролик қонуннинг 50 дан ортиқ ҳар хил исботи топилган, ҳозирги вақтда бундан ҳам ортиқ.

3. Кубик ва биквадратик чегирмалар учун ўзаролик қонуннинг исботи К.Якобининг 1836-1837 йилларда Кёнигсберг университетида ўқиган маърузаларида келтирилган, лекин, ҳатто бу ҳол учун ҳам, бу қонуннинг таърифлаш жуда мураккаб.

4. 71-теореманинг натижаси шуни кўрсатадики 1 дан p-1 гача бўлган сонлар орасида p модул бўйича квадратик чегирмаларнинг сони бу сонларнинг ярмига, яъни $\frac{p-1}{2}$ га тенг. Табиий равишда савол туғилади: агар Q<p-1 бўлса, у ҳолда p модул бўйича 1 дан Q гача бўлган сонлар орасида

квадратик чегирма ва квадратик ночегирмалар қандай тақсимланган.

1918 йилда сонлар назариясининг йирик мутахассиси, жаҳондаги Академияларни кўпларининг аъзоси И.М.Виноградов ва венгер математиги Д.Пойа бир-бирига боғлиқ бўлмаган ҳолда қуйидаги теоремани исбот қилишди.

Теорема (Виноградов-Пойа теоремаси). R орқали p модул бўйича 1,2,...,Q сонлар орасидаги квадратик чегирмаларни белгилаймиз. У ҳолда

$$R = \frac{1}{2}Q + \theta\sqrt{p}\ln p,\ |\theta| < 1.$$

Бу теоремадан кўрамизки, агар Q сони $\sqrt{p}\ln p$ дан катта бўлса, у ҳолда 1 дан Q гача бўлган сонларнинг тақрибан ярими p туб модул бўйича квадратик чегирма бўлади.

Шунга ўхшаш теоремани n-даражали чегирма учун ҳам И.М.Виноградов исбот қилган.

5. Гаусс «Арифметик тадқиқотлар» да 3 дан 97 гача бўлган туб сонлар ва уларнинг даражалари учун индекслар жадвалини келтирган ва асос учун бошланғич илдиз кўрсатилган.

6. Немис математиги Якоби (Jacobi, Карл Густав Яков, 1804-1851) 1839 йилда чоп этилган «Canon Arithmeticos» асарида 1000 дан кичик бўлган туб сонлар учун индекслар жадвалини тузган.

9- БОБ. ТАҚҚОСЛАМАЛАР НАЗАРИЯСИНИНГ АРИФМЕТИКАГА ТАДБИҚЛАРИ

43-§. БЎЛИНИШ АЛОМАТЛАРИ

Бўлиниш аломатларини текшириш масаласи қуйидагидан иборат. Фараз қилайлик N берилган натурал сон бўлиб, m унинг берилган (натурал) бўлувчиси бўлсин; шундай $f(N)$ арифметик функцияни тузиш керакки, у қуйидаги шартларни қаноатлантирсин:

1) N ва $f(N)$ бир вақтда m га бўлинади ёки бўлинмайди;

2) N етарлича кичик бўлган ҳоллардан ташқари $|f(N)| < N$;

3) Берилган N учун $f(N)$ озми-кўпми осонроқ ҳисобланади.

Агар N сон m га бўлинишини билиш керак бўлса, $f(N)$ ни ҳисобланади, агар бордию $|f(N)|$ жуда ҳам катта сон бўлса, у ҳолда $f(|f(N)|)$ ни ҳисобланади ва х.к. бу жараён N соннинг m га бўлинишини бевосита текшириш мумкин бўлган, етарлича кичик сон ҳосил қилингунга қадар давом эттирилади.

Шуни таъкидлаш керакки, $m = p^{\alpha}$ га бўлиниш аломатини топиш етарли, чунки N сон $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ га бўлиниши учун $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ га бўлиниши зарур ва кифоядир. $f(N)$ функцияни тузиш усулини француз математиги Б. Паскал (1623-1662) топган эди.

1. *Паскал усули.* Хар бир N натурал сонни ўнлик саноқ системасига ёйиш мумкин

$$N = a_0 + a_1 10 + a_2 10^2 + ... + a_n 10^n,$$

бунда $a_0, a_1, a_2, ..., a_n$ ўнлик рақамлар.

Бу ерда $M = f(N)$ни тузиш учун 10^kни m модул бўйича абсолют қиймати билан энг кичик чегирма r_k га алмаштириш натижасида

$$f(N) = a_0 + a_1 r_1 + a_2 r_2 + ... + a_n r_n;$$

$$N \equiv a_0 + a_1 r_1 + a_2 r_2 + ... + a_n r_n (\mathrm{mod}\, m)$$

ҳосил бўлади. Шундай қилиб, қўйидагига эга бўлдик

$$M = f(N) \equiv N (\mathrm{mod}\, m).$$

Энди биз бу умумий усулнинг хусусий ҳолларини кўриб чиқамиз.

1. $m = 2$ бўлсин. Бунда $r_k = 0 \quad (k = 1,2,...)$; демак, $N \equiv a_0 (\mathrm{mod}\, 2)$; бу иккига бўлинишнинг маълум аломати.

2. $m = 3$ бўлсин. Бунда $r_k = 1 \quad (k = 1,2,...)$, чунки $10 \equiv 1 (\mathrm{mod}\, 3)$ демак, $N \equiv a_0 + a_1 + ... + a_n (\mathrm{mod}\, 3)$, бу ҳам 3 га бўлинишнинг маълум аломати.

3. $m = 7$ бўлсин. Бунда $r_1 = 3, r_2 = 2, r_3 = -1, r_4 = -3, r_5 = -2, r_6 = 1, r_7 = 3, r_8 = 2$ ва ҳ.к. даврий равишда давом этади. Демак,

$$N \equiv (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + ... (\mathrm{mod}\, 7).$$

М и с о л л а р:

1. $\underline{25}\,\underline{613}$ сон 7 га бўлинади чунки $(3 + 3 \cdot 1 + 2 \cdot 6) - (5 + 3 \cdot 2) = 7$, яъни M сон 7 га бўлинади.

2. $\underline{5}\,\underline{065}\,\underline{788}$ сон 7 га бўлинади, чунки $(8 + 3 \cdot 8 + 2 \cdot 7) - (5 + 3 \cdot 6 + 2 \cdot 0) + 5 = 28$ сон 7 га бўлинади.

3. $\underline{8}\,\underline{134}\,\underline{165}$ сонни 7 га бўлганда ҳосил бўлган қолдиқни топинг.

Ечиш: $M=(5+3\cdot 6+2\cdot 1)-(4+3\cdot 3+2\cdot 1)+8=18\equiv 4(\mathrm{mod}\,7)$. Демак, қолдиқ 4 га тенг.

4. $m=9$ бўлсин. Бунда $10\equiv 1(\mathrm{mod}\,9)$ бўлганлиги учун барча $r_k=1$. Демак, $N=a_1+a_2+\ldots+a_n(\mathrm{mod}\,9)$ бу аломат 3 га бўлиниш аломатига ўхшайди, яъни берилган сонни рақамларининг йиғиндиси 9 га бўлиниши керак.

5. $m=11$ бўлсин. У ҳолда $10\equiv -1(\mathrm{mod}\,11)$. Демак, $10^k\equiv(-1)^k(\mathrm{mod}\,11)$ ва $M=(a_0+a_2+a_4+\ldots)-(a_1+a_3+a_5+\ldots)$ тенглик бажарилади. Демак, M сон 11 га бўлинса, у ҳолда N ҳам 11 га бўлинади, агар M ни 11 га бўлганда қолдиқ r бўлса, у ҳолда N ни 11 га бўлганда ҳам қолдиқ r бўлади.

М и с о л: $N=79924251$ бўлсин, бу сон 11 га бўлинади, чунки $M=(1+2+2+9)-(5+4+9+7)=-11$ сон 11 га бўлинади.

