НАВОИЙ ПЕДАГОГ ХОДИМЛАРНИ ҚАЙТА ТАЙЁРЛАШ ВА МАЛАКАСИНИ ОШИРИШ ИНСТИТУТИ

АЛГЕБРА ВА СОНЛАР НАЗАРИЯСИ

(Маърузалар матни)
4-қисм

УМУМИЙ МАТЕМАТИКА КАФЕДРАСИ

Тузувчилар: Катта укитувчи: Нормуродов Ш.У.
Укитувчилар : Жумаев С.С

НАВОИЙ-2005й

Кириш

Мазкур маъруза матнлар туплами алгебра ва сонлар назариясидан педагогика университетлари бакалавриат йуналиши буйича «Математика ва информатика» булимида тахсил оладиган талабалар учун ёзилган булиб , унда 34 соатга мулжаллаб 17 та маъруза баён этилган.

Матнлар тупламида бутун сонлар халкасида булиниш назарияси ва таккосламалар назарияларига оид куплаб тушунчалар ёритилган.

Айрим матнларда теоремалар, хоссаларнинг исботлари келтирилмаган холлар хам учрайди.Лекин уларнинг исботларини талаба каердан урганиши учун курсатма берилган. Куплаб тушунчалар мисоллар ёрдамида ёритиб берилган.

Тупламда талабаларнинг мустакил таълим мавзуларини урганинишлари учун купгина матнларнинг батафсил ёзилишига эътибор берилган.

1 – маъруза

Туб ва мураккаб сонлар. Бутун соннинг туб купайтувчиларга ёйилмаси (2 соат)

Режа:

1. Туб соннинг таърифи.
2. Мураккаб соннинг таърифи.
3. Туб ва мураккаб сонларнинг баъзи хоссалари.
4. Бутун соннинг туб купайтувчиларга ёйилмаси.
5. Мисол.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси. II кисм. Т.: Укитувчи. 1995й.(22-24-бетлар).
2. Куликов Л.Я. Алгебра и теория чисел. М.: Высш. шк.1979 г. (стр. 365-367).

Таъриф. Факат иккита турли натурал булувчиларга эга булган натурал сон туб сон дейилади.

Бу таърифга кура 2,3,5,7,11,13,17,... сонларни туб сонлар булади.

Таъриф. Натурал булувчиларининг сони иккитадан ортик булган натурал сон мураккаб сон дейилади.

Бу таърифга кура 4,6,8,9,10,12,14,... сонлари мураккаб сонлар булади.

1 сони туб сон хам эмас, мураккаб сон хам эмас. Чунки, 1 сони туб ва мураккаб сонлар таърифларини каноатлантирмайди.

Туб ва мураккаб сонлар куйидаги баъзи бир хоссаларга эга:

1^o. $a>1$ мураккаб соннинг 1 дан бошка энг кичик натурал булувчиси p булса, у холда p сон туб сон булади.

2^o. Хар кандай натурал a ва p туб сонлари ёки узаро туб, ёки a сон p га булинади.

3^o. Агар ab купайтма бирор p туб сонга булинса, у холда купайтувчилардан камида биттаси p га булинади.

1,2,3 – хоссаларнинг исботи [1] да келтирилган.

Натижа. Агар купайтма p туб сонга булиниб, унинг барча купайтувчилари туб сонлардан иборат булса, у холда бу купайтувчилардан бири p га тенг булади.

Теорема. 1 дан бошка ихтиёрий натурал сон ёки туб сон ёки туб сонлар купайтмаси шаклида ёзилади, агар бу купайтмада купайтувчиларнинг урни эътиборга олинмаса, у холда бу купайтма ягона булади.

Исботи. $a>1$ натурал сон булсин. Ушбу

$$a=p_1 p_2...p_n \ (p_i - \text{туб сон}, i=\overline{1,n}, n>1) \qquad (1)$$

купайтманинг мавжудлиги ва ягоналигини курсатамиз.

1. а туб сон булса, у холда теорема исбот булади.

