$$\exists q \in N,\ a = bq$$

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

$$n = p_1^{\alpha_1} p_2^{\alpha_2}$$

$$\tau(n) = (\alpha_1$$

$$\sigma(n) = \frac{p_1^{\alpha_1}}{p_1 - 1}$$

$$a \equiv b \pmod{m} \Leftrightarrow$$

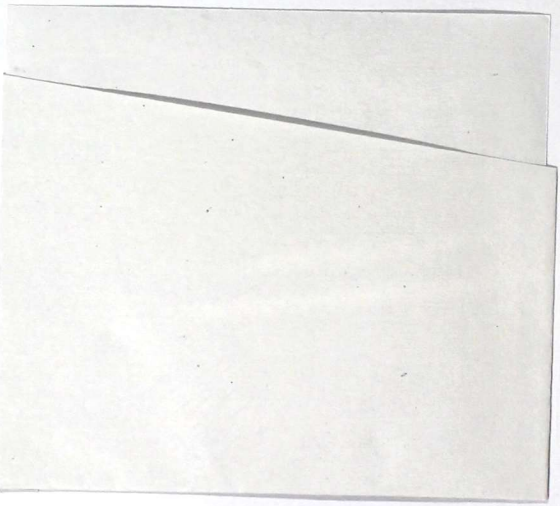
$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

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

$$(a, p)=1,\ a^{p-1} \equiv 1 \pmod{p}$$

ТУРСУНОВ Д. А.
ЭШАРОВ Э. А.
ТУРСУНОВ Э. А.

САНДАР ТЕОРИЯСЫ



КЫРГЫЗ РЕСПУБЛИКАСЫНЫН БИЛИМ ЖАНА ИЛИМ МИНИСТРЛИГИ

ОШ МАМЛЕКЕТТИК УНИВЕРСИТЕТИ

ТОМСК МАМЛЕКЕТТИК АРХИТЕКТУРАЛЫК КУРУЛУШ УНИВЕРСИТЕТИ

ТУРСУНОВ Д.А., ЭШАРОВ Э.А., ТУРСУНОВ Э.А.

САНДАР ТЕОРИЯСЫ

Окуу колдонмо

Ош – 2011

УДК 511

ББК 22.13

Т 88

Окуу колдонмо ОшМУнун Окумуштуулар кеңешинин чечими боюнча басмага сунушталган. Токтом №2, 25.10.2011-ж.

Рецензенттер:

Сатаров Ж. – физ.-мат.илимдеринин доктору, профессор,

Мадраимов С. – пед.илимдеринин кандидаты, профессор.

Д.А. Турсунов. Сандар теориясы. Окуу колдонмо/ Д.А. Турсунов, Э.А. Эшаров, Э.А. Турсунов -Ош:2011. –168 б.

ISBN 978 -9967-03-732-8

Окуу колдонмо «математика», «колдонмо математика жана информатика», «физика», «информатика», «колдонмо информатика» адистиктери боюнча окуган студенттер, атайын мектептин окуучулары жана мугалимдери үчүн сунушталат.

Т 1602030000-11

УДК 511

ББК 22.11

ISBN 978 -9967-03-732-8

МАЗМУНУ

Кириш сөз

Сан түшүнүгү математикадагы негизги түшүнүктөрдүн бири болуп саналат. Математиканы сандарсыз элестетүүгө болбойт. Ошондуктан сандар теориясы курсу математиктерди, информатиктерди, программистерди, өзгөчө математика мугалимин даярдоодо чоң мааниге ээ.

Математиктер үчүн түзүлгөн мамлекеттик стандартка ылайык сандар теориясы курсу төмөнкүлөрдү өз ичине камтыйт:

I. Бөлүнүүчүлүк теориясынын негиздери (бүтүн сандардын алкагында бөлүнүүчүлүк катышы жана анын касиеттери; Эң чоң жалпы бөлүүчү; Евклиддин алгоритми; Өз ара жөнөкөй сандар жана алардын негизги касиеттери; Эң кичине жалпы эселүү; Жөнөкөй жана курама сандар; Арифметикалык функциялар; Үзгүлтүксүз чынжырлуу бөлчөктөр).

II. Салыштыруулар теориясы (Салыштыруулар жана алардын негизги касиеттери; берилген модулу боюнча чегериштердин классы; Эйлердин жана Ферманын теоремалары; бир белгисиздүү биринчи даражадагы салыштыруулар жана аларды чечүүнүн усулдары; биринчи даражадагы салыштыруулардын системасы; жогорку даражадагы салыштыруулар; квадраттык чегериштер; модулу так жана жөнөкөй сан болгон экинчи даражадагы салыштырууларды чечүү; Лежандрдын жана Якобинин символдору; баштапкы тамырлар; индекстер жана алардын касиеттери; салыштырууларды индекстердин жардамында чечүү; салыштыруулардын колдонулуштары)

Окуу колдонмо ушул түшүнүктөрдүн баарын өз ичине камтыйт. Андан сыртқары тиркемеде Pascal программалоо тилинде түзүлгөн программалардын коддору келтирилген. Практикада көпчүлүк учурларда чоң сандар менен иштөөгө туура келет, эсептөөнү жеңилдетүү максатында бул программаларды колдонуу максатка ылайык.

Сандар теориясы бүтүн сандардын касиеттерин үйрөнөт. Бүтүн сандардын көптүгү бизге белгилүү болгондөй Z менен белгиленет жана ал оң, терс натуралдык сандарды, нөлдү өз ичине камтыйт б.а. $Z=\{\ldots, -3, -2, -1, 0, 1, 2, 3,\ldots\}$. Ошондуктан мындан ары биз *a, b, c,*... сандар дегенде бүтүн сандарды гана түшүнөбүз.

Окуу колдонмодо орун алган кемчилдиктерди көрсөтүп анын сапатын жакшыртууга багытталган пикирлерин билгизген физика-математика илимдеринин доктору, профессор Г.Матиевага жана ф.-м.и.к., доцент Г.Борбоевага чоң ыразычылыгыбызды билдиребиз. Окуу колдонмо сандар теориясы боюнча кыргыз тилинде жазылган алгачкы колдонмолордун бири болгондуктан, алдын ала ыразычылык билдирүү менен, сын пикирлериңизди d_osh@rambler.ru, elzare78@rambler.ru электрондук даректерге жөнөтүүңүздөрдү суранабыз.

Белгилөөлөр

$\forall$ – каалагандай, бардыгы үчүн;

$\exists$ – жашайт, табылат;

$*, \cdot$ – көбөйтүү амалы;

$\Rightarrow$ – келип чыгат;

$\in$ – тиешелүү, таандык;

$\wedge$ – жана;

$\vee$ – же;

Def. – аныктама;

N, R – тиешелүү түрдө натуралдык жана чыныгы сандардын көптүгү;

т.д. – теорема далилденди.

§1. Бүтүн сандардын алкагында бөлүнүүчүлүк катышы жана анын касиеттери

1. Бөлүнүүчүлүк катышы жана анын касиеттери

Эгерде $a, b \in Z$ болсо, анда ар дайым

$$a+b \in Z,\ a-b \in Z,\ a \cdot b \in Z$$

болот. Бирок ар дайым эле $a/b \in Z$ боло бербейт. Бүтүн сандардын көптүгү бөлүү амалына (катышына) карата туюк эмес, б.а.

$$\forall a, b \in Z,\ bx = a$$

теңдеме ар дайым бүтүн тамырга ээ болбойт. Мисалы; $2x+3=0$ барабардыкты туура теңдештикке айландыруучу бүтүн сан жок. Бирок айрым учурларда $\frac{a}{b}$ катышы бүтүн сан боло тургандай $a, b \in Z$ сандары жашайт.

Мисалдар

1) Эгерде $a \in Z$, $b = \pm 1$ болсо, анда $\frac{a}{b} = \pm a \in Z$ болот;

2) Эгерде $a = 0$ болуп, $b \neq 0$ болсо, анда $\frac{a}{b} = 0$ болот;

3) Эгерде $a = bk$, $k \in Z$, $b \neq 0$ болсо, анда $\frac{a}{b} \in Z$ болот.

Def 1. Эгерде b, a бүтүн сандар үчүн $a=bq$ шартын канааттандырган q бүтүн саны жашаса, анда a саны b санына бөлүнөт же b саны a санын бөлөт деп аталат.

Эгерде a саны b санына бөлүнсө, анда $b \mid a$ же $a \vdots b$ – көрүнүшүндө белгилинет көбүнчө $b \mid a$ болсо, b саны a

санының **бөлүүчүсү** деп да аталат. $a=bq$ туюнтмада a – бөлүнүүчү, b – бөлүүчү, q – тийинди деп аталат.

Төмөнкү орун алат:

$\forall a,b \in Z,\ a \vdots b \Leftrightarrow b \neq 0 \wedge (\exists q \in Z)\ \ a = bq$.

Мисал. Төмөнкү барабардыктарды карайлы:

$$21=7\cdot 3, \qquad 0=9\cdot 0, \qquad -85=17\cdot(-5).$$

Мында биз 21 саны 7ге бөлүнөт, 0 саны 9га бөлүнөт, –85 саны 17ге бөлүнөт деп айта алабыз. Же болбосо 7 саны 21ди бөлөт, 9 саны 0дү бөлөт, 17саны –85ди бөлөт деп айтууга болот.

Теорема 1. Эгерде a жана $b \neq 0$ болуп, $a = bq$ барабардыгын канааттандыруучу q саны жашаса (табылса), анда ал жалгыз гана болот.

Далилдөө. Далилдөөнү карама-каршысынан жүргүзөбүз. Айталы $a = bq$ шартын канааттандыруучу жок дегенде эки ар түрдүү q_1 жана q_2 сандар табылсын, б.а. $a=bq_1$ жана $a=bq_2$ болсун. Анда барабардыктардын сол жактары барабар болгондуктан, алардын оң жактары да барабар экендиги келип чыгат, б.а. $b(q_1-q_2)=0$ болот. Бирок, $b\neq 0$ болгондуктан жана Z бүтүн сандардын көптүгүндө нөлдүн бөлүүчүсү болбогондуктан $q_1-q_2=0 \Rightarrow q_1=q_2$ келип чыгат. Мындан биз карама-каршылыкка келдик. Демек, q тийинди жалгыз гана болот экен. т.д.

Бөлүнүүчүлүк катышынын касиеттери

1^0. $\forall a\in Z, a\neq 0, \quad 0 \vdots a$;

2^0. $\forall a\in Z, a \vdots 1$;

3^0. $\forall a\in Z, a \vdots a$;

4^0. $\forall a, b, c \in Z, b \neq 0, c \neq 0, a \vdots b \wedge b \vdots c \Rightarrow a \vdots c$;

5^0. $\forall a, b\in Z, b \neq 0, a \neq 0, a \vdots b \wedge b \vdots a \Rightarrow b = a \vee b = -a$;

6^0. $\forall a, b, c\in Z, c\neq 0, \ a \vdots c \Rightarrow ab \vdots c$;

7^0. $\forall a, b, c\in Z, \ a \vdots c \wedge b \vdots c \Rightarrow (ua+vb) \vdots c$;

8^0. $\forall a, b \in Z,\ a:b \wedge a \neq 0 \Rightarrow |a| \geq |b|$;

9^0. $\forall a, b \in Z,\ a:b \Rightarrow a:(-b)$;

10^0. $\forall a, b, c, t, q \in Z,\ a:c \wedge b:c \wedge a=bq+t \Rightarrow t:c$;

11^0. $\forall a, b \in Z,\ a:b \Leftrightarrow |a|:|b|$;

12^0. $\left(\forall\ b_i,\ a \in Z,\ a \neq 0,\ (i=\overline{1.r})\right) b_1 / a \wedge b_2 / a \wedge \ldots \wedge b_r / a$ болуп $\lambda_1, \lambda_2, \ldots, \lambda_r$ каалагандай бүтүн сандар болсо, анда

$$(b_1\lambda_1+b_2\lambda_2+\ldots+b_r\lambda_r) / a \text{ болот.}$$

Биз бул касиеттерден акыркысын гана далилдейли. Калган касиеттер окурманга өз алдынча далилдөө үчүн сунушталат.

12^0-касиетти далилдөө. Бөлүнүүчүлүктүн аныктоосунун негизинде

$$b_i = aq_i \quad \left(i=\overline{1.r}\right),$$

барабардыгы орун ала тургандай q_i лер табылат. Барабардыктын эки жагын тең тиешелүү түрдө λ_i ге көбөйтүп, натыйжаны мүчөлөп кошобуз, анда

$$\sum_{i=1}^{r} b_i\lambda_i = \sum_{i=1}^{r} aq_i\lambda_i,$$

барабардыгы пайда болот. Акыркы барабардык $\sum_{i=1}^{r} b_i\lambda_i$ ны a санына бөлүнүшүн көрсөтөт. Касиет далилденди.

2. Калдыктуу бөлүү

Def 2. a жана $b \neq 0$ бүтүн сандары үчүн

1) $a=bq+r$;

2) $0 \leq r < |b|$,

шарттарын канааттандыруучу q жана r сандарын табуу, a санын b санына калдыктуу бөлүү деп аталат. Мында q – толук эмес тийинди, r –калдык деп аталат.

Теорема 2. Каалагандай a жана $b \neq 0$ бүтүн сандары үчүн a ны bга ар дайым калдыктуу бөлүүгө болот жана ал жалгыз болот.

Далилдөө. Алгач ар дайым a санын b санына бөлүүгө боло тургандыгын далилдейбиз. Мүмкүн болгон бардык учурларды карап чыгалы:

1) $\forall a \in Z$, $b>0$.

b га эселүү болгон бардык бүтүн сандарды өсүү тартибинде жайгаштыралы:

$$..., b\cdot(-2), b\cdot(-1), b\cdot 0, b\cdot 1, b\cdot 2, ...$$

Айталы bq саны a дан чоң эмес b нын эң чоң эселүүсү болсун. Анда $a \geq bq$ жана

$$a<b(q+1) \Rightarrow bq \leq a < b(q+1) \Rightarrow 0 \leq a-bq < b$$

келип чыгат.

Эгерде $a-bq=r$ деп алсак, анда $0 \leq r < b$ жана $a = bq + r$ болот.

2) $\forall a \in Z$, $b<0$.

$b<0$ болгондуктан $(-b)>0$ болот, 1) учурду эске алсак a саны $(-b)$ га калдыктуу бөлүнөт, бул q жана r сандары жашайт дегенди билдирет б.а.

$$a=(-b)q+r,\ 0 \leq r < |-b| \text{ же } a=b(-q)+r,\ 0 \leq r < |b|.$$

Ар дайым калдыктуу бөлүүгө боло тургандыгы далилденди. Эми калдыктуу бөлүүнүн жалгыздыгын далилдейбиз.

Далилдөөнү карама-каршысынан жүргүзөбүз. Айталы a саны b санына бир түрдүү бөлүнбөсүн, б.а.

$\exists\, q_1, q_2, r_1, r_2 \in Z$: $a=bq_1+r_1,\ 0 \leq r_1 < |b|$,

$$a=bq_2+r_2,\ 0 \leq r_2 < |b|$$

болсун, анда $bq_1+r_1=bq_2+r_2$ же $b(q_1-q_2)=r_2-r_1$ болот. $0 \leq r_1 < |b|$ жана $0 \leq r_2 < |b|$ дан $|r_1-r_2| < |b|$ келип чыгат. Бирок $b(q_1-q_2)=r_2-r_1$ ден (r_2-r_1)ди b га бөлүнө тургандыгы келип чыгат. Бул $r_2-r_1=0$ же $r_2=r_1$ болгондо гана аткарылат, анда $b(q_1-q_2)=0 \Rightarrow q_1-q_2=0$ же $q_1=q_2$, себеби $b \neq 0$. Демек, $q_1=q_2$ жана $r_1=r_2$. Жалгыздыгы далилденди.

3. Математикалык индукция усулу

Математикалык индукция усулу далилдөөнү талап кылган натуралдык сандардан көз каранды болгон $A(n)$ математикалык сүйлөмдөрдү далилдөө үчүн колдолунат. Бул метод чектүүдөн чексизге өтүүдөгү математиканын күчүн көрсөтөт.

Математикалык индукция усулун колдонуунун алгоритми

Мейли бизге $A(n)$ ырастоосун ар кандай $n \in N$ үчүн тууралыгын далилдөө талап кылынсын.

1-кадам. $A(1)$ дин тууралыгы (чын экендиги) текшерилет, айрым учурларда эгерде $n \geq n_1$ шарт коюлган болсо, анда $A(n_1)$ дин тууралыгы текшерилет.

2-*кадам.* $A(n)$ $n=2,3,\ldots,k$ калагандай k натуралдык сан үчүн туура деп божомолдойбуз.

3-*кадам.* 2-кадамды пайдаланып $A(k+1)$дин туура (чын) экендиги далилденет.

Эгерде бул кадамдар ийгиликтүү басып өтүлсө анда $A(n)$ – ырастоосу ар кандай $n \in N$ үчүн туура (чын) болот.

Мисал 1. Математикалык индукция усулун колдонуп төмөнкү барабардыкты далилдегиле:

$$1+2+3+\ldots+n=n(n+1)/2.$$

Далилдөө. 1-кадам. $n=1$ үчүн текшеребиз:

$$1=1(1+1)/2 \Rightarrow 1=1.$$

2-кадам. $n=k$ үчүн барабардык туура болсун деп божомолдойбуз:

$$1+2+3+\ldots+k=k(k+1)/2.$$

3-кадам. $n=k+1$ үчүн далилдейбиз, б.а.

$$1+2+3+...+k+(k+1)=(k+1)(k+2)/2$$

барабардыгын чын экендигин көрсөтөбүз.

Акыркы барабардыктын сол жагынан оң жагын келтирип чыгарабыз:

$$\underbrace{1+2+3+...+k}_{k(k+1)/2}+(k+1)=k(k+1)/2+(k+1)=(k+1)(k+2)/2\ ,$$

мында биз алгачкы k кошулуучунун суммасы үчүн 2-кадамды эске алдык.

Мисал 2. Далилдегиле $(4^n+6n-1)\vdots 9$.

Далилдөө. 1-кадам. $n=1$: $(4+6-1)=9\vdots 9$ туура;

2-кадам. $n=k$: $(4^k+6k-1)\vdots 9$ аткарылсын деп божомолдойбуз;

3-кадам. $n=k+1$: $(4^{k+1}+6(k+1)-1)\vdots 9$ далилдейбиз.

$$(4\cdot 4^k+6k+5)=4(4^k+6k-1)-9(2k-1),$$

2-кадам бонча 1-кашаа 9га бөлүнөт, 2 кашаа 9га бөлүнөт, анда алардын айрымасыда 9га бөлүнөт.

Өз алдынча иштөө үчүн көнүгүүлөр

1) Эгерде $a=42157$ санын кандайдыр бир b санына бөлгөндө тийинди $q=231$ болсо, b менен калдык r ди тапкыла.
2) Эгерде $mn+pq$ туюнтма $m-p$ га бөлүнсө, анда бул туюнтманы $m-n$ ге да бөлүнө тургандыгын далилдегиле, мында $m, p, q, n\in Z$.
3) Эгерде $(ad-bc)\vdots n$, $(a-b)\vdots n$, $(b,n)=1$ болсо, $(c-d)\vdots n$ экендигин далилдегиле, мында $a, b, c, d, n\in Z$.
4) Эгерде беш орундуу $\overline{abcde}$ сан 41 ге бөлүнсө, анда $\overline{eabcd}$, $\overline{deabc}$, $\overline{cdeab}$, $\overline{bcdea}$ сандары да 41 ге бөлүнө тургандыгын далидегиле. Ар бир тамгага бир цифра туура келет.
5) $(m^5-m)\vdots 30$, $m\in N$ экендигин далидегиле.
6) Кандайдыр бир алты орундуу сан 5 цифра менен аяктайт. Эгерде бул цифраны сол жактан биринчи орунга алып

өткөндө, пайда болгон сан алгачкы сандан 4 эсе чоң болсо, анда алгачкы санды тапкыла.

7) $n(n+1)(2n+1)\vdots 6$, $n \in N$ экендигин далилдегиле.

8) $n(n^2+5)\vdots 6$, $n \in N$ экендигин далилдегиле.

9) Эгерде бөлчөктүн алымы так сандардын квадраттарынын айырмасы, ал эми бөлүмү ушул так сандардын квадраттарынын суммасы болсо, анда бөлчөк 2 ге кыскара тургандыгын жана 4кө кыскарбай тургандыгын далилдегиле.

10) Эгерде $\overline{abcd}$ төрт орундуу сан кандайдыр бир сандын толук квадраты болуп, $b=c$, $a+1=d$ болсо, бул 4 орундуу санды тапкыла.

11) Беш удаалаш келген сандардын квадраттарынын суммасы толук квадрат боло албай тургандыгын далилдегиле.

12) Сумманы тапкыла: $S = 7 + 77 + 777 + ... + \underbrace{77...7}_{n \text{ цифра}}$.

13) $2^{2^n}+1$ саны 7 менен аяктай тургандыгын далилдегиле, мында $n>1$ – натуралдык сандар.

14) 1 жана 6 цифраларынын ортосуна 15 саны жазылганда 1156 саны пайда болот. Ал эми пайда болгон санды түзүүчү цифралардын ортосуна дагы 15 саны жазылса 111556 саны пайда болот, ж.б.у.с. Пайда болгон сандардын толук квадрат болушун далилдегиле.

15) $\forall m, n \in N$, $mn(m^4 - n^4)\vdots 30$ экендигин далилдегиле.

16) $\forall n \in Z$, $3n^2+2$ туюнтма толук квадрат боло албай тургандыгын далилдегиле.

17) $\forall n \in N$, $(n+1)(n+2)...(n+n)\vdots 2^n$ экендигин далилдегиле.

Далилдегиле (18-42)

18) $(n^4+6n^3+11n^2+6n)\vdots 24$;

19) $(n^5-5n^3+4n)\vdots 120$;

20) $(n^5 - n) \vdots 30$;

21) $(n^7 - n) \vdots 42$;

22) $(2^{4n} - 6n) \vdots 10$;

23) $(4^{2n} - 3^{2n} - 7) \vdots 84$;

24) $(6^{2n-1} + 1) \vdots 7$;

25) $(n+1)(n+2) \ldots (n+n) \vdots 2^n$;

26) $(11^{n+2} - 12^{2n+1}) \vdots 133$;

27) $(10^n + 18n - 1) \vdots 27$;

28) $(3^{2n+3} + 40n - 27) \vdots 64$;

29) $(4^n + 6n - 1) \vdots 9$;

30) $(10^{n+1} - 9n - 10) \vdots 81$;

31) $(9^{n+1} - 8n - 9) \vdots 16$;

32) $(5^n + 2 \cdot 3^{n-1} + 1) \vdots 8$;

33) $(3^{2n+3} - 24n + 37) \vdots 64$;

34) $(6^{2n} + 3^{n+2} + 3^n) \vdots 11$;

35) $(n^3 + 3n^2 - n - 3) \vdots 48$;

36) $(n^4 - 4n^3 - 4n^2 + 16n) \vdots 384$;

37) $(3^{4n-1} + 3^{4n-2} + \ldots + 3^2 + 3 + 1) \vdots 40$;

38) $(n^4 + 6n^3 + 11n^2 + 6n) \vdots 12$;

39) $(n^5 - 5n^3 + 4n) \vdots 12$;

40) $(9^{n+1} - 8n - 9) \vdots 4$;

41) $(3^{2n+3} - 24n + 37) \vdots 16$;

42) $(3^{4n-1} + 3^{4n-2} + \ldots + 3^2 + 3 + 1) \vdots 8$.

43) Эгерде $a > b > 0$ болсо, анда a ны bга бөлгөндө пайда боло турган калдык $a/2$ ден кичине экендигин далилдегиле.

44) Каалагандай так сандын квадратын 8ге бөлгөндөгү калдык 1ге барабар экендигин далилдегиле.

45) Эгерде a ны bга бөлгөндө пайда боло турган калдык r болсо, анда a^n ди b^n ге бөлгөндөгү калдык менен r^n ди bга бөлгөндөгү калдык барабар экендигин далилдегиле.

46) Эгерде a^5 ди 7ге бөлгөндөгү калдык 5ке барабар болсо, анда a ны 7ге бөлгөндөгү калдыкты тапкыла.

47) 23^n санын 7ге бөлгөндөгү калдыкты тапкыла, $n \in N$.

48) 65^{6n}, 65^{6n+1}, 65^{6n+2}, 65^{6n+3}, 65^{6n+4}, 65^{6n+5} сандарын 9га бөлгөндөгү калдыктарды тапкыла, $n \in N$.

49) каалаган сандын квадраты же 3кө бөлүнөт же 3кө бөлгөндөгү калдык 1ге барабар боло тургандыгын далилдегиле.

50) a жана bны mге бөлгөндө пайда боло турган калдыктар барабар болгон учурда гана $(a-b)$ саны mге бөлүнө тургандыгын далилдегиле.

§2. Эң чоң жалпы бөлүүчү (ЭЧЖБ). Евклиддин алгоритми

1. ЭЧЖБ

Def 1. Эгерде $a_1, a_2, ..., a_n$ бүтүн сандарынын ар бири $\delta \neq 0$ бүтүн санына бөлүнсө, анда $\delta \in Z$ бул сандардын жалпы бөлүүчүсү деп аталат.

Def 2. Эгерде $d \neq 0$ саны $a_1, a_2, ..., a_n$ сандарынын

1) жалпы бөлүүчүсү болсо,

2) d саны $a_1, a_2, ..., a_n$ сандарынын каалагандай жалпы бөлүүчүсүнө бөлүнсө,

анда d саны $a_1, a_2, ..., a_n$ бүтүн сандарынын эң чоң жалпы бөлүүчүсү (ЭЧЖБ) деп аталат.

Теорема 1. $a_1, a_2, ..., a_n$ бүтүн сандарынын ЭЧЖБсы анын белгисине чейинки тактыкта бир маанилүү аныкталат (б.а. эгерде $a_1, a_2, ..., a_n$ сандарынын ЭЧЖБсы d_1 жана d_2 болсо, анда $d_1 = d_2$ же $d_1 = -d_2$).

Далилдөө. Айталы $a_1, a_2, ..., a_n$ сандарынын ЭЧЖБсы d_1 жана d_2 болсун. Анда d_1 бул сандардын каалагандай жалпы бөлүүчүсүнө бөлүнөт $d_1 \vdots d_2$. Аналогиялуу түрдө $d_2 \vdots d_1$ келип чыгат. Бирок $d_1 \vdots d_2$ жана $d_2 \vdots d_1$ катыштары $d_1 = d_2$ же $d_1 = -d_2$ болгон учурда гана аткарылат. Теорема далилденди.

$a_1, a_2, ..., a_n$ сандарынын ЭЧЖБсынын ар дайым оң маанисин алабыз жана бул маанини $d = (a_1, a_2, ..., a_n)$ деп белгилейбиз.

Мисал. 100 жана 140 сандарынын ЭЧЖБсын тапкыла?

Чыгаруу. 100 жана 140 сандарын бөлүүчүлөрүн аныктайлы:

$A = \{1, 2, 4, 5, 10, 20, 25, 50, 100\}$,

$B = \{1, 2, 4, 5, 7, 10, 14, 20, 28, 35, 70, 140\}$.

Бул көптүктөрдүн кесилишүүсүн аныктайлы:

$$A \cap B = \{1, 2, 4, 5, 10, 20\}.$$

Демек, (100, 140)=20, себеби 20 саны A∩B көптүктүн каалаган элементине бөлүнөт.

2. Евклиддин алгоритми

Def 1 ден a_1, a_2,..., a_n сандарынын ЭЧЖБсы ар дайым эле жашайт деп айта албайбыз. Бирок ЭЧЖБнын ар дайым жашашын Евклиддин алгоритми деп аталуучу усул менен көрсөтүүгө болот. Бул усул төмөнкү леммаларга таянат (негизделет).

Лемма 1. Эгерде $a \vdots b$ болсо, анда $(a, b)=b$ болот.

Далилдөө. Биринчиден $a \vdots b$ жана $b \vdots b$ болгондуктан, b саны aнын жана b нын бөлүүчүсү болот. Экинчиден, эгерде a нын жана b нын каалаган жалпы бөлүүчүсү c болсо, анда ал b нында бөлүүчүсү болот. Def 2нин эки шарты тең аткарылгандыктан $(a, b)=b$ экендиги келип чыгат.

Лемма 2. Эгерде $a=bq+r$ ($a\neq0$, $b\neq0$, $r\neq0$) болсо, анда $(a, b)=(b, r)$ болот.

Далилдөө. Мейли a нын жана b нын жалпы бөлүүчүсү δ болсун, анда $a \vdots \delta$ жана $b \vdots \delta$ болот. $a=bq+r$ болгондуктан, $r = a - bq$ дагы δ га бөлүнөт б.а. $r \vdots \delta$. Ошондуктан a нын жана b нын каалаган жалпы бөлүүчүсү b нын жана r дин дагы жалпы бөлүүчүсү болот. Тескерисинче, эгерде $b \vdots \delta$ жана $r \vdots \delta$ болсо, анда $a = bq+r$ дагы δ га бөлүнөт. Ошондуктан b нын жана r дин каалаган жалпы бөлүүчүсү a нын жана b нын да жалпы бөлүүчүсү болот. Демек, a нын жана b нын жалпы бөлүүчүлөрүнүн А көптүгү, b жана r дин жалпы бөлүүчүлөрүнүн В көптүгү менен дал келет, б.а. $A = B$.

Мейли $(a, b) = d$ болсун, анда $d \in A$ жана d саны A көптүгүнүн каалаган элементине бөлүнөт. $A = B$ болгондуктан, $d \in B$ жана d саны B көптүгүнүн каалагандай элементине бөлүнөт, б.а.

$(b, r)=d$. Мындан $(a, b) = (b, r)$ экендиги келип чыгат. Ошентип Лемма 2 далилденди.

a жана *b* сандарынын ЭЧЖБсын табуу үчүн Евклиддин алгоритми

Евклиддин алгоритми төмөнкү кадамдар менен ишке ашат:

1-кадам: a санын b санына бөлөбүз, $a>b>0$, эгерде бөлүнсө, анда $(a, b)=b$ болот, эгерде бөлүнбөсө, анда 2-кадамга өтөбүз;

2-кадам: $a=bq_0+r_1$ болот. b санын r_1 ге бөлөбүз, эгерде бөлүнсө, анда $(b, r_1)=r_1 \Rightarrow (a, b) = (b, r_1)=r_1$ болот, эгерде бөлүнбөсө, анда 3-кадамга өтөбүз;

3-кадам: $b=r_1q_1+r_2$ болот. r_1 санын r_2 ге бөлөбүз, эгерде бөлүнсө, анда $(r_1, r_2)=r_2 \Rightarrow (a, b) = (b, r_1) = (r_1, r_2)=r_2$ болот, эгерде бөлүнбөсө, анда кийинки кадамга өтөбүз, ушул процессти калдык нөл болгонго чейин улантабыз.

Ар бир кадамда калдык кемип барат

$$0\le r_n<\ldots<r_2<r_1<b,$$

жана алар натуралдык сандар болушат, ошондуктан кандайдыр бир кадамда калдыксыз бөлүүнү алабыз, б.а. калдык нөлгө барабар болуп калат. Акыркы нол эмес калдык a жана b сандарынын ЭЧЖБсы болот.

Бул алгоритмди теорема көрүнүшүндө баяндайлы:

Теорема 2. Эгерде $a=bq_0+r_1;\ 0\le r_1<b,$

$b=r_1q_1+r_2;\ 0\le r_2<r_1,$

. . .

$r_{n-2}=r_{n-1}q_{n-1}+r_n;\ 0\le r_n<r_{n-1},$

$r_{n-1}=r_nq_n,$

болсо, анда $(a,b)=r_n$ болот.

Далилдөө. Лемма 2нин негизинде 1-жолчодон $(a, b)=(b, r_1)$, 2-жолчодон $(b, r_1) = (r_1, r_2)$, ж.б.у.с. келип чыгат. Демек $(a, b)=(r_{n-1}, r_n)$. Бирок $r_{n-1}:r_n$, анда лемма 1дин негизинде

$(r_{n-1}, r_n) = r_n$ болот. Ошондуктан $(b, r_1)=r_n$. Төмөнкүдөй мисалдарды карайлы:

Мисал 1. 2346 жана 646 сандарнын ЭЧЖБсын табалы.

$2346=3\cdot646+408,$

$646=1\cdot408+238,$

$408=1\cdot238+170,$

$238=1\cdot170+68,$

$170=2\cdot68+34,$

$68=2\cdot34.$

Акыркы нол эмес калдык $r_5=34$, демек, $(2346, 646)=34$.

Эми эки сандын ЭЧЖБсүн Евклиддин алгоритминин жардамында мамыча түрүндө табалы.

Мисал 2. $(525, 231)$ =?

525	231	2	$525=231\cdot2+63$
462			
231	63	3	$231=63\cdot3+42$
189			
63	42	1	$63=42\cdot1+21$
42			
42	**21**	2	$42=21\cdot2$
42			
0			

Бул жерде акыркы нөл эмес калдык 21 болуп жатат. Ошондуктан, 2-теорема боюнча 525 жана 231 сандарынын ЭЧЖБсы 21 болот.

Демек, Евклиддин алгоритминен $\forall a, b \in Z$ сандарынын ЭЧЖБсынын жашашы келип чыгат. Албетте (0,0) дон башка, себеби бул сандар үчүн ЭЧЖБ жашабайт.

Качан a_1, a_2,..., a_n сандарынын ЭЧЖБсы жашайт деген сурооно төмөнкү теорема жооп берет.

Теорема 3. Эгерде $(a_1, a_2,..., a_{n-1})=\delta$ жана $d=(\delta, a_n)$ болсо, анда $(a_1, a_2, ..., a_n)=d$ болот.

Далилдөө. $d=(\delta, a_n)$ болгондуктан $a_n \vdots d$ жана $\delta \vdots d$ келип чыгат.

Ал эми $(a_1, a_2,..., a_{n-1})=\delta$ болгондуктан, $\forall k,\ 1\le k\le n-1,\ a_k \vdots \delta \Rightarrow a_k \vdots d$.

Демек, d саны $a_1, a_2,..., a_n$ сандардын жалпы бөлүүчүсү болот.

Эми d нын ЭЧЖБ экендигин көрсөтөбүз. Мейли d_1 саны a_1, $a_2,..., a_n$ дердин жалпы бөлүүчүсү болсун. Анда d_1 саны $a_1, a_2,..., a_{n-1}$ сандардын да жалпы бөлүүчүсү болот жана $\delta \vdots d_1$. Бирок $a_n \vdots d_1$, себеби $(\delta, a_n) = d \vdots d_1$. Анда d саны $a_1, a_2,..., a_n$ сандарынын каалагандай жалпы бөлүүчүсүнө бөлүнөт, мындан $(a_1, a_2,..., a_n)=d$ келип чыгат.

Бул теоремадан төмөнкү натыйжа келип чыгат:

Натыйжа. Эгерде $(a_1, a_2)=d_1$, $(d_1, a_3)=d_2$, ..., $(d_{n-2}, a_n)=d_{n-1}$ болсо, анда $(a_1, a_2,..., a_n)=d_{n-1}$ болот.

Далилдөө. Далилдөөнү математикалык индукция усулу менен жүргүзөлү. $n=2$ болгондо $(a_1,a_2)=d_1$ аткарылат. Мейли $n=k>2$ үчүн далилденген болсун. Анда $(a_1, a_2) = d_1, (d_1, a_3) = d_2$, ..., $(d_{k-2}, a_n) = d_{k-1}$ ден $(a_1, a_2,..., a_k)=d_{k-1}$ болот. Эгерде $(d_{k-1}, a_{k+1})=d_k$ болсо, анда теорема 3 түн негизинде $(a_1, a_2,..., a_n)=d_{n-1}$ болот. Демек, ырастоо $n=k+1$ үчүн да туура экен. Математикалык индукциянын принциби боюнча $\forall n\in N$ үчүн ырастоо туура болот.

3-Теореманын бул натыйжасы бир канча чектүү сандагы сандардын ЭЧЖБсын табуунун жолун көрсөтөт: алгач $(a_1, a_2)=d_1$ табылат, андан соң $(d_1, a_3)=d_2$ ге ээ болобуз, ж.б. акырында $(d_{n-1}, a_n)=d_{n-1}$ ны алабыз. Ошондо $(a_1, a_2,..., a_n)=d_{n-1}$ болот.

Жогоруда айтылгандар боюнча төмөнкү төрт сандын ЭЧЖБсын табууну карайлы.

Мисал. (988, 2014, 42598, 6726)=?

Чыгаруу. Бул сандардын ЭЧЖБсын табуу үчүн Евклиддин алгоритмин удаалаш пайдаланалы:

$d_1=(988, 2014)=26$,

$d_2=(26, 42598)=2$,

$d_3=(2, 6726)=2$ ээ болобуз.

Демек, $d=(988, 2014, 42598, 6726)=2$ болот.

3. ЭЧЖБнын касиеттери

1^0. Эгерде $(a_1, a_2,..., a_n)=\delta$ болсо, анда δ саны $a_1, a_2,..., a_n$ сандардын жалпы бөлүүчүсүнүн эң чоңу болот.

Далилдөө. Белгилөө боюнча $(a_1, a_2,..., a_n)=\delta>0$, болгондуктан $(a_1, a_2,..., a_n)=d$ саны δ га бөлүнөт. Анда $d\geq\delta$ келип чыгат. Бирок δ – жалпы бөлүүчүлөрдүн эң чоңу, d – жалпы бөлүүчүлөрдүн бири болгондуктан $\delta\geq d$ болот. Ал эми $d\geq\delta$ жана $\delta\geq d$ барабарсыздыктарынан $\delta=d$ экендиги келип чыгат.

2^0. Эгерде $(a, b)=d$ болсо, анда $(k\,a,\ k\,b)=k\,d \quad k\neq 0$ болот.

Далилдөө. Бул касиетти Теорема 2 нин жардамында далилдейбиз:

$$ak=b\,k\,q_0+r_1k;$$
$$b\,k=r_1\,k\,q_1+r_2k;$$
$$\cdots$$
$$r_{n-2}k=r_{n-1}\,k\,q_{n-1}+r_nk;$$
$$r_{n-1}\,k=r_n\,k\,q_n,$$

демек, $(ak, bk)=kr_n=(a, b)\,k$.

3^0. Эгерде $a\vdots\delta, b\vdots\delta$ болсо, анда $\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{1}{\delta}(a,b)$.

Далилдөө. $(a,b)=\left(\frac{a}{\delta}\delta,\frac{b}{\delta}\delta\right)=\left(\frac{a}{\delta},\frac{b}{\delta}\right)\delta \Rightarrow \left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{1}{\delta}(a,b)$ болот.

4^0. Эгерде $(a, b)=d$ болсо, анда $\exists\, x, y\in Z$: $ax+by=d$ болот.

Мында $ax+by=d$ барабардыгы a жана b сандарынын ЭЧЖБсынын бул сандар аркылуу сызыктуу туюнтулушу деп аталат.

Далилдөө. Евклиддин алгоритмин эске алсак:

$$r_1=a-dq_0=ax_1+by_1,$$

мында $x_1=1, y_1=-q_0,\ x_1, y_1\in Z$;

$$b=r_1q_1+r_2 \Rightarrow r_2=b-r_1q_1=b-(ax_1+by_1)q_1=-ax_1q_1+b(1-q_1y_1)=ax_2+by_2,$$

мында $x_2=-x_1q_1, y_2=1-q_1y_1,\ x_2, y_2\in Z$;

бул процессти улантып, $r_n=ax_n+by_n$ деп алабыз, $x_n, y_n\in Z$; $r_n=d$ болгондуктан $d=ax+by$ болот, $x=x_n$, $y=y_n$.

Мисал. 90 жана 35 сандарынын ЭЧЖБсын бул сандар аркылуу сызыктуу туюнткула.

Чыгаруу. Евклиддин алгоритмин колдонобуз:

$$90=35\cdot2+20 \Rightarrow 20=90-35\cdot2,$$
$$35=20\cdot1+15 \Rightarrow 15=35-20\cdot1,$$
$$20=15\cdot1+5 \Rightarrow 5=20-15\cdot1$$
$$15=5\cdot3.$$

Демек, $(90, 35)=5$. Анда

$$5=90-35\cdot2-(35-(90-35\cdot2))=2\cdot90+(-5)\cdot35 \Rightarrow 5=2\cdot90+(-5)\cdot35 \Rightarrow x=2, y=-5.$$

5^0. Эгерде $(a_1, a_2,..., a_n)=d$ болсо, анда $\exists\, x_1, x_2,..., x_n\in Z$: $\sum_{i=1}^{n} a_ix_i = d$ болот.

Өз алдынча иштөө үчүн көнүгүүлөр

1) Эгерде $a=cq+r$, $b=cq_1+r_1$, a, b, q, q_1, r, r_1 – терс эмес бүтүн сандар, c – оң бүтүн сан болсо, анда $(a, b, c)=(c, r, r_1)$ экендигин далилдегиле.

Төмөнкү a жана b сандары боюнча $d=(a, b)$ ны тапкыла жана $d=ax+by$ орун ала тургандай $x, y\in Z$ терди тапкыла [2-7]:

2) $a=899$, $b=493$; 3) $a=1445$, $b=629$; 4) $a=903$, $b=731$;
5) $a=1786$, $b=705$; 6) $a=4543$, $b=885$; 7) $a=6919$, $b=1443$.

8) Эгерде a, b, c – так сандар болсо, $(a,b,c)=\left(\frac{a+b}{2},\frac{a+c}{2},\frac{c+b}{2}\right)$ барабардыгынын орун алышын далилдегиле.

9) $\forall a,b\in N$, $(a,b)=(5a+3b,13a+8b)$ экендигин далилдегиле.