2. *Сонларни бўлинишининг бошқа аломатлари.*

Фараз қилайлик $(10,m)=1$ бўлиб 10 сони m модул буйича δ кўрсаткичга тегишли бўлсин. У ҳолда $r_\delta\equiv 10^\delta\equiv 1(\mathrm{mod}\,m)$ дан бошлаб, қолдиқлар такрорланади: $r_j=r_{\delta+j}$. Шунинг учун

$$M=f(N)=a_0+a_1r_1+\ldots+a_{\delta-1}r_{\delta-1}+r_\delta+a_{\delta+1}r_1+a_{\delta+2}r_2+\ldots=$$
$$=(a_0+a_\delta+\ldots)+(a_1+a_{\delta+1}+\ldots)r_1+\ldots+(a_{\delta-1}+a_{2\delta-1}+\ldots)r_{\delta-1}.$$

Юқорида биз кўрган эдикки 10 сони 3 ва 9 модуллар бўйича 1 кўрсаткичга ва 11 модул бўйича 2 кўрсатгичга тегишли бўлади. Шунинг учун бу ҳолларда қолдиқлар мос равишда r_1 ва r_2 дан бошлаб такрорланади.

Паскал усулини на фақат 10-ли система учун, балки ихтиёрий q асосли саноқ системаси учун ҳам қараш мумкин.

Агар m модул бўйича 10 сони δ кўрсатгичга тегишли бўлса, у ҳолда 10^δ асосли саноқ системасида қуйидагиларга эга бўламиз:

$$N = A_0 + A_1 10^{\delta} + ... + A_n (10^{\delta})^n,$$

$$10^{\delta} \equiv 1(\mathrm{mod}\, m), 10^{2\delta} \equiv 1(\mathrm{mod}\, m), ..., 10^{n\delta} \equiv 1(\mathrm{mod}\, m),$$

$$N \equiv A_0 + A_1 + ... + A_n (\mathrm{mod}\, m),$$

бунда $A_0, A_1, ..., A_n$ сонлар N соннинг ўнлик саноқ системасида рақамларини ўнг томондан бошлаб δ тадан ажратиш натижасида ҳосил бўлган δ - хонали рақамлар.

3. Хусусий ҳоллар. а) 11 га булинишнинг янги аломати.

Бунда δ=2 деб олиб N сонни юзлик саноқ системасида тасвирлаймиз:

$$N = A_0 + A_1 100 + A_2 \cdot 100^2 + ... + A_n 100^n,$$

бунда A_i «рақамлар» 1 дан 99 гача қийматларни қабул қилади. Бунда $100 \equiv 1(\mathrm{mod}11)$ ва $100^k \equiv 1(\mathrm{mod}11)$ бўлганлиги учун

$$N \equiv A_0 + A_1 + A_2 + ... + A_n (\mathrm{mod}11)$$

таққослама ўринли бўлади. Бу аломат 3 ва 9 га бўлиниш аломатига ўхшайди.

М и с о л.

а) $N = \underline{5}\,\underline{71}\,\underline{89}\,\underline{35}\,\underline{41}$ сон учун

$$N \equiv 41 + 35 + 89 + 71 + 5 \equiv -3 + 2 + 1 + 5 + 5 = 10(\mathrm{mod}11).$$

Демак, N ни 11га бўлганда 10 қолдиқ қолади.

б) $N = \underline{85}\,\underline{32}\,\underline{13}\,\underline{45}\,\underline{67}$ учун

$$N \equiv 67 + 45 + 13 + 32 + 85 \equiv 1 + 1 + 2 - 1 - 3 = 0(\mathrm{mod}11).$$

Демак N сони 11 га бўлинади

2. $m = 37$ бўлсин. Бунда 10 сони 37 модул ўйича 3 кўрсаткичга тегишли, чунки $10 \equiv 10$; $10^2 \equiv 26$; $10^3 \equiv 1(\mathrm{mod}37)$. Шунинг учун ҳам N сонни минглик саноқ системасида тасвирласак

$$N = A_0 + A_1 1000 + ... + A_n \cdot 1000^n,$$

у ҳолда

$$N \equiv A_0 + A_1 + ... + A_n (\mathrm{mod}\, 37).$$

М и с о л. N=9 751 432 521 сон учун $N \equiv 521 + 432 + 751 + 9 \equiv 11(\mathrm{mod}\, 37)$, яъни берилган N сонни 37 га бўлганда 11қолдиқ қолади. Ниҳоят, $10^3 \equiv -1(\mathrm{mod}\, 7)$ ва $10^3 \equiv -1(\mathrm{mod}\, 13)$ бўлганлиги учун минглик саноқ системасида қўйидагиларга эга бўламиз:

$$N \equiv A_0 - A_1 + A_2 - ....(\mathrm{mod}\, 7),$$

$$N \equiv A_0 - A_1 + A_2 - ....(\mathrm{mod}\, 13).$$

М и с о л. $N = 221\,725$ учун

$$N \equiv 725 - 221 = 504 \equiv 0(\mathrm{mod}\, 7),$$

$$N \equiv 725 - 221 = 504 \equiv 10(\mathrm{mod}\, 13).$$

Демак, $N = 221\,725$ сон 7 га бўлинади, 13 га бўлганда 10 қолдик қолади.

44- §. ДАРАЖАНИ БЎЛИШДА ҲОСИЛ БЎЛГАН ҚОЛДИҚНИ ТОПИШ

Фараз қилайлик $(a, m) = 1$ бўлсин, у ҳолда $a \equiv r(\mathrm{mod}\, m)$ дан $a^k \equiv r^k (\mathrm{mod}\, m)$ келиб чиқади; $(r, m) = 1$ бўлганлиги учун Эйлер теоремасидан фойдаланиш маъқулдир. Ҳақиқатан, $r^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$ бўлганлиги сабабли $k = \varphi(m)q + c(0 \le c < q)$ тенгликдан фойдаланиб,

$a^k \equiv r^k \equiv (r^{\varphi(m)})^q r^c \equiv r^c (\mathrm{mod}\, m)$ ни ҳосил қиламиз.

М и с о л. $(\underline{3}\ \underline{277})^{1391}$ сонни 35 га бўлгандаги қолдиқ топилсин.

Е ч и ш. $277 - 3 \equiv 274 \equiv 1(\mathrm{mod}\, 7)$ бўлганлиги учун 3277 сон 7 га бўлинмайди, равшанки у 5 га ҳам бўлинмайди, яъни $(3277, 35) = 1$. Шунинг учун $(3277)^{1391} \equiv 22^{1391} (\mathrm{mod}\, 35)$.

Энди $(22, 35) = 1$ бўлганлиги учун Эйлер теоремасига кўра $22^{\varphi(35)} \equiv 1 (\mathrm{mod}\, 35)$, $22^{24} \equiv 1 (\mathrm{mod}\, 35)$, $\varphi(35) = 24$.

Сўнгра $1391 = 24 \cdot 57 + 23$ бўлганлиги сабабли

$$22^{1391} \equiv 22^{23} (\mathrm{mod}\, 35).$$

Равшанки,

$22 \equiv -13 (\mathrm{mod}\, 35)$, $22^2 \equiv -6 (\mathrm{mod}\, 35)$, $22^4 \equiv 36 \equiv 1 (\mathrm{mod}\, 35)$, $22^{20} \equiv 1 (\mathrm{mod}\, 35)$,

$22^3 \equiv (-13)(-6)) (\mathrm{mod}\, 35) \equiv 78 \equiv 8 (\mathrm{mod}\, 35)$; $22^{23} \equiv 8 (\mathrm{mod}\, 35)$.

Демак, $(3277)^{1391}$ сонни 35 га бўлганда 8 қолдиқ қолади.