2. а мураккаб сон булсин. У холда 1- хоссага кура а нинг 1 дан бошка энг кичик натурал булувчиси булган p_1 туб сон мавжуд булиб,

$$a=p_1a_1 \ (p\text{-туб сон}) \qquad (2)$$

тенглик уринли булади. Агар (2) да a_1 туб сон булса, у холда теорема исбот булади. Агар a_1 мураккаб сон булса, у холда 1-хоссага кура у p_2 туб булувчига булиб,

$$a=p_2a_2 \ (p_2\text{- туб сон}) \qquad (3)$$

тенглик уринли булади. (2) ва (3) тенгликлардан $a=p_1p_2a_2$ тенгликни хосил киламиз. Агар бу тенгликда a_2 туб сон булса, у холда теорема исбот булади. Агар a_2 мураккаб сон булса, у холда бу жараённи яна давом эттирамиз. Натижада $a=p_1 a_1$, $a_1=p_2a_2$,... $a_{n-1}=p_na_n$ тенгликларга эга буламиз. Бу жараён $a_n=p_1$ булгунга кадар давом эттирилади. Хосил булган тенгликларни хадлаб купайтирсак, натижада (1) ёйилма хосил булади.

Энди (1) ёйилманинг ягоналигини исбот килайлик.

Фараз килайлик, а сон (1) дан бошка, ушбу

$$a=q_1q_2... q_s \ (q_j\text{-туб сон},j=\overline{1,s}, s>1) \qquad (4)$$

ёйилмага хам эга булсин. (1) ва (4) ларнинг чап томонларининг тенглигидан

$$p_1p_2...p_n=q_1q_2...q_s \qquad (5)$$

тенгликни ёза оламиз. (5)нинг чап томонидаги хар бир туб сон унинг унг томонини булади. Лекин q_j ($j=\overline{1,s}$) лар хам туб сонлардир. Юкоридаги натижага кура q_j ларнинг бири бирорта p_i га ва аксинча $p_к$ ларнинг бири бирорта q_i га тенг булади. Демак, (1) ва (5) ёйилмалар тенг сондаги туб купайтувчилардан иборат.

n>s, n<s, n=s холлардан бири уринли булади.

1. n>s булиб, a_1:р булсин. У холда $q_1q_2...q_s$:p_1 булади.

Айтайлик, бу $q_1=p_1$ булганда уринли булсин. (5) нинг икки кисмини p_1 га кискартириб $p_2p_3...p_n=q_2q_3...q_s$ тенгликни хосил киламиз. Бу тенгликнинг чап томони p_2 га булинади. Айтайлик, бу $q_2=p_2$ булганда уринли булсин. Натижада $p_3p_4...p_n=q_3q_4...q_s$ тенгликни хосил киламиз. Шу жараённи давом эттириб энг сунггида $p_{s+1}p_{s+2}...p_n=1$ тенгликка келамиз. Лекин бу тенглик ту²ри эмас,чунки туб сонлар купайтмаси 1 га тенг булмайди. Демак, n>s булиши мумкин эмас.

2. n<s булсин. Бунда 1-холга кура $1=q_{n+1}q_{n+2}...q_s$ ноту²ри тенгликка эга буламиз. Демак, n<s хол хам булиши мумкин эмас.

Демак, n=s хол уринли булиб, $p_1=q_2$, $p_2=q_2$,...,$p_n=q_s$ тенгликларга эга буламиз, яъни (1) ва (4) ёйилмалар бир хил экан.

Бу теоремани арифметиканинг асосий теоремаси дейилади.

Мисол. 26=2·13, 58=2·29, 105=3· 5· 7.

Фараз килайлик (1) ёйилмада p_1 сон α_1 марта, p_2 сон α_2 марта ва хакозо p_n сон α_n марта учрасин. Бундай холда (1) ни

$$à = ð_1^{\alpha_1} ð_2^{\alpha_2} ... ð_n^{\alpha_n} \ (p_1<p_2<...<p_n, \alpha_i\geq 1\text{-натурал сон}, i=\overline{1,n}) \qquad (6)$$

куринишда ёзамиз. (6) тенглик а соннинг каноник ёйилмаси дейилади.

Мисол. $500=2^2 \cdot 5^3$, $23716=2^2 \cdot 7^2 \cdot 11^2$ каноник ёйилма. Лекин $1125=2^0 \cdot 3^2 \cdot 5^3$ каноник ёйилма эмас.