10) Эгерде (a, b)=1 болсо, анда $\frac{1}{a}+\frac{1}{a+b}$ кыскарбас бөлчөк экендигин көрсөткүлө.

11) Эгерде a_1, a_2,..., a_n сандарынын эң чоң жалпы бөлүүчүсү d болсо, анда $d=v_1a_1+v_2a_2+...+v_na$ барабардыгы орун ала тургандай v_1, v_2, ... v_m, бүтүн сандарынын жашашын далилдегиле.

12) Барабардык аткарылабы:

$(2^3\cdot5\cdot13\cdot45, 5^{23}\cdot11^6\cdot21)=(6\cdot35\cdot10, 17^4\cdot15\cdot55)$?

13) Натуралдык сандардын суммасы 153кө барабар. Алардын ЭЧЖБсын кабыл ала турган эң чоң маанисин тапкыла.

14) m жана a>1 натуралдык сандары үчүн төмөнкү барабардыкты далилдегиле:

$$\left(\frac{a^m-1}{a-1},\ a-1\right)=(a-1,\ m).$$

15) Эгерде d_1=ЭЧЖБ(a, b), d_2=ЭЧЖБ(x, y) болсо, анда ЭЧЖБ(ax, ay, bx, by)= d_1d_2 экендигин далилдегиле.

Төмөнкү сандардын ЭЧЖБсын тапкыла [16-19]:

16) 420, 630, 1155; 17) 1023, 1518, 14883;

18) 498, 2324, 42598; 19) 663, 731, 2516, 3655.

20) Эгерде a/b бөлчөк кыскарбас болсо, анда $\frac{b-a}{b}$ бөлчөгү да кыскарбас экендигин далилдегиле.

21) Эгерде ЭЧЖБ(a_1, c)= ЭЧЖБ(a_2, c)=1 болсо, анда ЭЧЖБ(a_1a_2, c)=1 болобу?

22) Эгерде ЭЧЖБ(a, b)=1, $c\vdots a$, $c\vdots b$ болсо, анда $c\vdots ab$ болобу?.

23) Эгерде ЭЧЖБ(a_1, a_2, …, a_n)=1, $c\vdots a_1$, $c\vdots a_2\wedge$, …, $\wedge\ c\vdots a_n$ болсо, анда $c\vdots a_1a_2\ldots a_n$ аткарылабы?

Төмөнкү барабардыктарды текшергиле [24-28]:

24) ЭҮЖБ(a, b)= ЭҮЖБ($-a$, b);

25) ЭҮЖБ(a, b)= ЭҮЖБ($a-b$, b);

26) ЭҮЖБ(a, b)= ЭҮЖБ($a+b$, $a-b$);

27) ЭҮЖБ(a, ЭҮЖБ (b, c))= ЭҮЖБ(ЭҮЖБ (a, b), c);

28) ЭҮЖБ(a_1, a_2,…, a_n)= ЭҮЖБ(a_2,…, a_n).

29) Эгерде үч удаалаш келген натуралдык сандардын ортосундагы сан кандайдыр бир сандын кубу болсо, анда бул үч натуралдык сандардын көбөйтүндүсү 504кө бөлүнө тургандыгын далилдегиле.

30) Далилдегиле $\left(a^{4n+1}-a\right)\vdots 30$, $a\in Z$, $n\in Z^+$.

Төмөнкүлөр орун алабы [31-35]:

31) ЭҮЖБ(a, c)=1 $\Rightarrow$ $b\vdots$ ЭҮЖБ(ab, c);

32) ЭҮЖБ(a, b)=1 $\Rightarrow$ ЭҮЖБ(ac, b)= ЭҮЖБ(b, c);

33) ЭҮЖБ(a, b)=1 $\Rightarrow$ ЭҮЖБ(a+b, ab)=1;

34) ЭҮЖБ(a, b)=1 $\Rightarrow$ ЭҮЖБ($5a+3b$, $8a+5b$)=1;

35) ЭҮЖБ(a, b)=1 $\Rightarrow$ ЭҮЖБ($11a+2b$, $18a+5b$)=1 $\vee$ ЭҮЖБ($11a+2b$, $18a+5b$)=19.

36) Далилдегиле:

a) ЭҮЖБ(n, $n+1$)=1; b) ЭҮЖБ(n, $2n-1$)=1;

c) ЭҮЖБ$\left(\frac{n(n+1)}{2}, 2n+1\right)=1$.

37) Төмөнкү бөлчөктөрдү кыскарбас экендигин далилдегиле:

a) $\frac{21n+4}{14n+3}$; b) $\frac{n+1}{2n+1}$.

38) Далилдегиле:

a) $2903^n-803^n-464^n+261^n \vdots 1897$; b) ЭҮЖБ($2^6-1$, $2^{15}-1$)=7;

c) ЭҮЖБ(2^n-1, 2^m-1)=2^d-1, мында d = ЭҮЖБ(m, n);

39) Төмөнкү удаалаштыкта каалаган эки сан өз-ара жөнөкөй экендигин далилдегиле

$$2+1,\ 2^2+1,\ 2^4+1,\ 2^8+1,\ \ldots,\ 2^{2^n}+1.$$

§3. Өз ара жөнөкөй сандар жана алардын негизги касиеттери

Def 1. Эгерде $(a_1, a_2,..., a_n)=1$ болсо, анда $a_1, a_2,..., a_n$ сандары өз ара жөнөкөй сандар деп аталышат.

Мисал. (11, 8)=1, (9, 14)=1. Ал эми 9 менен 15 өз ара жөнөкөй сан болбойт, себеби (9, 15)=3.

Касиеттери

1^0. $(a, b)=1 \Leftrightarrow \exists x, y \in Z$: $ax+by=1$.

Далилдөө. Зарылдыгы. Эгерде $(a, b)=1$ болсо, анда §2нин 4^0 боюнча $\exists x, y \in Z$: $ax+by=1$ болот.

Жетиштүүлүгү. Айталы $\exists x, y \in Z$: $ax+by=1$ жана $(a, b)=d$ болсун. Анда бөлүнүүчүлүктүн касиети боюнча $1 \vdots d$ болот. Демек, $d=1$ б.а. $(a, b)=1$.

2^0. Эгерде $(a, b)=1$, $a \vdots a_1$ жана $b \vdots b_1$ болсо, анда $(a_1, b_1)=1$ болот.

Далилдөө. $(a, b)=1 \Rightarrow \exists x, y \in Z$: $ax+by=1$. шарт боюнча $a=a_1q_1$, $b=b_1q_2$. Ошондуктан $a_1(q_1x)+b_1(q_2y)=1$ болот, бул барабардыктан $(a_1, b_1)=1$ келип чыгат.

3^0. Эгерде $(a, b)=d$ болсо, анда $\left(\frac{a}{d}, \frac{b}{d}\right)=1$ болот.

Далилдөө. $(a, b)=d \Rightarrow \exists x, y \in Z$: $ax+by=d \Rightarrow \frac{a}{d}x+\frac{b}{d}y=1 \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right)=1$.

4^0. Эгерде $a \cdot b \vdots c$, $(a, c)=1 \Rightarrow b \vdots c$.

Далилдөө. $(a, c)=1 \Rightarrow \exists x, y \in Z$: $ax+cy=1$ барабардыкты b га көбөйтөбүз: $abx+bcy=b$. Касиеттин шарты боюнча $a \cdot b \vdots c$, мындан $b \vdots c$ келип чыгат.

5^0. Эгерде $(a, b)=1$ болсо, анда $c \vdots a$ жана $c \vdots b$ болгондо гана $c \vdots ab$ болот.

Далилдөө. Зарылдыгы. $c \vdots ab \wedge ab \vdots a \wedge ab \vdots b \Rightarrow c \vdots a \wedge c \vdots b$.

Жетиштүүлүгү. $c \vdots a \Rightarrow c = aq$, бирок $c \vdots b$ жана $(a, b)=1$. 3-теореманын негизинде $q \vdots b$ келип чыгат. Анда $c=aq=abq_1$ болот б.а. $c \vdots ab$.

6^0. Эгерде $(a, c)=1$, $(b, c)=1$ болсо, анда $(a, b, c)=1$ болот.

Далилдөө. Далилдөөнү карама-каршысынан жүргүзөбүз.

Мейли $(ab, c)=d>1$ болсун. Анда $c \vdots d$. Касиеттин шарты боюнча $(a, c)=1$ анда 2^0ден $(a, d)=1$ болот. $ab \vdots d$ жана $(a, d)=1$ дан $b \vdots d$ келип чыгат. Демек, b жана c нын жалпы бөлүүчүсү d болот, бул $(b, c)=1$ дегенге карама-каршы келет. Бул карама-каршылыктан $(a, b, c)=1$ болушу келип чыгат.

7^0. Эгерде $(a_i, b_i)=1$, $i=1,...,n$ болсо, анда $\left(\prod_{i=1}^{n} a_i, \prod_{i=1}^{n} b_i\right)=1$ болот,

мында $\prod_{i=1}^{n} a_i = a_1 a_2 ... a_n$ – көбөйтүндү.

8^0. Эгерде $(a, b)=1$ болсо, анда $\forall n \in N$, $(a^n, b^n)=1$ болот.

Акыркы 7^0 жана 8^0ди далилдөө окурманга сунушталат.

Def 2. Эгерде $a_1, a_2, ..., a_n$ сандарынан түзүлгөн каалагандай түгөй өз ара жөнөкөй болсо, б.а. $(a_i, a_j)=1$, $i \neq j$, $i, j=1, 2, ..., n$ анда $a_1, a_2, ..., a_n$ сандары түгөйлөш өз ара жөнөкөй сандар деп аталышат.

Мисал. 7, 8, 9 – түгөйлөш өз ара жөнөкөй сандар, чындыгында $(7, 8)=1$, $(7, 9)=1$, $(8, 9)=1$.

Өз алдынча иштөө үчүн көнүгүүлөр

1) 1300 жана 1350 сандарынын арасындагы жөнөкөй сандарды тапкыла.
2) $2^{18}+3^{18}$ санын жөнөкөй көбөйтүүчүлөргө ажыраткыла.
3) Эгерде $n>1$, $n \in N$ болсо, анда n^4+1 курама сан экендигин далилдегиле.

4) Эгерде $n>1$, $n \in N$ болсо, анда n^4+n^2+1 курама сан экендигин көрсөткүлө.

5) Эгерде $4p^2+1$ жана $6p^2+1$ сандары жөнөкөй болушса, анда p жөнөкөй санын тапкыла.

6) $p+10$ жана $p+14$ сандары жөнөкөй боло тургандай p жөнөкөй санын тапкыла.

7) $p = 6k-1$ көрүнүшүндөгү жөнөкөй сандардын саны чексиз экендигин көрсөткүлө.

8) Эгерде $a>3$, $m = 3q_1+1$, $n = 3q_2+2$ болсо, анда a, $a+m$, $a+n$ сандары бир убакытта жөнөкөй боло албай тургандыгын далилдегиле.

9) $2p+1$ көрүнүшүндөгү бүтүн сандардын бардыгынын ичинен бир сан гана толук куб боло тургандыгын көрсөткүлө, мында p – жөнөкөй сан.

10) Эгерде p жөнөкөй саны $p>5$ болсо, анда анын квадратын 30 га бөлүүдөн келип чыга турган калдык 1 же 19 экендигин далилдегиле.

11) Эгерде p , q жөнөкөй сандары 3 төн чоң болушса, анда p^2-q^2 саны 24кө эселүү экендигин көрсөткүлө.

12) Көбөйтүүчүлөргө ажыраткыла: 235^2+972^2, $3^{10}+3^5+1$.

13) Эгерде жөнөкөй сан $1+2^k$ көрүнүшүнө ээ болсо, анда $k = 0$ же $k = 2^n$ ($n = 0, 1, \ldots$) экендигин көрсөткүлө.

14) Эгерде $(a, b)=1$, $(\alpha, \beta)=2^k$ же $(\alpha, \beta)=1$ болсо, анда $a^\alpha+b^\beta$ саны жөнөкөй сан экендигин далилдегиле.

15) Эгерде 2^n-1 жөнөкөй сан болсо, анда n да жөнөкөй сан экендигин далилдегиле.

§ 4. Эң кичине жалпы эселүү (ЭКЖЭ)

Def 1. Эгерде $M \in Z$ саны нөлдөн айрымалуу болгон $a_1, a_2,\ldots,a_n \in Z$ сандардын бардыгына бөлүнсө, анда M бул сандардын жалпы эселүүсү деп аталат.

Мисалы, $a_1, a_2,\ldots,a_n \in Z$ сандардын көбөйтүндүсү бул сандардын бардыгынын жалпы эселүүсү болот.

Def 2. Эгерде m саны $a_1, a_2,\ldots,a_n \in Z$ сандардын жалпы эселүүсү болуп жалпы эселүүлөрдүн бардыгы m санына бөлүнсө, анда m саны бул сандардын эң кичине жалпы эселүүсү деп аталат.

Мындан ары сандардын эң кичине жалпы эселүүсүн ЭКЖЭ деп кыскартып жазып кете беребиз.

Эгерде $a_1, a_2,\ldots,a_n \in Z$ сандарынын жалпы эселүүсү жашаса, анда ал жалпы эселүүнүн белгисине чейинки тактыкта аныкталат. Чындыгында, эгерде m_1 жана m_2 сандары $a_1, a_2,\ldots,a_n \in Z$ сандарынын ЭКЖЭси болсун, анда def 2 боюнча $m_1 : m_2$ жана $m_2 : m_1$ болот. Бул катыштар $m_1 = m_2$ же $m_1 = -m_2$ болгондо гана аткарылат. Мындан ары ЭКЖЭнин оң маанисин гана алабыз жана аны $m = [a_1, a_2, \ldots, a_n]$ деп белгилейбиз.

Төмөнкү теореманы далилдейли:

Теорема 1. a жана b сандарынын ЭКЖЭси

$$\frac{ab}{(a,b)}$$

формуласы менен табылат, мында (a, b) – a жана b сандарынын ЭЧЖБсы.

Жогорудагы белгилөө боюнча бул теореманы кыскача

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

деп да айтсак болот.

Далилдөө. Айталы $(a, b)=d$ болсун, анда $a=nd$ жана $b=kd$, $(n,k)=1$ болот. Мындан,

$$\frac{ab}{(a,b)}=\frac{ndkd}{d}=nkd=nb=ak.$$

Барабардыктан $\frac{ab}{(a,b)}$ саны aга жана bга бөлүнө тургандыгы келип чыгат, б.а. ал a нын жана b нын ЭЧЖЭси болот.

Эми aнын жана bнын каалагандай M жалпы эселүүсүн $\frac{ab}{(a,b)}$га бөлүнө тургандыгын көрсөтөбүз. Чындыгында $M \vdots a$ болгондуктан $\exists s \in Z$, $M=as=nds$.

$$M \vdots b \text{ жана } b=kd \Rightarrow nds \vdots kd \Rightarrow ns \vdots k.$$

Бирок $(n, k)=1$, анда §3төгү 4^0 боюнча $s \vdots k$ келип чыгат. Демек, $\exists t \in N, s=kt \Rightarrow M=nds=ndkt$, жана $\frac{ab}{(a,b)}=nkd \Rightarrow M \vdots \frac{ab}{(a,b)}$ болот.

Демек, $\frac{ab}{(a,b)}$ саны a жана b сандарынын ЭКЖЭси болот.

Касиеттери

1^0. $\forall a, b \neq 0, \exists [a, b]$.

Далилдөө. Эгерде $a, b \neq 0$ болсо, анда $\frac{ab}{(a,b)}$ туюнтма аныкталат б.а. $[a,b]=\frac{ab}{(a,b)}$ болот.

2^0. $\forall a$, $b \neq 0$ сандардын ЭКЖЭси бул сандардын оң жалпы эселүүлөрүнүн эң кичинеси болот.

Далилдөө. Чындыгында a жана b нын жалпы эселүүсү болгон M саны $m=\frac{ab}{(a,b)}$га бөлүнөт, ошондуктан $M \geq m$ болот.

Мисал. 100 жана 86 сандарынын ЭКЖЭсин тапкыла.

Чыгаруу. Алгач Евклиддин алгоритмы боюнча (100, 86) ны аныктайбыз:

$100=1\cdot 86+14;$

$86=6\cdot 14+2;$

$14=7\cdot 2;$

$(100, 86)=2 \Rightarrow [100,86]=100\cdot 43=4300.$

3^0. Эгерде $[a, b]=m \Rightarrow [k a, k b]=k m,\ k\neq 0.$

Далилдөө. $[ka,kb]=\dfrac{akkb}{(ak,bk)}=\dfrac{abk^2}{(a,b)k}=\dfrac{ab}{(a,b)}k=[a,b]k=mk.$

4^0. Эгерде $a\vdots k \wedge b\vdots k \Rightarrow \left[\dfrac{a}{k},\dfrac{b}{k}\right]=[a,b]\vdots k.$

Далилдөө. $\left[\dfrac{a}{k},\dfrac{b}{k}\right]=\dfrac{\dfrac{ab}{k^2}}{\left(\dfrac{a}{k},\dfrac{b}{k}\right)}=\dfrac{1}{k}\dfrac{ab}{(a,b)}=\dfrac{[a,b]}{k}=[a,b]\vdots k.$

Теорема 2. Эгерде $[a_1, a_2, \ldots,a_{n-1}]=\mu$ жана $[\mu, a_n]=m$ болсо, анда $[a_1, a_2, \ldots,a_n]=m$ болот.

Далилдөө. $[\mu, a_n]=m$ саны a_n ге жана μ га ал эми μ саны $a_1, a_2, \ldots, a_n$ сандырынын ар бирине бөлүнсө, анда m саны $a_1, a_2, \ldots, a_n$ сандарынын ар бирине бөлүнөт, б.а. алардын жалпы эселүүсү болот.

Мейли M – $a_1, a_2, \ldots, a_n$ сандарынын жалпы эселүүсү болсун. Анда M саны $a_1, a_2, \ldots, a_{n-1}$ сандарына бөлүнөт, мындан Mдин $[a_1, a_2, \ldots, a_{n-1}]=\mu$ га бөлүнүшүнөн, M саны a_n ге да бөлүнгөндүктөн, M дин $[\mu, a_n]=m$ ге да бөлүнүшү келип чыгат.

Теорема 3. Эгерде $[a_1, a_2]=m_1$, $[m_1, a_3]=m_2$, …, $[m_{n-2}, a_n]=m_{n-1}$ болсо, анда $[a_1, a_2, \ldots, a_n]=m_{n-1}$ болот.

Б.а. $a_1, a_2, \ldots, a_n$ сандарынын ЭКЖЭсин табуу үчүн алгач $[a_1, a_2]=m_1$ ди андан соң $[m_1, a_3]=m_2$ ни ж.б. $[m_{n-2}, a_n]$ лерди табуу

керек. Ал эми m_{n-1} саны $[a_1, a_2, \ldots, a_n]$ ге барабар болот. Төмөнкү сандардын ЭКЖЭсин табууну карайлы.

Мисал. [35, 77, 1141]=?

$$[35,77]=\frac{35\cdot 77}{(35,\ 77)}=\frac{35\cdot 77}{7}=35\cdot 11=385,$$

$$[385,1141]=\frac{385\cdot 1141}{(385,\ 1141)}=\frac{385\cdot 1141}{7}=385\cdot 163=62755.$$

Демек, [35, 77, 1141]=62755.

Теорема 4. Түгөйлөш өз-ара жөнөкөй $a_1, a_2, \ldots, a_n$ сандарынын ЭКЖЭси алардын көбөйтүндүсүнө барабар болот.

Далилдөө. Мейли $(a_i, a_j)=1$ $(i, j=1, 2,\ldots,n)$ болсун, анда

$$m_2=[a_1,a_2]=\frac{a_1a_2}{(a_1,a_2)}=a_1a_2;$$

$$m_3=[m_2,a_3]=\frac{m_2a_3}{(m_2,a_3)}=\frac{a_1a_2a_3}{(a_1,a_2,a_3)}=\frac{a_1a_2a_3}{(1,a_3)}=\frac{a_1a_2a_3}{1}=a_1a_2a_3;$$

Жогорудагыдай ой жүгүртүү менен $(n-1)$ – кадамда $m_n=[m_{n-1}, a_n]=a_1a_2\ldots a_n$ ге ээ болобуз.

Мисал. [37, 43, 95]=?

(37, 43)=1, (37, 95)=1, (43, 95)=1. Демек, [37, 43, 95]=37·43·95.

Өз алдынча иштөө үчүн көнүгүүлөр

Берилген сандардын ЭЧЖБ жана ЭКЖЭсин тапкыла [1-26]:

1) $a=1786$; $b=705$.
2) $a=4373$; $b=3281$.
3) $a=-826$; $b=822$.
4) $a=1068$; $b=899$.
5) $a=3655$; $b=1023$.
6) $a=31605$; $b=498$.
7) $a=3059$; $b=1352$.
8) $a=1518$; $b=731$.
9) $a=2737$; $b=1627$.
10) $a=2516$; $b=3360$.
11) $a=1488$; $b=1126$.
12) $a=9163$; $b=22083$.
13) $a=9234$; $b=6574$.
14) $a=294$; $b=2048$.
15) $a=3928$; $b=2937$.
16) $a=5473$; $b=2739$.

17) $a = 7362$; $b = 632$.

18) $a = 3726$; $b = 27364$.

19) $a = 37261$; $b = 372$.

20) $a = 8372$; $b = 3726$.

21) $a = 7261$; $b = 1372$.

22) $a = 372$; $b = 726$.

23) $a = 2261$; $b = 272$.

24) $a = 5312$; $b = 1326$.

25) $a = 3243$; $b = 145$.

26) $a = 1024$; $b = 256$.

x жана y натуралдык сандарын тапкыла [27-53]:

27) $\begin{cases} x + y = 150, \\ (x, y) = 30; \end{cases}$

28) $\begin{cases} x + y = 144, \\ (x, y) = 24; \end{cases}$

29) $\begin{cases} x \cdot y = 20, \\ [x, y] = 10; \end{cases}$

30) $\begin{cases} x \cdot y = 8400, \\ (x, y) = 20; \end{cases}$

31) $\begin{cases} x \cdot y = 720, \\ (x, y) = 4; \end{cases}$

32) $\begin{cases} (x, y) = 4, \\ [x, y] = 24; \end{cases}$

33) $\begin{cases} (x, y) = 4, \\ [x, y] = 12; \end{cases}$

34) $\begin{cases} (x, y) = 24, \\ [x, y] = 2496; \end{cases}$

35) $\begin{cases} x + y = 667, \\ [x, y] = 120 \cdot (a, b); \end{cases}$

36) $\begin{cases} x \cdot y = 168, \\ (x, y) = 14; \end{cases}$

37) $\begin{cases} \dfrac{x}{y} = \dfrac{11}{7}, \\ (x, y) = 45; \end{cases}$

38) $\begin{cases} \dfrac{x}{y} = \dfrac{5}{9}, \\ (x, y) = 28; \end{cases}$

39) $\begin{cases} \dfrac{x}{(x, y)} + \dfrac{y}{(x, y)} = 18, \\ [x, y] = 975; \end{cases}$

40) $\begin{cases} \dfrac{x}{y} = \dfrac{4}{3}, \\ (x, y) = 25; \end{cases}$

41) $\begin{cases} x + y = 180, \\ (x, y) = 30; \end{cases}$

42) $\begin{cases} x + y = 168, \\ (x, y) = 24; \end{cases}$

43) $\begin{cases} (x, y) = 12, \\ [x, y] = 72; \end{cases}$

44) $\begin{cases} x + y = 60, \\ [x, y] = 72; \end{cases}$

45) $\begin{cases} (x, y) = 5, \\ [x, y] = 495; \end{cases}$

46) $\begin{cases} x + y = 100, \\ [x, y] = 495; \end{cases}$

47) $\begin{cases} x + y = 40, \\ (x, y) = 4; \end{cases}$

48) $\begin{cases} x + y = 70, \\ (x, y) = 7; \end{cases}$

49) $\begin{cases} x + y = 100, \\ (x, y) = 10; \end{cases}$

50) $\begin{cases} x + y = 100, \\ [x, y] = 90; \end{cases}$

51) $\begin{cases} x + y = 49, \\ [x, y] = 70; \end{cases}$

52) $\begin{cases} (x, y) = 24, \\ [x, y] = 2496; \end{cases}$

53) $\begin{cases} x + y = 667, \\ [x, y] = 120(x, y); \end{cases}$

54) Далилдегиле

а) $[a,b,c] = \dfrac{abc(a,b,c)}{(a,b)(a,c)(b,c)}$;

б) $(a,b)(a,c)(b,c)[a,b][a,c][b,c] = a^2 b^2 c^2$.

§ 5. Жөнөкөй жана курама сандар

1. Жөнөкөй сандар жана алардын касиеттери

Def 1. Эгерде $n>1$, $n \in N$ саны өзүнө жана 1 ге гана бөлүнсө, анда ал жөнөкөй сан деп аталат.

Алгачкы натуралдык жөнөкөй сандар:

2, 3, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ...

Жөнөкөй сандардын арасында бир гана 2 жуп, калгандарынын бардыгы так сандар.

Def 2. Эгерде $n>1$, $n \in N$ саны n ден жана 1 ден айрымаланган жок дегенде бир натуралдык бөлүүчүгө ээ болсо, анда ал курама сан деп аталат.

Def 2 боюнча, эгерде n курама сан болсо, анда

$$\exists \delta \in N,\ n=n_1\delta,\ 1<n_1<n,\ 1<\delta<n.$$

1 саны жөнөкөй да, курама сан да эмес. Ошентип, натуралдык сандардын көптүгү үч камтылуучу көптүккө бөлүнөт, алар:

1) жөнөкөй сандар; 2) курама сандар; 3) 1 саны.

Каалагандай курама сан жалгыз түрдө жөнөкөй сандардын көбөйтүндүсү түрүндө туюнтулат, бул жөнөкөй сандардын теориясында негизги натыйжалардын бири болуп саналат.

Бул ырастоону далилдөө үчүн алгач жөнөкөй сандардын касиеттерине токтолобуз.

1^0. Эгерде p – жөнөкөй саны кандайдыр бир $n \neq 1$ санына бөлүнсө, анда $p=n$. Чындыгында, эгерде $p \neq n$ болсо, анда $p \vdots 1$, $p \vdots n$, $p \vdots p$ болот эле, мындан p – жөнөкөй сан эместиги келип чыгат.

2^0. Эгерде p_1, p_2 – ар түрдүү жөнөкөй сандар болушса ($p_1 \neq p_2$) анда p_2 саны p_1 ге бөлүнбөйт.

Далилдөө. p_2 – жөнөкөй сан болгондуктан, ал p_2 га жана 1ге гана бөлүнөт. Шарт боюнча $p_1 \neq p_2$, аныктама боюнча $p_1 \neq 1$, анда p_2 саны p_1 ге бөлүнбөйт.

3^0. $\forall n > 1, n \in N$ саны жок дегенде бир жөнөкөй санга бөлүнөт.

Далилдөө. Математикалык индукция усулун колдонобуз.

1) $n = 2$ болгон учурда туура, себеби $2 \vdots 2$.

2) Айталы $1 < k < n$ үчүн 3^0 касиет аткарылсын деп божомолдойлу;

3) 3^0 касиеттин орун алышын n үчүн далилдейбиз.

Эгерде n жөнөкөй болсо, анда ал $p = n$ жөнөкөй санына бөлүнөт. Бул учурда касиет дилилденди.

Эгерде n курама сан болсо, анда $n = ke$ $(1 < k < n, 1 < e < n)$ болот жана $k < n$ болгондуктан, 2)- кадам боюнча теорема орун алат, б.а. k саны жок дегенде бир p жөнөкөй санына бөлүнөт. Анда n саны да p га бөлүнөт. Касиет далилденди.

4^0. Эгерде $n \in N, p$ – жөнөкөй сан болсо, анда $n \vdots p$ же $(n, p) = 1$ болот.

Далилдөө. Мейли $d = 1$ болсун, анда $(n, p) = 1$ болот. Эгерде $d = p$ болсо, анда $n \vdots p$.

5^0. Эгерде $a_1 a_2 ... a_n \vdots p$ болсо, анда a_i лердин жок дегенде бирөөсү p га бөлүнөт.

Далилдөө үчүн математикалык индукция усулун колдонобуз.

1) Алгач $a_1 a_2$ ны карайлы: $a_1 a_2 \vdots p \Rightarrow a_1 \vdots p$.

Эгерде $a_1 \vdots p$ болсо, анда касиет далилденген болот. Эгерде a_1 саны p га бөлүнбөсө, анда $(a_1, p) = 1$ болот жана $a_2 \vdots p$ келип чыгат.

2) Мейли $a_1 a_2 ... a_k \vdots p$ орун алсын.

3) Бул касиеттин $a_1 a_2 ... a_{k+1}$ көбөйтүндүсү үчүн орун ала тургандыгын далилдейбиз.

$n = a_1 a_2 ... a_k a_{k+1}$ санын $n = (a_1, a_2, ..., a_k) a_{k+1} = m a_{k+1}$ көрүнүшүндө жазып алабыз. Эки көбөйтүүчү үчүн далилденген же $m \vdots p$ же $a_{k+1} \vdots p$.

Эгерде $a_{k+1} \vdots p$ болсо, касиет далилденген болот. Эгерде $m \vdots p$ болсо, анда 2)- кадам боюнча $a_1 a_2 ... a_k$ көбөйтүндүсүнүн көбөйтүүчүлөрүнүн жок дегенде бирөөсү p га бөлүнөт. Касиет далилденди.

2. Курама сандарды жөнөкөй сандардын көбөйтүндүсүнө ажыратуу

Теорема 1. Эгерде p жөнөкөй саны n курама санынын эң кичине бөлүүчүсү болсо, анда $p \le \sqrt{n}$ болот.

Далилдөө. p жөнөкөй саны n курама санынын эң кичине бөлүүчүсү болгондуктан, $n=p \cdot n_1$ болот, мында $p \le n_1$.

$$p \le n_1 \Rightarrow p^2 n_1 \le n_1 n \Rightarrow p^2 \le n \Rightarrow p \le \sqrt{n}.$$

Бул теоремадан төмөнкүдөй жыйынтык келип чыгат.

Эгерде n саны $\sqrt{n}$ ден ашпаган бир дагы жөнөкөй санга бөлүнбөсө, анда ал жөнөкөй сан болот. Тескери учурда n курама сан болот.

Мисал. n =97. $9 < \sqrt{97} < 10$.

97 саны 2, 3, 5, 7 сандарынын бирөөсүнө да бөлүнбөйт, демек, ал жөнөкөй сан.

Теорема 2. (Арифметиканын негизги теоремасы) Бирден чоң каалагандай натуралдык сан же жөнөкөй сан болот, же жөнөкөй сандардын көбөйтүндүсүнө ажырайт жана бул көбөйтүндү көбөйтүүчүлөрдүн жазылуу иретине чейинки тактыкта жалгыз болот.

Далилдөө. Алгач ажыралманын жашашын математикалык индукция усулу менен далилдейбиз.

1) Мейли n =2 болсун. 2 жөнөкөй сан болгондуктан, n =2 үчүн жогорудагы теорема орун алат.

2) Айталы, ырастоо n= k үчүн туура болсун.

3) Ырастоону n=k+1 үчүн далилдейбиз.

Эгерде n жөнөкөй сан болсо, анда ырастоо далилденген болот. Эгерде n курама сан болсо, анда аны $n=n_1 \cdot n_2$, $1<n_1<n$, $1<n_2<n$ көрүнүшүндө жазууга болот, ошондой эле n_1 жана n_2 сандары үчүн 2)- кадам боюнча $n_1=p_1 \cdot p_2 \cdot \ldots \cdot p_m$, $n_2=p_{m+1} \cdot p_{m+2} \cdot \ldots \cdot p_k$, барабардыктары аткарылат. Анда $n=n_1 \cdot n_2=p_1 \cdot p_2 \cdot \ldots \cdot p_k$ болот.

Эми ажыралманын жалгыздыгын далилдейли.

1) Мейли n=2 болсун, 2 жөнөкөй сан болгондуктан, аны жөнөкөй сандардын көбөйтүндүсү көрүнүшүндө жаза албайбыз. Демек, n=2 үчүн ырастоо туура.

2) Айталы ырастоо 2 $\leq k <n$ үчүн туура болсун.

3) Ырастоону n үчүн далилдейбиз.

Эгерде n жөнөкөй сан болсо, анда аны жөнөкөй сандардын көбөйтүндүсү көрүнүшүндө жаза албайбыз. Эгерде n курама сан болсо, жана ал эки ар түрдүү жөнөкөй сандардын көбөйтүндүсүнө ажыраса:

$$n=p_1 \cdot p_2 \cdot \ldots \cdot p_k, \quad n=q_1 \cdot q_2 \cdot \ldots \cdot q_s,$$

анда $p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ болот.

Бул барабардыктын сол жагы p_1ге бөлүнөт, анда оң жагында p_1ге бөлүнүшү керек. Мейли $q_1 \vdots p_1$ болсун, q_1 жөнөкөй сан жана $p_1>1$ болгондуктан $q_1=p_1$ болот. Барабардыкты p_1ге бөлүп жиберебиз:

$$p_2 \cdot p_3 \cdot \ldots \cdot p_k = q_2 \cdot q_3 \cdot \ldots \cdot q_s .$$

$p_2 \cdot p_3 \cdot \ldots \cdot p_k$ жана $q_2 \cdot q_3 \cdot \ldots \cdot q_s$ сандары n ден кичине болгондуктан 2-кадам боюнча $k=s$, $p_2=q_2, \ldots$, $p_s=q_s$ болот. Демек, $p_1=q_1$, $p_2=q_2, \ldots$, $p_s=q_s$. Мындан ажыралманын жалгыздыгы келип чыгат.

Бул ажыралмада барабар болгон жөнөкөй сандар кездешиши мүмкүн. Мисалы, p_1 жөнөкөй саны α_1 жолу, p_2

жөнөкөй саны α_2 жолу, ж.б. p_k жөнөкөй саны α_k жолу. Анда n натуралдык санын жөнөкөй сандардын көбөйтүндүсү көрүнүшүндөгү ажыралма

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \qquad (1)$$

көрүнүшүндө болот, мында $p_1<p_2<\ldots<p_k$.

(1) – n санынын каноникалык ажыралмасы деп аталат, жана бул ажыралма жалгыз болот.

Мисал. $100=2^2 \cdot 5^2$, $1176=2^3 \cdot 3 \cdot 7^2$.

Теорема 3. Эгерде $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ болсо, анда бул сандын бардык бөлүүчүлөрү $q = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ көрүнүшүндө болот, мында $0 \le \beta_i \le \alpha_i$, $i=1,2,\ldots,k$.

Теорема 4. Эгерде $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$ болсо, анда $(a, b) = p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_s^{\lambda_s}$ болот, мында $\lambda_i = \min(\alpha_i, \beta_i)$.

Теорема 5. Эгерде $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$ болсо, анда $[a, b] = p_1^{\mu_1} p_2^{\mu_2} \ldots p_s^{\mu_s}$ болот, мында $\mu_i = \max(\alpha_i, \beta_i)$.

Мисал. 972 жана 648 сандарынын ЭЧЖБсын жана ЭКЖЭсин тапкыла.

Чыгаруу. $972=2^2 \cdot 3^5$ жана $648=2^3 \cdot 3^4$ болгондуктан,

$(972, 648)=2^2 \cdot 3^4$, $[972, 648]= 2^3 \cdot 3^5$ болот.

3. Жөнөкөй сандардын көптүгү

Теорема (Евклиддин теоремасы) Жөнөкөй сандардын көптүгү чексиз.

Далилдөөнү карама-каршысынан жүргүзөбүз. Мейли жөнөкөй сандардын көптүгү чектүү болсун, $A=\{2=p_1, p_2,\ldots, p_k\}$, мында p_k жөнөкөй сандардын эң чоңу. А көптүгүнүн бардык элементтерин көбөйтүп ага 1 санын кошобуз:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1.$$

Бул сан $n > p_k$ болгондуктан ал жөнөкөй эмес, курама сан болушу керек. Эгерде курама сан болсо, анда ал жок дегенде бир жөнөкөй санга бөлүнүшү керек. Жөнөкөй сандардын бардыгы А көптүгүнө таандык. Демек, n саны $p_1, p_2, \ldots, p_k$ лардын бирөөсүнө бөлүнөт, мейли ал p_1 болсун. Анда $p_1 \cdot p_2 \cdot \ldots \cdot p_k : p_1$ жана $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1 : p_1$ ден $1 : p_1$ келип чыгат. Бирок 1 саны p_1 ге бөлүнбөйт, себеби $p_1 > 1$. Бул карама-каршылыктан теореманын далилдөөсү келип чыгат.

Демек, А көптүгү (жөнөкөй сандардын көптүгү) чексиз.

Теорема (жөнөкөй сандар жайгашкан интервалдар жөнүндө) Натуралдык сандардын катарында бир дагы жөнөкөй санды кармабаган жетишээрлик узундуктагы интервалдар жашайт.

Далилдөө. $\forall n \in N$ санын алып, төмөнкү удаалаштыкты түзөбүз:

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1.$$

Бул удаалаштык түзгөн сандардын баардыгы курама сандар. Биз n удаалаш курама сандарга ээ болдук.

Бул эки теоремадан натуралдык сандардын катарында жөнөкөй сандардын бөлүштүрүлүш мүнөзү өтө татаал экендиги келип чыгат. Бул маселе математикадагы оор маселелердин бири болуп саналат.

4. **Эратосфендин торчосу.**

Биздин доорго(заманга) чейинки III кылымда жашаган грек математиги Эратосфен, 1 ден n ге чейинки натуралдык сандардын арасынан жөнөкөй сандарды табуунун усулун тапкан, ошондуктан бул усул Эратосфен торчосу деп аталган. Эратосфендин торчосу:

$$1, 2, 3, 4, 5, 6, \ldots, n$$

сандардын арасынан жөнөкөй сандарды табуу үчүн алгач 1ди, анан 2ге эселүү, 3гө эселүү, ж.б. $p_k \le \sqrt{n}$ жөнөкөй сандарын

калтырып аларга эселүү болгон сандардын астын сызабыз. Асты сызылбай калган сандар 2, 3, 5, …, p_k лер жөнөкөй сандар болот.

Мисал. 20 га чейинки жөнөкөй сандарды Эратосфендин торчосунун жардамында тапкыла.

Чыгаруу. $3 < \sqrt{20} < 5$ болгондуктан 2ге жана 3кө эселүү болгон сандардын астын сызабыз:

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20.

Демек, 20 га чейинки жөнөкөй сандар булар:

2, 3, 5, 7, 11, 13, 17, 19.

Мисал. 323 саны жөнөкөй сан болобу?

Чыгаруу. $18 < \sqrt{323} < 19$ болгондуктан. 323тү 18ге чейинки жөнөкөй сандарга бөлөбүз, эгерде жок дегенде алардын бирөөсүнө бөлүнсө, анда 323 саны курама сан болот, а эгерде бирөөсүнө да бөлүнбөсө анда 323 жөнөкөй сан болот.

18ге чейинки жөнөкөй сандар булар: 2, 3, 5, 7, 11, 13, 17.

323:17 болгондуктан 323 курама сан болот.

Мисал. 2011 саны жөнөкөй сан болобу?

Чыгаруу. $44 < \sqrt{2011} < 45$ болгондуктан.

44кө чейинки жөнөкөй сандарга

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 39, 41, 43

бөлөбүз. 2011 саны бул сандардын бирөөсүнө да бөлүнбөйт ошондуктан ал жөнөкөй сан болот.

Өз алдынча иштөө үчүн көнүгүүлөр

Эратосфен торчосунун жардамында берилген сандардын арасындагы бардык жөнөкөй сандарды тапкыла [1-25]:

1) 1050 жана 1150;
2) 2100 жана 2200;
3) 1060 жана 1160;
4) 2300 жана 2400;
5) 1070 жана 1170;
6) 2350 жана 2450;
7) 1100 жана 1200;
8) 2550 жана 2650;

9) 1250 жана 1350;
10) 2745 жана 2900;
11) 1435 жана 1545;
12) 2900 жана 3100;
13) 1675 жана 1780;
14) 3390 жана 3450;
15) 1880 жана 2000;
16) 4550 жана 4670;
17) 5555 жана 5750;
18) 4660 жана 4770;
19) 5890 жана 6000;
20) 6100 жана 6250;
21) 6437 жана 6540;
22) 2355 жана 2455;
23) 4422 жана 4525;
24) 1122 жана 1222;
25) 3333 жана 3444.

Берилген натуралдык сандын жөнөкөй же курама экендигин аныктагыла [26, 50]

26) $n = 1559$; 27) $n = 1627$; 28) $n = 1783$; 29) $n = 3061$; 30) $n = 3709$;
31) $n = 4057$; 32) $n = 1987$; 33) $n = 2339$; 34) $n = 2671$; 35) $n = 3343$;
36) $n = 3659$; 37) $n = 4007$; 38) $n = 1051$; 39) $n = 1423$; 40) $n = 3623$;
41) $n = 3989$; 42) $n = 4027$; 43) $n = 3739$; 44) $n = 3083$; 45) $n = 1699$;
46) $n = 2803$; 47) $n = 3001$; 48) $n = 3229$; 49) $n = 1459$; 50) $n = 1181$.

§6. Арифметикалык функциялар

1. $\tau(n)$ функциясы

$n \in N$ дин бардык натуралдык бөлүүчүлөрүнүн санын аныктоочу функция $\tau(n)$ менен белгиленет.