45-§. ОДДИЙ КАСРНИ ЎНЛИ КАСРГА АЙЛАНТИРИШДА ҲОСИЛ БЎЛАДИГАН ДАВР УЗУНЛИГИНИ АНИҚЛАШ

Маълумки, махражи $(b, 10) = 1$ шартни қаноатлантирувчи қисқармас $\frac{a}{b}$ оддий касрни ўнли касрга айлантирганда чексиз даврий каср ҳосил бўлади. Биз тўғри каср билан чегараланамиз, чунки нотўғри каср $(a > b)$ дан аввал уни бутун қисмини ажратиб олиш мумкин. Равшанки, қисқармас тўғри касрнинг сурати a ҳаммаси бўлиб $\varphi(b)$ та b дан кичик ва b билан ўзаро туб қийматларни қабул қилиши мумкин.

Тўғри оддий касрни даврий касрга айлантириш учун одатда қўлланиладиган кетма-кет бўлиш амалини бажариб, қўйидагиларни ҳосил қиламиз

$$\begin{aligned} 10a &= bq_1 + r_1, \\ 10r_1 &= bq_2 + r_2, \\ &\cdots\cdots\cdots\cdots \\ 10r_{m-1} &= bq_m + r_m, \end{aligned} \qquad (120)$$

бунда барча r_i лар $0 < r_i < b$ шартни қаноатлантиради. Шунингдек, $q_1 < 10$, $b > a$; шунга ўхшаш $q_2 < 10$, чунки $b > r_1$ ва ҳ.к. Демак, барча q_i лар ўнлик рақамлардир: Энди барча r_i лар b билан ўзаро тублигини кўрсатамиз. Ҳақиқатан, $(10,\ b) = 1$, $(a, b) = 1$ бўлганлиги сабабли $(10a,\ b) = 1$, бундан эса (120)- тенгликдан $(r_1, b) = 1$ ва шунга ўхшаш (120)- тенгликларнинг қолганларидан $(r_2, b) = 1$, $(r_3, b) = 1$,... келиб чиқади. Шундай қилиб, ҳар хил r_i қолдиқлар b модул бўйича чегирмаларнинг келтирилган системасига тегишли бўлади. Маълумки, b модул буйича келтирилган чегирмаларнинг сони $\varphi(b)$ га тенг. Шунинг учун $m \le \varphi(b)$. Даврдаги рақамлар сонини топиш учун (120)-тенгликларни қуйидагича ёзиб оламиз:

$$\left.\begin{aligned} &10a \equiv r_1 \pmod b,\\ &10r_1 \equiv r_2 \pmod b,\\ &\cdots\cdots\cdots\cdots\\ &10r_{m-1} \equiv r_m \pmod b. \end{aligned}\right\} \qquad (121)$$

Бу тоққосламаларни бир-бирига кўпайтириб, $(r_1 \cdot r_2 \cdot \cdots r_{m-1}, b) = 1$ лиги сабабли, ҳосил бўлган тоққосламаларни $r_1 \cdot r_2 \cdot \cdots r_{m-1}$ га қисқартириб,

$$10^m a \equiv r_m \pmod b \qquad (122)$$

га эга бўламиз.

Энди фараз қилайлик m ихтиёрий сон бўлмасдан 10 сони b модул бўйича m кўрсаткичга тегишли, яъни

$$10^m \equiv 1 \pmod b \qquad (123)$$

таққосламаларни қаноатлантирадиган энг кичик сон бўлсин; (122) ва (123) дан қуйидаги тоққосламага келамиз:

$$a \equiv r_m \pmod b \qquad (124)$$

Маълумки a ва r_m сонлар $0 < a < b$, $0 < r_m < b$ шартларни қаноатлантирганлиги учун $r_m = a$ бўлиши лозим. Шундай қилиб, m та қадамдан сўнг қолдиқлар ва, демак, бўлинмалар ҳам такрорланиб келади:

$$r_{m+1} = r_1, \quad r_{m+2} = r_2, \ldots$$

Равшанки, m энг кичик даврга мос келади, чунки акс ҳолда $m' < m$ учун $a = r_{m'}$ бўлиб, (122) тенгликдан $10^{m'} \equiv 1 (\mathrm{mod}\, b)$ келиб чиқар эди. Бу эса m сон 10 нинг кўрсаткичи бўлишига зиддир. Демак, соф даврий каср ҳосил бўлади, даврдаги рақамларнинг сони (давр узунлиги) фақатгина касрнинг махражига боғлиқ. (122)- тенгликлардан кўрамизки

$$\frac{a}{b} = \frac{r_0}{b}, \ \frac{r_1}{b}, \ldots, \ \frac{r_k}{b}$$

Касрларнинг даврлари мос равишда $q_1 q_2 \ldots q_m, q_2 q_3 \ldots q_m q_1, \ldots, q_{k+1} \ldots q_m q_1 \ldots q_k$ лардан иборат. Шундай қилиб,

$$\frac{r_0}{b}, \frac{r_1}{b}, \ldots, \frac{r_{m-1}}{b}$$

касрлар соф даврий касрлар бўлиб, улар бир биридан даврдаги рақамларнинг циклик равишда алмашиб келиши билан фарқ қилади.

Юқорида келтирилган назарий мулоҳазалар яна ҳам тушунарли бўлиши учун қуйидаги мисолни қараймиз: $\frac{a}{b} = \frac{1}{7}$ бўлсин, у ҳолда Эйлер теоремасига кўра $10^{\varphi(7)} \equiv 10^6 \equiv 1 (\mathrm{mod}\, 7)$. Мабодо 10 нинг 7 модул бўйича даража кўрсаткичи m сони 6 дан кичик бўлмасмикан деган савол туғилади. Агар кичик бўлса, у ҳолда m 6 нинг бўлувчилари 1,2,3 бўлиши керак, лекин $10 \equiv 3, \ 10^2 \equiv 2, \ 10^3 \equiv 6 (\mathrm{mod}\, 7)$. Бундан кўрамизки $m = 6$ ва

10 сони 7 модул бўйича бошланғич илдиз бўлади. Демак, даврий касрнинг даврида 6 та рақам бўлар экан. Буни (121) дан бизнинг ҳол учун келиб чиқадиган қуйидаги тенгликлар ҳам тасдиқлайди:

$$10\cdot 1 = 7\cdot 1 + 3,$$
$$10\cdot 3 = 7\cdot 4 + 2,$$
$$10\cdot 2 = 7\cdot 2 + 6,$$
$$10\cdot 6 = 7\cdot 8 + 4,$$
$$10\cdot 4 = 7\cdot 5 + 5,$$
$$10\cdot 5 = 7\cdot 7 + 1.$$

Бу ердан:

$$\frac{1}{7} = 0,(142857), \qquad \frac{6}{7} = 0,(857142),$$
$$\frac{3}{7} = 0,(428571), \qquad \frac{4}{7} = 0,(571428),$$
$$\frac{2}{7} = 0,(285714). \qquad \frac{5}{7} = 0,(714285).$$

Бундан даврдаги рақамлар циклик равишда алмашиниши кўриниб турибди.

Фараз қилайлик каср олдингидек қисқармас бўлсин, лекин $(b,10) > 1$, яъни махраж 2 ёки 5, ёки 2 ва 5 га бўлинсин. Айтайлик $b = 2^{\alpha}5^{\beta}b_1$ бўлсин, бунда $(b_1,10) = 1$. Бу холда $\gamma = \max(\alpha,\beta)$ деб

$$\frac{10^{\gamma}a}{b} = \frac{a_1}{b_1}$$

сонни оламиз, бунда $\frac{a_1}{b_1}$ каср қисқармас ва b_1 махраж 10 билан ўзаро туб. Олдинги йўл билан бу касрни ўнли даврий касрга айлантирамиз:

$$\frac{a_1}{b_1} = k,(c_1c_2...c_m),$$

бунда k касрнинг бутун кисми, $(c_1c_2...c_m)$ унинг даври. Энди $\frac{a}{b}$ касрни хосил килиш учун $\frac{a_1}{b_1}$ ни 10^γ га бўлиш, яъни вергулни γ хонага чапга суриш керак, натижада

$$\frac{a}{b} = l,b_1b_2...b_\gamma(c_1c_2...c_m)$$

келиб чиқади. Бу эса аралаш даврий касрдир.