Текшириш саволлари

1. Туб сон деб нимага айтилади?
2. Мураккаб сон деб нимага айтилади?
3. Арифметиканинг асосий теоремасини баён этинг.

4. Туб ва мураккаб сонларнинг хоссаларини мисоллар ёрдамида тушунтириб беринг.
5. Мураккаб сонинг каноник ёйилмасига мисол келтиринг.

Таянч тушунчалар

1. Натурал,бутун сонлар.
2. Соннинг булувчилари.
3. Купайтмада купайтувчиларнинг урни (тартиби).

2,3-маърузалар

Булиниш муносабати. Колдикли булиш хакидаги теорема. Натурал сон натурал булувчиларининг сони ва
йи²индиси (4 соат)

Режа:

1. Бутун сонлар халкасида булиниш муносабати.
2. Булиниш муносабатининг хоссалари.
3. Колдикли булиш хакидаги теорема.
4. Натурал сон натурал булувчиларининг сони ва йи²индиси.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси. II кисм. Т.: Укитувчи. 1995 й. (6-9,28-30-бетлар).
2. Куликов Л.Я. Алгебра и теория чисел. М.:Высш. шк. 1972 г. (стр. 367-369).

Таъриф. Агар a ва в ≠ 0 бутун сонлар учун a=bq муносабатни каноатлантирувчи q бутун сон мавжуд булса, у холда a сон b сонга булинади ёки b сон a сонни булади дейилади.

Агар a сон b сонга булинса, у холда уни a⋮b ёки a/b куринишларда белгиланади. a=bq тенгликда a булинувчи, b булувчи, q булинма дейилади.

Теорема. Агар a≠0 ва b≠0 булиб, a=bq тенгликни каноатлантирувчи q сон мавжуд булса, у ягона булади.

Бу теореманинг исботи [1] да берилган.

Булиниш муносабати куйидаги хоссаларга эга:

1^0. (∀ a ∈ Z, a ≠ 0) 0⋮a;

2^0. (∀ a ∈ Z, a ≠ 0) a⋮a;

3^0. (∀ a ∈ Z) a⋮1;

4^0. (∀ a,b,c ∈ Z, b ≠ 0,c ≠ 0) ((a⋮b) ∧ (b⋮c)) => (a⋮c);

5^0. (∀ a,b ∈ Z, a ≠ 0, b ≠ 0) ((a⋮b)∧(b⋮a))=> (b=± a);

6^0. (∀ a,b,c ∈ Z, c ≠ 0) a⋮c => ab⋮c;

7^0. (∀ a,b∈ Z, c ≠ 0) ((a⋮c) ∧ (b⋮c)) => (a ± b)⋮c;

8^0. ($\forall$ a,b_i ∈Z, a ≠0, i=$\overline{1,n}$) ((b_1⋮a) ∧(b_2⋮a) ∧... ∧(b_n⋮a))=> (b_1c_1± b_2c_2±... ±b_nc_n)⋮a (c_i∈Z, i=$\overline{1,n}$).

4-хоссани исботлайлик. (a⋮b) <=> a=bq, (b⋮c) <=> b=cq_1 булиб, булардан a=bq=cq_1q=cq_2, яъни a=cq_2 тенглик келиб чикади.Бу эса a⋮c эканлигини билдиради.

Колган хоссалар хам шу усулда исботланади.

Теорема. Ихтиёрий a бутун сон, b натурал сонлар учун шундай ягона q бутун сон ва ягона манфиймас r бутун сон топиладики, натижада ушбу

$$a=bq+r \qquad (1)$$

$$0 \le r < b \qquad (2)$$

муносабатлар уринли булади.

Исботи. bq сон b нинг a дан катта булмаган энг катта карралиси булсин.У холда $bq \le a$ ва $a<bq+b$ муносабатлар уринли булади. Бу икки муносабатдан $bq \le a<b(q+1)$ муносабатни ёза оламиз.Бу куш тенгсизликнинг хар бир кисмига (-bq) ни кушиб $0 \le a-bq<b$ тенгсизликни хосил киламиз. Бу ерда a-bq=r белгилаш киритсак, (1) ва (2) муносабатларнинг уринли эканлиги келиб чикади.