Теорема 1. Эгерде $n \in N$ дин каноникалык формасы $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ болсо, анда

$$\tau(n) = (\alpha_1+1) \cdot (\alpha_2+1) \cdot \ldots \cdot (\alpha_k+1) \text{ болот.}$$

Далилдөө. n дин каноникалык формасы $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ көрүнүшүндө боло тургандыгы белгилүү, n дин каалагандай q бөлүүчүсүнүн каноникалык формасы $q = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$ көрүнүшүндө болот, мында $0 \le \beta_i \le \alpha_i$, $i=1,2,\ldots,k$. Ошондуктан β_1 көрсөткүчү α_1+1 сандагы ар түрдүү маанилерди кабыл алышы мүмкүн: 0, 1, 2, ..., α_1. β_2 көрсөткүчү α_2+1 сандагы ар түрдүү маанилерди кабыл алышы мүмкүн: 0, 1, 2, ..., α_2. б.а. $<\beta_1, \beta_2, \ldots, \beta_k>$ кортежинде 1-координата (α_1+1), 2-координата (α_2+1), ..., k- координата (α_k+1) сандагы маанилерди кабыл алышы мүмкүн. Анда комбинатористиканын көбөйтүү принциби боюнча, мындай кортеждердин саны $(\alpha_1+1) \cdot (\alpha_2+1) \cdot \ldots \cdot (\alpha_k+1)$ га барабар болот.

Мисал. 30 санынын бөлүүчүлөрүнүн санын тапкыла.

Чыгаруу. $30 = 2 \cdot 3 \cdot 5$ болот, ошондуктан $\tau(30) = (1+1)(1+1)(1+1) = 8$.

Чындыгында, 30 дун бөлүүчүлөрү: 1, 2, 3, 5, 6, 10, 15, 30. алардын саны 8ге барабар.

2. $\sigma(n)$ функциясы

$n \in N$ дин бардык натуралдык бөлүүчүлөрүнүн суммасын аныктөөчу функция $\sigma(n)$ менен белгиленет.

Теорема 2. Эгерде $n \in N$ дин каноникалык формасы

$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ болсо, анда $\sigma(n) = \frac{p_1^{\alpha_1}-1}{p_1-1} \frac{p_2^{\alpha_2}-1}{p_2-1} \ldots \frac{p_k^{\alpha_k}-1}{p_k-1}$ болот.

Далилдөө. Төмөнкүдөй көбөйтүндүнү карайлы:

$\left(p_1^0 + p_1^1 + p_1^2 + \ldots p_1^{\alpha_1}\right)\left(p_2^0 + p_2^1 + p_2^2 + \ldots p_2^{\alpha_2}\right) \ldots \left(p_k^0 + p_k^1 + p_k^2 + \ldots p_k^{\alpha_k}\right)$.

Эгерде кашааларды ачсак $p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ көрүнүшүндөгү кошулуучуларды алабыз, мында $\forall j, 1 \leqslant j \leqslant k$, $\beta_k \leqslant \alpha_k$. Бул кошулуучулардын бардыгы $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ санынын бөлүүчүлөрү болот жана бөлүүчүлөрдүн ар бири суммада бир жолудан гана кездешет. Ошондуктан

$\left(p_1^0 + p_1^1 + p_1^2 + \ldots p_1^{\alpha_1}\right)\left(p_2^0 + p_2^1 + p_2^2 + \ldots p_2^{\alpha_2}\right) \ldots \left(p_k^0 + p_k^1 + p_k^2 + \ldots p_k^{\alpha_k}\right)$

көбөйтүндү n дин бөлүүчүлөрүнүн суммасын берет. Ар бир сумма:

$$p_j^0 + p_j^1 + p_j^2 + \ldots p_j^{\alpha_j},\ 1 \leqslant j \leqslant k,$$

геометриялык прогрессия болгондуктан,

$$p_j^0 + p_j^1 + p_j^2 + \ldots + p_j^{\alpha_j} = \frac{p_j^{\alpha_j+1}-1}{p_j-1} \text{ болот.}$$

Мисал. 30 санынын бөлүүчүлөрүнүн суммасын тапкыла.

Чыгаруу. $30 = 2 \cdot 3 \cdot 5$ болгондуктан,

$$\sigma(30) = \frac{2^2-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{5^2-1}{5-1} = 3 \cdot 4 \cdot 6 = 72.$$

Демек, 30 санынын бөлүүчүлөрүнүн суммасы 72ге барабар. Чындыгында 1+2+3+5+6+10+15+30=72 болот.

3. E(x) функциясы

$x \in \Re$ санынын бүтүн бөлүгү, б.а. эгерде $n \leqslant x \leqslant n+1$, $n \in Z$ болсо, анда $E(x)=n$ болот.

Мисал. $E(7,25)=7$, $E(\pi)=3$, $E(-0,6)=-1$, $E(0)=0$.

Мейли $m, n \in N$ болсун. n ден ашпаган mге эселүү болгон натуралдык сандардын саны $E\left(\frac{n}{m}\right)$ге барабар. Чындыгында, эгерде $n=mq+r$, $0 \le r < m$ болсо, анда эселүү сандар m, $2m$, …, mq болот. Алардын саны qга барабар. Бирок, экинчи жактан $n = mq+r \Rightarrow \frac{n}{m} = q + \frac{r}{m}$, $0 \le \frac{r}{m} < 1$ болгондуктан, $E\left(\frac{n}{m}\right)=q$ болот.

Теорема 3. $n!$ дын каноникалык ажыралмасында p жөнөкөй санынын даражасы төмөндөгүгө барабар болот:

$$E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + \ldots + E\left(\frac{n}{p^k}\right) + \ldots$$

Далилдөө. $E(x)=0$, $0 \le x < 1$ болгондуктан, $n < p^k$ болгондо $E\left(\frac{n}{p^k}\right)=0$ болот. Ошондуктан, эгерде $p^s \le n < p^{s+1}$ болсо, анда акыркы нол эмес кошулуучу $E\left(\frac{n}{p^s}\right)$ болот.

Практикада бул эсептөөнү төмөнкүдөй жүргүзүү ыңгайлуу болот:

$n=pq_1+r_1$

$q_1=pq_2+r_2$

$q_2=pq_3+r_3$

…

$q_s=pq_{s+1}+r_s$ $(p>q_{s+1})$.

p нын даражасы $q_1+q_2+\ldots+q_s$ ге барабар болот.

Мисал. 900! дын каноникалык формасында 5 саны канчанчы даража менен катышат.

Чыгаруу. $900=5\cdot180$, $180=5\cdot36$, $36=5\cdot7+1$, $7=5\cdot1+2$,

Демек, $5^{180+36+7+1} = 5^{254}$ болот.

Мисал 10! дын каноникалык ажыралмасын тапкыла.

Чыгаруу. 10га чейинки жөнөкөй сандарды аныктайбыз, алар: 2, 3, 5, 7 болот. Алардын даражаларын табалы:

$10=2\cdot5$, $5=2\cdot2+1$, $2=2\cdot1$;

$10=3\cdot3+1$, $3=3\cdot1$;

$10=5\cdot2$;

$10=7\cdot1+3$.

Демек, $10!=2^{5+2+1}\cdot3^{3+1}\cdot5^2\cdot7^1=2^8\cdot3^4\cdot5^2\cdot7^1$.

4. Эйлердин функциясы

Эйлердин функциясы m аргумент үчүн $\varphi(m)$ болуп белгиленет. Бул функция бардык натуралдык сандар үчүн аныкталган болуп, m ден ашпаган жана m менен өз ара жөнөкөй болгон натуралдык сандардын санын аныктайт. Эйлердин функциясы төмөнкү формула менен эсептелет:

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_n}\right),$$

мында p_1, p_2, …, p_n – сандары $m=p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n}$ каноникалык ажыралмадагы жөнөкөй бөлүүчүлөр. Жекече учурда $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$ жана $\varphi(p)=p-1$ болот.

Мисал. 1) $\varphi(125)=\varphi(5^3)=5^2(5-1)=100$;

2) $\varphi(29)=29-1=28$ (29 жөнөкөй сан);

3) $\varphi(360)=360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=\frac{1440}{15}=96$.

5. Мультипликативдүү функциялар

Жогоруда каралган функцияларды жалпылайбыз.

Def 1. Эгерде $\theta(a)$ функциясы төмөнкү эки шартты канаатандырса, анда ал мультипликативдүү функция деп аталат:

1) $\theta(a)$ функциясынын аныкталуу аймагы оң бүтүн сандар, a

нын жок дегенде бир маанисинде $\theta(a) \neq 0$.

2) Каалагандай өз ара жөнөкөй a_1 жана a_2 оң сандары үчүн

$$\theta(a_1 a_2) = \theta(a_1)\theta(a_2)$$

барабардыгы орун алат.

Мисал. 1) $\theta(a)=a^s$, мында s – каалагандай чыныгы же комплекстик сан.

2) Эйлердин функциясыда мультипликативдик функция б.а. $a, b, \ldots, l$ сандары өз ара жөнөкөй болгондо

$$\varphi(a \cdot b \cdot \ldots \cdot l) = \varphi(a)\varphi(b)\ldots\varphi(l) \text{ болот.}$$

Касиеттери

1^0.Каалагандай $\theta(a)$ мультипликативдүү функциясы үчүн $\theta(1)=1$ болот.

Далилдөө. Айталы $\theta(a_0) \neq 0$ болсун, анда

$$\theta(a_0)=\theta(a_0 \cdot 1)=\theta(a_0)\theta(1), \qquad 1=\theta(1) \text{ болот.}$$

2^0. Эгерде a_1, a_2, a_3, ..., a_k сандары өз ара жөнөкөй сандар болушса, анда $\theta(a_1 a_2 a_3 \ldots a_k)= \theta(a_1)\theta(a_2)\theta(a_3)\ldots\theta(a_k)$ болот.

Далилдөө. Мультипликативдүү функциянын аныктоосун түздөн-түз пайдалануу менен төмөнкүнү алабыз:

$$\theta(a_1 a_2 a_3 \ldots a_k)=\theta(a_1)\theta(a_2 a_3 \ldots a_k)=\ldots=\theta(a_1)\theta(a_2)\theta(a_3)\ldots\theta(a_k).$$

Жекече учурда

$$\theta\left(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_k^{\alpha_k}\right)= \theta\left(p_1^{\alpha_1}\right)\theta\left(p_2^{\alpha_2}\right)\theta\left(p_3^{\alpha_3}\right)\ldots\theta\left(p_k^{\alpha_k}\right) \qquad (1)$$

болот.

3^0. $\theta(1)=1$ санын жана $\theta(p^\alpha)$ га жөнөкөй сандын оң даражасын бөрө турган каалагандай санды алып, ар дайым мультипликативдүү функцияны түргүзүүгө болот. Жалпы учурда бул функцияны (1) барабардык менен аныктайбыз.

Далилдөө. Эгерде $a = p_1^{\alpha_1}...p_k^{\alpha_k}$ саны a_1 жана a_2 эки өз-ара жөнөкөй сандардын көбөйтүндүсү көрүнүшүндө берилген болсо, анда

$$\theta(a)=\theta(a_1)\theta(a_2),$$

барабардыгы орун алат.

Мисал. $\theta(1)=1$ жана $\theta(p^\alpha)=2$, $\alpha > 0$ деп алып мультипликативдүү функцияны тургузууга болот. Анда $k > 0$ үчүн $\theta\left(p_1^{\alpha_1}...p_k^{\alpha_k}\right)=2^k$ болот. Жекече учурда, төмөнкүлөрдү алабыз:

$\theta(1)=1$, $\theta(2)=2$, $\theta(3)=2$,
$\theta(4)=2$, $\theta(5)=2$, $\theta(6)=4$.

4^0. Эки $\theta_1(a)$ жана $\theta_2(a)$ мультипликативдүү функциялардын көбөйтүндүсү да $\theta(a)=\theta_1(a)\theta_2(a)$ мультипликативдүү функция болот.

Далилдөө. $\theta(1)=\theta_1(1)\theta_2(1)=1$ болот. Андан тышкары $(a_1, a_2)=1$ болгондо төмөндөгү орун алат:

$$\theta(a_1a_2)=\theta_1(a_1a_2)\theta_2(a_1a_2)=\theta_1(a_1)\theta_1(a_2)\theta_2(a_1)\theta_2(a_2)=$$
$$=\theta_1(a_1)\theta_2(a_1)\theta_1(a_2)\theta_2(a_2)=\theta(a_1)\theta(a_2).$$

5^0. $\theta_1(a)$, $\theta_2(a)$, $\theta_3(a)$,..., $\theta_k(a)$ мультипликативдүү функциялардын көбөйтүндүсү да мультипликативдүү функция болот.

Далилдөө. Далилдөө 4^0түн далилдөөсүнө окшош жүргүзүлөт. Аны удаалаш колдонуу менен көбөйтүндүнүн мультипликативдүү экендигине ынанабыз:

$$\theta_1(a)\theta_2(a)\theta_3(a)=(\theta_1(a)\theta_2(a))\theta_3(a),$$
$$\theta_1(a)\theta_2(a)\theta_3(a)\theta_4(a)=(\theta_1(a)\theta_2(a)\theta_3(a))\theta_4(a),$$
$$\dots$$
$$\theta_1(a)\theta_2(a)\dots\theta_{k-1}(a)\theta_k(a)=(\theta_1(a)\theta_2(a)\dots\theta_{k-1}(a))\theta_k(a).$$

6^0. Айталы $\theta(a)$ – мультипликативдүү функция жана $a = p_1^{\alpha_1}...p_k^{\alpha_k}$ – a санынын каноникалык ажыралмасы болсун. Эгерде

$\sum_{d\backslash a}$ символу менен a санынын бардык d бөлүүчүлөрүнө жайылтылган сумманы белгилеп алсак, анда

$$\sum_{d\backslash a}\theta(d)=\left(1+\theta(p_1)+\theta\left(p_1^2\right)+...+\theta\left(p_1^{\alpha_1}\right)\right)..\left(1+\theta(p_k)+\theta\left(p_k^2\right)+...+\theta\left(p_k^{\alpha_k}\right)\right)$$

болот

(a=1 болгондо барабардыктын оң жагы 1 ге барабар деп алынат 1).

Далилдөө. Каситетти далилдөө үчүн барабардыктын оң жагындагы кашааларды ачып чыгабыз. Ошондо биз

$$\theta\left(p_1^{\beta_1}\right)\theta\left(p_2^{\beta_2}\right)..\theta\left(p_k^{\beta_k}\right)=\theta\left(p_1^{\beta_1}p_2^{\beta_2}...p_k^{\beta_k}\right);$$

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

көрүнүшүндөгү кошулуучулардын суммасын алабыз. Бул болсо барабардыктын оң жагын берет.

Өз алдынча иштөө үчүн көнүгүүлөр

1) Эгерде $\varphi(a)$=3600 жана $a=3^{\alpha}5^{\beta}7^{\gamma}$ болсо, a ны тапкыла.

2) Эгерде $\varphi(a)$=120, $a=pq$, (p, q)=1, $p-q$=2 болсо, a ны тапкыла.

3) Эгерде $\varphi(a)$=11424, $a=p^2q^2$, (p, q)=1 болсо, a ны тапкыла.

4) Эгерде $\varphi(a)$=462000, $a=p_1^{\alpha_1}p_1^{\alpha_1}...p_n^{\alpha_n}$, $\alpha_k>1$, k=1,2,...,n болсо, a ны тапкыла.

5) Теңдемени чыгаргыла $\varphi(7^x)$=705894.

6) Барабардыкты далилдегиле:

а) $\varphi(4n)=2\varphi(2n)$, *b*) $\varphi(4n+2)=\varphi(2n+1)$.

7) Теңдемени чыгаргыла $\varphi(x)=12$.

8) Теңдемени чыгаргыла $\varphi(2x)=\varphi(3x)$.

9) x ты тапкыла

а) $\varphi(x)=x/2$; *b*) $\varphi(x)=2x/3$; *c*) $\varphi(x)=x/3$; *d*) $\varphi(x)=x/4$.

10) $\varphi(m)$, $m\ge3$ дин мааниси ар дайым жуп сан экендигин далидегиле.

11) Гаусстун $\sum_{d/a}\varphi(d)=a$ формуласын a нын төмөнкү маанилери үчүн текшергиле:

а) 72; b) 80; c) 360; d) 375; е) 957; ж) 2800.

12) $\varphi(5x)=\varphi(7x)$ теңдеме бүтүн сандарда чечилбөөчү экендигин далилдегиле.

Берилген n натуралдык сандын натуралдык бөлүүчүлөрүнүн санын жана суммасын; n ден чоң болбогон жана n менен өзара жөнөкөй сандардын санын тапкыла [13-37]:

13) $n=360$; 14) $n=430$; 15) $n=345$; 16) $n=542$; 17) $n=894$;
18) $n=895$; 19) $n=635$; 20) $n=324$; 21) $n=890$; 22) $n=784$;
23) $n=895$; 24) $n=334$; 25) $n=234$; 26) $n=324$; 27) $n=534$;
28) $n=654$; 29) $n=865$; 30) $n=990$; 31) $n=765$; 32) $n=779$
33) $n=745$; 34) $n=558$; 35) $n=410$; 36) $n=525$; 37) $n=912$.

n ! ды каноникалык көрүнүшүн тапкыла [38-62]:

38) $n=55$; 39) $n=53$; 40) $n=64$; 41) $n=92$; 42) $n=45$;
43) $n=67$; 44) $n=87$; 45) $n=50$; 46) $n=52$; 47) $n=63$;
48) $n=38$; 49) $n=65$; 50) $n=34$; 51) $n=90$; 52) $n=35$;
53) $n=66$; 54) $n=96$; 55) $n=68$; 56) $n=87$; 57) $n=37$;
58) $n=99$; 59) $n=57$; 60) $n=79$; 61) $n=94$; 62) $n=67$.

§ 7. Үзгүлтүксүз (чынжырлуу) бөлчөктөр

Евклиддин алгоритмин эске алуу менен төмөнкүдөй барабардыктардын системасын алабыз:

$$a=bq_1+r_2;\ \ 0\le r_2<b,$$

$$b=r_2q_2+r_3;\ \ 0\le r_3<r_1,$$

$$\ldots$$

$$r_{n-2}=r_{n-1}q_{n-1}+r_n;\ \ 0\le r_n<r_{n-1},$$

$$r_{n-1}=r_nq_n,$$

Барабардыктардын 1-син b га, 2-син r_2 ге, ж.б.у.с., акыркысын r_n ге бөлүп жиберип, төмөнкү барабардыктарга ээ болобуз:

$$\frac{a}{b}=q_1+\frac{r_2}{b}=q_1+\frac{1}{\frac{b}{r_2}},$$

$$\frac{b}{r_2}=q_2+\frac{r_3}{r_2}=q_2+\frac{1}{\frac{r_2}{r_3}},$$

$$\ldots$$

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

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

Мындан төмөнкүдөй бөлчөктү алабыз:

$$\frac{a}{b}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ldots\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}} \qquad (1)$$

Def 1. $\frac{a}{b}$ катышынын (1) көрүнүшү анын үзгүлтүксүз чынжыр-луу бөлчөккө ажыратылышы деп аталат.

$q_1,\ q_1+\frac{1}{q_2},\ q_1+\cfrac{1}{q_2+\cfrac{1}{q_3}},\ \ldots$ сандары үзгүлтүксүз бөлчөктүн бөлүктөрү деп аталышат. Үзгүлтүксүз бөлчөк: $\frac{a}{b}=\overline{(q_1,q_2,\ldots,q_n)}$ көрүнүшүндө белгиленет, q_1 – үзгүлтүксүз бөлчөктүн бүтүн бөлүгү деп аталат, $q_2,\ q_3,\ldots,q_n$ дер үзгүлтүксүз бөлчөктүн бөлүкче бөлүмдөрү деп аталышат.

Ар кандай бүтүн санды бир бөлүктөн турган үзгүлтүксүз бөлчөк деп кароого болот. $\frac{1}{a}$ бөлчөк эки бөлүктөн турган үзгүлтүксүз бөлчөк деп каралат (бүтүн бөлүгү 0).

Мисал. $\frac{95}{42}$ санын үзгүлтүксүз бөлчөккө ажыраткыла.

$$\frac{95}{42}=2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{2}}}},\quad \frac{95}{42}=\overline{(2,3,1,4,2)}.$$

Биз жогоруда ар кандай рационалдык санды чектүү үзгүлтүксүз бөлчөккө ажыратууга мүмкүн экендигин карадык. Эми тескери маселени карайбыз б.а. ар кандай чектүү үзгүлтүксүз бөлчөк кандайдыр бир рационалдык санды береби? Бул маселени чечүү үчүн төмөнкүдөй жаңы түшүнүктү – ылайыктуу бөлчөктөрдү кийрип алабыз:

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

$$\delta_n = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}.$$

Акыркы ылайыктуу бөлчөк $\frac{a}{b}$ рационалдык сандын өзү болот. Каалагандай ылайыктуу бөлчөктү эсептөө үчүн P_0=1, Q_0=0, P_1=q_1, Q_1=1 деп төмөнкүлөрдү жазып алабыз:

$$\delta_1 = \frac{q_0}{1} = \frac{P_1}{Q_1},$$

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

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

Математикалык индукция усулунун негизинде δ_kны төмөнкүдөй жазууга болот:

$$\delta_k = \frac{P_k}{Q_k} = \frac{q_k \cdot P_{k-1} + P_{k-2}}{q_k \cdot Q_{k-1} + Q_{k-2}},$$

мында P_k=$q_k P_{k-1}$+P_{k-2}, Q_k=$q_k Q_{k-1}$+Q_{k-2}.

Калагандай P_k жана Q_k ны эсептөө үчүн төмөнкү схеманы кийирип алабыз:

		q_1	q_2	…	q_{k-1}	q_k	…	q_n
P_k	P_0=1	P_1=q_1	P_2		P_{k-1}	P_k		P_n
Q_k	Q_0=0	Q_1=1	Q_2		Q_{k-1}	Q_k		Q_n

Мисал. $\overline{(2,3,1,4,2)}$ ге туура келген ылайыктуу рационалдык санды тапкыла.

Чыгаруу.

		2	3	1	4	2
P_k	1	2	7	9	43	95
Q_k	0	1	3	4	19	42

Демек, $\overline{(2,3,1,4,2)} = \frac{95}{42}$.

Мисал. $\frac{105}{38}$ кыскарбас бөлчөктү үзгүлтүксүз бөлчөккө ажыраткыла.

Чыгаруу. Евклиддин алгоритмин пайдаланабыз.

$$105 = 38 \cdot 2 + 29$$
$$38 = 29 \cdot 1 + 9$$
$$29 = 9 \cdot 3 + 2$$
$$9 = 2 \cdot 4 + 1$$
$$2 = 1 \cdot 2 + 0$$

$$\frac{105}{38} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}}$$

Ошондуктан жогорудагы схема төмөндөгүдөй көрүнүшкө келет:

q_s		2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

Касиеттери.

1^0. Айталы $\Delta_k = P_kQ_{k-1} - P_{k-1}Q_k$ болсун. $P_k=q_kP_{k-1}+P_{k-2}$, $Q_k=q_kQ_{k-1}+Q_{k-2}$ барабардыктарын пайдаланып, Δ_k ны төмөнкүчө өзгөртүп жазабыз:

$$\Delta_k = P_kQ_{k-1} - P_{k-1}Q_{k-1} = (q_kP_{k-1} + P_{k-2})Q_{k-1} - P_{k-1}(q_kQ_{k-1} + Q_{k-2}) =$$
$$= -(P_{k-1}Q_{k-2} - P_{k-2}Q_{k-1}) = -\Delta_{k-1}.$$

Демек, $\Delta_k = -\Delta_{k-1} = \Delta_{k-2} = -\Delta_{k-3} = \ldots$, б.а. Δ лар бирдей абсолюттук чоңдукка ээ жана $\Delta_1=P_1Q_0-Q_1P_0=q_1\cdot 0-1\cdot 1=-1$ болгондуктан ар кандай $1\le k\le n$ үчүн $\Delta_k=(-1)^k$ болот. Мындан $(P_k, Q_k)=1$ экендиги келип чыгат. Себеби, эгерде $(P_k, Q_k)=d>1$ десек, анда $(-1)^k$ дагы d га бөлүнө тургандыгы келип чыгат.

2^0. $\forall k>1$: $\delta_k - \delta_{k-1} = \dfrac{(-1)^k}{Q_kQ_{k-1}}$.

Чындыгында,

$$\delta_k - \delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_kQ_{k-1} - Q_kP_{k-1}}{Q_kQ_{k-1}} = \frac{(-1)^k}{Q_kQ_{k-1}} \Rightarrow |\delta_k - \delta_{k-1}| = \frac{1}{Q_kQ_{k-1}}.$$

Ар кандай иррационалдык санды да үзгүлтүксүз бөлчөккө ажыратууга болот. Бирок бул ажыралма чексиз көп бөлүккө ээ болот.

Мисал. $\sqrt{28}$ үзгүлтүксүз бөлчөккө ажыраткыла. $\sqrt{28} = 5 + \dfrac{1}{\alpha}$,

$\alpha>1$ болгондуктан $\alpha = \dfrac{1}{\sqrt{28}-5} = \dfrac{\sqrt{28}+5}{3} = 3 + \dfrac{1}{\beta}; \beta > 1.$

$$\beta = \frac{3}{\sqrt{28}-4} = \frac{3\left(\sqrt{28}+4\right)}{12} = \frac{\sqrt{28}+4}{4} = 2 + \frac{1}{\gamma}.$$

$\gamma = 1 + \dfrac{1}{\delta}$, $\delta = \dfrac{3}{\sqrt{28}-5} = \sqrt{28}+5 = 10 + \dfrac{1}{t}$, $\sqrt{28} = 5 + \dfrac{1}{t}$. Биз алгачкы иррационалдык санга кайтып келдик, $t=\alpha$ болот. Бул процессти

улантсак дагы кайрадан мурдагы бөлчөк кайталанат. Натыйжада төмөнкүгө ээ болобуз:

$$\sqrt{28} = 5 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{\alpha}}}}}}.$$

Өз алдынча иштөө үчүн көнүгүүлөр

Берилген бөлчөктү үзгүлтүксүз (чектүү чынжыр) бөлчөк түрүндө туюнткула жана анын ылайыктуу бөлчөктөрүн тапкыла [1-25]:

1) $\frac{707}{500}$; 2) $\frac{157}{225}$; 3) $\frac{167}{153}$; 4) $\frac{3107}{2341}$; 5) $-\frac{602}{367}$;

6) $-\frac{117}{343}$; 7) $-\frac{99}{170}$; 8) $-\frac{83}{217}$; 9) $\frac{521}{143}$; 10) $-\frac{602}{367}$;

11) $-\frac{149}{330}$; 12) $\frac{105}{38}$; 13) $\frac{245}{83}$; 14) $\frac{64}{25}$; 15) $\frac{73}{43}$;

16) $\frac{99}{464}$; 17) $-1\frac{11}{50}$; 18) $-2\frac{11}{39}$; 19) $-4\frac{25}{41}$; 20) $\frac{2633}{1810}$;

21) $\frac{121}{35}$; 22) $-2\frac{25}{64}$; 23) $-4\frac{5}{11}$; 24) $\frac{2432}{1713}$; 25) $\frac{2367}{1313}$.

Берилген иррационалдык сандарды чектүү чынжыр бөлчөк аркылуу туюнткула [26-50]:

26) $\frac{\sqrt{37}-3}{4}$; 27) $\frac{\sqrt{37}-1}{3}$; 28) $\frac{\sqrt{7925}-69}{14}$; 29) $\frac{\sqrt{13}-13}{3}$;

30) $\frac{\sqrt{101}-1}{4}$; 31) $\frac{\sqrt{37}+3}{4}$; 32) $\frac{5\sqrt{2}}{2}$; 33) $\frac{2(\sqrt{14}+2)}{5}$;

34) $\frac{25-\sqrt{61}}{4}$; 35) $\frac{29+\sqrt{21}}{10}$; 36) $\frac{138-\sqrt{5}}{79}$; 37) $\frac{18+\sqrt{506}-3}{28}$;

38) $\frac{4\sqrt{95}-18}{13}$; 39) $\frac{2+\sqrt{5}}{3}$; 40) $\frac{2+\sqrt{7}}{2}$; 41) $1-\sqrt{31}$;

42) $\frac{1+\sqrt{31}}{2}$; 43) $\frac{3-\sqrt{7}}{3}$; 44) $\frac{7-\sqrt{5}}{3}$; 45) $\frac{76+\sqrt{285}}{94}$;

46) $\frac{23-\sqrt{17}}{3}$; 47) $\frac{5-\sqrt{23}}{13}$; 48) $\frac{4+\sqrt{37}}{32}$; 49) $\frac{24-\sqrt{41}}{5}$;

50) $\frac{6-\sqrt{22}}{7}$.

§ 1. Салыштыруулар жана алардын негизги касиеттери

Def 1. Эгерде a жана b сандарын m ге бөлгөндө бирдей калдык келип чыкса, б.а. $a=mq_1+r$, $b=mq_2+r$ болсо, анда a жана bлар барабар (бирдей) калдыктуу же m модулу боюнча салыштырылуучу деп аталат жана $a \equiv b(\text{mod } m)$ көрүнүшүндө белгиленет. $a \equiv b(\text{mod } m)$ жазуусу a саны b менен m модулу боюнча салыштырылат деп окулат.

Теорема. Эгерде $a \equiv b(\text{mod } m)$ болсо, анда $(a-b) \vdots m$ болот, жана тескерисинче эгерде $(a-b) \vdots m$ болсо, анда $a \equiv b(\text{mod } m)$ болот.

Натыйжа. $\forall a \in Z, \forall m \in N, a=mq+r \Rightarrow a \equiv r \ (\text{mod } m)$.

Эгерде $r=0$ болсо, анда $a \equiv 0(\text{mod } m) \Rightarrow a \vdots m$ жана тескерисинче, эгерде $a \vdots m$ болсо, анда $a \equiv 0(\text{mod } m)$.

Касиеттери.

1^0. $\forall a \in Z, \ a \equiv a(\text{mod } m)$.

Далилдөө. Каалаган $a \in Z$ үчүн $a-a=0$ жана $0 \vdots m$ болгондуктан $(a-a)=0 \vdots m$ болот, мындан жана жогордагы теореманын негизинде $a \equiv a(\text{mod } m)$ келип чыгат.

2^0. $a \equiv b(\text{mod } m) \Rightarrow b \equiv a(\text{mod } m)$.

Далилдөө. $a \equiv b(\text{mod } m) \Rightarrow (a-b) \vdots m \Rightarrow (a-b) = -(b-a) \vdots m$

$\Rightarrow (b-a) \vdots m \Rightarrow b \equiv a(\text{mod } m)$.

3^0. $a \equiv c \ (\text{mod } m), \ b \equiv c \ (\text{mod } m) \Rightarrow a \equiv b \ (\text{mod } m)$.

Далилдөө. $a \equiv c(\text{mod } m) \wedge b \equiv c(\text{mod } m) \Rightarrow (a-c) \vdots m \wedge$

$(b-c) \vdots m \Rightarrow (a-c+b-b) \vdots m \Rightarrow ((a-b)+(b-c)) \vdots m \Rightarrow a \equiv b \ (\text{mod } m)$.

4^0. $a \equiv b \ (\text{mod } m), \ c \equiv d \ (\text{mod } m) \Rightarrow a \pm c \equiv b \pm d \ (\text{mod } m)$.

Далилдөө. Эки учурду өзүнчө жазып алабыз:

1) $a \equiv b \pmod m$, $c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$;

2) $a \equiv b \pmod m$, $c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$.

1-син далилдейбиз, 2-си окурманга сунушталат.

$a \equiv b \pmod m$, $c \equiv d \pmod m \Rightarrow (a-b) \vdots m \wedge (c-d) \vdots m \Rightarrow$

$(a-b+c-d) \vdots m \Rightarrow (a+c-(b+d)) \vdots m \Rightarrow a + c \equiv b + d \pmod m$.

5^0. $a + c \equiv b \pmod m \Rightarrow a \equiv b - c \pmod m$.

Далилдөө.

$a + c \equiv b \pmod m \Rightarrow (a + c - b) \vdots m \Rightarrow (a - (b - c)) \vdots m \Rightarrow a \equiv b - c \pmod m$.

6^0. $a \equiv b \pmod m \Rightarrow a \pm mk \equiv b \pmod m \vee a \equiv b \pm mk \pmod m$.

Далилдөө.

$a \equiv b \pmod m \Rightarrow (a - b) \vdots m \Rightarrow (a - b \pm mk) \vdots m \Rightarrow a \pm mk \equiv b \pmod m$.

7^0. $a \equiv b \pmod m$, $c \equiv d \pmod m \Rightarrow ac \equiv bd \pmod m$.

Далилдөө. $a \equiv b \pmod m$, $c \equiv d \pmod m$ $(a-b) \vdots m \wedge (c-d) \vdots m \Rightarrow$

$(a-b)(c-d) \vdots m^2 \Rightarrow (ac - ad - bc + bd - bd + bd) \vdots m^2 \Rightarrow$

$(ac - bd) - d(a - b) - b(c - d) = qm^2 \Rightarrow (ac - bd) - dmq_1 - bmq_2 = qm^2$

$\Rightarrow (ac - bd) = m(dq_1 + bq_2 + qm) \Rightarrow ac \equiv bd \pmod m$.

8^0. $a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$, $n \in N$.

Далилдөө. $a \equiv b \pmod m \Rightarrow (a - b) = mq$ барабардыктын эки жагын тең $a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + a^2b^{n-3} + ab^{n-2} + b^{n-1}$ га көбөйтөбүз:

$(a-b)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + a^2b^{n-3} + ab^{n-2} + b^{n-1}\right) = a^n - b^n$;

$mq\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + a^2b^{n-3} + ab^{n-2} + b^{n-1}\right) = mq_1$.

$a^n - b^n = mq_1 \Rightarrow a^n \equiv b^n \pmod m$.

9^0. $a \equiv b \pmod m \Rightarrow ak \equiv bk \pmod m$, $k \in N$.

Далилдөө. $a \equiv b \pmod m \Rightarrow a - b = mq \Rightarrow k(a-b) = mqk \Rightarrow ak \equiv bk \pmod m$.

10^0. $ak \equiv bk \pmod m \wedge (k, m) = 1 \Rightarrow a \equiv b \pmod m$.

Далилдөө. $ak \equiv bk \pmod m \Rightarrow k(a-b) \vdots m \wedge (k, m) = 1 \Rightarrow (a-b) \vdots m \Rightarrow$

$a \equiv b \pmod m$.

11^0. $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$, $a_i \in Z$, $i=0,1,\ldots n$, $\wedge\ x \equiv x_l \pmod m \Rightarrow$ $f(x) \equiv f(x_l) \pmod m$.

Бул касиет 4^0, 8^0, 9^0 касиеттердин жардамында далилденет. Калган касиеттердин далилдөөсү окурманга сунушталат.

12^0. $a \equiv b \pmod m \wedge a=a_1d,\ b=b_1d,\ m=m_1d \Rightarrow a_1 \equiv b_1 \pmod{m_1}$.

13^0. $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, …, $a \equiv b \pmod{m_k} \Rightarrow a \equiv b \pmod M$, мында $M=[m_1, m_2, \ldots, m_k]$.

14^0. $a \equiv b \pmod m \wedge m \vdots d \Rightarrow a \equiv b \pmod d$.

15^0. $a \equiv b \pmod m \wedge a \vdots d,\ m \vdots d \Rightarrow b \vdots d$.

Өз алдынча иштөө үчүн көнүгүүлөр

1) Эгерде n так сан болсо, анда $n^2-1 \equiv 0 \pmod 8$ болорун далилдегиле.
2) Эгерде p – жөнөкөй сан болсо, анда $(a+b)^p \equiv a^p+b^p \pmod p$ экендигин далилдегиле.
3) Эгерде $100a+10b+c \equiv 0 \pmod{21}$ болсо, анда $a-2b+4c \equiv 0 \pmod{21}$ экендигин далилдегиле.
4) Эгерде $3^n \equiv -1 \pmod{10}$ болсо, анда $3^{n+4} \equiv -1 \pmod{10}$ экендигин далилдегиле.
5) $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$ экендигин далилдегиле.
6) Текшергиле $3^{14} \equiv -1 \pmod{29}$.
7) 1532^5-1 ди 9 га бөлгөндөгү калдыкты тапкыла.
8) Эгерде p жөнөкөй сан болсо, анда $C_{p-1}^k \equiv (-1)^k \pmod p$ болорун далилдегиле.
9) Эгерде $ac \equiv bd \pmod m \wedge a \equiv b \pmod m \wedge (a, m)=1$ болсо, анда $c \equiv d \pmod m$) экендигин далилдегиле.
10) Эгерде $a^{100} \equiv 2 \pmod{73} \wedge a^{101} \equiv 69 \pmod{73}$ болсо, анда a санын 73 гө бөлгөндөгү калдыкты тапкыла.

11) Эгерде $\frac{11a+2b}{19} \in Z$ болсо, анда $\frac{18a+5b}{19} \in Z$ экендигин далилдегиле.

12) Далилдегиле

$1^{2k+1}+2^{2k+1}+3^{2k+1}+\ldots+(p-1)^{2k+1} \equiv 0(\text{mod } p)$, $p>2$ – жөнөкөй сан.

13) Эгерде $a \equiv b \pmod{p^n}$ болсо, анда $a^p \equiv b^p \pmod{p^{n+1}}$ экендигин далилдегиле, мында p – жөнөкөй сан.

§ 2. Берилген модулу боюнча чегериштердин классы

Бардык бүтүн сандарды кандайдыр бир m санга бөлгөндө 0, 1, 2, …, (m –1) калдыктар пайда болот. Ар бир калдыкка сандардын бир классы туура келет.

m модулга бөлгөндө бирдей (барабар) калдык кала турган сандардын көптүгүн бир класс деп карайбыз. Класстарды тиешелүү түрдө $C_0, C_1, \ldots, C_{m-1}$ аркылуу белгилейли.

Def 1. C_0, C_1, …, C_{m-1} класстар m модулу боюнча чегериштердин классы деп аталат.

Калдыктын жана тийиндинин жашашы жана жалгыздыгы жөнүндөгү теореманын негизинде чегериштердин m модулу боюнча ар түрдүү класстары жалпы элементке ээ болбойт. Бүтүн сандардын көптүгү өз ара кесилишпөөчү класстарга ажралат. C_r классынын элементтери $mq+r$ көрүнүшүнө ээ болот, анын элементтеринин бардыгын qга ар түрдүү маанилерди берүү менен аныктоо мүмкүн. Мисалы, m =10 болгондо 3 калдык пайда кыла тургандай сандар $10q$ +3 көрүнүшкө ээ жана q=0, ±1, ±2,… десек, –27, –17, –7, 3, 13, 23, … классы пайда болот.

Эгерде эки бүтүн сан m модулу боюнча бир класска таандык болсо, анда алар m модулу боюнча салыштырылуучу болушу түздөн-түз келип чыгат.

Def 2. m модулу боюнча ар бир класстан бирден алынып түзүлгөн сандардын көптүгү m модулу боюнча чегериштердин толук системасы деп аталат.

Мисалы, m=10 модулу боюнча $10q$, $10q+1$, …, $10q+9$ класстарды пайда кылуу мүмкүн. Ошондуктан ар биринен бирден алынып түзүлгөн система мисалы,

30, 21, 102, 33, 54, 15, 6, 187, –12, –51

10 модулу боюнча түзүлгөн чегериштердин толук системасы болот.

Чегериштердин m модулу боюнча толук системасы катарында $\{0, 1, 2, \ldots, (m-1)\}$ көптүк алынат. Айрым учурларда болсо абсолюттук чоңдугу боюнча эң кичине чегериштер алынат. Эгерде m жуп болсо, анда эң кичине чегериштер $\left\{0, \pm 1, \pm 2, \ldots, \pm\frac{m-2}{2}, \pm\frac{m}{2}\right\}$ болот, эгерде m так болсо, анда эң кичине чегериштер $\left\{0, \pm 1, \pm 2, \ldots, \pm\frac{m-3}{2}, \pm\frac{m-1}{2}\right\}$ болот.

Теорема (сызыктуу форма жөнүндө). Эгерде $ax+b$ сызыктуу формасындагы x өзгөрүлмөсү, каалагандай b бүтүн саны $(a, m)=1$ болгондо m модулу боюнча чегериштердин толук системасын түзсө, анда $ax+b$ өзгөрүлмөсү дагы m модулу боюнча чегериштердин толук системасын түзөт.

Далилдөө. Чындыгында, пайда болгон система төмөнкү шарттарды канааттандырат:

1) Системадагы сандардын саны m ге барабар болот, себеби x тин ордуна m ар түрдүү маани берилет;

2) Пайда болгон сандар m модулу боюнча ар түрдүү класска таандык болот. Бул сүйлөмдү карама-каршысынан далидейбиз. Алар ар түрдүү класска таандык болбосун, б.а. $ax_1+b \equiv ax_2+b \pmod m$ болсун деп алалы. Анда $ax_1 \equiv ax_2 \pmod m$ болот. Эгерде $(a, m)=1$ экендигин эске алсак анда $x_1 \equiv x_2 \pmod m$ келип чыгат. Бирок мындай болушу мүмкүн эмес, себеби теоремanын шарты боюнча x саны m модулу боюнча чегериштердин толук системасын түзөт, б.а. $x_1 \neq x_2$. Биз карама-каршылыкка келдик. Демек, $ax+b$ сандары m модулу боюнча ар түрдүү класстардын өкүлдөрү болушат.

2. Чегериштердин келтирилген системасы

Def 3. m модулу менен өз ара жөнөкөй болгон чегериштердин класстарынан бирден элемент алынып түзүлгөн

көптүк чегериштердин m модулу боюнча келтирилген системасы деп аталат.

Чегериштердин толук системасы сыяктуу келтирилген системаны да үч көрүнүшүн алууга болот:

1) эң кичине оң чегериштердин келтирилген системасы;

2) абсолюттук чоңдугу боюнча эң кичине терс чегериштердин келтирилген системасы;

3) абсолюттук чоңдугу боюнча эң кичине чегериштердин келтирилген системасы.