Энди тескари масалани кўриб чиқамиз: берилган даврий касрнинг қийматини ифодалайдиган оддий касрни топиш талаб қилинади. Шуни таъкидлаш лозимки, чексиз ўнли каср бу яқинлашувчи чексиз қаторнинг ўзи, унинг йиғиндисини топишимиз керак. Фараз қилайлик бизга соф даврий каср берилган бўлсин $t = k,(a_1a_2...a_m)$, у холда

$$t = k + \left(\frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_m}{10^m}\right) + \frac{1}{10^m}\left(\frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_m}{10^m}\right) + ...+ =$$

$$= k + \left(10^{m-1}a_1 + 10^{m-2}a_2 + ... + 10^{m-2}\right)\left(\frac{1}{10^m} + \frac{1}{10^{2m}} + ...\right)$$

Охирги қавслардаги ифоданинг биринчи касри ва махражи 10^{-m} бўлган чексиз геометрик прогрессиянинг йиғиндиси бўлиб,

$$\frac{1}{10^m} : \left(1 - \frac{1}{10^m}\right) = \frac{1}{10^{m-1} - 1}$$

га тенг, $10^m - 1$ эса m та тўққизликдан иборат сонни ифодалайди. Шундай қилиб,

$$t = k + \frac{10^{m-1}a_1 + 10^{m-2}a_2 + ... + a_m}{10^m - 1}$$

М и с о л. Соф даврий каср оддий касрга айлантирилсин. $t = 5,(312) = 5\frac{312}{999} = 5\frac{104}{333}$.

Энди бизга аралаш даврий каср берилган бўлсин: $t = k,b_1b_2...b_\gamma(c_1c_2...c_m)$. Уни қуйидагича тасвирлаш мумкин

$$t = \left[kb_1b_2...b_\gamma,(c_1c_2...c_m)\right]:10^\gamma = \left[kb_1b_2...b_\gamma,\frac{c_1c_2...c_m}{10^m-1}\right]:10^\gamma =$$

$$= k + \frac{b_1 10^{\gamma-1} + b_2 10^{\gamma-2} + ... + b_\gamma}{10^\gamma} + \frac{c_1 10^{m-1} + c_2 10^{m-2} + ... + c_m}{10^m(10^m-1)}$$

ёки

$$t = k + \left[\left(b_1 10^{m+\gamma-1} + ... + b_\gamma 10^m + c_1 10^{m-1} + ... + c_m\right) - \left(b_1 10^{\gamma-1} + ... + b_\gamma\right)\right] \cdot \frac{1}{10^\gamma(10^m-1)}$$

М и с о л. Аралаш каср оддий касрга айлантирилсин:

$$7,51(43) = 7\frac{5143-51}{9900} = 7\frac{5092}{9900} = 7\frac{1273}{2475}.$$

9-БОБ УЧУН МАШҚЛАР

1. Ўнлик саноқ системасида $7a36b5$ кўринишда ёзилган сон 1375 га бўлинади, a ва b ни топинг.
2. 37 га бўлинадиган уч хонали соннинг рақамларини даврий равишда алмаштирганда хосил бўладиган сонларнинг 37 га бўлинишини кўрсатинг.
3. Агар 6513 ва 3156 (рақамларининг тартиби тескари) сонларни қўшсак, у холда йиғинди 11 га бўлинишини, уларнинг айирмаси эса 9 га бўлинишини исбот қилинг. Умумий теореманинг таърифини келтиринг ва исбот қилинг.
4. 3^n та бир хил рақамлардан иборат бўлган соннинг 3^n га бўлинишини исбот қилинг.
5. Бешлик ва ўнлик саноқ системаларида 13 га бўлиниш аломатларини чиқаринг.
6. 13 асослик саноқ системасида 3,4 ва 7 га бўлиниш аломатларини чиқаринг.

6. 13 асослик саноқ системасида 3,4 ва 7 га бўлиниш аломатларини чиқаринг.

7. Махражи 29,31,43 бўлган касрларни ўнли касрларга ёйганда ҳосил бўладиган даврнинг узунлиги ва рақамлари топилсин.

8. Ушбу $\frac{5}{1658}$ касрни энг содда касрлар йиғиндиси шаклида ёзиб, даврдаги ва даврдан олдинги рақамларнинг сони аниқлансин ва берилган каср ўнли касрга ёйилсин.

9. Ушбу $\frac{1}{n}+\frac{1}{n+1}+\frac{1}{n+2}$ касрни аралаш даврий касрга ёйилшини кўрсатинг.

10. Иккилик саноқ системасида ёзилган $a=1000000001$ ва $b=1000000000000001$ сонларнинг энг катта умумий бўлувчисини топинг (Ж.9).

9- бобга доир тарихий маълумотлар

1. Ўнлик позицион саноқ сстемаси тахминан 5-асрда Ҳиндистонда пайдо бўлиб, 9-асрда ал-Хоразмийнинг «Ҳинд саноғи тўғрисида» рисоласи ёзилгандан кейин ўша пайтдаги араб давлатларида тарқалган, 10-асрда Испаниягача, 12-асрдан бошлаб Европанинг бошқа давлатларига ҳам тарқала бошлаган. Бу янги саноқ системаси билан ал-Хоразмий рисоласини арабчадан латинчага қилинган таржимаси орқали танишган. Европада фақат 16-асрда янги саноқ системаси фанда ва кундалик ҳаётда қўлланилла бошланди, Россияда эса 17-асрнинг охирида ва 18 – асрнинг бошида тўла қўлланиладиган бўлди.

Ҳозирги вақтда биз биламизки ихтиёрий q>1 натурал сонни олиб ҳар қандай n натурал сонни

$$n=a_m q^m+a_{m-1}q^{m-1}+\ldots+a_1 q+a_0$$

кўринишда ягона равишда тасвирлаш мумкин. Бунда a_i лар q асосли саноқ системасининг рақамлари бўлиб, 0,1,…,q-1

$$n = a_m a_{m-1} \ldots a_1 a_0$$

кўринишда ёзиш мумкин. q асосли саноқ системани биринчи бўлиб Б.Паскал (Paskal Blaise, 1623-1662) моҳиятини тушунди. «De numeris multiblisibus ex sola characterum additione agnoscendis» («Фақат рақамларни қўшиш ёрдамида сонларнинг бўлинишини аниқлаш ҳақида») асарини ёзди, бу асар 1665 йилда чоп этилди. Б.Паскал бу асарда биз 43-§ да келтирган бўлиниш аломатларини ҳам топди.

2. Мирзо Улуғбек расадхонасида ишлаган Fиёсиддин ал-Коший биринчи бўлиб математикада позицион саноқ асосида ўнли касрларни киритди ва назарий асослади, яъни ўнли касрлар арифметикасини яратди. 150 йилдан сўнг голландиялик Симон Стевиннинг (1584-1620) "Ўнинчи" (1585 й.) номли асари чиққандан кейин Европада ўнли касрлар билан танишиб ишлата бошладилар.

АРАЛАШ САВОЛЛАР

1. $2^{18}+3^{18}$ соннинг каноник ёйилмасини топинг (ж. $13\cdot 61\cdot 37\cdot 73\cdot 181$)

2. Ушбу $(x+n)^n - \frac{n}{1!}(x+n-1)^n + \frac{n(n-1)}{2!}(x+n-2)^n + \ldots + (-1)^n x^n = n!$ айниятни исботланг ва бундан, Ферма теоремасига таяниб, Вилсон теоремасини чиқаринг.

3. k нинг қайси қийматида $37^k \equiv 1 (\mathrm{mod}\, 11)$ таққослама ўринли бўлади?