Энди q ва r ларнинг ягоналигини курсатайлик.

Фараз килайлик (1) ва (2) муносабатлардан бошка

$$a=bq_1+r_1, \qquad (3)$$

$$0 \le r_1 < b, \qquad (4)$$

муносабатлар хам уринли булсин. (1) дан (3) ни айирайлик. У холда $0=b(q-q_1)+(r-r_1)$ ёки $r_1-r=b(q-q_1)$ тенглик хосил булади. Бу ерда $|r_1-r|<b$ муносабат уринли.

$r_1-r=b(q-q_1) \Leftrightarrow (r_1-r) \vdots b$. Бу эса $r_1-r=0$ булганда уринли булади. Бундан $r_1=r$ эканлиги келиб чикади. $r_1-r=0$ ни эътиборга олсак, $r_1-r=b(q-q_1)$ дан $b(q-q_1)=0$ келиб чикади. Лекин $\forall b \in N$ булгани учун $q-q_1=0$ булиб, бундан $q=q_1$ келиб чикади. Демак, q ва r лар ягона экан.

Агар (1) да $b \ne 0$ ихтиёрий бутун сон булса, у холда $0 \le r<|b|$ булади.

Бу теоремани колдикли булиш хакидаги теорема дейилади.

Таъриф. Агар $a=bq+r$ тенгликда $r \ne 0$ булса, у холда r га колдик, q га туликсиз булинма дейилади.

Мисол. –117 ни -7 га булгандаги колдик ва туликсиз булинма топилсин.

Ечиш. $-117=(-7)q+r$ дан q ва r ларни топайлик. Бунинг учун $117=7 \cdot 16+5$ тенгликни оламиз ва унинг икки кисмини (-1) га купайтирамиз, яъни $-117=(-7)16+(-5)$ тенгликни хосил киламиз. Бу тенгликнинг унг томонига 7 ни кушамиз ва айирамиз. У холда

$-117=(-7)16+(-5)+7+(-7)$ хосил булиб, бундан $-117=(-7)17+2$ ни хосил киламиз.Бу тенгликни $-117=(-7)q+r$ тенглик билан солиштириб, r=2, q=17 ларни топамиз.

Таъриф. Аникланиш сохаси ёки кийматлар сохаси ёки хар иккиси хам бутун сонлар туплами булган функцияга сонли функция дейилади.

Теорема.

$$n=\delta_1^{\alpha_1}\delta_2^{\alpha_2}\ldots\delta_k^{\alpha_k} \qquad (5)$$

соннинг булувчиси d булиши учун d соннинг каноник ёйилмаси

$$d=\delta_1^{\beta_1}\delta_2^{\beta_2}\ldots\delta_k^{\beta_k} \qquad (6)$$

булиб, бунда

$$\beta_i \le \alpha_I \ (i=\overline{1,k}) \qquad (7)$$

булиши зарур ва етарли.

I. Зарурлиги. $n \vdots d$ булсин. У холда (6) ва (7) нинг бажарилишини курсатайлик. p сон d соннинг туб булувчиси булсин. У холда $(n \vdots d) \wedge (d \vdots p) \Rightarrow n \vdots p$ булади. Лекин (5) дан куринадики, n сони $p_1,p_2,\ldots,p_к$ туб сонларга булинади. У холда p сони $p_1, p_2,\ldots,p_к$ сонлар ичида учрайди. Демак, d нинг каноник ёйилмасидаги p сон n нинг каноник ёйилмасида хам бор экан. Шу билан (6) исбот булди. Энди (7) ни исбот килайлик. Фараз килайлик (7) бажарилмасин.Айтайлик. $\alpha_I > \beta_I$ булсин.

n⋮d => n=dq дан $n=\delta_1^{\alpha_1}\delta_2^{\alpha_2}\dots\delta_k^{\alpha_k}=\delta_1^{\beta_1}\delta_2^{\beta_2}\dots\delta_k^{\beta_k}\cdot q$ нинг хар икки кисмини $p_1^{\alpha_1}$ га кискартириб $\frac{n}{\delta_1^{\alpha_1}}=\delta_2^{\alpha_2}\dots\delta_k^{\alpha_k}=\delta_1^{\beta_1-\alpha_1}\delta_2^{\beta_2}\dots\delta_k^{\beta_k}\cdot q$ ни хосил киламиз. $\beta_1>\alpha_1$ булгани учун $\beta_1-\alpha_1$ натурал сон булиб, $\frac{n}{\delta_1^{\alpha_1}}$ натурал сон икки хил усул билан туб сонлар купайтмасига ёйилди. Лекин арифметиканинг асосий теоремасига асосан бундай булиши мумкин эмас. Бу зиддиятнинг келиб чикишига сабаб $\beta_1>\alpha_1$ деганимиздир. Демак, (7) муносабат хам бажарилади.