Чегериштердин келтирилген системасын алардын чегериштеринин толук системасынан да түзүүгө болот. Ал үчүн толук системадан m модулу менен өз ара жөнөкөй болгон чегериштерди ажыратып алуу керек.

Мисал. 10 модулу боюнча чегериштердин толук системасы {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} болгондуктан, чегериштердин келтирилген системасы {1, 3, 7, 9} болот. Ошондой эле {1, 3, –3, –1} дагы чегериштердин келтирилген системасы болот.

Чегериштердин келтирилген системасындагы сандардын санын аныктоо үчүн, жогоруда айтып өтүлгөн, Эйлердин функциясы деп аталуучу $\varphi(m)$ функциясы колдонулат.

Эйлердин функциясы ар бир оң бүтүн m саны үчүн аныкталган, ал 0, 1, …, m–1 сандардын арасында m менен өз ара жөнөкөй болгон сандардын санын аныктайт.

Берилген сандардын көптүгү m модулу боюнча чегериштердин келтирилген системасы болушу үчүн төмөнкү үч шартын аткарылышы жетиштүү:

1) көптүктүн элементтеринин саны $\varphi(m)$ ге барабар болушу керек;

2) m модулу боюнча өз ара салыштырылуучу болбошу керек (б.а. модулу боюнча ар түрдүү класстын өкүлдөрү болушу керек);

3) m модулу менен өз ара жөнөкөй болушу керек.

Теорема (сызыктуу форма жөнүндө). Эгерде ax сызыктуу формасындагы x өзгөрүлмөсү m модулу боюнча чегериштердин келтирилген системасын түзсө анда $(a, m)=1$ болгондо ax дагы m модулу боюнча чегериштердин келтирилген системасын түзөт.

Далилдөө. Теореманы далилдөө үчүн ax тер дагы жогорудагы үч шартты канааттандырышын көрсөтүү жетиштүү.

1) ax өзгөрүлмө сандарынын саны $\varphi(m)$ ге барабар, себеби x тин ордуна биз удаалаш $\varphi(m)$ даана сан коебуз;

2) сызыктуу форма жөнүндөгү теореманын негизинде $ax+b$ өзгөрүлмөсү m модулу боюнча ар түрдүү класстардын өкүлдөрү. Демек, ax тер дагы ар түрдүү класстардын өкүлдөрү болот. Себеби x өзгөрүлмөсү ар түрдүү класстардан алынат жана $(a, m)=1$;

3) теореманын шарты боюнча $(a, m)=1$ болгондо x өзгөрүлмөсү m модулу боюнча чегериштердин келтирилген системасынын элементи болгондуктан, $(x, m)=1$ болот. Демек, $(ax, m)=1$.

Эскертүү. x жана ax чегериштеринин ар бири өзүнчө m модулу боюнча келтирилген чегериштердин системасын түзсө да, алар x тин бирдей маанилеринде ар түрдүү класстын өкүлдөрү болот. Чындыгында, $(x, m)=1$ болгондуктан, $ax \equiv x \pmod m$ салыштыруусу качан гана $a \equiv 1 \pmod m$ болгондо орун алат.

Эгерде x жана ax тердин модулу боюнча түзүлгөн терс эмес эң кичине чегериштердин системаларын ала турган болсок, бул системалардын элементтери жуп-жубу менен өз ара барабар болот, болгону алар орундары менен айрымаланышат.

Мисалы, $a=5$, $m=14$ болсун, анда $(5, 14)=1$ болот. $m=14$ модулу боюнча чегериштердин келтирилген системасы $\{1, 3, 5, 9, 11, 13\}$ болот. $m=14$ модулу боюнча $5x$ ти эсептейбиз:

$5 \cdot 1 \equiv 5 \pmod{14}$,

$5 \cdot 3 \equiv 15 \equiv 1 \pmod{14}$,

$5 \cdot 5 \equiv 25 \equiv 11 \pmod{14}$,

$5 \cdot 9 \equiv 45 \equiv 3 \pmod{14}$,

$5 \cdot 11 \equiv 55 \equiv 13 \pmod{14}$,

$5 \cdot 13 \equiv 65 \equiv 9 \pmod{14}$.

Демек, келтирилген система {5, 1, 11, 3, 13, 9} болот. {1, 3, 5, 9, 11, 13} системасы {5, 1, 11, 3, 13, 9} системасынан элементтеринин орду менен гана айрымаланат. Элементтеринин көбөйтүндүлөрү барабар болот:

$$1 \cdot 3 \cdot 5 \cdot 9 \cdot 11 \cdot 13 = 5 \cdot 1 \cdot 11 \cdot 3 \cdot 13 \cdot 9.$$

Өз алдынча иштөө үчүн көнүгүүлөр

1) Чегериштердин толук жана келтирилген системаларынын үч көрүнүшүн жазгыла:

a) $m=9$; b) $m=8$; c) $p=13$; d) $m=12$; e) $m=15$; f) $p=7$; g) $m=10$.

2) Төмөндөгү сандар берилген m модулу боюнча чегериштердин толук системасын түзүшө тургандыгын көрсөткүлө:

a) 25, –20, 16, 46, –21, 18, 37, –17; $m=8$.

b) 21, 2, –18, 28, –19, 40, –22, –2, 15; $m=9$.

c) 24, 18, –19, 37, 28, –23, –32, 5, 41, –35, –33; $m=11$.

3) Төмөндөгү сандар берилген m модулу боюнча чегериштердин келтирилген системасын түзүшө тургандыгын көрсөткүлө:

a) 19, 23, 25, –19; $m=12$.

b) 11, –1, 17, –19; $m=8$.

c) 13, –13, 29, –9; $m=10$.

§3. Эйлердин жана Ферманын теоремалары

1. Эйлердин теоремасы. Эгерде $(a, m)=1$ болсо, анда

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$$ болот.

Далилдөө. Сызыктуу форма жөнүндөгү 2-теореманы колдонобуз. ax формасын алып, x тин ордуна m модулу боюнча чегериштердин келтирилген системасындагы сандарды удаалаш коюп чыгабыз. Чегериштердин келтирилген системасын эң кичине оң сандардан түзүп алабыз. Эгерде x өзгөрүлмөсү кабыл ала турган эң кичине оң чегериштер $r_1, r_2,\ldots, r_k$ ($k=\varphi(m)$) болсо, анда ax формасы кабыл ала турган эң кичине чегериштер тиешелүү түрдө $r_1', r_2', \ldots, r_k'$ болот.

Демек, $ar_1 \equiv r_1' (\mathrm{mod}\, m)$,

$ar_2 \equiv r_2' (\mathrm{mod}\, m)$,

...

$ar_k \equiv r_k' (\mathrm{mod}\, m)$.

Аларды мүчөлөп көбөйтөбүз: $a^k \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_k \equiv r_1' \cdot r_2' \cdot \ldots \cdot r_k' (\mathrm{mod}\, m)$.

$r_1 \cdot r_2 \cdot \ldots \cdot r_k$ көбөйтүндү менен $r_1' \cdot r_2' \cdot \ldots \cdot r_k'$ көбөйтүндү барабар, жана алардын ар бири m модулу менен өз ара жөнөкөй. Себеби $(r_i, m)=1$. Ошондуктан төмөндөгү орун алат:

$$a^k \equiv 1 (\mathrm{mod}\, m).$$

Мындан $k=\varphi(m)$ болгондуктан, $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$ келип чыгат.

Мисалы, $m=8$, $a=5$ болсун. $(8, 5)=1$ болгондуктан $5^{\varphi(8)} \equiv 1 (\mathrm{mod}\, 8)$ экендигин көрсөтөбүз.

$$\varphi(8)=\varphi(2^3)=2^3-2^2=4,\ 5^2 \equiv 25 \equiv 1 (\mathrm{mod}\ 8) \Rightarrow 5^4 \equiv 625 \equiv 1 (\mathrm{mod}\ 8).$$

2. **Ферманын теоремасы**. Эгерде $(a, p)=1$ болсо, анда

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p)$$ болот.

Далилдөө. Ферманын теоремасы Эйлердин теоремасынын жекече учуру болот. Чындыгында $m=p$ болсо, $\varphi(p)=p-1$ болот.

Анда Эйлердин теоремасы боюнча $a^{p-1}\equiv 1(\text{mod } p)$ болот. $(a, p)=1$ болгондуктан $a^p\equiv a(\text{mod } p)$ келип чыгат.

Мисалы, $p=11$, $a=8$ болсун $8\equiv -3(\text{mod } 11)$ болгондуктан $8^{10}\equiv(-3)^{10}(\text{mod } 11)$ болот. Демек, $(-3)^2\equiv 9\equiv -2(\text{mod } 11)\Rightarrow$ $(-3)^{10}\equiv(-2)^5\equiv -32\equiv 1(\text{mod } 11)\Rightarrow 8^{10}\equiv 1(\text{mod } 11)$.

Ферманын теоремасынын тескериси орун албайт, б.а. $(a, n)=1$ болгондо $a^{n-1}\equiv 1(\text{mod } n)$ дин аткарылышынан n дин жөнөкөй экендиги келип чыкпайт.

Мисалы, эгерде $n=341$ болсо, анда $\varphi(341)=340$ болот, мейли $a=2$ болсун. Анда $2^{341-1}\equiv 1(\text{mod } 341)$, $2^{340}\equiv 1(\text{mod } 341)$ аткарылат, бирок $341=11\cdot 31$. Чындыгында $2^{10}\equiv 1024\equiv 1(\text{mod } 341)$, ошондуктан $2^{340}\equiv 1(\text{mod } 341)$ болот.

§4. Бир белгисиздүү биринчи даражадагы салыштыруулар жана аларды чечүүнүн усулдары

1. Бир белгисиздүү биринчи даражадагы салыштыруулар

Бир белгисиздүү биринчи даражадагы салыштыруулардын жалпы көрүнүшү $ax \equiv b \pmod m$ түрүндө болот, мында $a, b \in Z$.

Def 1. Эгерде $x=x_1$ сандарынын классы $ax \equiv b \pmod m$ салыштыруу-сун туура сандык салыштырууга айландырса, анда бул сандардын классы берилген салыштыруунун чечими деп аталат.

Эгерде $x=x_1$ саны салыштыруунун чечими болсо, анда $x=x_1+mt$, $t \in Z$ сандардын системасы да чечим болот. Бир класстагы бардык чечимдерди бир чечим деп кабыл алабыз. Төмөнкү учурларды карап чыгабыз:

1) $(a, m)=1$. Эгерде $ax \equiv b \pmod m$ салыштыруусу чечимге ээ болсо, анда ал чечим m модулу боюнча чегериштердин кандайдыр бир классынан турат. Белгилүү болгондой чегериштердин толук системасындагы ар бир чегеришке бир класс туура келет. Демек, x өзгөрүлмөсү чегериштердин толук системасын кабыл алат, анда сызыктуу форма жөнүндөгү 1-теореманын негизинде ax дагы чегериштердин толук системасын кабыл алат.

x белгисизинин кандайдыр бир x_0 маанисинде ax_0 чегериши менен b саны бир класска таандык болот, б.а. $ax_0 \equiv b \pmod m$. Мындан $x \equiv x_0 \pmod m$ классы $ax \equiv b \pmod m$ салыштыруусунун жалгыз чечими боло тургандыгы келип чыгат.

2) $(a, m)=d>1$. $ax \equiv b \pmod m$ салыштыруусун $ax-b=my$ көрүнүшүндө жазып алабыз, мында y – бүтүн сан. Демек, $ax-b=my$ барабардыкта $(m \vdots d \wedge a \vdots d) \Rightarrow b \vdots d$. Мындан, эгерде b саны dга бөлүнбөсө, анда $ax \equiv b \pmod m$ салыштыруусу чечимге ээ болбойт деген тыянак келип чыгат.

Эгерде b саны d га бөлүнсө, анда

$$ax \equiv b(\mathrm{mod}\, m) \Rightarrow a_1 x \equiv b_1(\mathrm{mod}\, m_1).$$

$(a_1, m_1)=1$ болгондуктан $a_1x \equiv b_1(\mathrm{mod}\, m_1)$ салыштыруусу m_1 модулу боюнча жалгыз x_0 чечимине ээ болот: $x \equiv x_0(\mathrm{mod}\, m_1) \Rightarrow x=x_0+tm_1$, $t \in Z$. Бул чечим $ax \equiv b(\mathrm{mod}\, m)$ салыштыруусун да канааттандырат. Бирок бул салыштыруу дагы башка чечимдерге ээ болот, жалпы чечимдеринин саны d га барабар, алар төмөнкүдөй көрүнүштө болушат:

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

Тыянак. 1) Эгерде $(a, m)=1$ болсо, анда $ax \equiv b(\mathrm{mod}\, m)$ салыштыруусунун чечими жашайт жана жалгыз болот;

2) $(a, m)=d>1$ жана b саны d га бөлүнбөсө, анда $ax \equiv b(\mathrm{mod}\, m)$ салыштыруусу чечимге ээ болбойт;

3) $(a, m)=d>1$ жана b саны d га бөлүнсө, анда $ax \equiv b(\mathrm{mod}\, m)$ салыштыруусунун чечимдеринин саны d га барабар болот.

Мисалдар.

1) $3x \equiv 7(\mathrm{mod}\ 11)$ салыштыруунун чечимин тапкыла.

Чыгаруу. $(3, 11)=1$ болгондуктан чечим жашайт жана жалгыз болот. $m=11$ модулу боюнча чегериштердин толук системасы $\{0, \pm1, \pm2, \pm3, \pm4, \pm5\}$ болот. Түздөн түз текшерип көрүү менен $x \equiv -5(\mathrm{mod}11)$ чечим боло тургандыгына ынанабыз.

2) $3x \equiv 7(\mathrm{mod}\ 15)$ салыштыруунун чечимин жашабастыгын далилдегиле.

Чыгаруу. $(3, 15)=3>1$ жана 7 саны 3кө бөлүнбөгөнү үчүн салыштыруунун чечими жашабайт.

3) $9x \equiv 6(\mathrm{mod}\ 15)$ салыштыруунун чечимдерин тапкыла.

Чыгаруу. $(9, 15)=3>1$, $(6, 15)=3$ болгондуктан салыштыруунун чечими жашайт. Чындыгында салыштырууну $3x \equiv 2(\mathrm{mod}\ 5)$ көрүнүшүндө жазып алууга болот, $(3, 5)=1$ болгондуктан, бул салыштыруу 5 модулу боюнча жалгыз чечимге ээ болот, $x \equiv -1(\mathrm{mod}\ 11)$. $d=3$ болгондуктан берилген салыштыруу 3 чечимге ээ болот:

$x_1 \equiv -1 (\text{mod } 11)$, $x_2 \equiv 4 (\text{mod } 11)$, $x_3 \equiv 9 (\text{mod } 11)$.

2. Биринчи даражадагы салыштырууларды чечүүнүн усулдары

Бир белгисиздүү салыштырууну чечүүнүн бир нече усулдары бар. Алар менен таанышып чыгабыз. Айталы бизге $ax \equiv b (\text{mod } m)$ салыштыруусу берилген болсун.

1) **Тандоо усулу**. $ax \equiv b (\text{mod } m)$ салыштыруудагы x тин ордуна чегериштердин толук системасындагы бардык чегериштер удаалаш коюлат, алардын кайсы бири салыштырууну туура салыштырууга айландырса, ошол чечим болот. Биз жогорудагы 2 мисалды ушул усул менен чыгардык. Бирок модул чоң сан болгондо бул усулду колдонуу ыңгайлуу болбойт.

Мисал. $4x \equiv 3 (\text{mod } 5)$ салыштыруунун чечимин тапкыла.

Чыгаруу. (4, 5)=1 болгондуктан чечим жашайт жана жалгыз болот. m=5 модулу боюнча чегериштердин толук системасы {0, ±1, ±2} болот. Түздөн түз текшерип көрүү менен $x \equiv 2 (\text{mod } 11)$ чечим боло тургандыгына ынанабыз.

2) **Коэффициенттерди өзгөртүү усулу**. Практикада салыштыруунун касиеттеринен пайдаланып, белгисиздин алдындагы коэффициентти жана b ны оң жакта пайда болгон сан x тин коэффициентине бөлүнө тургандай өзгөртүү мүмкүн.

Эгерде $(b, m)=d>0$ болсо, жаңы өзгөрүлмөгө өтүү максатка ылайыктуу болот.

Мисал. 1) $7x \equiv 5 (\text{mod } 9) \Rightarrow 7x \equiv (5+9) (\text{mod } 9) \Rightarrow 7x \equiv 14 (\text{mod } 9)$, (7, 9)=1 болгондуктан $x \equiv 2 (\text{mod } 9)$ болот.

2) $17x \equiv 25 (\text{mod } 28) \Rightarrow 17x+28x \equiv 25 (\text{mod } 28) \Rightarrow 45x \equiv 25 (\text{mod } 28)$, (9, 28)=1 болгондуктан $9x \equiv 5 (\text{mod } 28) \Rightarrow 9x \equiv (5-140) (\text{mod } 28) \Rightarrow 9x \equiv -135 (\text{mod } 28) \Rightarrow x \equiv -15 (\text{mod } 28) \Rightarrow x \equiv 13 (\text{mod } 28)$.

) **Эйлердин теоремасын колдонуп**. Эйлердин теоремасы боюнча $(a, m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 (\mathrm{mod} m)$. Бул салыштырууну $a^{\varphi(m)} b \equiv b (\mathrm{mod}\, m)$ көрүнүшүндө жазып, $ax \equiv b (\mathrm{mod} m)$ менен салыштырабыз. Анда $x = a^{\varphi(m)-1} b (\mathrm{mod} m)$ келип чыгат. Мисал ыгарууда $a^{\varphi(m)-1} b$ туюнтмасын m модулу боюнча эң кичине негеришке келтирип алуу керек.

Мисал. $3x \equiv 7 (\mathrm{mod}\ 11)$ салыштырууну Эйлердин теоремасын пайдаланып чыгаргыла.

Чыгаруу. $3x \equiv 7 (\mathrm{mod}\ 11) \Rightarrow x \equiv 3^{\varphi(11)-1} 7 (\mathrm{mod}\ 11)$, $\varphi(11)=10$,

$3^2=9 \equiv -2 (\mathrm{mod}\ 11) \Rightarrow 3^4 \equiv 4 (\mathrm{mod}\ 11) \Rightarrow 3^5 \equiv 12 (\mathrm{mod}\ 11) \Rightarrow 3^9 \equiv 4 (\mathrm{mod}\ 11)$ болгондуктан $x \equiv 7 \cdot 3^9 (\mathrm{mod}\ 11) \equiv 28 (\mathrm{mod}\ 11) \equiv 6 (\mathrm{mod}\ 11)$, $x \equiv 6 (\mathrm{mod}\ 11)$ болот.

Бирок салыштыруунун модулу жетишээрлик даражада чоң болгондо бул усулдарды пайдалануу ыңгайлуу эмес. Мындай учурда төмөнкү усулду колдонгон максатка ылайыктуу болот.

4) **Үзгүлтүксүз бөлчөктөр усулу**. $ax \equiv b (\mathrm{mod} m)$, $(a, m)=1$, $a>0$ салыштыруусу берилген болсун. $\frac{m}{a}$ бөлчөгүн үзгүлтүксүз бөлчөккө ажыратабыз. Анын ылайыктуу бөлчөктөрүн $\frac{P_k}{Q_k}$ ($k=1, 2, \ldots, n$) деп белгилейбиз. $(P_k, Q_k)=1$ болгондуктан, $P_n=m$, $Q_n=a$. Анда үзгүлтүксүз бөлчөктүн $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n$ касиетинен $m Q_{n-1} - P_{n-1} a = (-1)^n$ келип чыгат. Акыркы барабардыктан

$$P_{n-1} a = -(-1)^n + m Q_{n-1} \text{ же } P_{n-1} a \equiv (-1)^{n-1} (\mathrm{mod}\, m)$$

келип чыгат. Акыркы салыштыруунун эки жагын тең $(-1)^{n-1} b$ га көбөйтөбүз:

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

Эгерде $ax \equiv b (\mathrm{mod}\, m)$ экендигин эске алсак, анда

$x \equiv (-1)^{n-1} b\, P_{n-1} (\mathrm{mod}\, m)$ келип чыгат. Мында P_{n-1} саны $\frac{m}{a}$ бөлчөгүнүн (n–1) -ылайыктуу бөлчөгүнүн алымы. $ax \equiv b (\mathrm{mod}\, m)$ салыштыруусу жалгыз чечимге ээ болгондуктан, анын чечими

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

Мисал 1. $285 \equiv 177 (\mathrm{mod}\, 924)$ салыштырууну чыгаргыла.

Чыгаруу. (285, 924)=3, 177=3·59 болгондуктан салыштырууну 3кө кыскартабыз: $95 \equiv 59 (\mathrm{mod}\, 308)$.

$\frac{308}{59}$ бөлчөгүн ылайыктуу бөлчөктөргө ажыратабыз:

$308 = 95 \cdot 3 + 23,$

$95 = 23 \cdot 4 + 3,$

$23 = 3 \cdot 7 + 2,$

$3 = 2 \cdot 1 + 1,$

$2 = 2 \cdot 1.$

Демек, $q_1=3$, $q_2=4$, $q_3=7$, $q_4=1$, $q_5=1$. Таблицаны толтурабыз:

q_k	0	3	4	7	1	2
P_k	1	3	13	94	107	308

Демек, $P_{n-1}=P_4=107$. Мындан $x \equiv (-1)^4 \cdot 107 \cdot 59 (\mathrm{mod}\, 308)$ же $x \equiv 153 (\mathrm{mod}\, 308)$. Анда

$x_1 \equiv 153 (\mathrm{mod}\, 924)$, $x_2 \equiv 461 (\mathrm{mod}\, 924)$, $x_3 \equiv 769 (\mathrm{mod}\, 924)$ берилген салыштыруунун чечимдери болушат.

Мисал 2. Төмөнкү салышытрууну чыгаргыла:

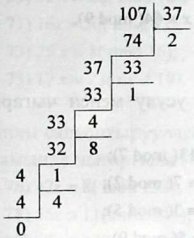
$$111x \equiv 75 (\mathrm{mod}\, 321).$$

Чыгаруу. Бул жерде (111, 321) = 3, 75 саны 3кө эселүү. Ошондуктан салыштыруу үч чечимге ээ болот.

Салыштырууну эки жагын жана модулун 3кө кыскартып жиберебиз:

$$37x \equiv 25 (\mathrm{mod}\, 107).$$

Пайда болгон салыштырууну үзгүлтүксүз бөлчөктөрдү пайдаланып чыгарабыз:



q		2	1	8	4
P_s	1	2	3	26	107

Демек, каралып жаткан учурда n=4, P_{n-1}=26, b=25 болгондуктан чечим төмөнкүдөй болот:

$$x \equiv -26 \cdot 25 \equiv 99 \pmod{107}.$$

Берилген салыштыруунун чечимдери:

$x_1 \equiv 99 \pmod{321}$, $x_2 \equiv 99+107 \pmod{321}$, $x_3 \equiv 99 + 2 \cdot 107 \pmod{321}$ б.а.

$x_1 \equiv 99 \pmod{321}$, $x_2 \equiv 206 \pmod{321}$, $x_3 \equiv 313 \pmod{321}$ болот.

Өз алдынча иштөө үчүн көнүгүүлөр

Берилген салыштырууларды касиеттердин жардамында чыгаргыла [1-25]:

1) $7x \equiv 8 \pmod{13}$;
2) $4x \equiv 3 \pmod{16}$;
3) $6x \equiv 11 \pmod{14}$;
4) $12x \equiv 7 \pmod{21}$;
5) $8x \equiv 10 \pmod{14}$;
6) $24x \equiv 3 \pmod{13}$;
7) $11x \equiv -32 \pmod{27}$;
8) $32x \equiv 5 \pmod{19}$;
9) $16x \equiv 50 \pmod{23}$;
10) $24x \equiv 3 \pmod{11}$;
11) $25x \equiv 1 \pmod{37}$;
12) $5x \equiv 8 \pmod{6}$;
13) $17x \equiv 23 \pmod{41}$;
14) $41x \equiv 32 \pmod{17}$;
15) $32x \equiv 43 \pmod{51}$;
16) $54x \equiv 32 \pmod{15}$;
17) $27x \equiv 38 \pmod{17}$;
18) $45x \equiv 23 \pmod{13}$;

19) $-7x \equiv 5 (\mod 3)$;
20) $-4x \equiv 7 (\mod 11)$;
21) $23x \equiv 8 (\mod 11)$;
22) $52x \equiv 31 (\mod 13)$;
23) $29x \equiv 13 (\mod 19)$;
24) $15x \equiv 64 (\mod 9)$.
25) $39x \equiv 25 (\mod 13)$.

Берилген салыштырууларды тандоо усулу менен чыгаргыла [26-50]:

26) $4x \equiv 7 (\mod 3)$;
27) $5x \equiv 13 (\mod 7)$;
28) $13x \equiv 11 (\mod 4)$;
29) $12x \equiv 7 (\mod 2)$;
30) $-8x \equiv 10 (\mod 6)$;
31) $24x \equiv 3 (\mod 5)$;
32) $11x \equiv -32 (\mod 7)$;
33) $32x \equiv 5 (\mod 9)$;
34) $16x \equiv 50 (\mod 3)$;
35) $45x \equiv 3 (\mod 11)$;
36) $25x \equiv 1 (\mod 6)$;
37) $5x \equiv 18 (\mod 6)$;
38) $17x \equiv 23 (\mod 9)$;
39) $4x \equiv 32 (\mod 13)$;
41) $3x \equiv -4 (\mod 5)$;
42) $5x \equiv 3 (\mod 13)$;
43) $3x \equiv 7 (\mod 5)$;
44) $4x \equiv 23 (\mod 13)$;
44) $23x \equiv 5 (\mod 3)$;
45) $14x \equiv 5 (\mod 11)$;
46) $22x \equiv -3 (\mod 7)$;
47) $35x \equiv 13 (\mod 7)$;
48) $24x \equiv 17 (\mod 5)$;
49) $34x \equiv 7 (\mod 9)$;
50) $14x \equiv 5 (\mod 7)$.

Берилген салыштырууларды Эйлердин теоремасынын жардамында чыгаргыла [51-75]:

51) $10x \equiv 3 (\mod 7)$;
52) $2x \equiv 5 (\mod 9)$;
53) $13x \equiv 5 (\mod 17)$;
54) $8x \equiv 15 (\mod 19)$;
55) $4x \equiv 23 (\mod 9)$;
56) $34x \equiv 15 (\mod 29)$;
57) $14x \equiv 24 (\mod 16)$;
58) $45x \equiv 32 (\mod 29)$;
59) $21x \equiv -32 (\mod 7)$;
60) $22x \equiv 5 (\mod 19)$;
61) $3x \equiv 12 (\mod 7)$;
62) $24x \equiv 15 (\mod 9)$;
63) $33x \equiv 7 (\mod 8)$;
64) $41x \equiv 25 (\mod 19)$;
65) $26x \equiv 32 (\mod 15)$;
66) $27x \equiv 25 (\mod 29)$;

67) $11x \equiv 2(\mod 24)$;
68) $56x \equiv 11(\mod 19)$;
69) $52x \equiv 22(\mod 18)$;
70) $58x \equiv 3(\mod 15)$;
71) $16x \equiv 50(\mod 13)$;
72) $45x \equiv 3(\mod 31)$;
73) $25x \equiv 1(\mod 16)$;
74) $5x \equiv 18(\mod 26)$;
75) $17x \equiv 23(\mod 19)$.

Берилген салыштырууларды чектүү чынжырлуу бөлчөктөрдүн жардамында чыгаргыла [76-100]:

76) $47x \equiv 8(\mod 133)$;
77) $74x \equiv 3(\mod 156)$;
78) $56x \equiv 11(\mod 144)$;
79) $62x \equiv 7(\mod 421)$;
80) $38x \equiv 10(\mod 149)$;
81) $24x \equiv 3(\mod 153)$;
82) $121x \equiv 32(\mod 247)$;
83) $32x \equiv 5(\mod 219)$;
84) $46x \equiv 50(\mod 273)$;
85) $24x \equiv 3(\mod 101)$;
86) $25x \equiv 1(\mod 367)$;
87) $15x \equiv 8(\mod 756)$;
88) $117x \equiv 23(\mod 451)$;
89) $41x \equiv 32(\mod 717)$;
90) $32x \equiv 43(\mod 501)$;
91) $54x \equiv 32(\mod 185)$;
92) $247x \equiv 38(\mod 817)$;
93) $45x \equiv 23(\mod 193)$;
94) $37x \equiv 5(\mod 243)$;
95) $4x \equiv 7(\mod 111)$;
96) $13x \equiv 32(\mod 19)$;
97) $24x \equiv 15(\mod 69)$;
98) $13x \equiv 7(\mod 58)$;
99) $43x \equiv 25(\mod 119)$;
100) $26x \equiv 32(\mod 115)$.

Берилген $ax \equiv b(\mod m)$ салыштырууну aга тескери класс аркылуу чыгаргыла [101-125]:

101) $57x \equiv 8(\mod 33)$;
102) $14x \equiv 3(\mod 56)$;
103) $67x \equiv 11(\mod 44)$;
104) $42x \equiv 7(\mod 21)$;
105) $28x \equiv 10(\mod 49)$;
106) $14x \equiv 3(\mod 53)$;
107) $21x \equiv 32(\mod 47)$;
108) $32x \equiv 5(\mod 19)$;
109) $86x \equiv 50(\mod 73)$;
110) $54x \equiv 3(\mod 81)$;
111) $35x \equiv 1(\mod 67)$;
112) $35x \equiv 8(\mod 56)$;
113) $17x \equiv 23(\mod 51)$;
114) $61x \equiv 32(\mod 17)$;
115) $2x \equiv 43(\mod 51)$;
116) $84x \equiv 32(\mod 85)$;

117) $47x \equiv 38(\text{ mod } 17)$;
118) $35x \equiv 23(\text{ mod } 93)$;
119) $37x \equiv 5(\text{ mod } 43)$;
120) $42x \equiv 7(\text{ mod } 11)$;
121) $7x \equiv 138(\text{ mod } 27)$;
122) $5x \equiv 23(\text{ mod } 13)$;
123) $12x \equiv 17(\text{ mod } 19)$;
124) $15x \equiv 23(\text{ mod } 33)$;
125) $14x \equiv 35(\text{ mod } 18)$.

§ 5. Биринчи даражадагы салыштыруулардын системасы

Ар түрдүү модулга ээ болгон бир өзгөрүлмөлүү салыштыруулардын системасынын жалпы көрүнүшү төмөнкүдөй болот:

$$\begin{cases} a_1 x \equiv b_1 (\mathrm{mod}\ m_1), \\ a_2 x \equiv b_2 (\mathrm{mod}\ m_2), \\ \ldots \\ a_n x \equiv b_n (\mathrm{mod}\ m_n). \end{cases}$$

Системанын чечимин табуу үчүн алгач системанын биринчи салыштыруусунун $x \equiv \alpha (\mathrm{mod}\ m)$ чечими табылат, мында α аркылуу m_1 модулу боюнча чегериштердин терс эмес эң кичинесин же абсолюттук чоңдугу боюнча эң кичинесин алабыз. Ошентип биз системанын 1-салыштыруусун канааттандырган $x = m_1 t + \alpha$ сандардын классын алабыз. Бул $x = m_1 t + \alpha$ маанини системанын 2-салыштыруусуна коюп төмөнкүнү алабыз:

$$a_2(m_1 t + \alpha) \equiv b_2 (\mathrm{mod}\ m_2).$$

Ушул салыштыруунун чечимин табабыз, б.а. салыштырууну канааттандырган t сандардын классын табабыз. Табылган $t = m_2 t_1 + \beta$ сандардын классын системанын 3-салыштыруусуна коебуз ж.б.у.с. Бул процессти улантып, аягында бул системадагы бардык салышыштырууларды канааттандырган сандардын классын алабыз.

Мисал 1. $\begin{cases} 3x \equiv 1 (\mathrm{mod}\ 5), \\ 5x \equiv 4 (\mathrm{mod}\ 7), \end{cases}$ системанын чечимин тапкыла.

Чыгаруу. Системанын 1-салыштыруусун чыгарабыз:

$3x \equiv 1 (\mathrm{mod}\ 5) \Rightarrow x \equiv 2 (\mathrm{mod}\ 5) \vee x = 2 + 5t$. x тын табылган маанисин системанын 2-салыштыруусуна коебуз жана аны чыгарыбыз:

$5(2+5t) \equiv 4 (\mathrm{mod}\ 7) \Rightarrow 10 + 25t \equiv 4 (\mathrm{mod}\ 7) \Rightarrow 25t \equiv 6 (\mathrm{mod}\ 7) \Rightarrow$

$4t \equiv 1 (\mathrm{mod}\ 7) \Rightarrow t \equiv 2 (\mathrm{mod}\ 7) \Rightarrow t = 2 + 7t_1$.

Демек, $x = 2 + 5(2 + 7t_1) = 12 + 35t_1$, $t \in Z$.

Эгерде системанын жок дегенде бир салыштыруусу чечимге ээ болбосо, анда система чечимге ээ болбойт.

Мисал 2. $\begin{cases} 3x \equiv 1 (\mathrm{mod}\ 20), \\ 2x \equiv 3 (\mathrm{mod}\ 15), \end{cases}$ системанын чечимин тапкыла.

Чыгаруу. Системанын 1-салыштыруусун чыгарабыз:
$3x \equiv 1 (\mathrm{mod}\ 20) \Rightarrow x \equiv 7 (\mathrm{mod}\ 20) \vee x = 7 + 20t$. x тын табылган маанисин системанын 2-салыштыруусуна коебуз жана аны чыгарыбыз:
$2(7+20t) \equiv 3 (\mathrm{mod}\ 15) \Rightarrow 40t \equiv 4 (\mathrm{mod}\ 15)$, $(40, 15) = 5$ жана 4 саны 5ке бөлүнбөгөнү үчүн бул салыштыруу чечимге ээ эмес. Демек, берилген система да чечимге ээ болбойт.

Эгерде

$$\begin{cases} x \equiv \alpha_1 (\mathrm{mod}\ m_1), \\ x \equiv \alpha_2 (\mathrm{mod}\ m_2), \\ \ldots \\ x \equiv \alpha_n (\mathrm{mod}\ m_n), \end{cases}$$

системасында $m_1, m_2, \ldots, m_n$ модулдары жуп-жубу менен жөнөкөй болушса, анда анын чечимин

$$x_0 = \frac{M}{m_1} y_1 \alpha_1 + \frac{M}{m_2} y_2 \alpha_2 + \ldots + \frac{M}{m_n} y_n \alpha_n$$

формуласынын жардамында табууга болот, мында $M = [m_1, m_2, \ldots, m_n]$, y_i лер $\frac{M}{m_i} y_i \equiv 1 (\mathrm{mod}\ m_i)$ салыштыруусунун чечимдери, $i = 1, 2, \ldots$.

Системанын чечими $x \equiv x_0 (\mathrm{mod}\ M)$ болот.

Мисал 3. Төмөнкү системаны чыгаргыла:

$$\begin{cases} x \equiv b_1 (\mathrm{mod}\, 4), \\ x \equiv b_2 (\mathrm{mod}\, 5), \\ x \equiv b_3 (\mathrm{mod}\, 7). \end{cases}$$

Чыгаруу. $4 \cdot 5 \cdot 7 = 35 \cdot 4 = 28 \cdot 5 = 20 \cdot 7$ жана $35 \cdot 3 \equiv 1 (\mathrm{mod}\ 4)$, $28 \cdot 2 \equiv 1 (\mathrm{mod}\ 5)$, $20 \cdot 6 \equiv 1 (\mathrm{mod}\ 7)$ болгондуктан,

$$x_0 = 35\cdot 3b_1 + 28\cdot 2b_2 + 20\cdot 6b_3 = 105b_1 + 56b_2 + 120b_3$$

жана системаны канааттандырган x тин маанилери

$$x = 105b_1 + 56b_2 + 120b_3 (\mathrm{mod}\ 140)$$ болот.

Мисал үчүн

$$\begin{cases} x \equiv 1 \pmod 4, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7, \end{cases}$$

болгондо $x \equiv 105\cdot 1 + 56\cdot 3 + 120\cdot 2 \equiv 93 (\mathrm{mod}\ 140)$ болгондуктан,

$$\begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 2 \pmod 5, \\ x \equiv 6 \pmod 7, \end{cases}$$

болот жана системаны канааттандырган x тин маанилери

$$x \equiv 105\cdot 3 + 56\cdot 2 + 120\cdot 6 \equiv 27 (\mathrm{mod}\ 140)$$ болот.