4. Агар $(n,6)=1$ бўлса, у ҳолда $n^2 \equiv 1 (\mathrm{mod}\, 24)$ лигини исбот қилинг.

5. $(a+b)^p$ нинг Ньютон биноми бўйича ёйилмасидан фойдаланиб, $(a+b)^p \equiv a^p + b^p (\mathrm{mod}\, p)$ ва

$(x_1 + x_2 + \ldots + x_n)^p \equiv x_1^p + x_2^p + \ldots + x_n^p (\mathrm{mod}\, p)$

таққосламаларни исбот қилинг.

6. Олдинги машқдаги теоремадан Ферма теоремасини ҳосил қилинг.

6. Олдинги машқдаги теоремадан Ферма теоремасини ҳосил қилинг.

7. Ферма теоремасидан Эйлер теоремасини келтириб чиқаринг.

8. 17 туб соннинг бошланғич илдизлари топилсин ва, 10 асос бўйича индекслар жадвали маълум бўлган ҳолда, 6 асос бўйича индекслар жадвали топилсин.

9. 10 модул бўйича $3, 5, 7$ ва 9 сонлар қайси даража кўрсаткичларга тегишли бўлади?

10. Махражи $37, 41, 239, 271$ бўлган касрларни ўнли касрларга ёйганда ҳосил бўладиган даврнинг узунлиги ва рақамлари топилсин.

11. 1) $\varphi(4554)$ ва 2) $\varphi(1246500)$ ни топинг.

12. 2-лик саноқ системасида қайси касрлар чекли систематик соф даврий ва қайсилари аралаш даврий касрларга айланади. Агар саноқ системасининг асоси 12 бўлсачи?

13. Сонларнинг бўлиниш аломатини қўллаб, 421594632 соннинг каноник ёйилмасини топинг

14. $((26373)^{61}+23)^{82}$ сонни 97 га бўлганда ҳосил бўладиган қолдиқни топинг.

15. $2^{1093}-2$ сон $(1093)^2$ га бўлинадими?

16. Фараз қилайлик $m>0$ ва $\tau_m(n)$ миқдор $x_1x_2\ldots x_m=n$ ($x_1, x_2, \ldots, x_m$ бир-бирига боғлиқ бўлмаган равишда натурал қийматларни қабул қилади) тенглама ечимларининг сонини белгиласин. Равшанки, $\tau_1(n)=n$, $\tau_2(n)=\tau(n)$.

Қуйидагиларни исбот қилинг:

1) $\tau_m(n)$ – мултипликатив функция.

2) Агар q-туб сон, $\alpha\geq 0$ ва $m>1$ бўлса, у ҳолда

$$\tau_m\left(p^\alpha\right)=\frac{(\alpha+1)(\alpha+2)\ldots(\alpha+m-1)}{1\cdot 2\ldots(m-1)}.$$

17. Фараз қилайлик $f(n)$ мултипликатив функция бўлсин. У ҳолда $F(n)=\sum_{d\backslash n} f(d)$ нинг мултипликативлигини исбот қилинг.

18. Фараз қилайлик $f(n)$ барча n натурал сонлар учун аниқланган ва $F(n)=\sum_{d\backslash n} f(d)$ – мултипликатив функция, у ҳолда $f(n)$ нинг мултипликативлигини исбот қилинг.

19. Олдинги машқдаги теоремани қўллаб, $\varphi(n)$ учун 34-теоремани исбот қилинг.

20. Фараз қилайлик m, n, a, b натурал сонлар бўлсин. Қуйидаги бўлиниш муносабатлари (айний таққосламалар)ни кўрсатинг:

1) $n^3+11n \vdots 6$,
2) $10^{3n}-1 \vdots 3^{n+2}$,
3) $4^{2m+1}+3^{2m+1} \vdots 7$,
4) $4^n+15n-1 \vdots 9$,
5) $2^{2n-1}\,3^{n+2}+1 \vdots 11$,
6) $ab(a^4-b^4) \vdots 30$,
7) $a^{n+4}-a^4 \vdots 30$,
8) $n^2(n^6-1) \vdots 504$,
9) $2^{12n+2}+3^{3n+2} \vdots 13$
10) $n(n+1)\cdots(2n-3)(2n-2) \vdots 2^{n-1}$

6000 дан ошмаган туб сонлар жадвали

2	167	389	631	883	1153	1447	1709	2011	2309	2621
3	173	397	641	887	1163	1451	1721	2017	2311	2633
5	179	401	643	907	1171	1453	1723	2027	2333	2647
7	181	409	647	911	1181	1459	1733	2029	2339	2657
11	191	419	653	919	1187	1471	1741	2039	2341	2659
13	193	421	659	929	1193	1481	1747	2053	2347	2663
17	197	431	661	937	1201	1483	1753	2063	2351	2671
19	199	433	673	941	1213	1487	1759	2069	2357	2677
23	211	439	677	947	1217	1489	1777	2081	2371	2683
29	223	443	683	953	1223	1493	1783	2083	2377	2687
31	227	449	691	967	1229	1499	1787	2087	2381	2689
37	229	457	701	971	1231	1511	1789	2089	2383	2693
41	233	461	709	977	1237	1523	1801	2099	2389	2699
43	239	463	719	983	1249	1531	1811	2111	2393	2707
47	241	467	727	991	1259	1543	1823	2113	2399	2711
53	251	479	733	997	1277	1549	1831	2129	2411	2713
59	257	487	739	1009	1279	1553	1847	2131	2417	2719
61	263	491	743	1013	1283	1559	1861	2137	2423	2729

67	269	499	751	1019	1289
71	271	503	757	1021	1291
73	277	509	761	1031	1297
79	281	521	769	1033	1301
83	283	523	773	1039	1303
89	293	541	787	1049	1307
97	307	547	797	1051	1319
101	311	557	809	1061	1321
103	313	563	811	1063	1327
107	317	569	821	1069	1361
109	331	571	823	1087	1367
113	337	577	827	1091	1373
127	347	587	829	1093	1381
131	349	593	839	1097	1399
137	353	599	853	1103	1409
139	359	601	857	1109	1423
149	367	607	859	1117	1427
151	373	613	863	1123	1429
157	379	617	877	1129	1433
163	383	619	881	1151	1439

1567	1867	2141	2437	2731
1571	1871	2147	2441	2741
1579	1873	2153	2447	2749
1583	1877	2161	2459	2753
1597	1879	2179	2467	2767
1601	1889	2203	2473	2777
1607	1901	2207	2477	2789
1609	1907	2213	2503	2791
1613	1913	2221	2521	2797
1619	1931	2237	2531	2801
1621	1933	2239	2539	2803
1627	1949	2243	2543	2819
1637	1951	2251	2549	2833
1657	1973	2267	2551	2837
1663	1979	2269	2557	2843
1667	1987	2273	2579	2851
1669	1993	2281	2591	2857
1693	1997	2287	2593	2861
1697	1999	2293	2609	2879
1699	2003	2297	2617	2887

2897	3221	3529	3821	4127	4447
2903	3229	3533	3823	4129	4451
2909	3251	3539	3833	4133	4457
2917	3253	3541	3847	4139	4463
2927	3257	3547	3851	4153	4481
2939	3259	3557	3853	4157	4483
2953	3271	3559	3863	4159	4493
2957	3299	3571	3877	4177	4507
2963	3301	3581	3881	4201	4513
2969	3307	3583	3889	4211	4517
2971	3313	3593	3907	4217	4519
2999	3319	3607	3911	4219	4523
3001	3323	3613	3917	4229	4547
3011	3329	3617	3919	4231	4549
3019	3331	3623	3923	4241	4561
3023	3343	3631	3929	4243	4567
3037	3347	3637	3931	4253	4583
3041	3359	3643	3943	4259	4591
3049	3361	3659	3947	4261	4597