II. Етарлилиги. (6) ва (7) муносабатлар берилган. Исбот килиш керак n:d эканлигини. Хакикатан,

$$n=\delta_1^{\alpha_1}\cdot\delta_2^{\alpha_2}\cdot\dots\cdot\delta_k^{\alpha_k}=\delta_1^{\alpha_1}\cdot\delta_2^{\alpha_2}\cdot\dots\cdot\delta_k^{\alpha_k}\cdot\frac{d}{\delta_1^{\beta_1}\delta_2^{\beta_2}\dots\delta_k^{\beta_k}}=$$

$$=\delta_1^{\alpha_1-\beta_1}\cdot\delta_2^{\alpha_2-\beta_2}\cdot\dots\cdot\delta_k^{\alpha_k-\beta_k}\cdot d$$

булиб, бу ерда $\alpha_I>\beta_I$ булгани учун $\alpha_1-\beta_1,\alpha_2-\beta_2,\dots,\alpha_k-\beta_k$ лар натурал сонлар булади. Демак, n=dq булиб n⋮d келиб чикади.

n натурал соннинг барча натурал булувчилари сонини τ(n), n нинг барча натурал булувчилари йи²индини эса σ(n) оркали белгилайлик.

Куйидаги леммени исботсиз келтирамиз:

Лемма. x_i узгарувчининг барча кийматларининг сони $n_i(i=\overline{1,k})$ булса, у холда $(x_1,x_2,\dots\dots x_k)$ куринишдаги барча нукталар сони $n_1n_2\dots n_k$ купайтмага тенг.

Теорема. $n=\delta_1^{\alpha_1}\delta_2^{\alpha_2}\dots\delta_k^{\alpha_k}$ сон учун $\tau(n)=(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$ булади.

Исботи. n соннинг булувчиси d булса, у холда юкоридаги теоремага кура $d=\delta_1^{\beta_1}\delta_2^{\beta_2}\dots\delta_k^{\beta_k}\ (\beta_i\le a_i,\ i=\overline{1,k})$ булади. d сонга $\beta_1,\beta_2,\dots,\beta_к$ нукталарни мос куямиз, яъни $d\leftrightarrow(\beta_1,\beta_2,\dots,\beta_к)$ булади.

$\beta_I=0,1,2,\dots,\alpha_I$, яъни β_I нинг кийматлар сони (α_I+1)булади.

β_1 нинг кийматлар сони α_1+1 та, β_2 нинг кийматлар сони α_2+1 та ва хакозо $\beta_к$ нинг кийматлари сони $\alpha_к+1$ та булади. У холда юкоридаги леммага кура $\beta_1,\beta_2,\dots,\beta_к$ нукталар сони $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_к+1)$ га тенг булади. $\beta_1,\beta_2,\dots,\beta_к$ нукталарга d сон мос куйилганлиги ва d сон n нинг булувчиси булганлигидан $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_к+1)$ купайтма n соннинг барча натурал булувчилари сони булади. Демак, $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_к+1)=\tau(n)$ экан.

Мисол. n=180 нинг барча натурал булувчилари сонини топинг.

Ечиш. $180=2^2\cdot3^2\cdot5$ булгани учун $\alpha_1=2,\alpha_2=2,\alpha_3=1$ булиб, $\tau(180)=(2+1)(2+1)(1+1)=18$, $\tau(180)=18$ булади. Демак, 180 нинг 18 та натурал булувчиси мавжуд экан.