Өз алдынча иштөө үчүн көнүгүүлөр

Салыштыруулардын системасын чыгаргыла [1-25]:

1) $\begin{cases} 3x \equiv 5 (\mathrm{mod}\ 7), \\ 2x \equiv 1 (\mathrm{mod}\ 5), \\ 4x \equiv 7 (\mathrm{mod}\ 11); \end{cases}$ 2) $\begin{cases} 2x \equiv 15 (\mathrm{mod} 17), \\ 2x \equiv 11 (\mathrm{mod} 5), \\ 14x \equiv 7 (\mathrm{mod} 21); \end{cases}$ 3) $\begin{cases} 5x \equiv 9 (\mathrm{mod} 17), \\ 21x \equiv 4 (\mathrm{mod} 15), \\ 4x \equiv 7 (\mathrm{mod} 9); \end{cases}$

4) $\begin{cases} 13x \equiv 5 (\mathrm{mod} 27), \\ 22x \equiv 31 (\mathrm{mod} 5), \\ 14x \equiv 27 (\mathrm{mod} 11); \end{cases}$ 5) $\begin{cases} 11x \equiv 5 (\mathrm{mod} 17), \\ 21x \equiv 11 (\mathrm{mod} 15), \\ 34x \equiv 27 (\mathrm{mod} 21); \end{cases}$ 6) $\begin{cases} 6x \equiv 19 (\mathrm{mod} 17), \\ 3x \equiv 54 (\mathrm{mod} 15), \\ 41x \equiv 7 (\mathrm{mod} 29); \end{cases}$

7) $\begin{cases} -3x \equiv 5 (\mathrm{mod} 37), \\ 12x \equiv 31 (\mathrm{mod} 25), \\ 14x \equiv 37 (\mathrm{mod} 9); \end{cases}$ 8) $\begin{cases} 7x \equiv 4 (\mathrm{mod} 7), \\ 9x \equiv 27 (\mathrm{mod} 15), \\ 4x \equiv 37 (\mathrm{mod} 21); \end{cases}$ 9) $\begin{cases} 43x \equiv 9 (\mathrm{mod} 17), \\ 23x \equiv 4 (\mathrm{mod} 15), \\ 26x \equiv 7 (\mathrm{mod} 9); \end{cases}$

10) $\begin{cases} 7x \equiv 5 (\mathrm{mod} 13), \\ 22x \equiv 11 (\mathrm{mod} 5), \\ 34x \equiv 57 (\mathrm{mod} 31); \end{cases}$ 11) $\begin{cases} 43x \equiv 15 (\mathrm{mod} 57), \\ 52x \equiv 11 (\mathrm{mod} 35), \\ 8x \equiv 47 (\mathrm{mod} 21); \end{cases}$ 12) $\begin{cases} 33x \equiv 19 (\mathrm{mod} 17), \\ 21x \equiv 34 (\mathrm{mod} 15), \\ 24x \equiv 27 (\mathrm{mod} 9); \end{cases}$

13) $\begin{cases} 7x \equiv 85 (\mathrm{mod}\, 37), \\ 23x \equiv 11 (\mathrm{mod}\, 25), \\ 24x \equiv 47 (\mathrm{mod}\, 11); \end{cases}$ 14) $\begin{cases} 45x \equiv 49 (\mathrm{mod}\, 17), \\ 52x \equiv 35 (\mathrm{mod}\, 25), \\ 8x \equiv 72 (\mathrm{mod}\, 23); \end{cases}$ 15) $\begin{cases} 32x \equiv 9 (\mathrm{mod}\, 17), \\ 18x \equiv 24 (\mathrm{mod}\, 15), \\ 29x \equiv 37 (\mathrm{mod}\, 9); \end{cases}$

16) $\begin{cases} x \equiv 35 (\mathrm{mod}\, 27), \\ -2x \equiv 21 (\mathrm{mod}\, 5), \\ 4x \equiv -7 (\mathrm{mod}\, 15); \end{cases}$ 17) $\begin{cases} 5x \equiv -4 (\mathrm{mod}\, 17), \\ -12x \equiv 11 (\mathrm{mod}\, 15), \\ 14x \equiv 7 (\mathrm{mod}\, 21); \end{cases}$ 18) $\begin{cases} 32x \equiv 69 (\mathrm{mod}\, 17), \\ 26x \equiv 24 (\mathrm{mod}\, 15), \\ 15x \equiv 17 (\mathrm{mod}\, 9); \end{cases}$

19) $\begin{cases} 14x \equiv 5 (\mathrm{mod}\, 7), \\ -11x \equiv -3 (\mathrm{mod}\, 15), \\ 35x \equiv -7 (\mathrm{mod}\, 11); \end{cases}$ 20) $\begin{cases} 36x \equiv 75 (\mathrm{mod}\, 17), \\ 42x \equiv 101 (\mathrm{mod}\, 5), \\ 19x \equiv 47 (\mathrm{mod}\, 21); \end{cases}$ 21) $\begin{cases} 27x \equiv 4 (\mathrm{mod}\, 17), \\ 9x \equiv 2 (\mathrm{mod}\, 15), \\ 4x \equiv 7 (\mathrm{mod}\, 11); \end{cases}$

22) $\begin{cases} 3x \equiv -5 (\mathrm{mod}\, 7), \\ 2x \equiv 3 (\mathrm{mod}\, 5), \\ 4x \equiv 7 (\mathrm{mod}\, 19); \end{cases}$ 23) $\begin{cases} 17x \equiv 4 (\mathrm{mod}\, 27), \\ 3x \equiv 27 (\mathrm{mod}\, 15), \\ 14x \equiv 37 (\mathrm{mod}\, 21); \end{cases}$ 24) $\begin{cases} 33x \equiv 9 (\mathrm{mod}\, 17), \\ 3x \equiv 14 (\mathrm{mod}\, 15), \\ 6x \equiv 17 (\mathrm{mod}\, 9); \end{cases}$

25) $\begin{cases} -3x \equiv 5 (\mathrm{mod}\, 37), \\ 12x \equiv 31 (\mathrm{mod}\, 25), \\ 14x \equiv 37 (\mathrm{mod}\, 9); \end{cases}$

Салыштыруулардын системасын чыгаргыла [26-50]:

26) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 7), \\ x \equiv 1 (\mathrm{mod}\, 5), \\ x \equiv 7 (\mathrm{mod}\, 11); \end{cases}$ 27) $\begin{cases} x \equiv 15 (\mathrm{mod}\, 17), \\ x \equiv 11 (\mathrm{mod}\, 5), \\ x \equiv 7 (\mathrm{mod}\, 21); \end{cases}$ 28) $\begin{cases} x \equiv 9 (\mathrm{mod}\, 17), \\ x \equiv 4 (\mathrm{mod}\, 15), \\ x \equiv 7 (\mathrm{mod}\, 9); \end{cases}$

29) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 27), \\ x \equiv 31 (\mathrm{mod}\, 5), \\ x \equiv 27 (\mathrm{mod}\, 11); \end{cases}$ 30) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 17), \\ x \equiv 11 (\mathrm{mod}\, 15), \\ x \equiv 27 (\mathrm{mod}\, 21); \end{cases}$ 31) $\begin{cases} x \equiv 19 (\mathrm{mod}\, 17), \\ x \equiv 54 (\mathrm{mod}\, 15), \\ x \equiv 7 (\mathrm{mod}\, 29); \end{cases}$

32) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 37), \\ x \equiv 31 (\mathrm{mod}\, 25), \\ x \equiv 37 (\mathrm{mod}\, 9); \end{cases}$ 33) $\begin{cases} x \equiv 4 (\mathrm{mod}\, 7), \\ x \equiv 27 (\mathrm{mod}\, 15), \\ x \equiv 37 (\mathrm{mod}\, 21); \end{cases}$ 34) $\begin{cases} x \equiv 9 (\mathrm{mod}\, 17), \\ x \equiv 4 (\mathrm{mod}\, 15), \\ x \equiv 7 (\mathrm{mod}\, 9); \end{cases}$

35) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 13), \\ x \equiv 11 (\mathrm{mod}\, 5), \\ x \equiv 57 (\mathrm{mod}\, 31); \end{cases}$ 36) $\begin{cases} x \equiv 15 (\mathrm{mod}\, 57), \\ x \equiv 11 (\mathrm{mod}\, 35), \\ x \equiv 47 (\mathrm{mod}\, 21); \end{cases}$ 37) $\begin{cases} x \equiv 19 (\mathrm{mod}\, 17), \\ x \equiv 34 (\mathrm{mod}\, 15), \\ x \equiv 27 (\mathrm{mod}\, 9); \end{cases}$

38) $\begin{cases} x \equiv 85 (\mathrm{mod}\, 37), \\ x \equiv 11 (\mathrm{mod}\, 25), \\ x \equiv 47 (\mathrm{mod}\, 11); \end{cases}$

39) $\begin{cases} x \equiv 49 (\mathrm{mod}\, 17), \\ x \equiv 35 (\mathrm{mod}\, 25), \\ x \equiv 72 (\mathrm{mod}\, 23); \end{cases}$

40) $\begin{cases} x \equiv 9 (\mathrm{mod}\, 17), \\ x \equiv 24 (\mathrm{mod}\, 15), \\ x \equiv 37 (\mathrm{mod}\, 9); \end{cases}$

41) $\begin{cases} x \equiv 35 (\mathrm{mod}\, 27), \\ x \equiv 21 (\mathrm{mod}\, 5), \\ x \equiv -7 (\mathrm{mod}\, 15); \end{cases}$

42) $\begin{cases} x \equiv -4 (\mathrm{mod}\, 17), \\ x \equiv 11 (\mathrm{mod}\, 15), \\ x \equiv 7 (\mathrm{mod}\, 21); \end{cases}$

43) $\begin{cases} x \equiv 69 (\mathrm{mod}\, 17), \\ x \equiv 24 (\mathrm{mod}\, 15), \\ x \equiv 17 (\mathrm{mod}\, 9); \end{cases}$

44) $\begin{cases} x \equiv 15 (\mathrm{mod}\, 27), \\ x \equiv 2 (\mathrm{mod}\, 5), \\ x \equiv -7 (\mathrm{mod}\, 13); \end{cases}$

45) $\begin{cases} x \equiv 4 (\mathrm{mod}\, 7), \\ x \equiv 5 (\mathrm{mod}\, 13), \\ x \equiv -7 (\mathrm{mod}\, 21); \end{cases}$

46) $\begin{cases} x \equiv 9 (\mathrm{mod}\, 17), \\ x \equiv 4 (\mathrm{mod}\, 15), \\ x \equiv 7 (\mathrm{mod}\, 9); \end{cases}$

47) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 7), \\ x \equiv -3 (\mathrm{mod}\, 15), \\ x \equiv -7 (\mathrm{mod}\, 11); \end{cases}$

48) $\begin{cases} x \equiv 75 (\mathrm{mod}\, 17), \\ x \equiv 101 (\mathrm{mod}\, 5), \\ x \equiv 47 (\mathrm{mod}\, 21); \end{cases}$

49) $\begin{cases} x \equiv 29 (\mathrm{mod}\, 17), \\ x \equiv 14 (\mathrm{mod}\, 15), \\ x \equiv 17 (\mathrm{mod}\, 9); \end{cases}$

50) $\begin{cases} x \equiv 11 (\mathrm{mod}\, 17), \\ x \equiv 6 (\mathrm{mod}\, 15), \\ x \equiv 8 (\mathrm{mod}\, 9). \end{cases}$

§6. Жогорку даражадагы салыштыруулар

1. Модулу так сан болгон жогорку даражадагы салыштыруулар

Эгерде салыштыруунун модулу курама сан болсо, анда аны ар дайым жөнөкөй санга айландырууга болот. Ошондуктан биз алгач модулу жөнөкөй сан болгон салыштырууларды карайбыз. Коэффициенттери бүтүн сандар болгон

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,$$

көп мүчөнү алабыз.

Def 1. Эгерде a_0 саны p га бөлүнбөсө жана x белгисиз сан үчүн $f(x)\equiv 0(\mathrm{mod}\ p)$ салыштыруусу орун алса, анда бул салыштыруу n-даражадагы бир белгисиздүү салыштыруу деп аталат.

Def 2. Эгерде $f(x)\equiv 0(\mathrm{mod}\ p)$ салыштыруусунун бардык коэффициенттери p га бөлүнсө, анда ал салыштыруу даражага ээ эмес деп аталат. Себеби $\forall k\in Z$ саны салыштыруунун чечими болот.

Мисалы, $28x^2+7x+14\equiv(\mathrm{mod}\ 7)$ салыштыруусу даражага ээ эмес, себеби 28, 7, 14 коэффициенттеринин бардыгы 7ге бөлүнөт.

Жогорку даражадагы салыштырууларды чечүүдөн мурда алардын үстүнөн элеметардык өзгөртүп түзүлөрдү аткаруу (жөнөкөйлөтүп алуу) мүмкүн. Алгач бардык a_i (i=0,1,…,n) коэффициенттерин p модулу боюнча абсолюттук эң кичине δ чегериши менен алмаштырып алуу абзел.

Мисалы, $25x^3+17x^2-13\equiv 0(\mathrm{mod}\ 11)$ салыштыруусунда $25\equiv 3(\mathrm{mod}\ 11)$, $17\equiv -5(\mathrm{mod}\ 11)$, $13\equiv 2(\mathrm{mod}\ 11)$ болгондуктан, аны $3x^3-5x^2-2\equiv 0(\mathrm{mod}\ 11)$ көрүнүшүндө жазууга болот. $(a_0, p)=1$ болгондуктан, $a_0y\equiv 1(\mathrm{mod}\ p)$ салыштыруусу ар дайым жалгыз чечимге ээ болот. $a_0y\equiv 1(\mathrm{mod}\ p)$ салыштыруусунун чечимин $f(x)\equiv 0(\mathrm{mod}\ p)$

салыштыруусунун эки жагына көбөйтөбүз, ошондо x^nдин коэффициенттинин ордуна 1 ди койсок болот. Чындыгында жогорудагы мисалыбызда, $3x^3-5x^2-2\equiv 0 \pmod{11}$ салыштыруусунда, $3y\equiv 1 \pmod{11}$ салыштыруусу жалгыз $y\equiv 4 \pmod{11}$ чечимге ээ болот. $3x^3-5x^2-2\equiv 0 \pmod{11}$ салыштыруусунун эки жагын $y\equiv 4 \pmod{11}$ салыштыруусуна көбөйтөбүз, натыйжада $x^3+2x^2+3\equiv 0 \pmod{11}$ салыштырууга ээ болобуз.

Def 3. Чечимдеринин көптүгү дал келген салыштыруулар тең күчтүү салыштыруулар деп аталат.

Теорема 1. Даражасы $n>p$, модулу p жөнөкөй сан болгон салыштыруу ар дайым даражасы $p-1$ ден чоң болбогон салыштырууга тең күчтүү болот.

Далилдөө. Калдыктуу бөлүү жөнүндөгү теореманын негизинде $n\in N, p-1\in N$ үчүн төмөнкү барабардык орун алат:

$$n=(p-1)k+r,\ 1\le r<p-1.$$

Бул жерде биз калдыкты 0 дон $p-2$ ге чейин эмес, 1 ден $p-1$ ге чейин алдык. Себеби $p-1$ модулу боюнча чегериштердин толук системасы үчүн $\{0, 1,\ldots, p-2\}$ системасынын ордуна $\{1,\ldots, p-1\}$ толук системасын алууга болот ($p-1\equiv 0 \pmod{p-1}$). Ферманын теоремасы боюнча $x\equiv x^p \pmod{p}$ салыштыруусу каалаган x тер үчүн орун алат. Бул салыштыруунун эки жагын тең удаалаш x^{r-1}, $x^{(p-1)+r-1}$, $x^{2(p-1)+r-1}$,..., $x^{(k-1)(p-1)+r-1}$ лерге көбөйтүп, төмөнкүлөргө ээ болобуз:

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

Эгерде бул салыштырууларды мүчөлөп көбөйтсөк төмөндөгүнү алабыз:

$$x^r \equiv x^{k(p-1)+r} \pmod{p},\ 1\le r\le p-1.$$

Бирок $n=k(p-1)+r$ болгондуктан, $x^n \equiv x^r \pmod p$, $1 \le r \le p-1$ келип чыгат.

Мисал. $x^{19}+3x^{17}-3x^{11}-3x^5+3x^2+1 \equiv 0 \pmod 7$ салыштыруунун даражасын төмөндөткүлө.

Чыгаруу. 7–1=6 жана 19=18+1, 17=12+5, 11=6+5 болгондуктан, берилген салыштырууну $x+3x^5-3x^5-3x^5+3x^2+1 \equiv 0 \pmod 7$ же $3x^5-3x^2-x-1 \equiv 0 \pmod 7$ көрүнүшүндө жазууга болот.

Теорема 2. *n*-даражадагы модулу жөнөкөй сан болгон салыштыруунун чечимдеринин саны *n* ден ашып кетпейт.

Далилдөө. Айталы $f(x) \equiv 0 \pmod p$ салыштыруусу берилген болуп, $x \equiv x_1 \pmod p$ анын чечими болсун, б.а. $f(x_1) \equiv 0 \pmod p$ салыштыруусу чын болсун. Анда Безунун теоремасынын негизинде $f(x)=(x-x_1)f_1(x)+f(x_1)$ болот, мында $f_1(x)$ – даражасы $n-1$ ден чоң болбогон көп мүчө, $f(x_1)$ болсо p га калдыксыз бөлүнө турган сан. Эгерде $f(x_1) \equiv 0 \pmod p$ экендигин эске алсак, анда $f(x) \equiv 0 \pmod p$ салыштыруусун $f(x) \equiv (x-x_1)\, f_1(x) \pmod p$ көрүнүшүндө жаза алабыз. Мындан $(x-x_1)\, f_1(x) \equiv 0 \pmod p$ келип чыгат. Эгерде $f_1(x) \equiv 0 \pmod p$ салыштыруусу кандайдыр бир $x \equiv x_2 \pmod p$ чечимине ээ болсо, x тин бардык маанилеринде теңдеш аткарылуучу $f_1(x) \equiv (x-x_2)\, f_2(x) \pmod p$ салыштырууга ээ болобуз. Жогоруда айтылгандарды $f_2(x)$ге карата колдонууга болот. Бул процессти улантып, төмөнкү эки ырастоонун бири ар дайым аткарыла тургандыгына ынанабыз.

1) k кадамдан кейин чечимге ээ болбогон $(n-k)$- даражалуу $f_k(x) \equiv 0 \pmod p$ салыштырууга ээ болобуз;

2) Биринчи даражалуу $(x-x_1)a_0 \equiv 0 \pmod p$ салыштырууга ээ болобуз.

1- учурда $f(x) \equiv 0 \pmod p$ салыштыруусун төмөнкүдөй көрүнүшкө алып келебиз:

$$f(x) \equiv (x-x_1)\,(x-x_2)\,\ldots(x-x_k)f_k(x) \pmod p,$$

ал эми 2- учурда болсо $f(x) \equiv 0 \pmod p$ салыштыруусун

$$f(x) \equiv a_0(x-x_1)(x-x_2)\,\ldots(x-x_n) \pmod p$$

көрүнүшкө алып келебиз.

1- учурда $f(x)\equiv 0(\mathrm{mod}\ p)$ салыштыруу $x_1, x_2,\ldots, x_k$ лардан башка чечимге ээ болбойт. Чындыгында, эгерде $x\equiv x_{k+1}(\mathrm{mod}\ p)$ чечими жашап, $x_{k+1}\equiv x_1(\mathrm{mod}\ p)$, $x_{k+1}\equiv x_2(\mathrm{mod}\ p)$, ..., $x_{k+1}\equiv x_k(\mathrm{mod}\ p)$ орун албаса, анда $f_k(x_{k+1})\equiv 0(\mathrm{mod}\ p)$ салыштыруусу аткарылат эле. Бул болсо $f_k(x)\equiv 0(\mathrm{mod}\ p)$ салыштыруусун чечимге ээ эмес дегенге карама-каршы. Теорема далилденди.

Теорема 3. Эгерде модулу p жөнөкөй сан болгон n-даражадагы салыштыруунун чечимдеринин саны n ден ашык болсо, анда салыштыруунун бардык коэффициенттери p га бөлүнөт.

Далилдөө. Айталы

$f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n\equiv 0(\mathrm{mod}\ p)$

салыштыруусу берилген болуп, анын ар түрдүү чечимдери α_1, α_2, α_3,... α_n,... α_m болсун. Берилген салыштырууну төмөнкүдөй жазып алабыз:

$$a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)\ldots(x-\alpha_m)\equiv 0(\mathrm{mod}\ p).$$

xтин ордуна удаалаш α_{n+1}, α_{n+2}, $\alpha_{n+1},\ldots$, α_m дерди коебуз:

$$a_0(\alpha_{n+1}-\alpha_1)(\alpha_{n+1}-\alpha_2)\ldots(\alpha_{n+1}-\alpha_n)\ldots(\alpha_{n+1}-\alpha_m)\equiv 0(\mathrm{mod}\ p).$$

бирок $\alpha_{n+1}-\alpha_i\equiv 0(\mathrm{mod}\ p)$, $i=1,\ldots,n$ аткарылбайт. Ошондуктан $a_0\equiv 0(\mathrm{mod}\ p)$ келип чыгат. Муну эске алып, берилген салыштырууну төмөнкүдөй жазып алабыз:

$$a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n\equiv 0(\mathrm{mod}\ p).$$

Бул салыштыруунун чечимдеринин саны $n-1$ден ашык болуп, алар $\beta_1, \beta_2, \ldots, \beta_{n-1}, \beta_n,\ldots, \beta_k$ болсун. Жогорудагыга окшоштуруп

$$a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n\equiv 0(\mathrm{mod}\ p)$$

салыштыруусун төмөнкүдөй жазып алууга болот:

$$a_1(x-\beta_1)(x-\beta_2)\ldots(x-\beta_k)\equiv 0(\mathrm{mod}\ p),$$

бул жерде дагы $\beta_n-\beta_i\equiv 0(\mathrm{mod}\ p)$, $i=1,\ldots,n-1$ аткарылбай тургандыгын эске алып, $a_1\equiv 0(\mathrm{mod}\ p)$ деген тыянак келебиз.

Ошентип, биз модулу жөнөкөй сан болгон салыштыруунун чечимдеринин саны анын даражасынан чоң болгондо a_0

жана a_1 коэффициенттеринин p модулга бөлүнүшүн далилдедик. Ушул усул менен ой жүгүртүп $f(x)$тин бардык коэффициенттерин p га бөлүнүшүн далилдөөгө болот. Теорема далилденди.

Эскертүү. Модулу курама сан болгондо бул теорема орун албайт. Мисалы, $x^2-5x+6\equiv 0 \pmod 6$ салыштыруусу төрт чечимге ээ $x\equiv 0 \pmod 6$, $x\equiv 2 \pmod 6$, $x\equiv 3 \pmod 6$, $x\equiv 5 \pmod 6$.

Теорема 4. x^n дин коэффициенти $a_0=1$ болгондо $n<p$ даражадагы $f(x)\equiv 0 \pmod p$ салыштыруусу n чечимге ээ болушу үчүн x^p-x ти $f(x)$ ге бөлүүдөн келип чыккан калдык көп мүчөнүн бардык коэффициенттери p га бөлүнүшү зарыл жана жетиштүүү.

Теорема 5. Эгерде $f(x)\equiv 0 \pmod m$ салыштыруусунун эки жагын $(k, m)=1$ шартын канаатандырган k бүтүн санына көбөйтсөк, келип чыккан салыштыруу $f(x)\equiv 0 \pmod m$ салыштыруусуна тең күчтүү болот.

Теорема 6. Эгерде $p>2$ – жөнөкөй сан болсо, анда $x^2\equiv 1 \pmod p$ салыштыруусунун чечимдери $x_1=1+pt_1$, $x_2=-1+pt_2$, $t_1, t_2\in Z$ болот.

Теорема 7. (Вильсондун теоремасы). Эгерде p жөнөкөй сан болсо, анда $(p-1)!\equiv -1 \pmod p$ болот.

Теорема 8. Эгерде p жөнөкөй сан болсо, анда $(p-2)!\equiv 1 \pmod p$ болот.

Теорема 9. Эгерде $(n-1)!\equiv -1 \pmod n$ болсо, анда n жөнөкөй сан болот.

2. Модулу курама сан болгон жогорку даражадагы салыштыруулар

Эгерде a_0 саны $m_1 \cdot m_2 \cdot \ldots \cdot m_n$ санына бөлүнбөсө жана $(m_i, m_j)=1$, $i \neq j$, $i, j=1,2,\ldots,n$, болсо, анда

$$f(x)=a_0x^n+\ldots+a_n \equiv 0 (\mathrm{mod}\ m_1 \cdot m_2 \cdot \ldots \cdot m_n), \tag{1}$$

салыштыруусу төмөнкү системага тең күчтүү болот:

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\ m_1), \\ f(x) \equiv 0 (\mathrm{mod}\ m_2), \\ \ldots \\ f(x) \equiv 0 (\mathrm{mod}\ m_n), \end{cases} \tag{2}$$

(1)-нин чечимдеринин саны (2) системадагы салыштыруулардын ар биринин чечимдеринин көбөйтүндүсүнө барабар болот. Ал эми

$$f(x) \equiv 0 \left(\mathrm{mod}\ p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}\right) \tag{3}$$

салыштыруусу

$$\begin{cases} f(x) \equiv 0 \left(\mathrm{mod}\ p_1^{\alpha_1}\right), \\ f(x) \equiv 0 \left(\mathrm{mod}\ p_2^{\alpha_2}\right), \\ \ldots \\ f(x) \equiv 0 \left(\mathrm{mod}\ p_n^{\alpha_n}\right), \end{cases} \tag{4}$$

системага тең күчтүү, мында α_i – терс эмес бүтүн сандар, p_i лер жөнөкөй сандар.

Системадагы $f(x) \equiv 0 \left(\mathrm{mod}\ p_1^{\alpha_1}\right)$ салыштыруусун чечүү $f(x) \equiv 0 (\mathrm{mod}\ p_1)$ салыштырууну чечүүдөн башталат. $f(x)=0 (\mathrm{mod}\ p_1)$ салыштыруусунун $x \equiv b_1 (\mathrm{mod}\ p)$ же $x=pt_1+b_1$ чечими табылат жана анын жардамында төмөнкүдөй салыштыруу түзүлөт:

$$\frac{f(b_1)}{p} + f'(b_1)t_1 \equiv 0 (\mathrm{mod}\ p).$$

Мындагы $f'(b_1) - f(x)$ тин 1-тартиптеги туундусунун $x=b_1$ деги мааниси. Бул салыштыруунун чечимин $t_1=pt_2+b_1$ деп алсак, анда $x=pt_1+b_1$ жана $t_1=pt_2+b_1$ ден $x=p^2t_2+b_2$ ны алабыз. Андан соң

$\frac{f(b_2)}{p^2} + f'(b_2)t_2 \equiv 0 (\mathrm{mod}\, p)$ салыштыруусу чечилет, анын чечими $x=p^3t_3+b_3$ болот, ж.б.у.с. Эсептөөнү $x=p^{\alpha}t_{\alpha}+b_{\alpha}$ ны алганга чейин улантабыз, мына ушул $x \equiv b_{\alpha} (\mathrm{mod}\, p^{\alpha})$ же $x=p^{\alpha}t_{\alpha}+b_{\alpha}$, $f(x) \equiv 0 \left(\mathrm{mod}\, p_1^{\alpha_1}\right)$ салыштыруусунун чечими болот.

Эгерде $f'(p_i)$ саны p га бөлүнсө, анда t_i чечими жашабайт, ошондуктан $x=pt_1+b_1$, туюнтмасы $f(x) \equiv 0 \left(\mathrm{mod}\, p_1^{\alpha_1}\right)$ салыштыруусунун чечими болбойт.

Эгерде (2) системада (ошондой эле (4)дө) жок дегенде бир салыштыруу чечимге ээ болбосо, анда система биргелешпеген болот. Ошондуктан (1) дагы (ошондой эле (3)дагы) чечимге ээ болбойт.

Өз алдынча иштөө үчүн көнүгүүлөр

Берилген салыштырууларды жөнөкөйлөткүлө:

1) $x^{233}+345x^{132}-567x^{109}+346x^{98}+45x^{56}-463x^{37}-24x^{15}+x^9+467 \equiv 0 (\mathrm{mod}\, 5)$;

2) $245x^{274}+345x^{123}-507x^{119}+346x^{98}+45x^{54}-463x^{27}-24x^{15}+x-67 \equiv 0 (\mathrm{mod}\, 7)$;

3) $x^{233}+345x^{132}-567x^{109}+346x^{98}+45x^{56}-463x^{37}-24x^{15}+x^9+467 \equiv 0 (\mathrm{mod}\, 13)$;

4) $245x^{274}+345x^{123}-507x^{119}+346x^{98}+45x^{54}-463x^{27}-24x^{15}-x+67 \equiv 0 (\mathrm{mod}\, 11)$;

5) $5^{435}+325x^{203}-57x^{100}+634x^{98}+45x^{52}-63x^{25}-24x^{15}+x+167 \equiv 0 (\mathrm{mod}\, 3)$;

6) $45x^{294}+545x^{223}-677x^{97}+334x^{90}-465x^{57}+43x^{28}-264x^{11}+244x+674 \equiv 0 (\mathrm{mod}\, 3)$;

7) $245x^{274}+345x^{123}-507x^{119}+346x^{98}+45x^{54}-463x^{27}-24x^{15}+x+67 \equiv 0 (\mathrm{mod}\, 5)$;

8) $245x^{274}+345x^{123}+507x^{119}+346x^{98}+45x^{54}-463x^{27}-24x^{15}+x+67 \equiv 0 (\mathrm{mod}\, 13)$;

9) $x^{233}+345x^{132}-567x^{109}+346x^{98}+45x^{56}-463x^{37}+24x^{15}+x^9+467 \equiv 0 (\mathrm{mod}\, 3)$;

10) $x^{233}+345x^{132}-567x^{109}+346x^{98}-45x^{56}-463x^{37}-24x^{15}+x^9+467 \equiv 0 (\mathrm{mod}\, 11)$;

11) $x^{233}+345x^{132}-567x^{109}-346x^{98}+45x^{56}-463x^{37}-24x^{15}+x^9+467 \equiv 0 (\mathrm{mod}\, 7)$;

12) $x^{233}+345x^{132}-567x^{109}+346x^{98}+45x^{56}-463x^{37}-24x^{15}+x^9+467 \equiv 0 (\mathrm{mod}\, 13)$;

13) $745x^{394}+545x^{223}-677x^{97}+334x^{90}-465x^{57}-43x^{28}-264x^{11}+244x-674 \equiv 0 (\mathrm{mod}\, 13)$;

14) $-45x^{294}+545x^{223}-677x^{97}+334x^{90}+465x^{57}-43x^{28}-264x^{11}-244x+674 \equiv 0 (\mathrm{mod}\, 5)$;

15) $453^{594}-545x^{223}-677x^{97}+334x^{90}+465x^{57}-43x^{28}-264x^{11}-244x-$

$-674 \equiv 0 \pmod 7$;

16) $-45x^{294}+545x^{223}+677x^{97}+334x^{90}+465x^{57}-43x^{28}-264x^{11}+244x-674 \equiv 0 \pmod{11}$;

17) $145x^{245}-55x^{123}-77x^{99}+34x^{95}-165x^{50}-473x^{23}-64x^{12}+44x^{9}-124 \equiv 0 \pmod 3$;

18) $345x^{245}+55x^{123}+77x^{99}+34x^{95}+165x^{50}-473x^{23}+64x^{12}-44x^{9}+124 \equiv 0 \pmod{13}$;

19) $-145x^{345}+55x^{123}-77x^{99}+34x^{95}-165x^{50}-473x^{23}-64x^{12}+44x^{9}-124 \equiv 0 \pmod 5$;

20) $245x^{445}+55x^{123}-77x^{99}+34x^{95}+165x^{50}-473x^{23}+64x^{12}+44x^{9}+124 \equiv 0 \pmod 7$;

21) $145x^{145}+76x^{103}-47x^{90}+32x^{65}+15x^{5}-43x^{2}+6x+24 \equiv 0 \pmod{17}$;

22) $761x^{345}+415x^{233}-247x^{100}+337x^{84}+195x^{74}-73x^{23}+64x^{12}+44x^{9}+194 \equiv 0 \pmod 5$;

23) $975x^{285}+735x^{214}-767x^{119}+394x^{105}+465x^{70}-173x^{63}+344x^{62}+124x^{91} \equiv 0 \pmod 7$;

24) $763x^{534}+732x^{323}-237x^{129}+354x^{125}+865x^{110}-473x^{93}+604x^{72}+234x^{11} \equiv 0 \pmod 5$;

25) $934x^{333}+143x^{203}-232x^{119}+549x^{94}+765x^{53}-73x^{26}+984x^{22}+49x^{11}+9 \equiv 0 \pmod 3$.

§7. Квадраттык чегериштер

Экинчи даражадагы салыштыруунун жалпы көрүнүшү,

$$Ax^2+Bx+C\equiv 0(\text{mod } M)$$

түрүндө болот, аны ар дайым $x^2\equiv d(\text{mod } m)$ көрүнүшкө алып келүүгө болот. Чындыгында

$$Ax^2+Bx+C\equiv 0(\text{mod } M)\Rightarrow 4A^2x^2+4ABx+4AC\equiv 0(\text{mod } 4MA)\Rightarrow$$
$$(2xA+B)^2-B^2+4AC\equiv 0(\text{mod } 4MA).$$

Эгерде $2Ax+B=y$, $B^2-4AC=d$, $4MA=m$ деп алсак, анда акыркы салыштыруу

$$y^2\equiv d(\text{mod } m)$$

көрүнүшүнө келет. $Ax^2+Bx+C\equiv 0(\text{mod } M)$ салыштыруусунун ар бир чечими $y^2\equiv d(\text{mod } m)$ салыштыруусунда да канааттандырат, бирок тескериси ар дайым орун ала бербейт.

Def 1. Эгерде $(a, m)=1$ болгондо $x^2\equiv a(\text{mod } m)$ салыштыруусу чечимге ээ болсо, анда a саны m модулу боюнча квадраттык чегериш деп аталат.

Def 2. Эгерде $(a, m)=1$ болгондо $x^2\equiv a(\text{mod } m)$ салыштыруусу чечимге ээ болбосо, анда a саны m модулу боюнча квадраттык чегериш эмес деп аталат.

Def 3. Эгерде $(a, m)=1$ болгондо $x^n\equiv a(\text{mod } m)$ салыштыруусу чечимге ээ болсо, анда a саны m модулу боюнча n-даражадагы чегериш деп аталат, а эгерде чечимге ээ болбосо, анда a саны m модулу боюнча n-даражадагы чегериш эмес деп аталат. $n=3$ төкубдук, $n=4$ төбиквадраттык деп аталат.

Эгерде m модулу курама сан болсо, анда $x^2\equiv a(\text{mod } m)$ салыштыруусу төмөнкү үч түрдүү салыштырууга келтирилет:

1) $x^2\equiv a(\text{mod } p)$, p – так жана жөнөкөй сан;
2) $x^2\equiv a(\text{mod } p^\alpha)$, $(\alpha>1)$;
3) $x^2\equiv a(\text{mod } 2^\alpha)$, $(\alpha\geq 1)$.

Эгерде a саны p модулу боюнча квадраттык чегериш болсо, анда $x^2 \equiv a \pmod p$ салыштыруусу ар дайым эки ар түрдүү чечимге ээ болот.

Мисал. 1) $4x^2-11x-3\equiv 0 \pmod{13}$ салыштыруунун чечими табылсын.

Чыгаруу. $11\equiv 24 \pmod{13}$, $3\equiv 16 \pmod{13}$ болгондуктан $4x^2-24x-16\equiv 0 \pmod{13}$, эгерде (4, 13)=1 экендигин эске алсак анда $x^2-6x-4\equiv 0 \pmod{13} \Rightarrow x^2-6x+9\equiv 0 \pmod{13} \Rightarrow$

$(x-3)^2\equiv 0 \pmod{13} \Rightarrow x\equiv 3 \pmod{13}$.

2) $3x^2-7x+8\equiv 0 \pmod{17}$ салыштыруунун чечимин тапкыла.

Чыгаруу. $3x^2-7x+8\equiv 0 \pmod{17} \Rightarrow 3x^2-24x-9\equiv 0 \pmod{17} \Rightarrow$

$x^2-8x-3\equiv 0 \pmod{17} \Rightarrow (x-4)^2-19\equiv 0 \pmod{17} \Rightarrow (x-4)^2\equiv 19 \pmod{17} \Rightarrow$

$(x-4)^2\equiv 2+34 \pmod{17} \Rightarrow x-4\equiv \pm 6 \pmod{17} \Rightarrow x-4\equiv 6 \pmod{17} \wedge$

$x-4\equiv -6 \pmod{17} \Rightarrow x_1\equiv 10 \pmod{17}$, $x_2\equiv -2 \pmod{17}$.

§8. Модулу так жана жөнөкөй сан болгон экинчи даражадагы салыштырууларды чечүү

Айталы, бизге эки мүчөлүү экинчи даражадагы модулу так жана жөнөкөй сан болгон салыштыруу берилсин

$$x^2 \equiv a \pmod{p}, \ (2, p)=1. \qquad (1)$$

Эгерде $a \equiv 0 \pmod{p}$ болсо, анда $x^2 \equiv 0 \pmod{p}$ болот, бул салыштыруунун чечими $x \equiv 0 \pmod{p}$ болот. Ушул учурда гана берилген салыштыруу тривиалдык чечимге ээ болот. Мындан ары биз $(a, p)=1$ деп, тривиалдык эмес чечимдерди издейбиз. (1) салыштыруунун модулу так жана жөнөкөй сан болгондуктан, анын чечими модул боюнча чегериштердин келтирилген системасына таандык (тиешелүү) болот.

Теорема 1. Эгерде (1)нин чечими $x \equiv x_1 \pmod{p}$ болсо, анда $x \equiv -x_1 \pmod{p}$ дагы анын чечими болот.

Далилдөө. Ар дайым $x^2 \equiv (-x_1)^2 \pmod{p}$ аткарылат. Мындан, x_1 (1)ди канааттандырса, анда $(-x_1)$ дагы аны канааттандырат деп айта алабыз.

Салыштыруунун чечиминин аныктоосунун негизинде ар бир чечимге бир класс туура келиши бизге белгилүү. Биз x_1 жана $(-x_1)$дин p модулу боюнча ар түрдүү класстын өкүлдөрү экендигин көрсөтүшүбүз керек. Ал үчүн карама-каршысынан ой жүгүртөбүз, б.а. x_1 жана $(-x_1)$лер p модулу боюнча бир класска тиешелүү (таандык) болушсун. Анда

$$x_1 \equiv -x_1 \pmod{p} \Rightarrow 2x_1 \equiv 0 \pmod{p} \Rightarrow x_1 \equiv 0 \pmod{p},$$

себеби $(2, p)=1$. Бирок, акыркы салыштыруу $(a, p)=1$ деген шартка жана чечимдин тривиалдык эместигине карама-каршы келет. Демек, x_1 жана $(-x_1)$лер p модулу боюнча ар түрдүү класстарга тиешелүү (таандык) болушат.

Салыштыруунун модулу кичине жөнөкөй сан болгондо, аны тандоо усулу менен чечүү максатка ылайыктуу болот.
Ал үчүн p модулу боюнча чегериштердин келтирилген

$$\pm 1, \pm 2, \pm 3, ..., \pm \frac{p-1}{2}$$

системасындагы ар бир чегеришти удаалаш (1)ге коюп отурбастан, x ти $1, 2, ..., \frac{p-1}{2}$ лер менен алмаштыруу жетиштүү.
Бул учурда сол жакта

$$1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2 \qquad (2)$$

сандар пайда болот.

Теорема 2. (2) сандардын ар бири p модулу боюнча ар түрдүү класстарга тиешелүү болушат.
Далилдөө. Далилдөөнү карама-каршысынан жүргүзөбүз. Б.а. $1 \le k \le l \le \frac{p-1}{2}$ болгондо, $k^2 \equiv l^2 (\mathrm{mod}\, p)$ болсун. Мындай учурда (1) салыштыруу $x \equiv \pm k (\mathrm{mod}\ p)$ жана $x \equiv \pm l (\mathrm{mod}\ p)$ көрүнүшүндөгү төрт чечимге ээ болот эле. Мындай болушу мүмкүн эмес, себеби модулу жөнөкөй сан болгон экинчи даражадагы салыштыруунун чечимдеринин саны экиден көп (ашык) эмес.

Натыйжа. p модулу боюнча түзүлгөн чегериштердин келтирилген системасындагы $\frac{p-1}{2}$ чегериши квадраттык чегериш, ал эми $\frac{p-1}{2}$ чегериши квадраттык чегериш эмес болот.
Мисал. 11 модулу боюнча эң кичине оң квадраттык чегериштерди тапкыла.

Чыгаруу. Бул чегериштерди табуу үчүн төмөнкү эсептөөлөрдү жүргүзөбүз. $\frac{11-1}{2}=5$ болгондо 1, 2, 3, 4, 5 сандардын квадраттарын карап чыгабыз:

$$1^2\equiv1,\ 2^2\equiv4,\ 3^2\equiv9,\ 4^2\equiv16\equiv5,\ 5^2\equiv25\equiv3.$$

Демек, 11 модулу боюнча квадраттык чегериштер 1, 4, 9, 5, 3. Ал эми 2, 6, 7, 8, 10 сандары квадраттык чегериш эместер болот.

Теорема 3. (Эйлердин критерийи). Эгерде $(a, p)=1$ болгондо $a^{\frac{p-1}{2}}\equiv1(\mathrm{mod}\,p)$ салыштыруусу орун алса, анда (1) салыштыруу эки чечимге ээ болот, ал эми $a^{\frac{p-1}{2}}\equiv-1(\mathrm{mod}\,p)$ болгондо бир да чечимге ээ болбойт.

Далилдөө. Ферманын теоремасынын негизинде $a^{p-1}\equiv1(\mathrm{mod}\ p)$ аткарылат. p – жөнөкөй сан болгондуктан

$$a^{p-1}-1=\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)$$

болот. Мындан $\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)\equiv0(\mathrm{mod}\,p)$ келип чыгат.

Салыштыруунун негизинде $a^{\frac{p-1}{2}}-1$ жана $a^{\frac{p-1}{2}}+1$ көбөйтүүчүлөрдөн жок дегенде бирөөсү p га бөлүнүшү зарыл. Бул эки көбөйтүүчү бир убакытта p га бөлүнбөйт, себеби алардын айрымасы болгон ±2 саны p га бөлүнбөйт $(2, p)=1$.

Эгерде a квадраттык чегериш болсо, анда $a^{\frac{p-1}{2}}\equiv1(\mathrm{mod}\,p)$ болот. Чындыгында, мындай учурда x тин ушундай мааниси табылат, ал маани үчүн $(x, p)=1$ болгондо, $a=x^2(\mathrm{mod}\,p)$ болот. Акыркы салыштырууну $\frac{p-1}{2}$ даражага көтөрөбүз:

$$a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} (\mathrm{mod}\, p) \equiv x^{p-1} \equiv 1(\mathrm{mod}\, p).$$

Жогорудагы натыйжанын негизинде p модулу боюнча $\frac{p-1}{2}$ квадраттык чегериш жашайт. Бирок, биз a ны белгисиз деп карасак, (4) салыштыруу жогорудагылардын негизинде $\frac{p-1}{2}$ ден кем болбогон чечимге ээ болот эле. (4) салыштыруунун модулу жөнөкөй сан болгондуктан жана анын коэффициенттери pга бөлүнбөгөнү үчүн чечимдердин саны салыштыруунун даражасынан, б.а. $\frac{p-1}{2}$ ден көп (ашык) боло албайт.

Демек, бардык квадраттык чегериштер үчүн гана (4) орун алат. Анда $(a, p)=1$ шартын канааттандыруучу квадраттык чегериш эмес a сандары жана ушулар үчүн гана $a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p)$ аткарылат. Эйлердин критерийи далилденди.

§9. Модулу курама сан болгон экинчи даражадагы салыштырууларды чечүү

Жогоруда айтып өткөндөй, m модулу курама сан болгондо $x^2 \equiv a \pmod{m}$ салыштыруу төмөнкү үч түрдүү салыштырууга келтирилет:

4) $x^2 \equiv a \pmod{p}$, p – так жана жөнөкөй сан;

5) $x^2 \equiv a \pmod{p^\alpha}$, $(\alpha > 1)$;

6) $x^2 \equiv a \pmod{2^\alpha}$, $(\alpha \geq 1)$.

1) учурду жогоруда карадык. Эми 2) учурду, б.а. төмөнкү салыштырууну карайбыз:

$$x^2 \equiv a \pmod{p^\alpha}; \quad \alpha > 0, (a, p) = 1, \tag{1}$$

мында p – так жана жөнөкөй сан.

Эгерде $f(x) = x^2 - a$ деп алсак, анда $f'(x) = 2x$ болот, жана $x \equiv x_1 \pmod{p}$

$$x^2 \equiv a \pmod{p}, \tag{2}$$

салыштыруунун чечими болсо, анда

$(a, p)=1$ден $(x_1, p)=1$ келип чыгат, бирок p – так сан болгондуктан, $(2x_1, p)=1$ болот, б.а. $f'(x_1)$ саны p га бөлүнбөйт. Ошондуктан (1) салыштыруунун чечимин табуу үчүн §6нын 2пунктун пайдаланууга болот. Мында (2)нин ар бир чечими (1)нин бир чечимин берет. Төмөнкү тыянак келип чыгат:

Эгерде (1) салыштыруу p модулу боюнча квадраттык чегериш болсо, анда ал эки чечимге ээ болот, ал эми p модулу боюнча квадраттык чегериш эмес болсо, анда бир да чечимге ээ болбойт.

Эми 3) учурду изилдейбиз.

$$x^2 \equiv a \pmod{2^\alpha}; \quad \alpha > 0, (a, 2) = 1. \tag{3}$$

Бул учурда $f'(x_1)=2x_1$ 2ге бөлүнөт, ошондуктан §6нын 2пунктун пайдаланууга болбойт. Эгерде (3) салыштыруу чечилүүчү болсо, анда $(a, 2)=1$ ден $(x, 2)=1$ келип чыгат.

Натыйжада $\left(\frac{2}{x}\right)=(-1)^{\frac{x^2-1}{8}}$ ны алабыз. Мындан x^2-1 дин 8ге бөлүнүшү келип чыгат. Ошондуктан, (3)нү төмөнкү көрүнүшкө келтиребиз:

$$(x^2-1)+1\equiv a(\bmod 2^{\alpha}).$$

Демек, бул салыштыруу чечилүүчү болушу үчүн

$$a\equiv(\bmod 4)\ \ \alpha=2 \text{ де};\quad a\equiv 1(\bmod 8)\ \ \alpha\geq 3 \text{ дъ} \qquad (4)$$

аткарылышы зарыл.