4751	5051	5399	5683
4759	5059	5407	5689
4783	5077	5413	5693
4787	5081	5417	5701
4789	5087	5419	5711
4793	5099	5431	5717
4799	5101	5437	5737
4801	5107	5441	5741
4813	5113	5443	5743
4817	5119	5449	5749
4831	5147	5471	5779
4861	5153	5477	5783
4871	5167	5479	5791
4877	5171	5483	5801
4889	5179	5501	5807
4903	5189	5503	5813
4909	5197	5507	5821
4919	5209	5519	5827
4931	5227	5521	5839

3061	3371	3671	3967
3067	3373	3673	3989
3079	3389	3677	4001
3083	3391	3691	4003
3089	3407	3697	4007
3109	3413	3701	4013
3119	3433	3709	4019
3121	3449	3719	4021
3137	3457	3727	4027
3763	3461	3733	4049
3167	3463	3739	4051
3169	3467	3761	4057
3181	3469	3767	4073
3187	3491	3769	4079
3191	3499	3779	4091
3203	3511	3793	4093
3209	3517	3797	4099
3217	3527	3803	4111

4271	4603	4933	5231	5527	5843
4273	4621	4937	5233	5531	5849
4283	4637	4943	5237	5557	5851
4289	4639	4951	5261	5563	5857
4297	4643	4957	5273	5569	5861
4327	4649	4967	5279	5573	5867
4337	4651	4969	5281	5581	5869
4339	4657	4973	5297	5591	5879
4349	4663	4987	5303	5623	5881
4357	4673	4993	5309	5639	5897
4363	4679	4999	5323	5641	5903
4373	4691	5003	5333	5647	5923
4391	4703	5009	5347	5651	5927
4397	4721	5011	5351	5653	5939
4409	4723	5021	5381	5657	5953
4421	4729	5023	5387	5659	5981
4423	4733	5039	5393	5669	5987
4441					

БОШЛАНҒИЧ ИЛДИЗЛАР ВА ИНДЕКСЛАР ЖАДВАЛИ

Туб сон 5.

Бошланғич илдизлар: 2, 3. Асос 2.

I.

N.	1	2	3	4
I.	4	1	3	2

N.

I.	1	2	3	4
N.	2	4	3	1

Туб сон 7.

Бошланғич илдизлар: 3,5. Асос 3.

I.

N.	1	2	3	4	5	6
I.	6	2	1	4	5	3

N.

I.	1	2	3	4	5	6
N.	3	2	6	4	5	1

Туб сон 11.

Бошланғич илдизлар: 2, 6, 7, 8. Асос 2.

I.

N.	1	2	3	4	5	6	7	8	9	10
I.	10	1	8	2	4	9	7	3	6	5

N.

I.	1	2	3	4	5	6	7	8	9	10
N.	2	4	8	5	10	9	7	3	6	1

Туб сон 13.

Бошланғич илдизлар: 2, 6, 7, 11. Асос 6.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		12	5	8	10	9	1	7	3	4
1	2	11	6							

N.

I.	0	1	2	3	4	5	6	7	8	9
0 1		6	10	8	9	4	2	12	7	3 5
	11	1								

Туб сон 17.

Бошланғич илдизлар: 3, 5, 6, 7, 10, 11, 12, 14. Асос 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		16	10	11	4	7	5	9	14	6 2
1	1	13	15	12	3	8				

N.

I.	0	1	2	3	4	5	6	7	8	9
0 1		10	15	14	4	6	9	5	16	7
		3	13	11	8	12	1			

Туб сон 19.

Бошланғич илдизлар: 2, 3, 10, 13, 14, 15. Асос 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		18	17	5	16	2	4	12	15	10
1	1	6	3	13	11	7	14	8	9	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	5	12	6	3	11	15	17	18
1	9	14	7	13	16	8	4	2	1	

Туб сон 23.

Бошланғич илдизлар: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21. Асос 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		22	8	20	16	15	6	21	2	18
1	1	3	14	12	7	13	10	17	4	5
2	9	19	11							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	8	11	18	19	6	14	2	20
1	16	22	13	15	12	5	4	17	9	21
2	3	7	1							

Туб сон 29.

Бошланғич илдизлар: 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27. Асос 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		28	11	27	22	18	10	20	5	26
1	1	23	21	2	3	17	16	7	9	15
2	12	19	6	24	4	8	13	25	14	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	13	14	24	8	22	17	25	18
1	6	2	20	26	28	19	16	15	5	21
2	7	12	4	11	23	27	9	3	1	

Туб сон 31.

Бошланғич илдизлар: 3, 11, 12, 13, 17, 21, 22, 24.

Асос 17.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		30	12	13	24	20	25	4	6	26
1	2	29	7	23	16	3	18	1	8	22
2	14	17	11	21	19	10	5	9	28	27
3	15									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		17	10	15	7	26	8	12	18	27
1	25	22	2	3	20	30	14	21	16	24
2	5	23	19	13	4	6	9	29	28	11
3	1									

Туб сон 37.

Бошланғич илдизлар: 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35.

Асос 5.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		36	11	34	22	1	9	28	33	32
1	12	6	20	13	3	35	8	5	7	25
2	23	26	17	21	31	2	24	30	14	15
3	10	27	19	4	16	29	18			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		5	25	14	33	17	11	18	16	6
1	30	2	10	13	28	29	34	22	36	32
2	12	23	4	20	26	19	21	31	7	35
3	27	24	9	8	3	15	1			

Туб с он 41.

Бошланғич илдизлар: 6,7,11,12,13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

Асос 6.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		40	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7
4	1									

Туб сон 43.

Бошланғич илдизлар: 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.

Асос 28.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		42	39	17	36	5	14	7	33	34
1	2	6	11	40	4	22	30	16	31	29
2	41	24	3	20	8	10	37	9	1	25
3	19	32	27	23	13	12	28	35	26	15
4	38	18	21							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		28	10	22	14	5	11	7	24	27
1	25	12	35	34	6	39	17	3	41	30
2	23	42	15	33	21	29	38	32	36	19
3	16	18	31	8	9	37	4	26	40	2
4	13	20	1							

Туб сон 47.

Бошланғич илдизлар: 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45

Асос 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		46	30	18	14	17	2	38	44	36
1	1	27	32	3	22	35	28	42	20	29
2	31	10	11	39	16	34	33	8	6	43
3	19	5	12	45	26	9	4	24	13	21
4	15	25	40	37	41	7	23			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	6	13	36	31	28	45	27	35
1	21	22	32	38	4	40	24	5	3	30
2	18	39	14	46	37	41	34	11	16	19
3	2	20	12	26	25	15	9	43	7	23
4	43	44	17	29	8	33	1			

Туб сон 53.

Бошланғич илдизлар: 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50,51

Асос 26.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		52	25	9	50	31	34	38	23	18
1	4	46	7	28	11	40	48	42	43	41
2	29	47	19	39	32	10	1	27	36	6
3	13	45	21	3	15	17	16	22	14	37
4	2	33	20	30	44	49	12	8	5	24
5	35	51	26							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		26	40	33	10	48	29	12	47	3
1	25	14	46	30	38	34	36	35	9	22
2	42	32	37	8	49	2	52	27	13	20
3	43	5	24	41	6	50	28	39	7	23
4	15	19	17	18	44	31	11	21	16	45
5	4	51	1							

Туб сон 59.

Бошланғич илдизлар: 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40,42, 43, 44, 47, 50, 52, 54, 55, 56.

Асос 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		58	25	32	50	34	57	44	17	6
1	1	45	24	23	11	8	42	14	31	22
2	26	18	12	27	49	10	48	38	36	4
3	33	7	9	19	39	20	56	41	47	55
4	51	2	43	13	37	40	52	53	16	30
5	35	46	15	28	5	21	3	54	29	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	41	56	29	54	9	21	14	32
1	25	14	22	43	17	52	48	8	21	33
2	35	55	19	13	12	2	20	23	53	58
3	49	18	3	30	5	50	28	44	27	34
4	45	37	16	42	7	11	51	38	26	24
5	4	40	46	47	57	39	36	6	1	

Туб сон 61.