Теорема. $n=\delta_1^{\alpha_1}\delta_2^{\alpha_2}\cdots\delta_k^{\alpha_k}$ булса, у холда $\tau(n)=\frac{\delta_1^{\alpha_1+1}-1}{\delta_1-1}\cdot\frac{\delta_2^{\alpha_2+1}-1}{\delta_2-1}\cdots\frac{\delta_k^{\alpha_k+1}-1}{\delta_k-1}$ булади.

Исботи. Ушбу

$$A=\left(1+\delta_1+\delta_1^2+\dots+\delta_1^{\alpha_1}\right)\left(1+\delta_2+\delta_2^2+\dots+\delta_2^{\alpha_2}\right)\cdots\left(1+\delta_k+\delta_k^2+\dots+\delta_k^{\alpha_k}\right)$$

ифодани олайлик.

Бу ифодада кавсларни очганда хар бир кушилувчи $\delta_1^{\beta_1}\delta_2^{\beta_2}\ldots\delta_k^{\beta_k}$ куринишидаги ифода булиб, $\beta_i \le \alpha_i, (i=\overline{1,k})$ булади. Демак, А нинг ёйилмасидаги хар бир кушилувчи n нинг булувчисидан иборат булади. У холда А ифода n нинг барча булувчиларининг йи²индисига тенг булади,яъни $\tau(n)=A$ булади.

$$1+\delta_1+\delta_1^2+\cdots+\delta_1^{\alpha_1}=\frac{\delta_1^{\alpha_1+1}-1}{\delta_1-1},\ 1+\delta_2+\delta_2^2+\cdots+\delta_2^{\alpha_2}=\frac{\delta_2^{\alpha_2+1}-1}{\delta_2-1},\ldots$$

$$,1+\delta_k+\delta_k^2+\cdots+\delta_k^{\alpha_k}=\frac{\delta_k^{\alpha_k+1}-1}{\delta_k-1}$$

эканлигидан

$$\tau(n)=\frac{\delta_1^{\alpha_1+1}-1}{\delta_1-1}\cdot\frac{\delta_2^{\alpha_2+1}-1}{\delta_2-1}\cdots\frac{\delta_k^{\alpha_k+1}-1}{\delta_k-1}$$

келиб чикади.

Мисол. 180 нинг барча натурал булувчилари йи²индисини топинг.

$180=2^2\cdot 3^2\cdot 5$ булгани учун $\alpha_1=\alpha_2=2$, $\alpha_3=1$, $p_1=2$, $p_2=3$, $p_3=5$ булиб,

$$\tau(180)=\frac{2^{2+1}-1}{2-1}\cdot\frac{3^{2+1}-1}{3-1}\cdot\frac{5^{1+1}-1}{5-1}=7\cdot 13\cdot 6=546,\ \tau(180)=546$$

булади.

$\tau(n)$ ва $\sigma(n)$ функциялари сонли функциялар булади.

Текшириш саволлари

1. Кайси вактда a сон b сонга булинади дейилади?
2. Булиниш муносабати хоссаларини баён этинг?
3. Колдикли булиш хакидаги теоремани баён этинг?
4. Сонли функция деб нимага айтилади?
5. $\tau(n)$ ва $\sigma(n)$ сонли функциялар хакидаги теоремаларни баён этинг ва мисоллар келтирнг?

Таянч тушунчалар

1. Натурал, бутун сонлар ва улар устида амаллар.
2. Туплам.
3. Халка.

4,5-маърузалар

Энг катта умумий булувчи ва энг кичик умумий булинувчи. Узаро туб сонлар. Евклид алгоритми (4 соат)

Режа:

1. Энг катта умумий булувчи (ЭКУБ).
2. Энг кичик умумий булинувчи (каррали) (ЭКУК).
3. Узаро туб сонлар ва уларнинг хоссалари.
4. Евклид алгоритми.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси II кисм. Т.: Укитувчи. 1995 й. (9-16-бетлар).

2. Куликов Л.Я. Алгебра и теория чисел. М.: Высш. шк. 1979 г. (стр. 372-380).

Таъриф. a ва b бутун сонларнинг иккисини хам буладиган сон шу сонларнинг умумий булувчиси дейилади.

Биз факат натурал булувчилар билан шу²улланамиз.

Мисол. 12 ва 18 сонларининг умумий булувчилари 1, 2, 3, 6. булади.