Айталы, (4) шарт аткарылсын, анда чечимди төмөнкүдөй аныктайбыз:

Эгерде $\alpha\leq 3$ болсо, анда салыштырууну бардык так сандар канааттандырат. Ошондуктан $x^2\equiv a(\bmod 2)$ салыштыруу бир чечимге ээ болот: $x\equiv 1(\bmod 2)$; $x^2\equiv a(\bmod 4)$ салыштыруу эки чечимге ээ болот: $x\equiv 1; 3(\bmod 4)$; ал эми $x^2\equiv a(\bmod 8)$ салыштыруу төрт чечимге ээ болот: $x\equiv 1; 3; 5; 7(\bmod 8)$.

$\alpha=4, 5, \ldots$ учурун кароодо бардык так сандарды эки арифметикалык прогрессияга бириктирүү пайдалуу:

$$x=\pm(1+4t_3) \qquad (5)$$

$$(1+4t_3\equiv 1(\bmod 4);\quad -1-4t_3\equiv -1\equiv 3(\bmod 4)).$$

(5)теги сандардын ичинен кайсылары $x^2\equiv a(\bmod 16)$ салыштыруунун чечими боло тургандыгын аныктайлы:

$$(1+4t_3)^2\equiv a(\bmod 16),\ t_3\equiv\frac{a-1}{8}(mod\,2),$$

$$t_3=t'_3+2t_4,$$

$$x=\pm(1+4t'_3+8t_4)=\pm(x_4+8t_4).$$

Акыркы сандардын кайсы бири $x^2\equiv a(\bmod 32)$ салыштыруунун чечими боло тургандыгын аныктайбыз:

$$(x_4+8t_4)^2\equiv a(\bmod 32), t_4=t'_4+2t_5,\ x=\pm(x_5+16t_5),$$

ж.б.у.с. Ушул жол менен $\forall\alpha>3$ учурда (3)нү канааттандыруучу x тин мааниси

$$x=\pm(x_a+2^{a-1}t_a)$$

көрүнүшүндө боло тургандыгына ишинебиз.

x тин бул маанилери (3)нүн төрт ар түрдүү чечимин берет.

$x \equiv x_a;\ x_a + 2^{\alpha-1};\ -x_a;\ -x_a - 2^{\alpha-1} \pmod{2^\alpha}$

(алгачкы экөөсү 4 модулу боюнча 1 менен, ал эми акыркы экөөсү –1 менен салыштырылат).

Мисал. $x^2=57 \pmod{64}$ салыштыруу төрт чечимге ээ болот, себеби $57\equiv 1 \pmod 8$. x ти $x=\pm(1+4t_3)$ көрүнүшүндө жазып алып,төмөнкүлөрдү табабыз:

$$(1+4t_3)^2 \equiv 57 \pmod{16}, \qquad 8t_3 \equiv 56 \pmod{16},$$
$$t_3 \equiv 1 \pmod 2, \quad t_3 = 1 + 2t_4,\ x = \pm(5 + 8t_4),$$
$$(5+8t_4)^2 \equiv 57 \pmod{32}, \qquad 5\cdot 16t_4 \equiv 32 \pmod{32},$$
$$t_4 \equiv 0 \pmod 2, \quad t_4 = 2t_5, \qquad x = \pm(5 + 16t_5),$$
$$(5+61t_5)^2 \equiv 57 \pmod{64}, \qquad 5\cdot 32t_5 \equiv 32 \pmod{64},$$
$$t_5 \equiv 1 \pmod 2, \qquad t_5 = 1 + 2t_6,\ x = \pm(21 + 32t_6).$$

Ошондуктан берилген салыштыруунун чечимдери:

$x_1 \equiv 21 \pmod{64}$, $x_2 \equiv -21 \pmod{64}$,

$x_3 \equiv 53 \pmod{64}$, $x_4 \equiv -53 \pmod{64}$ болот.

§10. Лежандрдын жана Якобинин символдору

Лежандрдын символу. Бул символ төмөнкүдөй аныкталат:

$a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$ жана $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$ салыштыруулары

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p),$$

көрүнүшүндөгү бир салыштырууга бириктирилет. Мында $\left(\frac{a}{p}\right)$ символу Лежандрдын символу деп аталат, жана +1 же –1 деп белгиленет. a саны Лежандрдын символунун алымы, ал эми p болсо бөлүмү деп аталат.

Эгерде $\left(\frac{a}{p}\right)=1$ болсо, анда a саны p модулу боюнча квадраттык чегериш болот, ошондуктан $x^2 \equiv a (\mathrm{mod}\, p)$ салыштыруу эки ар түрдүү чечимге ээ болот, а эгерде $\left(\frac{a}{p}\right) = -1$ болсо, анда a саны p модулу боюнча квадраттык чегериш эмес болот, ошондуктан $x^2 \equiv a (\mathrm{mod}\, p)$ салыштыруу чечилбейт.

Лежандрдын символун Эйлердин критерийинин жардамында табууга болот:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\, p),$$

бирок a жана p чоң сан болгондо эсептөө татаал болуп кетет. Бирок, төмөнкү касиеттерди пайдалануу эсептөө жеңилдейт:

1^0. Эгерде $a \equiv b (\mathrm{mod}\, p)$ болсо, анда $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ болот.

2^0. $\left(\frac{1}{p}\right) = 1$.

3^0. $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

4^0. $\left(\frac{2}{p}\right)\equiv(-1)^{\frac{p^2-1}{8}}$.

5^0. $\left(\frac{ab...k}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)...\left(\frac{k}{p}\right)$, мында a, b, ..., k лар p менен өз ара жөнөкөй сандар.

6^0. $\left(\frac{a^n}{p}\right)=\left(\frac{a}{p}\right)^n$, $n\in N$,

7^0. $\left(\frac{a^{2n}}{p}\right)=1$, $n\in N$.

8^0. $\left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right)$.

9^0. $\left(\frac{ab...l}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)...\left(\frac{l}{p}\right)$, мында a, l, p, q – ар түрдүү так жөнөкөй сандар.

10^0. $\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$, мында p, q – өз ара жөнөкөй так сандар.

Мисал 1. $x^2\equiv5(\mathrm{mod}\ 29)$ квадраттык чегериштин чечими жашайбы?

Чыгаруу. $5^{14}\equiv1(\mathrm{mod}\ 29)$ болгондуктан, $\left(\frac{5}{29}\right)=1$ болот. Демек, 5 саны 29 модулу боюнча квадраттык чегериш болот, ошондуктан берилген салыштыруу эки чечимге ээ болот.

Мисал 2. $x^2\equiv3(\mathrm{mod}29)$ квадраттык чегериштин чечимдерин тапкыла.

Чыгаруу. Берилген квадраттык чегериштин чечимдери жашабайт, себеби

$3^{14} \equiv -1 (\mathrm{mod}\ 29)$ болгондуктан $\left(\frac{3}{29}\right) = -1$ келип чыгат. Мындан 3 саны 29 модулу боюнча квадраттык чегериш эмес болот.

Якобинин символу

Якобинин символу Лежандрдын символунун жалпыланышы болуп саналат.

Айталы p – бирден чоң бүтүн так сан, $p = p_1 p_2 \ldots p_n$ – анын каноникалык ажыралмасы (алардын арасында $p_i = p_j$, $i, j = 1,2,\ldots,n$ болушу мүмкүн), $(a, p) = 1$ болсун. Анда Якобинин символу $\left(\frac{a}{p}\right)$ төмөндөгү барабардык менен аныкталат

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_n}\right).$$

Лежандрдын символунун касиеттеринен Якобинин символу үчүн төмөнкү касиеттер келип чыгат:

1^0. Эгерде $a \equiv a_1 (\mathrm{mod}\ p)$ болсо, анда $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$ болот.

Далилдөө:

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_n}\right) = \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\ldots\left(\frac{a_1}{p_n}\right) = \left(\frac{a_1}{p}\right),$$

Себеби $(a - a_1) \vdots p \Rightarrow (a - a_1) \vdots p_k$, $k = 1, 2, \ldots, n$.

2^0. $\left(\frac{1}{p}\right) = 1$.

Далилдөө. Чындыгында,

$$\left(\frac{1}{p}\right) = \left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\ldots\left(\frac{1}{p_n}\right) = 1.$$

3^0. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Далилдөө.

$$\left(\frac{-1}{p}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_n}\right)=(-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots+\frac{p_n-1}{2}};$$

бирок

$$\frac{p-1}{2}=\frac{p_1p_2\ldots p_n-1}{2}=\frac{\left(1+2\frac{p_1-1}{2}\right)\left(1+2\frac{p_2-1}{2}\right)\cdots\left(1+2\frac{p_n-1}{2}\right)-1}{2}=,$$

$$=\frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots+\frac{p_n-1}{2}+2N.$$

Ошондуктан, эгерде $a^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}\,p)$ экендигин эске салсак, анда $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ болот.

$4^0.\ \left(\frac{ab..l}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right).$

Далилдөө:

$$\left(\frac{ab..l}{p}\right)=\left(\frac{ab..l}{p_1}\right)\cdots\left(\frac{ab..l}{p_n}\right)=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{l}{p_1}\right)\cdots\left(\frac{a}{p_n}\right)\left(\frac{b}{p_n}\right)\cdots\left(\frac{l}{p_n}\right).$$

Бирдей алымга ээ болгон символдорду топтоштуруп $\left(\frac{ab..l}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right)$ барабардыгына ээ болобуз. Мындан төмөнкү натыйжа келип чыгат:

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right).$$

$5^0.\ \left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$

Далилдөө.(3^0 - касиетке окшош далилденет)

$$\left(\frac{2}{p}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_n}\right)=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_n^2-1}{8}};\qquad (*)$$

бирок

$$\frac{p^2-1}{8}=\frac{p_1^2p_2^2\ldots p_n^2-1}{8}=\frac{\left(1+8\frac{p_1^2-1}{8}\right)\left(1+8\frac{p_2^2-1}{8}\right)\ldots\left(1+8\frac{p_n^2-1}{8}\right)-1}{8}=,$$

$$=\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_n^2-1}{8}+2N$$

Ошондуктан (*) дан $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ келип чыгат.

6^0. Эгерде p, q – оң, так жана өз ара жөнөкөй сандар болушса, анда

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$ болот.

Далилдөө. Айталы qнын каноникалык ажыралмасы $q=q_1q_2\ldots q_s$ болсун (алардын арасында $q_i=q_j$, $i,j=1,2,\ldots,n$ болушу мүмкүн). Төмөнкүнү алабыз

$$\left(\frac{q}{p}\right)=\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right)\ldots\left(\frac{q}{p_n}\right)=\prod_{\alpha=1}^{n}\prod_{\beta=1}^{s}\left(\frac{q_\beta}{p_\alpha}\right)=(-1)^{\sum_{\alpha=1}^{n}\sum_{\beta=1}^{s}\frac{p_\alpha-1}{2}\cdot\frac{q_\beta-1}{2}}\prod_{\alpha=1}^{n}\prod_{\beta=1}^{s}\left(\frac{p_\alpha}{q_\beta}\right)=$$

$$=(-1)^{\left(\sum_{\alpha=1}^{n}\frac{p_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{q_\beta-1}{2}\right)}\left(\frac{p}{q}\right)$$

3^0 касиеттегидей, төмөнкүнү алабыз

$$\frac{p-1}{2}=\sum_{\alpha=1}^{n}\frac{p_\alpha-1}{2}+2N,\quad \frac{q-1}{2}=\sum_{\beta=1}^{s}\frac{q_\beta-1}{2}+2N_1,$$

акыркы формуладан

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$ келип чыгат.

Мисал. Төмөнкү салыштыруу канча чечимге ээ болот:

$$x^2\equiv 219 \pmod{383}.$$

Чыгаруу. Эгерде 6^0, 1^0, 4^0 түн натыйжасын, 6^0, 1^0, 4^0, 5^0, 6^0, 1^0, 3^0 касиеттерин удаалаш колдонсок, анда

$$\left(\frac{219}{383}\right)=-\left(\frac{383}{219}\right)=-\left(\frac{164}{219}\right)=-\left(\frac{41}{219}\right)=-\left(\frac{219}{41}\right)=-\left(\frac{14}{41}\right)=$$
$$=-\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)=-\left(\frac{7}{41}\right)=-\left(\frac{41}{7}\right)=-\left(\frac{-1}{7}\right)=1$$

келип чыгат. Демек, берилген салыштыруу эки чечимге ээ болот.

Өз алдынча иштөө үчүн көнүгүүлөр

1) Лежандрдын символун эсептөө менен, төмөнкү салыштыруулардын чечилүүчү экендигин аныктагыла жана алардын чечимдерин тапкыла:
   a) $x^2\equiv 6 \pmod 7$; b) $x^2\equiv 10 \pmod{13}$;
   c) $x^2\equiv 3 \pmod{11}$; d) $x^2\equiv 5 \pmod{11}$;
   e) $x^2\equiv 12 \pmod{13}$; f) $x^2\equiv 13 \pmod{17}$.
2) Төмөнкү салыштырууларды $x^2\equiv d \pmod p$ көрүнүшүндө келтирип чыгаргыла:
   a) $3x^2+7x+8\equiv 0 \pmod{17}$; b) $3x^2+4x+7\equiv 0 \pmod{31}$;
   c) $5x^2-11x+16\equiv 0 \pmod{41}$; d) $12x^2+8x-15\equiv 0 \pmod{47}$;
   e) $5x^2+x+4\equiv 0 \pmod{13}$; f) $4x^2-11x-3\equiv 0 \pmod{23}$.
3) Эгерде $p=4k+3$ көрүнүшүндөгү жөнөкөй сан жана a саны p модулу боюнча квадраттык чегериш болсо, анда $x^2\equiv a \pmod p$ салыштыруунун чечими $x\equiv\pm a^{k+1} \pmod p$ боло тургандыгын далилдегиле.
4) Салыштырууларды чыгаргыла.
   a) $x^2\equiv 2 \pmod{311}$; b) $x^2\equiv 3 \pmod{47}$.
5) Эгерде $p=8k+5$ көрүнүшүндөгү жөнөкөй сан жана a саны p модулу боюнча квадраттык чегериш болсо, анда $x^2\equiv a \pmod p$ салыштыруунун чечими $x\equiv\pm a^{k+1}2^{(2k+1)t} \pmod p$ боло тургандыгын далилдегиле, мында $t=0, 1$.
6) Салыштырууларды чыгаргыла.
   a) $x^2\equiv 7 \pmod{29}$; b) $x^2\equiv 3 \pmod{37}$.

7) Төмөнкү теңдеменин $x, y \in Z$ чечимдери жок экендигин далилдегиле: $5x^2-11y=7$.

8) $13y=x^2-21x+110$ аныкталбаган теңдемени чыгаргыла.

9) Эгерде $p=8k+7$ жөнөкөй сан болсо, анда $2^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$, ал эми $p=8k+3$ жөнөкөй сан болсо, анда $2^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$ экендигин далилдегиле.

10) 3 саны квадраттык чегериш боло турган p жөнөкөй санын тапкыла.

11) 3 саны квадраттык чегериш эмес боло турган p жөнөкөй санын тапкыла.

12) Эгерде $p=4k+3$ жөнөкөй сан болсо, анда a же $(-a)$ нын бирөөсү квадраттык чегериш, ал эми экинчиси квадраттык чегериш эмес боло тургандыгын далилдегиле.

13) Эгерде $p=4k+1$ жөнөкөй сан болсо, анда a жана $(-a)$ бир учурда квадраттык чегериш же квадраттык чегериш эмес боло тургандыгын далилдегиле.

Лежандрдын символун аныктагыла [14-38]:

14) $\frac{4563}{197}$; 15) $\frac{673}{251}$; 16) $\frac{5467}{349}$; 17) $\frac{9876}{617}$;

18) $\frac{5798}{659}$; 19) $\frac{5876}{941}$; 20) $\frac{4566}{1021}$; 21) $\frac{5435}{1091}$;

22) $\frac{2435}{419}$; 23) $\frac{10234}{1511}$; 24) $\frac{14634}{1811}$; 25) $\frac{2545}{1777}$;

26) $\frac{3545}{1723}$; 27) $\frac{54376}{2011}$; 28) $\frac{5433}{2063}$; 29) $\frac{24354}{2371}$;

30) $\frac{54567}{2693}$; 31) $\frac{3543}{2699}$; 32) $\frac{43254}{2999}$; 33) $\frac{23543}{3323}$;

34) $\frac{4567}{693}$; 35) $\frac{13543}{2699}$; 36) $\frac{53254}{2999}$; 37) $\frac{73543}{3323}$;

38) $\frac{45543}{3699}$.

Якобинин символун аныктагыла [39- 63]:

39) $\frac{235}{414}$; 40) $\frac{1234}{1514}$; 41) $\frac{1434}{1812}$; 42) $\frac{255}{178}$;

43) $\frac{435}{455}$; 44) $\frac{234}{111}$; 45) $\frac{634}{411}$; 46) $\frac{545}{77}$;

47) $\frac{567}{693}$; 48) $\frac{243}{699}$; 49) $\frac{254}{99}$; 50) $\frac{543}{332}$;

51) $\frac{547}{264}$; 52) $\frac{353}{299}$; 53) $\frac{434}{272}$; 54) $\frac{233}{338}$;

55) $\frac{367}{125}$; 56) $\frac{4355}{1020}$; 57) $\frac{4344}{1032}$; 58) $\frac{3543}{323}$;

59) $\frac{567}{325}$; 60) $\frac{1355}{1120}$; 61) $\frac{1344}{1132}$; 62) $\frac{2543}{425}$;

63) $\frac{6543}{4120}$.

§11. **Баштапкы тамырлар**

Эйлердин теоремасынын негизинде $(a, m)=1$ болгондо

$$a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m), \qquad (1)$$

салыштыруусу аткарылат. Эгерде (1)-салыштыруунун эки жагын тең k-даражага көтөрө турган болсок, анда

$$a^{k\ \varphi(m)}\equiv 1(\mathrm{mod}\ m), \qquad (2)$$

салыштыруусун алабыз. Демек, (1) жана (2)ден $(a, m)=1$ болгондо ар дайым ушундай $\gamma\in N$ табылат жана, ал үчүн

$$a^{\gamma}\equiv 1(\mathrm{mod}\ m), \qquad (3)$$

орун алат.

(3) салыштырууну канааттандырган натуралдык сандардын көптүгүнүн эң кичине элементин min γ ны δ аркылуу белгилейли. Каалагандай натуралдык сандардын көптүгү эң кичине элементке ээ болгондуктан δ ар дайым жашайт.

Def 1. Эгерде $(a, m)=1$ болуп, (3) салыштырууну канааттандыр-ган γ ($\gamma>0$) лардын эң кичинеси δ болсо, анда a саны m модулу боюнча δ көрсөткүчүнө таандык (тиешелүү) деп аталат.

Аныктамадан $\delta\le\varphi(m)$ келип чыгат.

Def 2. Эгерде $\delta=\varphi(m)$ болгондо (3) салыштыруу орун алса, анда a саны m модулу боюнча баштапкы тамыр деп аталат.

Каалагандай a саны үчүн тиешелүү көрсөткүчтү табууну төмөнкү мисалдарда карап өтөбүз.

Мисал. $m=7$ модулу боюнча 2, 3, 5 сандары тиешелүү болгон көрсөткүчтөр табылсын.

Чыгаруу. 1) $a=2$, $\varphi(7)=6$ болгондуктан $2^1, 2^2, 2^3, 2^4, 2^5, 2^6$ даражаларды 7 модулу боюнча карап чыгабыз:

$2\equiv 2(\mathrm{mod}\ 7)$, $2^2\equiv 4(\mathrm{mod}\ 7)$, $2^3\equiv 1(\mathrm{mod}\ 7)$.

2 нин башка даражаларын кароонун кажети жок, себеби акыркы $2^3 \equiv 1 (\text{mod } 7)$ салыштыруу (3)-гө окшош. Демек, 2 саны 7 модулу боюнча $\delta=3$ көрсөткүчкө тиешелүү экен.

2) $a=3$;

$3 \equiv 3 (\text{mod } 7)$, $3^2 \equiv 9 \equiv 2 (\text{mod } 7)$, $3^3 \equiv 6 \equiv -1 (\text{mod } 7)$,

$3^4 \equiv 4 (\text{mod } 7)$, $3^5 \equiv 5 (\text{mod } 7)$, $3^6 \equiv 1 (\text{mod } 7)$.

Демек, 3 санынын 7 модулу боюнча тиешелүү көрсөткүчү $\delta=6$ болот экен.

3) $a=5$;

$5 \equiv 5 (\text{mod } 7)$, $5^2 \equiv 25 \equiv 4 (\text{mod } 7)$, $5^3 \equiv 20 \equiv 6 (\text{mod } 7)$,

$5^4 \equiv 16 \equiv 2 (\text{mod } 7)$, $5^5 \equiv 3 (\text{mod } 7)$, $5^6 \equiv 1 (\text{mod } 7)$.

Демек, 5 санынын 7 модулу боюнча тиешелүү көрсөткүчү $\delta=6$ болот экен.

2) жана 3)тө $\delta=\varphi(7)=6$ болгондуктан, 3 жана 5 сандары 7 модулу боюнча баштапкы тамырлар болушат. Демек, бир модул боюнча ар түрдүү баштапкы тамырлар жашайт экен.

Теорема 1. Кандайдыр бир m модулу боюнча түзүлгөн бир класстын бардык чегериштери ушул модул боюнча бирдей көрсөткүчкө тиешелүү болот.

Далилдөө. Далилдөөнү карама-каршысынан жүргүзөбүз.

$a \equiv a_1 (\text{mod } m)$, $a^{\delta} \equiv 1 (\text{mod } m)$ жана $a_1^{\delta_1} \equiv 1 (\text{mod } m)$ болгондо $\delta \neq \delta_1$ болсун. Аныктык үчүн $\delta < \delta_1$ же $\delta > \delta_1$ деп алабыз.

1) $\delta < \delta_1$ болушу мүмкүн эмес, себеби $a^{\delta} \equiv 1 (\text{mod } m)$ жана $a \equiv a_1 (\text{mod } m) \Rightarrow a^{\delta} \equiv a_1^{\delta} (\text{mod } m)$. Мындан $a^{\delta} \equiv 1 (\text{mod } m)$ болгондуктан $a_1^{\delta} \equiv 1 (\text{mod } m)$болот. Эгерде a_1 саны δ_1 көрсөткүчкө тиешелүү болсо, анда көрсөткүчтүн аныктоосу боюнча $\delta \geq \delta_1$ге ээ болобуз. Бул болсо $\delta < \delta_1$ шартына карама-каршы (тескери).

2) $\delta > \delta_1$ болсун. $a \equiv a_1 (\text{mod } m)$ салыштыруунун эки жагын δ_1-даражага көтөрөбүз:

$$a^{\delta} \equiv a_1^{\delta} (\mathrm{mod}\ m) \Rightarrow a^{\delta_1} \equiv 1 (\mathrm{mod}\ m).$$

a саны *m* модулу боюнча δ көрсөткүчкө тиешелүү болгондуктан, $\delta_1 \geq \delta$; $(\delta_1 \geq \delta) \wedge (\delta \geq \delta_1) \Rightarrow \delta = \delta_1$ га ээ болобуз. Теорема далилденди.

Демек, эгерде *a* саны *m* модулу боюнча δ көрсөткүчкө тиешелүү болсо, а менен *m* модулу боюнча тең калдыктуулар классынын бардык элементтери да ушул көрсөткүчкө тиешелүү болот экен. Б.а. берилген модул боюнча бир көрсөткүчкө тиешелүү сандардын классы жөнүндө сөз кылуу мүмкүн. *m* модул боюнча δ көрсөткүчкө тиешелүү болгон ар бир *a* саны *m* менен өз ара жөнөкөй болушу керек. Тескерисинче, б.а. $(a, m)=d>1$ болсо, $a^l \equiv 1 (\mathrm{mod}\ m)$ салыштыруу орун албайт.

Эгерде *a* саны *m* модулу боюнча баштапкы тамыр болсо, анда биз баштапкы тамырлар классы жөнүндө ой жүргүзөбүз.

Теорема 2. Эгерде $(a, m)=1$ болгондо $a^{\delta} \equiv 1 (\mathrm{mod}\ m)$ болсо, анда

$$1=a^0, a^1, a^2, \ldots a^{\delta-1}$$

сандардын системасы *m* модулу боюнча салыштыруу боло албайт.

Далилдөө. Далилдөөнү карама-каршысынан жүргүзөбүз. Айталы $\forall l,\ k \in \mathrm{N},\ a^l \equiv a^k (\mathrm{mod}\ m)$ орун алсын, мында $0 \leq k < l \leq \delta - 1$. $(a, m)=1$ болгондуктан $a^l \equiv a^k (\mathrm{mod}\ m)$ салыштыруунун эки жагын a^k га бөлүп жиберүүгө болот:

$$a^{l-k} \equiv 1 (\mathrm{mod}\ m),\ 0 < l-k \leq \delta.$$

Бирок бул салыштыруу орун албайт, себеби *a* саны *m* модулу δ көрсөткүчкө тиешелүү.

Натыйжа 1. $\varphi(m)=\delta$ болгондо

$$1=a^0, a^1, a^2, \ldots a^{\delta-1}$$

система *m* модулу боюнча чегериштердин келтирилген системасын түзөт.

Далилдөө. Чындыгында,

1) $1=a^0, a^1, a^2, \ldots a^{\delta-1}$ системада $\varphi(m)$ та элемент жашайт;

2) $(a, m)=1 \Rightarrow (a^k, m)=1$;

3) a^k элементтердин ар бири теорема 2нин негизинде m модулу боюнча ар түрдүү класстарга тиешелүү.

Бул үч шарт чегериштердин келтирилген системасынын шарттары болот.

Натыйжа 2. $m=p$ – жөнөкөй сан, a саны m модулу боюнча баштапкы тамыр болсо, анда

$$1=a^0, a^1, a^2, \ldots a^{\delta-1}$$

катары $1=a^0, a^1, a^2, \ldots a^{p-2}$ көрүнүшкө келет.

Мисал. 7 модулу боюнча 5 баштапкы тамыр үчүн $1=a^0, a^1, a^2, \ldots, a^{\delta-1}$ көрүнүшүндөгү система түзүлсүн.

Чыгаруу. $1=5^0, 5^1, 5^2, 5^3, 5^4, 5^5$ системаны түзөбүз. Ар бир даражаны 7 модул боюнча эң кичине оң чегериштер менен алмаштырабыз: 1, 3, 2, 6, 4, 5. Чындыгында, бул система 7 модулу боюнча чегериштердин келтирилген системасы болот.

Теорема 3. a саны m модулу боюнча δ көрсөткүчкө тиешелүү болгондо, $a^\gamma \equiv a^{\gamma_1} (\mathrm{mod}\ m)$ салыштыруу орун алуусу үчүн $\gamma \equiv \gamma_1 (\mathrm{mod}\ \delta)$ орун алуусу зарыл жана жетиштүү.

Далилдөө. Зарылдыгы. a саны m модулу боюнча δ көрсөткүчкө тиешелүү жана $a^\gamma \equiv a^{\gamma_1} (\mathrm{mod}\ m)$ салыштыруу орун алсын. Анда γ жана γ_1 ди төмөнкүдөй жазып алабыз:

$$\gamma=\delta q+r;\ 0 \le r < \delta;\ \gamma_1=\delta q_1+r_1;\ 0 \le r_1 < \delta$$

жана $r=r_1$ экендигин көрсөтөбүз. γ жана γ_1 дин бул маанилерин $a^\gamma \equiv a^{\gamma_1} (\mathrm{mod}\ m)$ салыштырууга коебуз:

$$a^{\delta q+r} \equiv a^{\delta q_1+r_1} (\mathrm{mod}\ m) \Rightarrow \left(a^\delta\right)^q a^r \equiv \left(a^\delta\right)^{q_1} a^{r_1} (\mathrm{mod}\ m).$$

Эгерде $a^\delta \equiv 1 (\mathrm{mod}\ m)$ экендигин эске алсак, анда $a^r \equiv a^{r_1} (\mathrm{mod}\ m)$ келип чыгат. Жогорудагы теорема 2нин негизинде бул салыштыруу $a^r = a^{r_1}$ болгондо гана орун алат, мындан $r=r_1$ жана $\gamma \equiv \gamma_1 (\mathrm{mod}\ \delta)$ экендиги келип чыгат.

Жетиштүүлүгү. $a^{\delta}\equiv 1(\mathrm{mod}\ m)$ жана $\gamma\equiv\gamma_1(\mathrm{mod}\ \delta)$ орун алсын. Акыркы салыштырууну барабардык аркылуу төмөндөгүдөй жазууга болот:

$$\gamma=\delta q+r;\ \gamma_1=\delta q_1+r;\ 0\le r<\delta.$$

a саны m модулу боюнча δ көрсөткүчкө тиешелүү болгондуктан,

$$a^{\delta q}\equiv 1(\mathrm{mod}\ m)\wedge a^{\delta q_1}\equiv 1(\mathrm{mod}\ m)\Rightarrow \left(a^{\delta}\right)^{q}\equiv\left(a^{\delta}\right)^{q_1}(\mathrm{mod}\ m)\Rightarrow$$

$$a^{\delta q}a^{r}\equiv a^{\delta q_1}a^{r}(\mathrm{mod}\ m)\Rightarrow a^{\delta q+r}\equiv a^{\delta q_1+r}(\mathrm{mod}\ m)\Rightarrow a^{\gamma}\equiv a^{\gamma_1}(\mathrm{mod}\ m)$$

эе болобуз. Теорема далилденди.

Натыйжа 3. $\gamma\equiv 0(\mathrm{mod}\ \delta)$ болгондо, жана ушул учурда гана $a^{\gamma}\equiv 1(\mathrm{mod}\ m)$ орун алат.

Далилдөө. Чындыгында, эгерде $\gamma\equiv\gamma_1(\mathrm{mod}\ \delta)$ салыштырууда $\gamma_1=0$ деп алсак, $a^{\gamma}\equiv a^{0}\equiv 1(\mathrm{mod}\ m)$ болот. Б.а. $\gamma\vdots\delta$ аткарылса, $a^{\gamma}\equiv 1(\mathrm{mod}\ m)$ болот.

Натыйжа 4. a санынын m модулу боюнча δ көрсөткүчү $\varphi(m)$ дин бөлүүчүсү болот. (Эгерде a баштапкы тамыр болсо, δ көрсөткүчү $\varphi(p)=p-1$ ди бөлөт.)

Далилдөө. Эйлердин теоремасынын негизинде $(a, m)=1$ болгондо $a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m)$ орун алат, тиешелүү δ көрсөткүчтүн аныктоосу боюнча $\delta\le\varphi(m)$ аткарылат. Демек, эгерде δ көрсөткүчтү табуу керек болсо, анда $1=a^{0}, a^{1}, a^{2}, \ldots, a^{\delta-1}$ системасындагы даражалардын бардыгын эсептеп отуруштун зарылчылыгы калбайт экен, анын ордуна даража көрсөткүчү $\varphi(m)$ ди бөлө турган даражаларды эсептеп койгон жетиштүү болот.

Мисал 1. $\bar{5}$ саны 7 модулу боюнча тиешелүү болгон көрсөткүчтү табуу үчүн $\varphi(7)=6$ болгондуктан 1, 2, 3, 6 көрсөткүчтөрдү текшерген жетиштүү.

Мисал 2. 7 санын 17 модулу боюнча тиешелүү көрсөткүчү табылсын.

Чыгаруу. $\varphi(17)=16$ болгондуктан, анын бөлүүчүлөрү 1, 2, 4, 8, 16 болот. Ошондуктан төмөнкүлөрү гана эсептейбиз:

$7^1\equiv 7 \pmod{17}$, $7^2\equiv 49\equiv -2 \pmod{17}$, $7^4\equiv 4 \pmod{17}$,

$7^8\equiv 16\equiv -1 \pmod{17}$, $7^{16}\equiv 1 \pmod{17}$.

Демек, $\delta=16$, $\varphi(17)=\delta$ болгондуктан 7 саны 17 модулу боюнча баштапкы тамыр болот.

Натыйжа 5. Эгерде a саны m модулу боюнча δ көрсөткүчүнө тиешелүү болсо, a^k саны ушул модул боюнча $\frac{\delta}{(\delta,k)}$ көрсөткүчүнө тиешелүү болот.

Далилдөө. a^k саны m модулу боюнча γ көрсөткүчүнө тиешелүү болсун, б.а. $a^{k\gamma}\equiv 1 \pmod{m}$ орун алсын. 1-натыйжанын негизинде бул салыштыруу $k\gamma\equiv 0 \pmod{\delta}$ орун алганда жана ушул учурда гана орун алат. Салыштыруунун төмөндөгүдөй касиетин эске алсак:

$$ad\equiv bd \pmod{m} \Rightarrow a\equiv b\left(\mod \frac{m}{(d,m)}\right),$$

анда $$k\gamma\equiv 0 \pmod{\delta} \Rightarrow \gamma\equiv 0\left(\mod \frac{\delta}{(\delta,k)}\right)$$

келип чыгат. Натыйжа далилденди.

Натыйжа 6. Эгерде $(\delta,\ k)=1$ болсо, a^k дагы δ көрсөткүчүнө тиешелүү болот.

Мисал. 3 саны 7 модулу боюнча 6 көрсөткүчүнө тиешелүү болгон эле. $3^4=81$ саны да 7 модулу боюнча 3 көрсөткүчүнө тиешелүү болот, себеби $\frac{6}{(6,4)}=\frac{6}{2}=3$. Чындыгында

$81\equiv -3 \pmod 7$, $81^2\equiv 2 \pmod 7$, $81^3\equiv 1 \pmod 7$.

§12. **Индекстер жана алардын касиеттери**

Биз жогоруда ар кандай p (p – жөнөкөй сан) модулу боюнча баштапкы тамыр жашашын көрсөткөн элек. Белгилүү болгондой g саны p модулу боюнча баштапкы тамыр болсо, анда

$$g^0, g^1, g^2, g^3, \ldots, g^{p-2} \qquad (1)$$

сандардын удаалаштыгы ушул p модулу боюнча чегериштердин келтирилген системасын түзөт. (1) катардын мүчөлөрү p менен өз ара жөнөкөй болушуп, алар p модулу боюнча $\varphi(p)=p-1$ класстын өкүлдөрү болот. Демек, эгерде $(a, p)=1$ болсо, анда (1) катарда p модулу боюнча a саны менен салыштырылуучу жалгыз элемент табылат, б.а.

$$a \equiv g^{\gamma} (\mathrm{mod}\ p) \qquad (2)$$

салыштыруу орун алат, мында $0<\gamma\leq p-2$.

Def 1. Эгерде g саны p модулу боюнча баштапкы тамыр болуп, $(a, p)=1$ болгондо (2) салыштыруу орун алса, $0\leq\gamma$ саны a санынын p модулу боюнча g негизине карата индекси деп аталат жана $\gamma=\mathrm{ind}_g a$ аркылуу белгиленет.

Эгерде a санынын негизи мурдатан берилген болсо, анда a нын индекси $\mathrm{ind}\, a$ аркылуу белгиленет.

Бул аныктоону пайдаланып, (2)ни төмөндөгүдөй жазууга болот:

$$a \equiv g^{\mathrm{ind}\, a} (\mathrm{mod} m). \qquad (3)$$

Жогорудагылардын негизинде $(a, p)=1$ шартын канааттандыруучу ар бир a саны g негиз боюнча

$$0, 1, 2, 3, \ldots, p-2 \qquad (4)$$

сандарынын бирөөсү менен аныкталуучу индекске ээ. Негиздин өзгөрүүсү менен индекс дагы жалпысынан өзгөрөт. Мисалы, 7 модулу боюнча 1, 2, 3, 4, 5, 6 сандары жана алар менен берилген 7 модулу боюнча салыштырылуучу бардык сандар 3 негизге карата

$3^0 \equiv 1 (\text{mod } 7)$, $3^2 \equiv 2 (\text{mod } 7)$, $3 \equiv 3 (\text{mod } 7)$, $3^4 \equiv 4 (\text{mod } 7)$,

$3^5 \equiv 12 \equiv 5 (\text{mod } 7)$, $3^3 \equiv 6 \equiv -1 (\text{mod } 7)$,

болгондуктан, тиешелүү түрдө 0, 2, 1, 4, 5, 3 индекстерге ээ. Эгерде негизи a=5 болсо, анда

$5 \equiv 5 (\text{mod } 7)$, $5^2 \equiv 25 \equiv 4 (\text{mod } 7)$, $5^3 \equiv 20 \equiv 6 (\text{mod } 7)$,

$5^4 \equiv 16 \equiv 2 (\text{mod } 7)$, $5^5 \equiv 3 (\text{mod } 7)$, $5^6 \equiv 1 (\text{mod } 7)$.

болгондуктан, 5 негизи боюнча түзүлгөн индекстер тиешелүү түрдө 0, 4, 5, 2, 1, 3 болот.

g саны p модулу боюнча баштапкы тамыр болгондуктан, башгапкы тамырдын аныктоосу боюнча

$$g^{p-1} \equiv 1 (\text{mod } p) \tag{5}$$

салыштыруусу орун алат. Бул салыштыруунун эки жагын k>0 даражага көтөрөбүз:

$$1 \equiv g^{k(p-1)} (\text{mod } p). \tag{6}$$

(2) жана (6) салыштырууларды мүчөлөп көбөйтөбүз :

$$a \equiv g^{\gamma + k(p-1)} (\text{mod } p). \tag{7}$$

(7) салыштыруудан (a, p)=1 шартын канааттандыруучу ар бир a саны g баштапкы тамыры боюнча чексиз индекске ээ экендигин көрөбүз. Бул индекстердин бардыгы

$$g^{\gamma} \equiv g^{\gamma_1} (\text{mod } p) \tag{8}$$

шартын канааттандырат. Мурдагы параграфтагы 3-теореманын негизинде (8)нин орун алышы үчүн

$$\gamma \equiv \gamma_1 (\text{mod } p-1) \tag{9}$$

шартынын аткарылышы зарыл жана жетиштүү. Демек, p модулу боюнча түзүлгөн жана p менен өз ара жөнөкөй болгон ар бир класска (9) салыштыруу менен аныкталуучу индекстердин көптүгү туура келет жана тескерисинче.

Эгерде $a \equiv b (\text{mod } p)$ болсо, анда жогорудагылардын негизинде

$$\text{ind } a \equiv \text{ind } b (\text{mod } p-1), \tag{10}$$

болот.

(2) жана (3) түн негизинде

$$g^{\gamma} \equiv g^{\operatorname{ind} a} (\operatorname{mod} p). \qquad (11)$$

Мындан

$$\gamma \equiv \operatorname{ind} a (\operatorname{mod} p-1), \qquad (12)$$

келип чыгат.

Касиеттери.

1^0. Көбөйтүндүнүн индекси p–1 модулу боюнча көбөйтүчүлөрдүн индекстеринин суммасы менен салыштырылат:

$$\operatorname{ind} ab\ldots k \equiv \operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} k (\operatorname{mod} p-1).$$

Далилдөө. Индекстин аныктоосу боюнча, төмөнкү салыштырууларды жазып алабыз:

$$a \equiv g^{\operatorname{ind} a} (\operatorname{mod} p),$$

$$b \equiv g^{\operatorname{ind} b} (\operatorname{mod} p),$$

...

$$k \equiv g^{\operatorname{ind} k} (\operatorname{mod} p).$$

Буларды мүчөлөп көбөйтөбүз. Анда

$ab...k \equiv g^{\operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} k} (\operatorname{mod} p)$ келип чыгат. Мындан, (2) жана (12) нин негизинде,

$$\operatorname{ind} ab\ldots k \equiv \operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} k (\operatorname{mod} p-1). \qquad (13)$$

келип чыгат.

2^0. Натуралдык көрсөткүчкө ээ болгон даражанын индекси p–1 модулу боюнча негиздин индекси менен даража көрсөткүчүнүн көбөйтүндүсүнө тең калдыктуу болот, б.а.

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a (\operatorname{mod} p-1).$$

Далилдөө. Айталы, $a=b=c=\ldots=k$ болсун. Анда 1^0 дин негизинде

$$\operatorname{ind} aa\ldots a \equiv \operatorname{ind} a + \operatorname{ind} a + \ldots + \operatorname{ind} a (\operatorname{mod} p-1)$$

же

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a (\operatorname{mod} p-1)$$ болот.

3^0. p каалагандай жөнөкөй сан болгондо бирдин индекси p–1 модулу боюнча нөл менен, g негизинин индекси болсо 1 менен тең калдыктуу болот.

Далилдөө. Чындыгында, $g^0 \equiv 1 (\mathrm{mod}\, p)$ жана $g^1 \equiv g (\mathrm{mod}\, p)$ болгондуктан $\mathrm{ind}\, 1 \equiv 0 (\mathrm{mod}\ p-1)$ жана $\mathrm{ind}\, g \equiv 1 (\mathrm{mod}\, p-1)$ болот. Демек, индекстер дагы логарифмдер сыяктуу касиеттерге ээ болот экен.

Индекстердин жадыбалы

Логарифмдердин жадыбалы сыяктуу, p модулу боюнча индекстердин жадыбалын түзүгө болот. Индекстердин негизи катарында p санынын ар бир баштапкы тамыры алынат. Алгачкы индекстер жадыбалын улуу орус окумуштуусу М.В. Остроградский түзгөн. Ал 1837 жылы 200го чейинки p модулдар үчүн индекстердин жадыбалын түзгөн. Бүгүнкү күндө мындай жадыбалдарды ЭЭМдин жардамында каалаган санга чейинки p модулдар үчүн түзүүгө болот.