Бошланғич илдизлар: 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59 Асос 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		60	47	42	34	14	29	23	21	24
1	1	45	16	20	10	56	8	49	11	22
2	48	5	32	39	3	28	7	6	57	25
3	43	13	55	27	36	37	58	33	9	2
4	35	18	52	41	19	38	26	40	50	46
5	15	31	54	51	53	59	44	4	12	17
6	30									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	39	24	57	21	27	26	16	38
1	14	18	58	31	5	50	12	59	41	44
2	13	8	19	7	9	29	46	33	25	6
3	60	51	22	37	4	40	34	35	45	23
4	47	43	3	30	56	11	49	2	20	17
5	48	53	42	54	52	32	15	28	36	55
6	1									

Туб сон 67.

Бошланғич илдизлар: 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63.

Асос 12.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		66	29	9	58	39	38	7	21	18
1	2	61	1	23	36	48	50	8	47	26
2	31	16	24	20	30	12	52	27	65	22
3	11	43	13	4	37	46	10	44	55	32
4	60	19	45	63	53	57	49	64	59	14
5	41	17	15	3	56	34	28	35	51	54
6	40	5	6	25	42	62	33			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		12	10	53	33	61	62	7	17	3
1	36	30	25	32	49	52	21	51	9	41
2	23	8	29	13	22	63	19	27	56	2
3	24	20	39	66	55	57	14	34	6	5
4	60	50	64	31	37	42	35	18	15	46
5	16	58	26	44	59	38	54	45	4	48
6	40	11	65	43	47	28	1			

Туб сон 71.

Бошланғич илдизлар: 7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69.

Асос 62.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		70	58	18	46	14	6	33	34	36
1	2	43	64	27	21	32	22	7	24	38
2	60	51	31	5	52	28	15	54	9	4
3	20	13	10	61	65	47	12	30	26	45
4	48	55	39	44	19	50	63	17	40	66
5	16	25	3	59	42	57	67	56	62	29
6	8	37	1	69	68	41	49	11	53	23
7	35									

N.

I.	0	1	2	3	4	5	6	7	8	9
0		62	10	52	29	23	6	17	60	28
1	32	67	36	31	5	26	50	47	3	44
2	30	14	16	69	18	51	38	13	25	59
3	37	22	15	7	8	70	9	61	19	42
4	48	65	54	11	43	39	4	35	40	66
5	45	21	24	68	27	41	57	55	2	53
6	20	33	58	46	12	34	49	56	64	63
7	1									

Туб сон 73.

Бошланғич илдизлар: 5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68.

Асос 5.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		72	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	
7	38	44	1-			66				

Туб сон 79.

Бошланғич илдизлар: 3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77. Асос 29.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		78	50	71	22	34	43	19	72	64
1	6	70	15	74	69	27	44	9	36	10
2	56	12	42	52	65	68	46	57	41	1
3	77	76	16	63	59	53	8	23	60	67
4	28	21	62	47	14	20	24	55	37	38
5	40	2	18	7	29	26	13	3	51	17
6	49	75	48	5	66	30	35	54	31	45
7	25	33	58	4	73	61	32	11	39	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		29	51	57	73	63	10	53	36	17
1	19	77	21	56	44	12	32	59	52	7
2	45	41	4	37	46	70	55	15	40	54
3	65	68	76	71	5	66	18	48	49	78
4	50	28	22	6	16	69	26	43	62	60
5	2	58	23	35	67	47	20	27	72	34
6	38	75	42	33	9	24	64	39	25	14
7	11	3	8	74	13	61	31	30	1	

Туб сон 83.

Бошланғич илдизлар: 2, 5,6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80

Асос 50.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		82	3	52	6	81	55	24	9	22
1	2	72	58	67	27	51	12	4	25	59
2	5	76	75	16	61	80	70	74	30	36
3	54	32	15	42	7	23	28	60	62	37
4	8	38	79	49	78	21	19	69	64	48
5	1	56	73	13	77	71	33	29	39	20
6	57	34	35	46	18	66	45	53	10	68
7	26	17	31	43	63	50	65	14	40	47
8	11	44	41							

N.

I.	0	1	2	3	4	5	6	7	8	9
0		50	10	2	17	20	4	34	40	8
1	68	80	16	53	77	32	23	71	64	46
2	59	45	9	35	7	18	70	14	36	57
3	28	72	31	56	61	62	29	39	41	58
4	78	82	33	73	81	66	63	79	49	43
5	75	15	3	67	30	6	51	60	12	19
6	37	24	38	74	48	76	65	13	69	47
7	26	55	11	52	27	22	21	54	44	42
8	25	5	1							

Туб сон 89.

Бошланғич илдизлар: 3,6,7,13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86

Асос 30.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		88	72	87	56	18	71	7	40	86
1	2	4	55	65	79	17	24	82	70	53
2	74	6	76	31	39	36	49	85	63	29
3	1	57	8	3	66	25	54	77	37	64
4	58	67	78	59	60	16	15	34	23	14
5	20	81	33	10	69	22	47	52	13	45
6	73	19	41	5	80	83	75	32	50	30
7	9	26	38	68	61	35	21	11	48	46
8	42	84	51	27	62	12	43	28	44	

N.

I.	0	1	2	3	4	5	6	7	8	9
0		30	10	33	11	63	21	7	32	70
1	53	77	85	58	49	46	45	15	5	61
2	50	76	55	48	16	35	71	83	87	29
3	69	23	67	52	47	75	25	38	72	24
4	8	62	80	86	88	59	79	56	78	26
5	68	82	57	19	36	12	4	31	40	43
6	44	74	84	28	39	13	34	41	73	54
7	18	6	2	60	20	66	22	37	42	14
8	64	51	17	65	81	27	9	3	1	

Туб сон 97.

Бошланғич илдизлар: 3,6,7,13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86

Асос 30.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		96	86	2	76	11	88	53	66	4
1	1	82	78	83	43	13	56	19	90	27
2	87	55	72	79	68	22	73	6	33	47
3	3	26	46	84	9	64	80	41	17	85
4	77	71	45	44	62	15	69	60	58	10
5	12	21	63	14	92	93	23	29	37	65
6	89	32	16	57	36	94	74	51	95	81
7	54	25	70	20	31	24	7	39	75	42
8	67	8	61	91	35	30	34	49	52	18
9	5	40	59	28	50	38	48			

N.

I.	0	1	2	3	4	5	6	7	8	9
0		10	3	30	9	90	27	76	81	34
1	49	5	50	15	53	45	62	38	89	17
2	73	51	25	56	75	71	31	19	93	57
3	85	74	61	28	86	84	64	58	95	77
4	91	37	79	14	43	42	32	29	96	87
5	94	67	88	7	70	21	16	63	48	92
6	47	82	44	52	35	59	8	80	24	46
7	72	41	22	26	66	78	4	40	12	23
8	36	69	11	13	33	39	2	20	6	60
9	18	83	54	55	65	68	1			

АДАБИЁТЛАР

Дарсликлар ва ўқув қўлланмалар

1. Айерленд К., Роузен М. Классическое введение в современную теорию чисел. Перевод с английского. М.:Мир 1987.
2. Арнольд И.В. Теория чисел. М.: Учпедгиз, 1939.
3. Боревич З.И., Шафаревич И.Р. Теория чисел. М.Наука, 1985.
4. Бухштаб Б.А. Теория чисел. М.: Просвещение, 1966.
5. Венков Б.А. Элементарная теория чисел. М. – Л: 1935.
6. Виноградов И.М. Основы теории чисел. 8-е издание. М.: Наука, 1972.
7. Виноградов И.М. Сонлар назарияси асослари. Т.: Ўқув педнашр, 1959.
8. Гекке Э. Лекции по теории алгебраических чисел. М.:ГТТИ, 1940.
9. Диксон Л.Е. Введение в теорию чисел. Изд. АН ГССР, Тбилиси, 1941.
10. Лежен-Дирихле П.Г. Лекции по теории чисел в обработке и с добавлениями Дедикина Р. Перевод с немецкого под редакцией Сегала Б.И., с приложениями статьи Делоне Б.Н. «Геометрия бинарных квадратичных форм» М.ОНТИ, 1936.
11. Михелович Ш.Х. Теория чисел. М.: Высшая школа, 1962.
12. Нарзуллаев Х.Н., Нарзуллаев У.Х. "Бир номаълумли таққосламалар" бўйича методик кўрсатмалар. Самарқанд, 1986.
13. Сушкевич А.К. Теория чисел. 2-е издание. Изд. Харьковского унив-та, 1956.
14. Хассе Г. Лекции по теории чисел. Перевод с немецкого Демьянова, под ред. И.Р. Шафаревича. ИИЛ, 1953.
15. Эдварс Г. Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел. Перевод с английского Калинина В.Л. и Скопина А.И., под редакцией Скубенко Б.Ф. – М.:Мир, 1980.
16. Хинчин А.Я. Элементы теории чисел. Энциклопедия элементарной математики. Том 1. Гостехиздат, 1951.
17. Dirichlet P.G.L. and Dedekind R., Lectures on Number Theory, AMS, 1999,
    275 p.
18. Helmut Koch, Number Thoery (Algebraik Numbers and Functions), AMS, 2000, 392 p.

Монографиялар, асарлар ва мақолалар

19. Виноградов И.М. Избранные труды. М.: Изд. АН СССР 1952.
20. Виноградов И.М. Особые варианты метода тригонометричных сумм. М.: Наука, 1976.
21. Виноградов И.М. Метод тригонометричных сумм в теореии чисел. М.: Наука, 1980.
22. Вон Р. Метод Харди-Литлвуда. Перевод с английского Лаврик А.А., под редакцией А.А . Карацубы. М.: Мир, 1985.
23. Гаусс К.Ф.Арифметические исследования в кн. «Труды по теории чисел». Общая редакция акад. Виноградова .И.М. Изд-во АН СССР, 1959.
24. Гельфонд А.О. Транстендентные и алгебраические числа. – М.: ГТТИ, 1952.
25. Делоне Б.Н. Петербургская школа теории чисел. М.: Изд-во АН СССР, 1947.
26. Дэвенпорт Г. Мультипликативная теория чисел. Перевод с английского Голубевой Е.П., под редакцией Чудакова Н.Г.– М.:Наука, 1971.
27. Ингам А.Е. Распределение простых чисел. Перевод с английского Райкова Д.А., с приложением статьи переводчика «О методе Ландау –Иксара доказательства асимптотического распределения простых чисел».– М.:ОНТИ, 1936.
28. Исраилов М.И. Нахождение числа решений линейных диофантовых уравнений и их приложений в теории инвариантных кубатурных формул. Сибирский математический журнал. 1981, 2, № 2, С.121-136.
29. Исраилов М.И. Ассимптотические разложения для числа решений диофантовой системы Гильберта - Камке с растущим числом слагаемых. Труды ЛОМИ. Исслед. По теории чисел, том 8, 1983.
30. Карацуба А.А. Основы аналитической теории чисел. – М.:Наука, 1983.
31. Касселс Дж. Введение в теорию диофантовых приблежений. Перевод с английского Полосуева А.М., под редакцией и дополнением Гельфонда А.О.– М.:ИЛ, 1961.
32. Касселс Дж. Введение в геометрию чисел. Перевод с английского Андрианова А.Н. и Богаченко И.В., под редакцией Малышева А.В. – М.: Мир, 1982.
33. Касселс Дж. Рациональные квадратичные формы. Перевод с английского Венкова Б.Б., под редакцией Малышева А.В. – М.: Мир, 1965.

34. Коробов Н.М. Теоритико-числовые методы в приближенном анализе. – М.:Наука, 1963.
35. Коробов Н.М. Оценки тригонометрических сумм и их приложения. М.: Наука, 1984.
36. Кубилюс И.П. Вероятностные методы в теории чисел. 2-е допол. издание Вильнюс, 1962.
37. Монтгомери Х. Мультипликативная теория чисел. Перевод с английского А.Ф.Лаврика – М.: Мир, 1974.
38. Постников А.Г. Введение в аналитическую теорию чисел. М.: Наука, 1971.
39. Прахар К. Распределение простых чисел. Перевод с немецкого А.А.Карацубы, под редакцией А.И. Виноградова. - М.: ИЛ, 1953.
40. Титчмарш Е.К. Теория дзета-функции Римана. Перевод с немецкого М.А.Евграфова, под редакцией А.О.Гельфонда. - М.: ИЛ, 1953.
41. Трост Э.Простые числа. Перевод с немецкого Н.И.Фельдмана, под редакцией А.О.Гельфонда, - М.ГИФМЛ, 1959.
42. Чандрасекхаран К. Арифметические функции. Перевод с английского А.Б.Шидловского – М.: Наука, 1975.
43. Чандрасекхаран К. Введение в аналитическую теорию чисел. Перевод с английского С.А.Степанова, под редакцией А.И.Виноградова. – М.: Мир, 1974.
44. Чебышев П.Л. Избранные труды. Отв. ред. акад.И.М.Виноградов. Изд-во АН СССР, М.:1955.
45. Чудаков Н. Введение в теории L-функций Дирихле. М.: Гостехиздат, 1947.
46. Хуа-Ло-Кен. Метод тригонометрических сумм в теорию чисел. М.: Наука, 1971.
47. Хинчин А.Я. Цепные дроби. М.: Наука, 1978.

Математика тарихига оид ва илмий-оммабоп китоблар

48. Вальфиш А.З. Уравнение Пелля. Тбилиси: Изд. АН Груз СССР, 1952.
49. Вилейтнер Г. История математики от Декарта до середины XIX столетия. Перевод с немецкого, под редакцией А.П.Юшкевича. М.: 1960.
50. Гельфонд А.О. О проблеме приблежения алгебраических чисел рациональными. «Математическое просвещение», вып.1, М.: ГТТИ, 1957.
51. Гельфонд А.О. Решение уравнений в целых числах. Популярные лекции по математике. Вып. 8-М.: ГТТИ, 1952.

53. Матвиевская Г.П. Учение о числе на средневековом Ближнем и Среднем Востоке. Ташкент: Фан, 1967.
54. Депман И.Я. История арифметики. М.: Просвещение, 1965.
55. Кольман Э. История математики в древности. М.: Физматгиз, 1961.
56. Мухаммад ал -Хорезми. Математические трактаты. пер. с араб. Ю.Х.Копелевича и Б.А.Розенфельда, коментарии Б.А.Розенфельда, Ташкент: "Фан", 1964.
57. Марджанишвили К.К. Простые числа. В сб. «Математика, ее содержание, методы и значение», Том 2. М.: изд. АН СССР, 1956.
58. Ожигова Е.П. Развитие теории чисел в России. Л.: Наука, 1972.
59. Постников А.Г., Романов Н.П. Упрощение элементарного доказательства А.Сельберга асимптотического закона распределения простых чисел. Успехи математических наук. Том 10. №4, 1955.
60. Серпинский В. О. Пифогоровы треугольники. Перевод с польского, учпедчиз, 1959.
61. Серпинский В. О. О решении уравнений в целых числах. Перевод с польского. М.: ФМ, 1961.
62. Сернинский В. Что мы знаем и чего не знаем о простых числах. Перевод с польского И.Г.Мельникова, М.-Л.ФМ, 1963.
63. Хинчин А.Я. Три жемчужины теории чисел. М.: Наука.

15. XI. 2001 йилда босишга рухсат этилди.
№ 250 буюртма, 12,75 босма табоқ,
ҳажми 60x84 1,16. Адади 100 нусха

СамДУ Нашр-матбаа маркази босмахонасида чоп этилди.
703004, Самарқанд ш., Университет хиёбони, 15.