Ар бир жадыбал эки бөлүктөн:

1) берилген N саны боюнча I индексти табуу;

2) Берилген I индекс боюнча N санды табуудан турат.

Кандайдыр бир p модул боюнча индекстердин жадыбалын түзүү үчүн:

1) p модулу боюнча g баштапкы тамыр табылат;

2) g^0, g^1, …, g^{p-2} даражалары p модулу боюнча эң кичине оң чегериштерге алмаштырылат.

Мисалы, p=11 боюнча индекстер жана аларга туура келген сандар жадыбалын түзөбүз:

2, 6, 7, 8 сандары 11 модулу боюнча баштапкы тамырлар болот. Чындыгында $\varphi(11)=10$ болгондуктан

$2^1 \equiv 2 (\mathrm{mod}\ 11)$, $2^2 \equiv 4 (\mathrm{mod}\ 11)$, $2^3 \equiv 8 (\mathrm{mod}\ 11)$, $2^4 \equiv 16 \equiv 5 (\mathrm{mod}\ 11)$,

$2^5 \equiv 10 (\mathrm{mod}\ 11)$, $2^6 \equiv 9 (\mathrm{mod}\ 11)$, $2^7 \equiv 7 (\mathrm{mod}\ 11)$, $2^8 \equiv 3 (\mathrm{mod}\ 11)$,

$2^9 \equiv 6 (\mathrm{mod}\ 11)$, $2^{10} \equiv 1 (\mathrm{mod}\ 11)$,

салыштырууларынын негизинде 2 баштапкы тамыр болот. Ошондой эле

$6^1 \equiv 6 \pmod{11}$, $6^2 \equiv 3 \pmod{11}$, $6^3 \equiv 7 \pmod{11}$, $6^5 \equiv -1 \pmod{11}$, $6^{10} \equiv 1 \pmod{11}$

орун алгандыктан, 11 модулу боюнча 6 дагы баштапкы тамыр болот.

Негиз 2 болгондо төмөнкү жадыбалды түзөбүз

N	1	2	3	4	5	6	7	8	9	10
I	10	1	8	2	4	9	7	3	6	5

I	1	2	3	4	5	6	7	8	9	10
N	2	4	8	5	10	9	7	3	6	1

Биринчи жадыбалдын жардамында сан боюнча индекс табылат. Экинчи жадыбал боюнча индекске карап, сан табылат.

p=43 модул боюнча 3, 5, 12, 18, 19, 20, 26, 28, 30, 33, 34 сандары баштапкы тамырлар болот. q=28 болгондо төмөнкү жадыбалга ээ болобуз:

I

N	0	1	2	3	4	5	6	7	8	9
0		42	39	17	36	5	4	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	5
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	14
3	16	18	31	8	9	37	4	26	40	2
4	13	20	1							

Жадыбалдагы жолчолор жана мамычалар тиешелүү түрдө сандын (индекстин) оңдук жана бирдик каанасын билдирет, алардын кесилишкен жеринде изделүү индекс (сан) турат.

Мисал 1. 37 санынын 43 модулу боюнча индекси табылсын.

Чыгаруу. I үчүн түзүлгөн жадыбалдан 4-жолчо жана 8-мамыча кесилишкен жерде 35 саны жайгашкан. Демек, $ind_{28}37=35$.

Мисал 2. 43 модулу боюнча индекси 18 болгон сан табылсын.

Чыгаруу. ind N=18(mod 43).

N үчүн түзүлгөн жадыбалдын 2-жолчо жана 9-мамычанын кесилишкен жерине 41 саны турат. Демек, N=41.

Эгерде изделүү сан (же индекс) жадыбалдагы эң чоң сандан да чоң болсо, анда бул сан каралып жаткан *p* же *p*–1 модул боюнча эң кичине оң чегериш менен алмаштырылып алынат.

Баштапкы тамырга ээ болгон ар кандай *m* модулу боюнча индекстердин жадыбалын түзүүгө болот. Себеби, мындай учурда да баштапкы тамырлардын даражалары *m* модулу боюнча чегериштердин келтирилген системасын түзөт.

§13. Салыштырууларды индекстердин жардамында чечүү

1. Эки мүчөлүү салыштыруулар. Индекстердин касиеттеринен пайдаланып, эки мүчөлүү салыштырууларды оңой эле чечүүгө болот. Эки мүчөлүү салыштырууларды чечүү үчүн берилген сан боюнча анын индекси (белгилүү негизге карата) жана тескерисинче берилген индекске карата, ага туура келүүчү санды табууга туура келет. Ушул себептен колдонмонун акырында тиркемеде 1ден 100 гө чейинки жөнөкөй сандардын индекстеринин жадыбалы келтирилген.

Айталы

$$ax^n \equiv b \pmod{p} \qquad (1)$$

салыштыруусу берилген болуп, $(a, p)=1$ болсун. Индекстер түшүнүгүн пайдаланып, (1)ди ага тең күчтүү болгон

$$\text{ind } a + n\,\text{ind}\,x \equiv \text{ind } b \pmod{p-1}$$

же

$$n\,\text{ind}\,x \equiv \text{ind } b - \text{ind } a \pmod{p-1} \qquad (2)$$

салыштыруу менен алмаштырабыз. ind$x$ ти белгисиз катарында карап, (2) салыштырууну чечебиз. Эгерде салыштыруу чечимге ээ болсо, төмөнкү эки учурдун бири болушу мүмкүн.

1-учур. $(n, p-1)=1$;

Бул учурда (2) салыштыруу ind$x$ ке карата жалгыз чечимге ээ болот.

2-учур. Эгерде ind$x=c$ чечим болсо, индекстер жадыбалынан пайдаланып, x табылат. x тин табылган мааниси p модул боюнча берилген салыштыруунун чечими болот

$$(n, p-1)=d>1.$$

Бул учур дагы эки учурга бөлүнөт:

а) ind b–ind$a$ саны d га бөлүнбөйт. Бул учурда салыштыруунун касиети боюнча (2) салыштыруу чечимге ээ болбойт. (1) жана (2) тең күчтүү болгондуктан, (1) дагы чечимге ээ болбойт.

б) ind b–ind$a$ саны d га бөлүнөт. Анда (2) салыштырууну төмөнкүдөй жазууга болот:

$$\frac{n}{d}\text{ind} \equiv \frac{\text{ind}b - \text{ind}a}{\text{d}}\left(\text{mod}\frac{p-1}{d}\right).$$

Бул жерде $\left(\frac{n}{d}, \frac{p-1}{d}\right)=1$ болгондуктан акыркы салыштыруу $\frac{p-1}{d}$ модул боюнча бир гана чечимге ээ болот. б.а. (2) салыштыруусу p–1 модул боюнча d чечимине ээ болот. Бул чечимдерди ind$x$ тер боюнча таап анан индекстер жадыбалы боюнча (1)дин чечимдерин табабыз.

Индекстер баштапкы тамырларга карата түзүлгөнү үчүн ар бир салыштыруунун чечимин албетте алгачкы берилген модул боюнча табуу керек. Себеби баштапкы тамырлар өзгөргөндө индекстер да өзгөрө тургандыгын жогоруда караганбыз.

Мисал. $x^5\equiv 14(\text{mod } 41)$ салыштыруунун чечими табылсын.
Чыгаруу. Салыштыруунун эки жагын индекстейбиз:

$$5\text{ind } x\equiv \text{ind}14(\text{mod } 40)$$

(колдонмонун акырындагы индекстердин жадыбалынан 41 модулу боюнча түзүлгөн жадыбал боюнча),

$$\text{ind}14=25,\ 5\text{ind } x\equiv 25(\text{mod } 40) \Rightarrow 5\text{ind } x\equiv 5(\text{mod } 8),\ (5, 40)=5$$

болгондуктан, берилген салыштыруу 41 модул боюнча 5 чечимге ээ болот. Бул чечимдер

$$\text{ind } x_1\equiv 5(\text{mod } 40),\ \text{ind } x_2\equiv 13(\text{mod } 40),\ \text{ind } x_3\equiv 21(\text{mod } 40),$$
$$\text{ind } x_4\equiv 29(\text{mod } 40),\ \text{ind } x_5\equiv 37(\text{mod } 40),$$

индекстеринен келип чыгат жана төмөндөгүдөй болушат:

$$x_1\equiv 27(\text{mod } 41),\ x_2\equiv 24(\text{mod } 41),\ x_3\equiv 35(\text{mod } 41),$$
$$x_4\equiv 22(\text{mod } 41),\ x_5\equiv 15(\text{mod } 41).$$

2. $x^n\equiv a(\text{mod } p)$ салыштыруусунун чечилүү критерийи

$x^n\equiv a(\text{mod } p)$ салыштыруусунун эки жагын тең индекстейбиз:

$$n\text{ind}x \equiv \text{ind}\, a \pmod{p-1} \qquad (4)$$

$(n, p-1)=d$ болгондо (4) салыштыруунун чечимге ээ болушу үчүн ind$a$ санынын d га бөлүнүшү зарыл жана жетиштүү б.а.

$$\text{ind}a \equiv 0 \pmod{d} \qquad (5)$$

орун алуусу зарыл. (5)ти p жана q аркылуу туюнтабыз:

Ал үчүн (5)тин эки жагын жана d ны $\frac{p-1}{d}$ га көбөйтөбүз. Анда

(5) салыштыруу

$$\frac{p-1}{d}\text{ind}a \equiv 0(\text{mod}\, p-1)$$

көрүнүшүнө келет. Индекстерди пайдаланып, акыркы салыштырууну

$$\text{ind}a^{\frac{p-1}{d}} \equiv 0(\text{mod}\, p-1)$$

көрүнүшүндө жазабыз. $0 \equiv \text{ind}\, 1 \pmod{p-1}$ болгондуктан жана жогорудагы салыштыруунун негизинде

$$a^{\frac{p-1}{d}} \equiv 1(\text{mod}\, p) \qquad (6)$$

келип чыгат.

(6) шарт – (3) салыштыруунун чечилүү критерийи болот.

(6) шарттан $n=2$ болгондо бизге белгилүү болгон Эйлердин критерийи келип чыгат. Чындыгында, p – так жана жөнөкөй сан болгондуктан $d=(2, p-1)=2$ болот жана (6) шарт $a^{\frac{p-1}{2}} \equiv 1(\text{mod}\, p)$ көрүнүшүнө келет. Бул болсо, $x^2 \equiv a \pmod{p}$ салыштыруусунун чечилүү критерийи.

Өз алдынча иштөө үчүн көнүгүүлөр

p модулу боюнча g баштапкы тамырыларынын индекстер жадыбалын түзгүлө [1-27]:

1) $p=73$, $g=5$; 2) $p=71$, $g=7$; 3) $p=67$, $g=2$;
4) $p=61$, $g=2$; 5) $p=59$, $g=2$; 6) $p=53$, $g=2$;
7) $p=47$, $g=5$; 8) $p=43$, $g=3$; 9) $p=41$, $g=6$;
10) $p=37$, $g=2$; 11) $p=31$, $g=3$; 12) $p=29$, $g=2$;

13) $p = 23,\ g = 5$; 14) $p = 19,\ g = 2$; 15) $p = 17,\ g = 3$;
16) $p = 13,\ g = 2$; 17) $p = 11,\ g = 2$; 18) $p = 17,\ g = 5$;
19) $p = 23,\ g = 7$; 20) $p = 19,\ g = 3$; 21) $p = 7,\ g = 3$;
22) $p = 7,\ g = 5$; 23) $p = 19,\ g = 10$; 24) $p = 17,\ g = 6$;
25) $p = 29,\ g = 3$; 26) $p = 27,\ g = 2$; 27) $p = 27,\ g = 6$.

Индекстердин жардамында салыштырууларды чыгаргыла [28-51]:

28) $5x^{23} \equiv 8(\mod 31)$;
29) $14x^{9} \equiv 3(\mod 59)$;
30) $12x^{32} \equiv 7(\mod 41)$;
31) $8x^{14} \equiv 10(\mod 43)$;
32) $2x^{45} \equiv 32(\mod 37)$;
33) $32\,x^{3} \equiv 5(\mod 19)$;
34) $54x^{14} \equiv 3(\mod 13)$;
35) $35\,x^{24} \equiv 1(\mod 5)$;
36) $17x^{21} \equiv 23(\mod 13)$;
37) $61x^{35} \equiv 32(\mod 17)$;
38) $4\,x^{8} \equiv 32(\mod 73)$;
39) $47x^{27} \equiv 38(\mod 17)$;
40) $37x^{5} \equiv 5(\mod 19)$;
41) $2x^{45} \equiv 7(\mod 11)$;
42) $45x^{62} \equiv 3(\mod 13)$;
43) $29x^{52} \equiv 53(\mod 17)$;
44) $57x^{5} \equiv 14(\mod 11)$.
45) $35x^{32} \equiv 8(\mod 11)$;
46) $17x^{34} \equiv 11(\mod 47)$;
47) $24x^{34} \equiv 43(\mod 3)$;
48) $14x^{52} \equiv 3(\mod 7)$;
49) $35x^{34} \equiv 23(\mod 71)$;
50) $6x^{54} \equiv 50(\mod 7)$;
51) $123x^{12} \equiv 25(\mod 13)$;
52) $53x^{45} \equiv 74(\mod 17)$;

§14. **Эсептөө системалары**

Сандарды жазуу үчүн ар түрдүү эсептөө системаларынан колдонулат. Эсептөө системалары экиге бөлүнөт: позициондук жана позициондук эмес болуп.

1. Позициондук эмес эсептөө системасы. Бул эсептөө системасында колдонулган ар бир белгинин (цифранын) ээлеген орду маанига ээ эмес. Б.а. разряд (бирдик, ондук, жүздүк ж.б.у.с.) деген түшүнүк жок. Алардын айрымдарын келтиребиз:

а) Римдин эсептөө системасы. Анын базисин жети сан түзөт, алар {1, 5, 10, 50, 100, 500, 1000}. Алар төмөнкүдөй белгиленет:
I – I, 5 – V, 10 – X, 50 – L, 100 – C, 500 – D, 1000 – M.
Мисалы, 2011 – MMXI, 2496 – MMCDXCVI.
Демек, 2496 санын римдин эсептөө системасында жазуу үчүн эки минди M белгисин эки жолу, 400 дү CM, 90ду XC, 6ны VI белгилери менен жазуу керек экен. Алар төмөнкүдөй маанига ээ:
I – бир бармак, V – бир колдогу бармактар саны, X – эки колдогу бармактар саны, C – латынча centum (жуз), M – латынча mille (миң) сөздөрүнүн баш тамгалары.

б) Египеттин эсептөө системасы, анын базисин төрт сан түзөт, алар {1, 10, 100, 1000}. Алар төмөнкүдөй белгиленет:
1 – I, 10 – ∩, 100 – ʃ, 1000 – ρ.
Мисалы, бул системада 352 саны ʃʃʃ∩∩∩∩∩ I I көрүнүшүндө жазылган.

в) Славяндардын эсептөө системасы, анын базисин 27 сан түзөт, алар {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 200, 300, 400, 500, 600, 700, 800, 900}. Алар төмөнкүдөй белгиленет:

белгилениши	сан	белгилениши	сан	белгилениши	сан
А	1	И	10	Р	100
В	2	К	20	С	200
Г	3	Л	30	Т	300
Д	4	М	40	У	400
Е	5	Н	50	Ф	500
S	6	ξ	60	Х	600
З	7	О	70	ψ	700
І	8	П	80	ω	800
Ъ	9	Ч	90	Ц	900

Мисалы, славяндардын эсептөө системасында 352 саны ТНАА көрүнүшүндө жазылган.

2. Позициондук эсептөө системасы. Позициондук эсептөө системаларында колдонулган ар бир белгинин (цифранын) мааниси анын ээлеген ордуна көз каранды. Көбүнчө негизи фиксирленген позициондук эсептөө системалары колдонулат. Эсептөө системаларынын бардыгы жалпы бир принциптин негизинде курулат б.а. төмөнкү теорема орун алат:

Теорема 1. $(m>1)\in N$, $M=\{0, 1, 2,..., m-1\}$ көптүгү m модул боюнча чегериштердин толук системасы болсун, анда $\forall a\in N$ санын

$$a = a_0 + a_1 m + a_2 m^2 + ... + a_r m^r, \quad a_i \in M, i = \overline{0, r} \qquad (1)$$

көрүнүшүндө жазууга болот жана бул жазуу (ажыралма) жалгыз болот.

Далилдөө. Алгач (1) нин жашашын көрсөтөбүз. Далилдөөнү математикалык индукция принцибин жардамында жүргүзөбүз. $1\le a<m$ болгондо $a\in M$ болуп, $a=a$ биз издеген барабардык болот. Айталы (1) ажыралма a дан кичине болгон бардык натуралдык сандар үчүн орун алсын. Анда калдыктуу бөлүү принцибинин негизингде

$$a=mq+a_0, \ a_0\in M \qquad (2)$$

болот, мында $q<a$. Жогоруда биз (1) ажыралма a дан кичине болгон бардык натуралдык сандар үчүн орун алсын деп алдык. Ошондуктан

$$q=a_1+a_2m+\ldots+a_rm^{r-1} \tag{3}$$

ажыралма жашайт. (3)тү (2)ге коебуз:

$$a=m(a_1+a_2m+\ldots+a_rm^{r-1})+a_0=a_1+a_1m+\ldots+a_rm^r.$$

Демек, (1) ажыралма a саны үчүн да орун алат. Математикалык индукция принцибинин негизинде (1) ажыралма ар кандай натралдык сан үчүн да жашайт.

Def 1. $a\in N$ санынын (1) көрүнүшү анын m дин даражалары боюнча ажыралмасы деп аталат.

(1)дин жалгыздыгын далилдөө. Дагы математикалык индукция усулун колдонобуз. $a<m$ шартындагы a саны M көптүгүнүн бир гана элементине барабар болот. Айталы $a\geq m$, a санынын өзү үчүн (1) көрүнүшүндөгү ажыралма жалгыз болбосун:

$$a=b_0+b_1m+b_2m^2+\ldots+b_nm^n=b_0+\left(b_1+b_2m+\ldots+b_nm^{n-1}\right)m.$$

Бул барабардыкты

$$a=b_0+mq_1 \tag{4}$$

көрүнүшүндө жазып алабыз. Калдыктуу бөлүүнүн жалгыздыгынын негизинде (2)-(4) барабардыктардан төмөнкүнү алабыз:

$$a_0=b_0,\ q=q_1 \Rightarrow a_1+a_2m+\ldots+a_rm^{r-1}=b_1+b_2m+\ldots+b_nm^{n-1}.$$

Бирок $q<a$ жана $q_1<a$ болгондуктан, математикалык индукция усулунун негизинде $r=n$ жана $a_i=b_i$, $i=1,2,\ldots,r$. Демек, (1) ажыралма жалгыз экен.

m дик эсептөө системасында жазылган санды кыскача

$$(a_ra_{r-1}\ldots a_1a_0)_m$$

аркылуу белгилешет. Бул жазууда ар бир цифра өзүнүн орду менен мүнөздөлөт. Мисалы, 232де 2 саны эки жолу жолугат. Эгерде 10дук эсептөө системасы деп алсак, анда $232=2\cdot102+3\cdot10+2$ болот. Ошондуктан оң жакта турган 2

бирдикти, сол жактагы 2 жүздүктү билдирет. Эгерде mдик эсептөө системасы деп алсак, анда $232=2\cdot m^2+2\cdot m+2$ болот.

Мисал. 10дук эсептөө системасында берилген $a=120$ санын $m=2$ эсептөө системасында жазгыла.

Чыгаруу. $120=1\cdot 2^6+1\cdot 2^5+1\cdot 2^4+0\cdot 2^3+1\cdot 2^2+1\cdot 2+1\cdot 2^0$ болот.

Ошондуктан 120_{10} саны экилик эсептөө системасында $(1110111)_2$ көрүнүшүндө жазылат.

Каалагандай эсептөө системасы өзүнүн **негизи** менен мүнөздөлөт.

Def 2. Берилген системада цифраларды сүрөтөө үчүн колдонулуучу ар түрдүү белги жана символдордун саны эсептөө системасынын негизи деп аталат.

Эсептөө системасынын негизи үчүн бирден чоң болгон ар кандай натуралдык санды алууга болот. Мисалы 2, 3, 4, ж.б. Мындан, поцизиондук эсептөө системаларынын көптүгү чексиз экендиги келип чыгат. Эгерде $m=2, 3, 4,\ldots$ болсо, анда тиешелүү түрдө экилик, үчтүк, төртүк ж.б. эсептөө системасы деп аталат.

Негизи m болгон эсептөө системасында сандар

$$a_{n-1}\,q^{n-1}+a_{n-2}\,q^{n-2}+\ldots+a_1\,q^1+a_0\,q^0+a_{-1}\,q^{-1}+\ldots+a_{-m}\,q^{-m},$$

көрүнүшүндө жазылат, мында a_i ($i=n-1,\ n-2,\ldots,\ -m$) эсептөө системасынын цифралары; n жана m – тиешелүү түрдө сандын бүтүн жана бөлчөк разряддары.

Мисалы:

разряддар 3 2 1 0 – 1

сан 1 0 1 1, $1_2=1\cdot 2^3+0\cdot 2^2+1\cdot 2^1+1\cdot 2^0+1\cdot 2^{-1}$

разряддар 2 1 0 – 1 – 2

сан 2 7 6, 5 $2_8=2\cdot 8^2+7\cdot 8^1+6\cdot 8^0+5\cdot 8^{-1}+2\cdot 8^{-2}$

Практикада көбүнчө 2, 8 жана 16лык эсептөө системалары колдонулат:

- **экилик эсептөө системасы** (0, 1 цифралары гана колдонулат);
- **сегиздик эсептөө системасы** (0, 1, 2, 3, 4, 5, 6, 7 цифралары гана колдонулат);
- **он алтылык эсептөө системасы** (0, 1, 2, 3, 4, 5, 6, 7, 8, 9 цифралары жана A, B, C, D, E, F симолдору колдонулат).

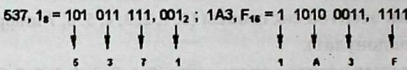
Бул эсептөө системаларындагы алгачкы сандарды жазып чыгабыз:

10дук	2лик	8дик	16лык
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9

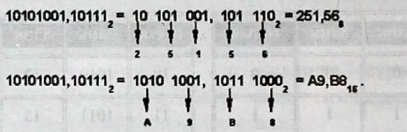
10дук	2лик	8дик	16лык
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F
16	10000	20	10
17	10001	21	11
18	10010	22	12
19	10011	23	13

Алардын ичинен эң жөнөкөй болгону бул экилик эсептөө системасы. 2лик эсептөө системасы компьютер үчүн ыңгайлуу, бирок адамзат үчүн 10дук эсептөө системасына салыштырганда татаал.

Сегиздик жана он алтылык эсептөө системасындагы сандарды экилик эсептөө системасына өткөрүү оңой. Мисалы

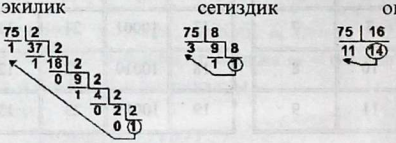


жана тескерисинче, экилик эсептөө системасындагы санды сегиздик жана он алтылык эсептөө системасына өткөрүү төмөндөгүдөй ишке ашат:



Кантип 10дук эсептөө системасындагы бүтүн санды негизи *m* болгон эсептөө системасына өткөрөбүз деген суроого мисал аркылуу жооп беребиз.

Мисал. 10дук эсептөө системасындагы 75 санын 2лик, 8дик жана 16лык эсептөө системасына өткөрөбүз:



Жооп: $75_{10}=1001011_2=113_8=EB_{16}$.

Демек, 10дук эсептөө системасындагы бүтүн санды негизи *m* болгон эсептөө системасына өткөрүү үчүн берилген санды *m*ге удаалаш бөлөбүз, калдык *m*ден кичине болгонго чейин. Пайда болгон калдыктарды тескерисинен (төмөндөн жогор

карай) жазуу менен негизи m болгон системадагы жаңы санды алабыз.

Мисал. $0,35_{10}$ санын 2лик, 8дик, 16лык эсептөө системасына өткөргүлө:

2ликте;

0,	35
	2
0	70
	2
1	40
	2
0	80
	2
1	60
	2
1	20

8дикте;

0,	35
	8
2	80
	8
6	40
	8
3	20

16лыкта

0,	35
	16
5	60
	16
9	60

жооп: $0,35_{10} = 0,01011_2 = 0,263_8 = 0,59_{16}$.

Экилик (сегиздик, он алтылык) эсептөө системасынан ондук системага өтүүнү карайбыз:

Мисал. $1011,1_2$; $276,52_8$; $1F3_{16}$ сандарын 10дук эсептөө системасына өткөргүлө.

Чыгаруу. Берилген сандардын үстүнө разряддарын жазып чыгабыз,

разряддар 3 2 1 0 – 1

сан 1 0 1 1, $1_2 = 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 + 1\cdot 2^{-1} = 11,5_{10}$

разряддар 2 1 0 – 1 – 2

сан 2 7 6, 5 $2_8 = 2\cdot 8^2 + 7\cdot 8^1 + 6\cdot 8^0 + 5\cdot 8^{-1} + 2\cdot 8^{-2} = 190,625_{10}$

разряддар 2 1 0

сан 1 F $3_{16} = 1\cdot 16^2 + 15\cdot 16^1 + 3\cdot 16^0 = 499_{10}$

Позициондук эсептөө системаларында жүргүзүлүүчү арифметикалык амалдар

2лик, 8дик, 16лык эсептөө системаларында кошуу, кемитүү, көбөйтүү бөлүү арифметикалык амалдарын карайбыз.

I. Кошуу амалы

2лик эсептөө системасында кошуу

+	0	1
0	0	1
1	1	10

8дик эсептөө системасында кошуу

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	10
2	2	3	4	5	6	7	10	11
3	3	4	5	6	7	10	11	12
4	4	5	6	7	10	11	12	13
5	5	6	7	10	11	12	13	14
6	6	7	10	11	12	13	14	15
7	7	10	11	12	13	14	15	16

16 лык эсептөө системасында кошуу

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10
2	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11
3	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12
4	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13
5	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14
6	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15
7	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16
8	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17
9	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18
A	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19
B	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A

C	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B
D	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C
E	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D
F	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E

Мисал 1. 10дук эсептөө системасындагы 15 жана 6 сандарын 2лик, 8дик, 16лык эсептөө системаларында суммасын тапкыла.
Чыгаруу. $15_{10}=1111_2=17_8=F_{16}$, $6_{10}=110_2=6_8=6_{16}$ болгондуктан,

10дукта

```
  1
+ 15
   6
  21
  | 5+6=11=10+1
  | 1+1=2
```

2ликте

```
  111
+ 1111
  0110
 10101
      | 1+0=1
      | 1+1=2=2+0
      | 1+1+1=3=2+1
      | 1+1=2=2+0
```

8дикте

```
  1
+ 17
   6
  25
  | 7+6=13=8+5
  | 1+1=2
```

16лыкта: $F_{16}+6_{16}$

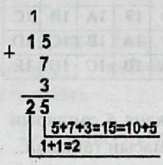
```
  1
+ F
   6
  15
  | 15+6=21=16+5
```

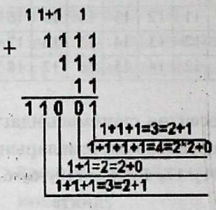
Жооп: $15+6=21_{10}=10101_2=25_8=15_{16}$.

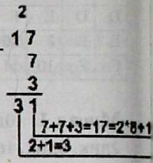
Текшерүү. Келип чыккан суммаларды 10дук эсептөө системасына өткөрөбүз:
$10101_2=2^4+2^2+2^0=16+4+1=21$,
$25_8=2\cdot8^1+5\cdot8^0=16+5=21$,
$15_{16}=1\cdot16_1+5\cdot16_0=16+5=21$.

Мисал 2. 10дук системада 15; 7 жана 3 сандарынын суммасын 2лик, 8дик, 16лык системаларда кошкула.
Чыгаруу.

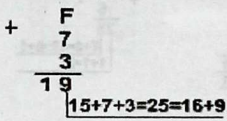
ондукта $15_{10}+7_{10}+3_{10}$ 2ликде $1111_2+111_2+11_2$ 8дикте $17_8+7_8+3_8$







16лыкта: $F_{16}+7_{16}+3_{16}$



Жооп: $5+7+3 = 25_{10} = 11001_2 = 31_8 = 19_{16}$.

Текшерүү:

$11001_2 = 2^4 + 2^3 + 2^0 = 16+8+1=25$,

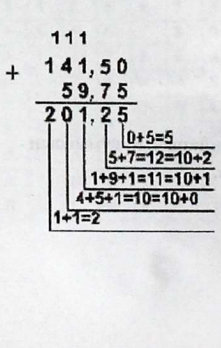
$31_8 = 3\cdot8^1 + 1\cdot8^0 = 24 + 1 = 25$,

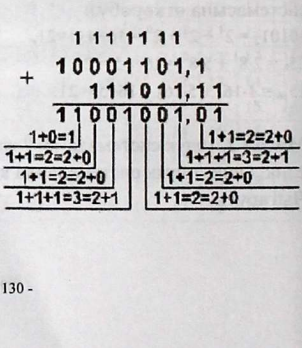
$19_{16} = 1\cdot16^1 + 9\cdot16^0 = 16+9 = 25$.

Мисал 3. 10дукта берилген 141,5 жана 59,75 сандарынын суммасын тапкыла.

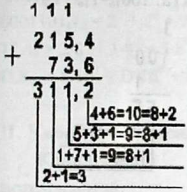
Чыгаруу.

10дукта $141,5_{10}+59,75_{10}$; 2ликте $10001101,1_2+111011,11_2$;

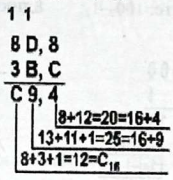




8дикте $215,4_8+73,6_8$



16лыкта $8D,8_{16}+3B,C_{16}$



Жооп: $141,5 + 59,75 = 201,25_{10} = 11001001,01_2 = 311,2_8 = C9,4_{16}$

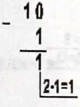
Текшерүү. $11001001,01_2$; $311,2_8$; $C9,4_{16}$ сандарын 10дукка өткөрөбүз:

$11001001,01_2 = 2^7 + 2^6 + 2^3 + 2^0 + 2^{-2} = 201,25;$
$311,2_8 = 3\cdot8^2 + 1\cdot8^1 + 1\cdot8^0 + 2\cdot8^{-1} = 201,25;$
$C9,4_{16} = 12\cdot16^1 + 9\cdot16^0 + 4\cdot16^{-1} = 201,25$.

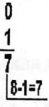
II. Кемитүү амалы

Мисал 4. 10_2; 10_8 жана 10_{16} сандарынан 1ди кемитебиз.

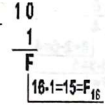
2ликте: $10_2–1_2$;



8дикте: $10_8–1_8$;

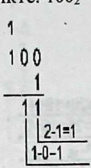


16лыкта: $10_{16}–1_{16}$.

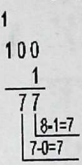


Мисал 5. 100_2; 100_8 жана 100_{16} сандарынан 1ди кемитебиз:

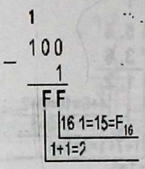
2ликте: 100_2-1_2;



8дикте: 100_8-1_8;



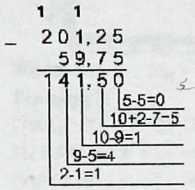
16лыкта: $100_{16}-1_{16}$.



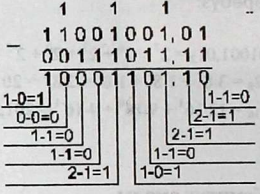
Жооп: $100_2-1_2=11_2$; $100_8-1_8=77_8$; $100_{16}-1_{16}=FF_{16}$.

Мисал 6. $201,25_{10}$ санынан $59,75_{10}$ санын кемиткиле.

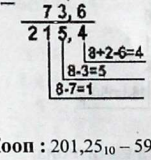
10дукта: $201,25_{10} - 59,75_{10}$;



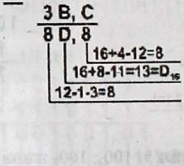
2ликте: $11001001,01_2-111011,11_2$



8дикте: $311,2_8-73,6_8$;



16лыкта: $C9,4_{16}-3B,C_{16}$.



Жооп : $201,25_{10} - 59,75_{10} = 141,5_{10}$;

$11001001,01_2-111011,11_2=10001101,1_2$;

$311,2_8-73,6_8= 215,4_8$;

$C9,4_{16}-3B,C_{16}= 8D,8_{16}$.

Тешерүү.

$10001101,1_2 = 2^7 + 2^3 + 2^2 + 2^0 + 2^{-1} = 141,5;$

$215,4_8 = 2 \cdot 8^2 + 1 \cdot 8^1 + 5 \cdot 8^0 + 4 \cdot 8^{-1} = 141,5;$

$8D,8_{16} = 8 \cdot 16^1 + D \cdot 16^0 + 8 \cdot 16^{-1} = 141,5.$

III. Көбөйтүү амалы

Каалагандай натуралдык санды m-дик эсептөө системасында

$$a = a_0 m^0 + a_1 m^1 + ... + a_r m^r + 0 m^{r+1} + ... = \sum_{i=0}^{\infty} a_i m^i$$

көрүнүшүндө жазып алып, көп мүчөнү көп мүчөгө көбөйткөндөй көбөйтөбүз. Эгерде коэффициенттерди көбөйтүүдө эсептөө системасынын негизинен чоң сан пайда болсо, анда негиз боюнча эң кичине оң чегериш алынат жана негизге эселүү болгон сан ушул сандан кейин келе турган цифрага кошулат. Көбөйтүү амалы да жадыбалдын жардамында жүргүзүлөт. Мисалы, 2лик, 8 дик жана 16лык эсептөө системаларында көбөйтүү жадыбалы төмөнкүчө аныкталат:

2лик эсептөө системасында көбөйтүү

×	0	1
0	0	0
1	0	1

8дик эсептөө системасында көбөйтүү

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	10	12	14	16
3	0	3	6	11	14	17	22	25
4	0	4	10	14	20	24	30	34

5	0	5	12	17	24	31	36	43
6	0	6	14	22	30	36	44	52
7	0	7	16	25	34	43	52	61

16 лык эсептөө системасында көбөйтүү

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	10	12	14	16	18	1A	1C	1E
3	0	3	6	9	C	F	12	15	18	1B	1E	21	24	27	2A	2D
4	0	4	8	C	10	14	18	1C	20	24	28	2C	30	34	38	3C
5	0	5	A	F	14	19	1E	23	28	2D	32	37	3C	41	46	4B
6	0	6	C	12	18	1E	24	2A	30	36	3C	42	48	4E	54	5A
7	0	7	E	15	1C	23	2A	31	38	3F	46	4D	54	5B	62	69
8	0	8	10	18	20	28	30	38	40	48	50	58	60	68	70	78
9	0	9	12	1B	24	2D	36	3F	48	51	5A	63	6C	75	7E	87
A	0	A	14	1E	28	32	3C	46	50	5A	64	6E	78	82	8C	96
B	0	B	16	21	2C	37	42	4D	58	63	6E	79	84	8F	9A	A5
C	0	C	18	24	30	3C	48	54	60	6C	78	84	90	9C	A8	B4
D	0	D	1A	27	34	41	4E	5B	68	75	82	8F	9C	A9	B6	C3
E	0	E	1C	2A	38	46	54	62	70	7E	8C	9A	A8	B6	C4	D2
F	0	F	1E	2D	3C	4B	5A	69	78	87	96	A5	B4	C3	D2	E1

Мисал.

1) $100111_2 \times 1000111_2 = 101011010001_2$;

2) $1170{,}64_8 \times 46{,}3_8 = 57334{,}134_8$;

3) $61{,}A_{16} \times 40{,}D_{16} = 18B7{,}52_{16}$.

× 100111	× 1170,64	× 61,A
1000111	46,3	40,D
+ 100111	+ 355 234	+ 4F 52
+ 100111	+ 7324 70	1868
+ 100111	47432 0	18B7,52
100111	57334,134	
101011010001		

IV. Бөлүү амалы 10дук эсептөө системасындагы бөлүү амалы сыяктуу аткарылат. Бөлүү учурунда көбөйтүү жадыбалын пайдалануу эсептөөнү жеңилдетет.

Өз алдынча иштөө үчүн көнүгүүлөр

1) Кайсы эсептөө системада 21 + 24 = 100 орун алат?
Чыгаруу. Мейли x – изделүүчү эсептөө системасынын негизи болсун. Анда $100_x = 1\cdot x^2 + 0\cdot x^1 + 0\cdot x^0$, $21_x = 2\cdot x^1 + 1\cdot x^0$, $24_x = 2\cdot x^1 + 4\cdot x^0$. Мындан, $x^2 = 2x + 2x + 5$ же $x^2 - 4x - 5 = 0$ келип чыгат. Бул квадраттык теңдеме эки тамырга ээ $x_1 = -1$, $x_2 = 5$. Оң тамырын (x=5) ти алабыз.
Жооп. 5тик эсептөө системасында.
2) Кайсы эсептөө системасында төмөнкүлөр орун алат:

a) 20 + 25 = 100; b) 22 + 44 = 110?

3) Эгерде $59_{10} = 214_x$ болсо, x ти тапкыла.
4) Төмөнкү сандарды 10дук эсептөө системасына өткөргүлө жана текшергиле:

a) 1011011_2;	f) 517_8;	l) $1F_{16}$;
b) 10110111_2;	g) 1010_8;	m) ABC_{16};
c) 011100001_2;	h) 1234_8;	n) 1010_{16};
d) $0,1000110_2$;	i) $0,34_8$;	o) $0,A4_{16}$;
e) $110100,11_2$;	к) $123,41_8$;	p) $1DE,C8_{16}$.

5) 10дук системасында берилген төмөнкү сандарды 2лик, 8дик, 16лык эсептөө системаларына өткөргүлө жана текшергиле:
a) 125_{10}; b) 229_{10}; c) 88_{10}; d) $37,25_{10}$; e) $206,125_{10}$.
6) 2лик системасында берилген төмөнкү сандарды 8дик жана 16лык эсептөө системаларына өткөргүлө жана текшергиле:

a) $1001111110111,0111_2$; d) $1011110011100,11_2$;
b) $1110101011,1011101_2$; e) $10111,1111101111_2$;

c) $10111001,101100111_2$; f) $1100010101,11001_2$.

7) 16лык эсептөө системасында берилген төмөнкү сандарды 2лик жана 8дик эсептөө системаларына өткөргүлө жана текшергиле:

a) $2CE_{16}$; b) $9F40_{16}$; c) $ABCDE_{16}$;

d) $1010,101_{16}$; e) $1ABC,9D_{16}$.

8) Көрсөтүлгөн аралыктагы бүтүн сандарды жазгыла:

a)2лик эсептөө системасында 101101_2 ден 110000_2 ге чейинки;

b) 3түк эсептөө системасында 202_3 ден 1000_3 ге чейинки;

c) 8дик эсептөө системасында 14_8 төн 20_8 га чейинки;

d) 16лык эсептөө системасында 28_{16} ден 30_{16} га чейинки.

Амалдарды аткаргыла [9-32]:

9) $((351_6 \cdot 14_6 - 1153_6 : 31_6 - 150_6) : 205_6) : 25_6$;

10) $((215_8 + 532_8) \cdot 16_8 - (11031_8 - 527_8) : 32_8) : 14775_8$;

11) $(3333_4 + 2222_4) \cdot 12_4 - (231020_4 + 3333333_4) : 23_4$;

12) $(4123_8 - 4221_8) \cdot 11_8 + (1222_8 + 773_8) : 3_8$; $3215_7 \cdot 24_7 -$
$- 11461_7 : 25_7 + 1532_7 - 115044_7$;

13) $(6325_7 + 456_7 - 150335_7 : 23_7 - 551_7) \cdot 5623_7$;

14) $120111_3 : 102_3 + (201_3 \cdot 12_3 - 11220_3) \cdot 20110_3$;

15) $(563_8 + 217_8) \cdot 15_8 + (2365_8 - 636_8) : 17_8 - 15122_8$;

16) $232011_5 : 104_5 + 1234_5 \cdot 322_5 - 122334_5$;

17) $23213_5 : 32_5 + 113_5 \cdot 34_5 - 15643_5$;

18) $20671_8 : 131_8 - 23765_8 + 53241_8 \cdot 453_8$;

19) $(425_6 \cdot 54_6 - 531_6 \cdot 43_6) : 245_6 + 321453_6$;

20) $150335_7 : 23_7 + 2341152_7 \cdot 321_7 - 23142_7$;

21) $11111101_2 : 10111_2 + 1100101_2 \cdot 1011_2 - 1010101_2$;

22) $33162_8 : 457_8 - 3422_8 + 1232145_8 \cdot 3452_8$;

23) $1111000111_2 : 10101_2 + 1011001_2 \cdot 101_2 - 100101_2$;

24) $1141043_5 : 23_5 + 23411_5 \cdot 32_5 - 34231_5$;

25) $471222_8 : 27_8 + 432564_8 \cdot 23134_8 - 345214_8$;

26) $51(10)3406_{11} : 548_{11} + 98(10)12_{11} \cdot 1232_{11} - 234219_{11}$;

27) $2032_4 : 22_4 + 33211_4 \cdot 3221_4 - 321121_4) \cdot 21_4$;

28) $1452_5 + 1141043_5 : 23_5 - 23411_5 \cdot 132_5$;

29) $1221_4 - 31214 \cdot 223_4 + 2032_4 : 22_4$;

30) $21120_3 + 20112_3 \cdot 2213 - 120111_3 : 102_3$;

31) $3452_6 \cdot 4354_6 + 1153_6 : 31_6 - 52341_6$;

32) $57623_8 \cdot 5634_8 - 3527_8 + 20671_8 : 131_8$.

a натуралдык санын *n* негизинен *m* жана *k* негиздерине өткөргүлө [33-57]:

33) $a = 124352$; $n = 6$; $m = 7$; $k = 12$.

34) $a = 675438$; $n = 9$; $m = 5$; $k = 11$.

35) $a = 8709546$; $n = 11$; $m = 3$; $k = 13$.

36) $a = 6738(10)4$; $n = 12$; $m = 2$; $k = 14$.

37) $a = 5643432$; $n = 7$; $m = 4$; $k = 8$.

38) $a = 87854632$; $n = 9$; $m = 5$; $k = 10$.

39) $a = 3421342$; $n = 5$; $m = 3$; $k = 7$.

40) $a = 234123564$; $n = 7$; $m = 5$; $k = 8$.

41) $a = 7564352$; $n = 8$; $m = 9$; $k = 4$.

42) $a = 1221221$; $n = 3$; $m = 2$; $k = 4$.

43) $a = 657332$; $n = 8$; $m = 6$; $k = 9$.

44) $a = 7756435$; $n = 8$; $m = 3$; $k = 10$.

45) $a = 23433213$; $n = 6$; $m = 4$; $k = 11$.

46) $a = 34554365$; $n = 8$; $m = 5$; $k = 12$.

47) $a = 445434$; $n = 7$; $m = 4$; $k = 8$.

48) $a = 6554543$; $n = 9$; $m = 5$; $k = 13$.

49) $a = 2245436$; $n = 8$; $m = 6$; $k = 11$.

50) $a = 343454$; $n = 7$; $m = 4$; $k = 9$.

51) $a = 567767$; $n = 9$; $m = 7$; $k = 12$.

52) $a = 765654$; $n = 8$; $m = 4$; $k = 9$.

53) $a = 54775$; $n = 8$; $m = 3$; $k = 11$.

54) $a = 42112$; $n = 7$; $m = 4$; $k = 9$.

55) $a = 153422$; $n = 6$; $m = 3$; $k = 7$.

56) $a = 7(11)761$; $n = 12$; $m = 9$; $k = 13$.

57) $a = 10(10)89$; $n = 11$; $m = 8$; $k = 129$.

§15. Салыштыруулардын колдонулуштары

1. $ax+by=c$, $(a, b, c\in Z)$ (1)

теңдемесинин бүтүн тамырларын табуу.

Эгерде $(a, b)=1$ болсо, анда (1) теңдеме бүтүн тамырларга ээ болот, алар жалпы учурда $x=x_1+bt$, $y=y_1-at$ көрүнүшүндө болушат же b терс болгондо төмөнкүдөй жазуу ыңгайлуу болот: $x=x_1-bt$, $y=y_1+at$.

Бул формулалардагы x_1, y_1 – теңдеменин бүтүн жекече чечимдери, t – каалагандай бүтүн сан.

Эгерде $(a, b)=d>1$ жана c саны d га бөлүнбөсө, анда $ax+by=c$ теңдемеси бүтүн тамырларга ээ болбойт.

Салыштыруулардын жардамында бул теңдеменин бүтүн тамырлары төмөндөгүдөй табылат:

$$ax+by=c$$

теңдемеден $ax\equiv c \pmod b$ салыштырууну жазып алабыз, мында b нын оң маанисин алынат. Салыштырууну канаатандырган x тин мааниси x_1 ге ыйгарылат, ал эми y тин мааниси x_1 дин маанисин теңдемеге x тин ордуна коюу менен түздөн түз аныкталат.

Мисал. $3x+4y=13$ теңдемени бүтүн тамырларын тапкыла.

Чыгаруу. $(3, 4)=1$ болгондуктан, теңдеменин бүтүн тамырлары жашайт. Теңдемеден $3x\equiv 13 \pmod 4$ салыштыруусуна ээ болобуз. 4 модулу боюнча чегериштердин $\{0, 1, 2, 3\}$ толук системасынан $x_1=3$тү табабыз. Анда $9+4y=13$ болот, мындан $y_1=1$ келип чыгат. Демек, $x=3+4t$, $y=1-3t$, $t\in Z$ болот.

2. Бөлүнүүчүлүк сынамалары

Бүтүн сандардын көптүгүнө тиешелүү болгон каалагандай N жана $m>1$ сандары берилген болсун. Көпчүлүк учурда N санын m ге бөлүүдөн келип чыккан эң кичине калдыкты табуу талап кылынат. Бул маселени чечүүнү жалпы усулун алгач француз математиги Б.Паскаль көрсөткөн. Биз азыр бул

усулду ондук, жүздүк жана миңдик эсептөө системалары үчүн баяндайбыз.

Айталы N натуралдык саны ондук эсептөө системасында берилген болсун. Анда N санын

$$N=a_0+a_1 10+a_2 10^2+\ldots+a_n 10^n$$

көрүнүшүндө жазууга болот. 10^k санынын m модул боюнча тиешелүү болгон чегериштеринин классынын абсолюттук эң кичине чегериши r_k болсун, б.а. $10^k \equiv r_k \pmod m \left(k=\overline{0,n},\ r_0=1\right)$ болсун. Анда N санын төмөнкүчө жазууга мүмкүн:

$$N\equiv a_0r_0+a_1r_1+a_2r_2+\ldots+a_nr_n \pmod m. \qquad (2)$$

Эерде $R_m= a_0r_0+a_1r_1+a_2r_2+\ldots+a_nr_n$ деп алсак, анда (2) төмөнкүдөй көрүнүшкө келет:

$$N\equiv R_m \pmod m.$$

Ушинтип, N саны өзүнөн кичине болгон R_m саны менен алмаштырылат. Б.а., (2) салыштыруу ондук системада Паскалдын бөлүнүүчүлүк сынамасын берет ($R_m=0$ болсо, N саны m ге калдыксыз бөлүнөтже r калдык $R_m\neq 0$гө барабар болот).Төмөнкү жекече учурларды карап чыгабыз:

1) $m=9$ болсун, б.а. биз азыр каалагандай натуралдык сандын 9 га бөлүнүүчүлүк белгисин (сынамасын) келтирип чыгарабыз.

$10\equiv 1 \pmod 9$ салыштыруунун эки жагын k-даражага көтөрөбүз:

$10^k\equiv 1 \pmod 9$. Демек, $r_k=1$, $k=0,1,\ldots,n$. Анда, R_m төмөнкү көрүнүшкө келет:

$$R_9=a_0+a_1+\ldots+a_n.$$

Бул сынама (белги) бизге белгилүү.

Демек, берилген сан 9га бөлүнүшү үчүн ал сандын цифраларынын суммасы 9 га бөлүнүшү жетиштүү экен.

2) $m=11$ болсун. Анда $10\equiv -1 \pmod{11} \Rightarrow 10^k\equiv(-1)^k \pmod{11}$. Мындан $R_{11}=a_0+a_2+a_4+\ldots-(a_1+a_3+a_5+\ldots)$ барабардыгы келип чыгат.

Мисал. N=3568921 санын 11ге бөлгөндөгү калдык табылсын.

$$R_{11}=1+9+6+3-(2+8+5)\equiv 19-15\equiv 4 \pmod{11}.$$

Демек, 3568921 санын 11ге бөлгөндөгү калдык 4 кө барабар экен.

3) m=7 болсун. Анда

$10^0 \equiv 1 (\text{mod } 7)$, $10^1 \equiv 3 (\text{mod } 7)$, $10^2 \equiv 2 (\text{mod } 7)$, $10^3 \equiv -1 (\text{mod } 7)$,

$10^4 \equiv -3 (\text{mod } 7)$, $10^5 \equiv -2 (\text{mod } 7)$, $10^6 \equiv 1 (\text{mod } 7)$, ...

болот. Демек,

$$R_7 = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + \ldots$$

Айталы 10 саны m модулу боюнча δ көрсөткүчүнө тиешелүү болсун. Анда көрсөткүчтүн аныктоосу боюнча

$$10^{\delta} \equiv 1 (\text{mod } m)$$

болгондуктан, $r_{\delta}=1$ болуп, $r_{\delta+1}=r_1$, $r_{\delta+2}=r_2$,..., $r_{2\delta}=r_{\delta}=1$ болот. б.а. калдыктар δ - кадамдан соң кайталанат. Анда (2) төмөнкү көрүнүшкө келет:

$$R_m = a_0 + a_1 r_1 + a_2 r_2 + \ldots + a_{\delta-1} r_{\delta-1} + a_{\delta} + a_{\delta-1} r_1 + \ldots \ .$$

Бизге белгилүү болгондой сандарды каалаган эсептөө системасында жазууга болот.Айталы, эсептөө системасынын негизи 10^{δ} жана бул негизге карата N сандын ажыралмасы

$$N = d_0 + d_1 10^{\delta} + d_2 10^{2\delta} + \ldots + d_n 10^{n\delta} \qquad (2)$$

болсун. $(10^{\delta})^n \equiv 1 (\text{mod } m)$ болгондуктан (2) салыштыруу

$$N \equiv d_0 + d_1 + d_2 + \ldots + d_n (\text{mod } m)$$

көрүнүшүнө келет. Демек, негизи 10^{δ} болгон системадагы сандын mге бөлүнүүчүлүк белгиси 10дук эсептөө системасындагы 9га бөлүнүүчүлүк белгисиндей болот экен.

Мисал 1. N сандын 100дүк эсептөө системасында 11ге бөлүнүүчүлүк белгисин келтирип чыгаргыла.

Чыгаруу. N санынын 100дүк эсептөө системасындагы жазылышы

$$N = b_0 + b_1 100 + b_2 100^2 + b_3 100^3 + \ldots + b_n 100^n$$

болот, жана $100 \equiv 1 (\text{mod } 11)$, $100^k \equiv 1 (\text{mod } 11)$ болгондуктан,

$$N = b_0 + b_1 + b_2 + b_3 + \ldots + b_n (\text{mod } 11)$$

орун алат. Мындан $R_{11} = b_0 + b_1 + b_2 + b_3 + \ldots + b_n$ келип чыгат.

Мисал 2. Жогорудагы мисалды пайдаланып N=3568921 санын 100дүк эсептөө системасында 11ге бөлүүдөн пайда болгон калдыкты тапкыла.

Чыгаруу. $R_{11} = 21+89+56+3 \equiv 169 \equiv 4 \pmod{11}$ болгондуктан, калдык 4 болот.

Мисал 3. N=83576289 санын 1000дик эсептөө системасында 37ге бөлүүдөн пайда болгон калдык табылсын.

Чыгаруу. 10 саны m=37 модул боюнча 3 көрсөткүчүнө тиешелүү, б.а. $10^3 \equiv 1 \pmod{37}$. Ошондуктан, эгерде N саны 1000дик эсептөө системасында берилген болсо,

$$N=c_0+c_1 1000+c_2 1000^2+\ldots+c_n 1000^n$$

анда $N \equiv c_0+c_1+c_2+\ldots+c_n \pmod{37}$ болот. Мындан 1000дик эсептөө системасында 37ге бөлүнүүчүлүк белгиси

$$R_{37}=c_0+c_1+c_2+c_3+\ldots+c_n$$

болот.

Биздин мисалда R_{37}=289+576+83≡23(mod 37) болгондуктан, калдык 23 болот.

Эми даражаны бөлүүдөн келип чыккан калдыкты эсептейбиз.

Бизге төмөндөгү белгилүү:

$$N \equiv r \pmod{m} \Rightarrow N^k \equiv r^k \pmod{m}.$$

Ошондуктан N^k даражаны r^k менен алмаштырабыз. r^k даражаны m ге бөлүүдөн келип чыга турган эң кичине оң чегериштн табуу үчүн ($r^k > m$ болгондо) $r \equiv r \pmod{m}$ салыштыруусу удаалаш керектүү даража көрсөткүчүнө көтөрүлөт, пайда болгон даража модул боюнча эң кичине оң чегериш менен алмаштырылат. (r, m)=1 болгондо Эйлердин теоремасын пайдалануу ыңгайлуу. Чындыгында, (r, m)=1 шартында $r^{\varphi(m)} \equiv 1 \pmod{m}$ болгондуктан жана $k=\varphi(m)q+l$, $0 \le l \le \varphi(m)$ барабардыктардын негизинде

$$r^k=(r^{\varphi(m)})^q r^l \equiv r^l \pmod{m}$$

келип чыгат.

Мисал 4. 1277^{261} санын 28ге бөлүүдөн пайда болгон калдык табылсын.

Чыгаруу. $1277 \equiv 17 \pmod{28} \Rightarrow 1277^{261} \equiv 17^{261} \pmod{28}$, $(17, 28)=1$ болгондуктан

$17^{\varphi(28)} \equiv 1 \pmod{28} \Rightarrow 17^{12} \equiv 1 \pmod{28}$.

$261=12 \cdot 21+9$ болгону үчүн $17^{261} \equiv 17^{9} \pmod{28}$ болот.

$17 \equiv 17 \pmod{28}$, $17^2 \equiv 289 \equiv 9 \pmod{28} \Rightarrow 17^4 \equiv 81 \equiv -3 \pmod{28}$,

$17^8 \equiv (-3)^2 \equiv 9 \pmod{28}$, $17^9 \equiv 9 \cdot 17 \equiv 13 \pmod{28}$.

Демек, $1277^{261} \equiv 17^{261} \equiv 17^9 \equiv 13 \pmod{28}$, б.а. 1277^{261} санын 28ге бөлгөндөгү калдык 13 экен.

Мисал 5. 14^{245} санын 90 го бөлгөндөгү калдыкты тапкыла.

Чыгаруу. Маселени $14^{245} \equiv x \pmod{90}, 0 \le x < 90$ салыштырууга алып келүүгө болот.

$$(90, 14)=2 \Rightarrow x \vdots 2 \Rightarrow x = 2x_1,\ 14 \cdot 14^{244} \equiv 2x_1 \pmod{90},$$

$$7 \cdot 14^{244} \equiv x_1 \pmod{45},\ (14, 45)=1.$$

Эйлердин теоремасы боюнча $14^{\varphi(45)} \equiv 1 \pmod{45} \Rightarrow 14^{24} \equiv 1 \pmod{45}$, $\varphi(45)=24$. Акыркы салыштырууну 10-даражага көтөрөбүз:

$14^{240} \equiv 1 \pmod{45}, 14^2 \equiv 16 \pmod{45}, 14^4 \equiv 31 \pmod{45}$

$14^{244} \equiv 31 \pmod{45} \Rightarrow x_2 \equiv 31 \pmod{45}$.

$x_1 \equiv 7 \cdot 31 \pmod{45}$, $x_1 \equiv 217 \pmod{45} \Rightarrow x_1 \equiv 37 \pmod{45}$,

$x \equiv 2 \cdot x_1 \pmod{90} \Rightarrow x \equiv 2 \cdot 37 \pmod{90} \Rightarrow x \equiv 74 \pmod{90}$.

Демек, калдык 74 кө барабар.

3. Кадимки бөлчөктү ондук бөлчөккө айландырганда пайда боло турган мезгилдин узундугун аныктоо

Бөлүмү 2ге жана 5ке бөлүнбөгөн ар кандай кыскарбас $\frac{a}{b}$ бөлчөгүн ондук бөлчөккө айландырганда, ал мезгилдүү чексиз ондук бөлчөк болот. Ар кандай мезгилдүү ондук бөлчөктүн

мезгилинин узундугун табууга болот. Мындай учурда төмөнкү эки учур болушу мүмкүн:

1-учур. Кыскарбас $\frac{a}{b}$ дурус бөлчөгүнүн (эгерде $\frac{a}{b}$ буруш бөлчөк болсо, анда анын бүтүн бөлүгүн ажыратуу менен дурус бөлчөккө алып келүүгө болот) бөлүмүндө 2 жана 5 сыяктуу бөлүүчүлөрү жашабасын, б.а. $(a, b)=1$, $(b, 10)=1$ болсун. Анда $(a, b)=1$ болгондуктан, a саны b модулу боюнча түзүлгөн чегериштердин келтирилген системасындагы кандайдыр бир чегеришке ушул b модулу боюнча тең калдыктуу болот.

Төмөнкү барабардыктардын удаалаштыгын карайлы:

$$\begin{aligned} 10a&=bq_1+r_1, && 0<r_1<b,\\ 10r_1&=bq_2+r_2, && 0<r_2<b,\\ 10r_2&=bq_3+r_3, && 0<r_3<b,\\ &\ldots\\ 10r_{m-1}&=bq_m+r_m, && 0<r_m<b, \end{aligned} \qquad (1)$$

мында $b>a$, $b>r_1$, $b>r_2$,... болгондуктан $q_1<10$, $q_2<10$,... болот.

Мындан төмөнкүлөрдүн аткарыла тургандыгы келип чыгат:

$(10, a)=1 \wedge (a, b)=1 \Rightarrow (10a, b)=1$, $(10a, b)=1 \Rightarrow (r_1, b)=1$;

$(10, b)=1 \wedge (r_1, b)=1 \Rightarrow (r_2, b)=1$.

Ошентип, $(r_i, b)=1$ экендигине ынанабыз. Демек, ар түрдүү r_i лер $(i=\overline{1, m})$ b модулу боюнча чегериштердин келтирилген системасын түзөт экен. Бизге белгилүү болгондой b модулу боюнча чегериштердин келтирилген системасындагы чегериштердин саны $\varphi(n)$ ге барабар. Ошондуктан $\varphi(b)$ же анын бөлүүчүсү δ кадамдан соң, бардык калдыктар жана алар менен бирге q_i толук эмес тийиндилер кайталана баштайт. $\frac{a}{b}$ кыскарбас бөлчөгүнүн мезгилиндеги сандар q_1, q_2, ..., q_m цифраларынан тургандыктан, бул бөлчөктүн мезгилинин узундугу $\varphi(b)$ ден чоң боло албайт.

Мезгилдеги сандардын санын табуу үчүн (1) барабардыктардан b модулу боюнча салыштырууларга өтөбүз:

$$\begin{aligned} &10a \equiv r_1 (\mathrm{mod}\ b),\\ &10r_1 \equiv r_2 (\mathrm{mod}\ b),\\ &10r_2 \equiv r_3 (\mathrm{mod}\ b),\\ &\quad \ldots,\\ &10r_{m-1} \equiv r_m (\mathrm{mod}\ b). \end{aligned} \qquad (2)$$

Бул салыштырууларды мүчөлөп көбөйтүп, төмөнкүнү алабыз:

$$10^m a r_1 r_2 \ldots r_{m-1} \equiv r_1 r_2 \ldots r_{m-1} r_m (\mathrm{mod}\, b).$$

$(r_1, r_2, \ldots, r_{m-1}, b) = 1$ болгондуктан, бул салыштыруунун эки жагын тең $r_1 r_2 \ldots r_{m-1}$ ге кыскартып, төмөнкүнү алабыз:

$$10^m a \equiv r_m (\mathrm{mod}\, b). \qquad (3)$$

Айталы, 10 саны b модулу боюнча m көрсөткүчкө тиешелүү болсун. Анда тиешелүү көрсөткүчтүн аныктоосунун негизинде төмөнкү салыштыруу орун алат:

$$10^m \equiv 1 (\mathrm{mod}\, b). \qquad (4)$$

(4) түн негизинде (3)түү төмөнкүдөй жазууга болот:

$$a \equiv r_m (\mathrm{mod}\, b). \qquad (5)$$

a, r_m сандарынын ар бири b дан кичине болгон оң сандар экендиги бизге белгилүү. Алар b модулу боюнча тең калдыктуу болушу үчүн барабар болушу, б.а. $a = r_m$ болушу керек. Демек, m кадамдан соң пайда боло турган калдык берилген бөлчөктүн алымына барабар болот, б.а. m кадамдан кийин калдыктар кайталанып келет экен:

$$r_{m+1} = r_1,\ r_{m+2} = r_2,\ r_{m+3} = r_3,\ \ldots$$

m саны (5) салыштыруу орун алган сандардын эң кичинеси, себеби 10 саны b модулу боюнча m көрсөткүчкө тиешелүү. a саны тиешелүү көрсөткүч болсо, көрсөткүчтүн аныктоосунун негизинде (4) салыштырууну канааттандыруучу даража көрсөткүчтөрдүн эң кичинеси болот. Мындан m саны

$\frac{a}{b}$ бөлчөгүнүн мезгилинин узундугу деген тыянакка келебиз.

Демек, (4) салыштыруу орун алганда, $\frac{a}{b}$ мезгилдүү бөлчөк болуп, мезгилдин узундугу бөлчөктүн бөлүмүнөн гана көз каранды болот экен.

(1)деги барабардыктардын ар бирин $\frac{1}{10b}$га көбөйтүп, төмөнкүнү алабыз:

$$\frac{a}{b}=\frac{q_1}{10}+\frac{r_1}{10b},$$

$$\frac{r_1}{b}=\frac{q_2}{10}+\frac{r_2}{10b},$$

...

$$\frac{r_{m-1}}{b}=\frac{q_m}{10}+\frac{r_m}{10b}.$$

Бул барабардыктардын негизинде төмөнкү ажыралмага ээ болобуз:

$$\frac{a}{b}=\frac{q_1}{10}+\frac{q_2}{10^2}+\frac{q_3}{10^3}+...+\frac{q_m}{10^m}+\frac{r_m}{10^m b}.$$

Бирок, жогоруда көрсөткөнүбүздөй $r_m=a$. Демек,

$$\frac{a}{b}=\frac{q_1}{10}+\frac{q_2}{10^2}+\frac{q_3}{10^3}+...+\frac{q_m}{10^m}+\frac{1}{10^m}\frac{a}{b}$$

болуп, $\frac{a}{b}$ бөлчөгүнүн мезгили $q_1q_2q_3...q_m$ болот. Жогорудагы барабардыктардын удаалаштыгынын негизинде

$\frac{r_1}{b}$ нын мезгили $q_2q_3...q_m\,q_1$;

$\frac{r_2}{b}$ нын мезгили $q_3...q_m\,q_1\,q_2$;

...

$\frac{r_k}{b}$ нын мезгили $q_{k+1}...q_k$ болот.

Ошентип, 10 саны b модулу боюнча m көрсөткүчкө таандык болсо, анда $\frac{a}{b}, \frac{r_1}{b}, \frac{r_2}{b}, ..., \frac{r_{m-1}}{b}$ бөлчөктөрү мезгилдүү бөлчөктөр болот да, бири-биринен мезгилиндеги цифралардын циклдык алмашып келүүсү менен айрымаланат экен.

Мисалы, $\frac{5}{37}$ бөлчөгүн ондук бөлчөккө айландырып, анын мезгилинин узундугун табуу талап кылынсын.

Чыгаруу. 10 санынын 37 модулу боюнча көрсөткүчүн аныктайбыз:

$\varphi(37)=36$ болгондуктан, $10, 10^2, 10^3, \ldots, 10^{36}$ даражаларды 37 модулу боюнча карап чыгабыз:

$10\equiv -27 \pmod{37}$, $10^2\equiv 26 \pmod{37}$, $10^3\equiv 1 \pmod{37}$, $10^4\equiv -27 \pmod{37}$.

Демек, 10 саны 37 модулу боюнча 3 көрсөткүчүнө таандык, б.а. $10^3\equiv 1 \pmod{37}$. Ошондуктан $\frac{5}{37}$ бөлчөгүнүн мезгили 3 цифрадан турат. Бул цифраларды аныктайлы:

$5\cdot 10=37\cdot 1+13,$

$13\cdot 10=37\cdot 3+19,$

$19\cdot 10=37\cdot 5+5.$

Бул барабардыктардын негизинде:

$$\frac{5}{37}=0,(135),\ \frac{13}{37}=0,(351),\ \frac{19}{37}=0,(513).$$

Эгерде 10 саны b модулу боюнча баштапкы тамыр болсо, анда $m=\varphi(b)$ болот эле. Бул учурда ондук бөлчөктүн мезгилиндеги сандардын саны $m=\varphi(b)$ ге барабар болот. Бирок, баштапкы тамыр ар кандай сандар үчүн жашабай тургандыгын биз мурда караганбыз.

Айталы, 10 саны b модулу боюнча баштапкы тамыр болбосун. Анда 10 саны тиешелүү болгон көрсөткүч $\varphi(b)$ дан кичине жана анын бөлүүчүсү болот. Мындай учурда $\varphi(b)=md$ барабардыгын жаза алабыз. Демек, алымдары 1 ден $\varphi(b)$ га чейинки сандарды кабыл ала турган, бөлүмдөрү болсо b га

барабар болгон бөлчөктөрдүн көптүгү d сандагы бөлчөктөр системасына ажыралат экен. Бөлчөктөрдүн бул системасын төмөнкүдөй жазып алабыз:

$$\frac{r_0}{b}, \frac{r_1}{b}, \frac{r_2}{b}, \ldots, \frac{r_{m-1}}{b};$$

$$\frac{s_0}{b}, \frac{s_1}{b}, \frac{s_2}{b}, \ldots, \frac{s_{m-1}}{b};$$

. . .

$$\frac{t_0}{b}, \frac{t_1}{b}, \frac{t_2}{b}, \ldots, \frac{t_{m-1}}{b}.$$

Бул жерде ар бир жолчодогу бөлчөктүн мезгили бири экинчисинен цифраларынын циклдык алмашуусу менен гана айрымаланышын биз жогоруда айтып өттүк.

Мейли, $d>1$ жана $s_0 \neq r_i \ \left(i=\overline{0,m-1}\right)$ болсун. Анда экинчи жолчодогу бөлчөктөр пайда болуп, алардын мезгилиндеги сандардын саны да m ге барабар болот.

s_i жана r_i лерден айрымаланган кандайдыр бир c_0 ($c_0<b$ жана (c_0, b)=1) санын алсак, 3-жолчодогу бөлчөктөрдүн системасын алабыз. Бул процессти улантып, биз d сандагы бөлчөктөрдүн системасын ээ болобуз.

Айтылган пикирлерди жогорудагы мисалга колдонолу. $\varphi(37)=36$ жана $36=3\cdot12$ болгондуктан биз 12 бөлчөктөрдүн системасын алабыз. Чындыгында, 5, 13, 19 га барабар болбогон бир санды, мисалы 2 ни алайлы, анда

$2\cdot10=37\cdot0+20,$

$20\cdot10=37\cdot5+15,$

$15\cdot10=37\cdot4+2,$

барабардыктарынын негизинде төмөнкү бөлчөктөрдүн системасын ээ болобуз: $\frac{2}{37}=0,(054)$, $\frac{20}{37}=0,(540)$, $\frac{15}{37}=0,(405)$.

Калган бөлчөктөр системалары жана алардын мезгилдери тиешелүү түрдө төмөнкүдөй болот:

$\frac{10}{37}, \frac{26}{37}, \frac{1}{37}$, $\frac{10}{37} = 0,(0,27)$;

$\frac{30}{37}, \frac{4}{37}, \frac{3}{37}$, $\frac{30}{37} = 0,(0,81)$;

$\frac{6}{37}, \frac{23}{37}, \frac{8}{37}$, $\frac{6}{37} = 0,(162)$;

$\frac{7}{37}, \frac{33}{37}, \frac{34}{37}$, $\frac{7}{37} = 0,(189)$;

$\frac{9}{37}, \frac{16}{37}, \frac{12}{37}$, $\frac{9}{37} = 0,(243)$;

$\frac{11}{37}, \frac{36}{37}, \frac{7}{37}$, $\frac{11}{37} = 0,(297)$;

$\frac{13}{37}, \frac{19}{37}, \frac{5}{37}$, $\frac{13}{37} = 0,(351)$;

$\frac{14}{37}, \frac{29}{37}, \frac{31}{37}$, $\frac{14}{37} = 0,(378)$;

$\frac{17}{37}, \frac{22}{37}, \frac{35}{37}$, $\frac{17}{37} = 0,(459)$;

$\frac{21}{37}, \frac{25}{37}, \frac{28}{37}$, $\frac{21}{37} = 0,(567)$.

Ар түрдүү бөлчөктөр системасынын мезгили бири экинчисинен циклдык алмаштыруунун жардамында келип чыкпайт. Эгерде дурус бөлчөктүн бөлүмү берилген болсо, бул бөлчөккө барабар болгон ондук бөлчөктүн мезгилинин узундугун индекстердин жардамында табууга болот.

Мисал. Бөлүмү b=41 болгон кыскарбас бөлчөктү ондук бөлчөккө айландырганда пайда болгон ондук бөлчөктүн мезгилинин узундугу табылсын.

Чыгаруу. Көрсөткүчтүн аныктоосунун негизинде, бул көрсөткүч төмөнкү салыштырууну канааттандыруучу көрсөткүчтөрдүн эң кичинеси болот:

$$10^x \equiv 1 (\mathrm{mod}\ 41).$$

Бул салыштырууну индекстердин жардамында чыгарабыз:

$$x\,ind\,10 \equiv ind\,1 (\mathrm{mod}\,40),\ \ ind\,10 = 8.$$

Мындан

$$8x \equiv 0(\mathrm{mod}\,40) \Rightarrow x \equiv 0(\mathrm{mod}\,5).$$

Акыркы салыштырууну канааттандыруучу эң кичине оң сан x=5 болот. Демек, бөлүмү 41ге барабар болгон кыскарбас бөлчөктөрдүн мезгилинин узундугу 5ке барабар болот экен.

2- учур. Кыскарбас $\frac{a}{b}$ бөлчөгүнүн бөлүмүнүн каноникалык ажыралмасында 2 же 5 сандары катышсын, б.а. $(b, 10)>1$ болуп, $b = 2^{\alpha}5^{\beta}b_1$, n=max(α, β) болсун.

Төмөнкү катышты карайлы:

$$\frac{10^n a}{b} = \frac{10^n a}{2^{\alpha}5^{\beta}b_1} = \frac{2^{n-\alpha}5^{n-\beta}a}{b_1} = \frac{a_1}{b_1},\ \text{мында}\ a = 2^{n-\alpha}5^{n-\beta}a.$$

$(b_1, 10)=1 \wedge (a, b_1)=1 \Rightarrow (a_1, b_1)=1.$

Эми $(b_1, 10)=1$ болгондуктан, $\frac{a_1}{b_1}$ кыскарбас бөлчөгүн ондук бөлчөккө айландырууга болот. Анда төмөнкү келип чыгат:

$$\frac{10^n a}{b} = \frac{a_1}{b_1} = H(q_1,\ q_2, q_3, ..., q_m) \Rightarrow \frac{a}{b} = \frac{H(q_1,\ q_2, q_3, ..., q_m)}{10^n}.$$

Эгерде $H = kk_1k_2...k_n$ болсо, анда $\frac{H}{10^n} = k, k_1\,k_2...k_n.$

Демек, $\frac{a}{b} = k, k_1\ k_2...k_n(q_1q_2...q_m).$

Ошентип, $(b, 10) \neq 1$ болгондо, $\frac{a}{b}$ бөлчөгүн ондук бөлчөккө айландырсак, аралаш мезгилдүү бөлчөк пайда болуп, анын мезгилинин узундугу 10 санынын b модулу боюнча тиешелүү болгон m көрсөткүчкө барабар болот. Үтүрдөн кийинки мезгилге чейинки цифралардын саны n=max(α, β) менен аныкталат.

Өз алдынча иштөө үчүн көнүгүүлөр

Берилген теңдемелерди бүтүн сандардын көптүгүндө чыгаргыла [1-26]:

1) $38x+117y=209$;
2) $23x-42y=72$;
3) $119x-68y=34$;
4) $15x+28y=185$;
5) $41x+114y=5$;
6) $90x-5y=5$;
7) $49x+9y=400$;
8) $10x-11y=15$;
9) $12x+31y=170$;
10) $31x-47y=23$;
11) $37x+23y=15$;
12) $101x+39y=89$;
13) $53x+17y=25$;
14) $-26x+174y=2$;
15) $64x-39y=15$;
16) $-6x+11y=29$;
17) $3827x+3293y=1869$;
18) $-10x+23y=17$;
19) $571x+359y=-10$;
20) $903x+5y=43$;
21) $51x+39y=-10$;
22) $93x+5y=123$;
23) $71x+59y=210$;
24) $43x+34y=23$;
25) $38x+35y=30$.
26) $121x+19y=61$

Төмөнкү бөлчөктөрдү ондук бөлчөккө айландырып, мезгилинин узундугун тапкыла [27-41]:

27) $\frac{3}{7}$; 28) $\frac{46}{27}$; 29) $\frac{9}{28}$; 30) $\frac{26}{55}$; 31) $\frac{203}{330}$;

32) $\frac{3}{37}$; 33) $\frac{11}{54}$; 34) $\frac{1}{7}$; 35) $\frac{17}{70}$; 36) $\frac{5}{33}$;

37) $\frac{7}{12}$; 38) $\frac{3}{17}$; 39) $\frac{11}{17}$; 40) $\frac{19}{23}$; 41) $\frac{43}{37}$.

42) $\frac{100}{179}$ жана $\frac{79}{179}$ сандарын ондук бөлчөккө айландырганда мезгилдеринин узундуктары барабар экендигин далилдегиле.

43) Эгерде $\sqrt{0,\overline{(a)}}=0,\overline{(b)}$ болсо, a жана b ны тапкыла.

Тиркеме 1

Pascal программалоо тилинде түзүлгөн программалардын коддору

1) Берилген *a* санын *b* санына бөлүнүүчүлүгүн аныктоочу программа

```
prog бөлүнөт;
var a,b: integer;
   begin
      read(a,b)
       if a/b=int(a/b) then writeln(a 'саны' b
'санына бөлүнөт')else writeln(a 'саны' b 'санына
бөлүнбөйт')
      end.
```

2) Берилген *a* жана *b* сандарынын эң чоң жалпы бөлүүчүсүн аныктоочу программа

```
prog ЭЧЖБ;
var a,b: integer;
   begin
      read(a,b)
      while a<>b do
      begin
         if a>b then a:=a-b else b:=b-a;
      end;
      writeln(a);
   end.
```

3) **Бул программаны пайдаланып берилген *a* жана *b* сандарынын эң кичине жалпы эселүүсүн аныктоочу программаны түзсө болот, ал үчүн** $[a,b]=\frac{ab}{(a,b)}$ **байланышты эске алуу жетиштүү**

```
prog ЭКЖЭ;
var a, b, t: integer;
   begin
      read(a,b)
    t:=a*b
    while a<>b do
      begin
         if a>b then a:=a-b else b:=b-a;
      end;
      writeln(t/a);
   end.
```

4) 10дук эсептөө системасындагы берилген *x* санын 2лик эсептөө системасына өткөрүүчү программа

```
program Эсептоо системасы
var n,s:real;
i,x:integer;
t:string;
begin
   read(x);
   s:=0;
   n:=2;
   while x>=2 do
   begin
      if x/2=int(x/2) then t:='0'+t else t:='1'+t;
      x:=int(x/2);
   end;
   if x=0 then t:='0'+t else t:='1'+t;
```

```
    write (x+' санынын экилик эсептоо
системасындагы жазылышы: '+t);
end.
```

5) Берилген *a* санына чейинки эгиз сандарды экранга чыгаруучу программа

Def. Эгерде *a* натуралдык санын өзүнөн башка бардык натуралдык бөлүчүлөрүнүн суммасы *b*га, ал эми *b*нын өзүнөн башка бардык натуралдык бөлүчүлөрүнүн суммасы *a*габарабар болсо, анда алар эгиз сандар деп аталат. Мисалы, 220менен 284 сандары эгиз сандарга мисал боло алат, себеби 220нын бөлүүчүлөрү 1,2,4,5,10,11,20,22,44,55,110 алардын суммасы: 1+2+4+5+10+11+20+22+44+55+110=284, ал эми 284түн бөлүүчүлөрү 1, 2, 4, 71, 142 алардын суммасы 1+2+4+71+142=220.

```
program Эгиз сандар
label 1;
var i, j, s, c, x, a: integer;
l,m:string;
begin
   read(a);
   write(a,' чейинки эгиз сандар:');
   for x:=2 to a-1 do
   begin
      c:=0;m:='0';
      for j:=1 to Round(x/2) do
      begin
         if x/j=int(x/j) then begin c:=c+j;
m:=m+'+'+IntToStr(j); end;
      end;
      for i:=x+1 to a do
      begin
```

```
        s:=0;l:='0';
        for j:=1 to Round(i/2) do
        begin
           if i/j=int(i/j) then begin s:=s+j;
l:=l+'+'+IntToStr(j); end;
           if s>x then goto 1;
        end;
        if (s=x) and (c=i) then
         begin
           write(IntToStr(i)+'-'+IntToStr(x)+'');
           write(IntToStr(i)+'='+l);
           write(IntToStr(x)+'='+m);
        end;
1:   end;
end.
```

6) Берилген *a* жана *b* сандарынын арасындагы курама сандарды экранга чыгаруучу программа

```
programm Курама сандар
label 1;
var i,j,s,a,b: integer;
begin
   write(a,'-',b,' чейинки курама сандар:');
   for i:=a to b do
   begin
      s:=0;
      for j:=1 to i do
      begin
         if i/j=int(i/j) then begin s:=s+1; if s>2
then goto 1; end;
      end;
      1: if s>2 then write(i);
   end;
end;
```

7) Берилген *a* жана *b* сандарынын арасындагы жөнөкөй сандарды экранга чыгаруучу программа

```
program Жөнөкөй сандар
lable 1;
ver a,b,s,i,j:integer;
begin
read(a,b);
for i:=a to b do
begin
   s:=0;
   for j:=1 to i do
   begin
      if (i/j=int(i/j)) then s:=s+1; if (s>2) then
goto 1;
   end;
1: if (s<=2) then write(i);
end;
end.
```

8) 1ден *a* га чейинки Фибоначчинин сандарын экранга чыгаруучу программа

Def. Эгерде a_1, a_2, a_3,...,a_{n-1},a_n,... удаалаштыгы $a_{k+2}=a_{k-1}+a_k$ шартын канааттандырса, анда ал Фибоначчинин удаалаштыгы деп аталат.

Удаалаштыкты түзгөн сандар Фибоначчинин сандары деп аталат.

Алгачкыларын жазып чыгалы:

1,1,2,3,5,8,13,21,34,55,89,....

Фибоначчинин сандарын экранга чыгаруучу программанын коду:

```
program Фибоначчи сандары
var x,i,j,c,a:integer;
begin
   read(a);
   write(a+' чейинки фибоначчинин сандары:');
   x:=a;
   i:=0;j:=1;c:=1;
   while c<x do
   begin
      write(' ',c);
      c:=i+j;
      i:=j;
      j:=c;
   end;
end.
```

Индекстердин жадыбалы

p=3

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

p=5

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

p=7

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

p=11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

p=13

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

p=17

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

p=19

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8

1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

p=23

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

p=29

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

p=31

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	9	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

p=37

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	34
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

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				

p=41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	4	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	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

p=43

N	0	1	2	3	4	5	6	7	8	9

0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

p=47

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

p=53

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	48	41
4	50	45	32	22	8	29	40	44	21	28

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20

p=59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

p=61

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	5	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24

1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	4	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	9	17	34	7
5	14	28	56	51	41	21	42	23	46	31

p=67

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	4	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	34	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	2	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

p=71

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	43	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

p=73

N	0	1	2	3	4	5	6	7	8	9
0		0	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							

I	0	1	2	3	4	5	6	7	8	9
0	1	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	66
7	38	44								

p=79

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11

3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

p=83

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	44							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	6	32	64	45	7	4
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	8	36	72	61	39	78	73

7	63	43	3	6	12	24	48	13	26	52
8	21	42								

p=89

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	54	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	74	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

p=97

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	56	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30

8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	13	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	65	81	17
9	85	37	88	52	66	39				

Адабияттар

1. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. – М.: Мир,1987. – 416с.
2. Алгебра и теория чисел: Учеб. Пособие для студентов-заочников II курса физ.-мат. фак. пед. ин-тов. Под редакцией Н.Я. Виленкина. – М.: Просвещение, 1984. – 192с.
3. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. – 384с.
4. Виноградов И.М. Основы теории чисел. – М.: Наука, 1981. – 176с.
5. Витов В.Ф., Неустроев Н.В., Рыбакова В.Е. Задачи по теории чисел. – Новгород: НГПИ,1989. – 50с.
6. Грибанов Б.У., Титов П.И. Сборник упражнений по теории чисел. – М.:
7. Просвещение,1964. – 144с.
8. Завало С.Т., Костарчук В.Н., Хацет Б.И. Алгебра и теория чисел. Часть 2. – Киев: Вища школа, 1980. – 408с.
9. Кочева А.А. Задачник-практикум по алгебре и теории чисел. Часть III. – М.: Просвещение,1984. – 41с.
10. Кудреватов Г.А. Сборник задач по теории чисел. – М.: Просвещение, 1970. – 128с.
11. Куликов Л.Я. Алгебра и теория чисел. – М.: Высшая школа, 1979. – 560с.
12. Куликов Л.Я. Сборник задач по алгебре и теории чисел: Учеб. Пособие для студентов физ.-мат. спец. пед. ин-тов/ А.И. Москаленко, А.А. Фомин. – М.: Просвещение, 1993. – 288 с.
13. Михелович Ш.Х. Теория чисел. – М.: Высшая школа, 1962. – 260с.
14. Неустроев Н.В. Рыбакова В.Е. Задачи повышенной трудности по теории чисел и алгебре многочленов. – Новгород: НГПИ, 1990 – 93с.
15. Практические занятия по алгебре и теории чисел. / М.П.Лельчук, И.И.Полевченко, А.М., Радьков, Б.Д.Чеботаревский. – Мн.: Вышейшая школа, 1986. – 302с.
16. Шнеперман Л.Б. Курс алгебры и теории чисел в задачах и упражнениях. Часть 1. – Мн.:Вышейшая школа, 1986. – 272с.
17. Шнеперман Л.Б. Курс алгебры и теории чисел в задачах и упражнениях. Часть 2. – Мн.:Вышейшая школа, 1987. – 256с.