Бу мисолдан куринадики, a ва b сонларнинг бир нечта умумий булувчилари мавжуд булиши. Бу умумий булувчилар тупламини $D_{a,\ b}$ оркали белгилайлик. Демак, $D_{12,\ 18}$ ={1, 2, 3, ,6} булади.

Таъриф. a ва b натурал сонлар умумий булувчиларининг энг каттасига шу сонларнинг энг катта умумий булувчиси (ЭКУБ) дейилади ва уни (a; b) куринишда белгиланади.

Мисол. (12;18)=6.

Таъриф. Агар (a; b)=1 булса, у холда a ва b натурал сонлар узаро туб сонлар дейилади.

Мисол. (7;11)=1 булгани учун 7 ва 11 сонлари узаро туб сонлар, лекин (12;18)=6 булгани учун 12 ва 18 сонлари узаро туб сонлар булмайди.

Агар A туплам. a∈N соннинг булувчилари туплами, B туплам b∈N соннинг булувчилари туплами булса, у холда $D_{a,b}$=A∩*B* булади.

Теорема. (a:b)=> *(a;b)= b.*

Исботи. a:b ва b:b. Демак, b сон a нинг хам, узининг х*ам* умумий булувчиси экан. Лекин бу сонлар учун b дан катта умумий булувчи йук. Чунки, b сон узидан катта сонга булинмайди. Шу сабабли b сон a ва b сонлар учун ЭКУБ булади. Демак, $D_{a,b}=D_b$ булади.

Мисол. 12:6 => (12; 6)=6.

Натижа. (a; b) = d булса, у холда шундай u ва v бутун сонлар топиладики, улар учун au+bv=d тенглик бажарилади.

Бу натижанинг исботи [1] да келтирилган.

Таъриф. a_1, a_2, ..., a_n бутун сонларнинг барчасини буладиган сон шу сонларнинг умумий булувчиси дейилади.

a_1, a_2, ..., a_n бутун сонларнинг умумий булувчилари бир нечта булиши мумкин. Уларнинг энг каттасига a_1,a_2,...,a_n сонларнинг ЭКУБ дейилади ва уни (a_1, a_2, ..., a_n) куринишида белгиланади.

Таъриф. Агар (a_1, a_2, ..., a_n)=1 булса, у холда a_1, a_2, ..., a_n натурал сонларни узаро туб сонлар дейилади.

Узаро туб сонлар куйидаги хоссаларга эга:

1°.((a; c)=1 ∧ (b;c)=1=>((ab;c)=1);

2°. ((ab:c)∧(a:c)=1)=>(b:c)(c≠0):

3°. ((a;b)=1)=>($(a^n;b^n)$=1) (∀n∈N);

4°. ((a;b)=d)=>($(\frac{a}{d};\frac{b}{d})$=1);

5°. ((a:b)∧(a:c)∧((b;c)=1)=>(a:bc) (b≠0, c≠0)

Бу хоссаларнинг исботи [1,2] да келтирилган.

Таъриф. Агар a_1, a_2, ..., a_n сонларнинг ихтиёрий иккитаси узаро туб булса, у холда улар жуфтлама узаро туб сонлар дейилади.

Мисол. (7; 9; 16)=1 ва (7,9)=1, (7,16)=1,(9,16)=1 булгани учун 7, 9, 16 сонлари жуфтлама узаро туб сонлар дейилади.

Теорема. a=bq+r => (a;b)=(b;r).

Исботи. d сон a ва b сонларнинг ихтиёрий умумий булувчиси булсин. У холда *a⋮d ва b⋮d булиб, a-bq=r дан r⋮d келиб* чикади. Демак, d сон b ва r сонларнинг хам умумий булувчиси экан.

Айтайлик, k сон b ва г сонларининг ихтиёрий умумий булувчиси булсин.

У холда *b⋮k ва r⋮k булиб, bq+r=a дан a⋮к* келиб чикади.

Демак, k сон a ва b ларнинг хам умумий булувчиси булар экан.

Шундай килиб, a ва b ларнинг барча умумий булувчилари b ва г ларнинг хам умумий булувчилари булар экан ва аксинча. У холда уларнинг ЭКУБлари хам бир хил, яъни (a; b)=(b; г) булади.

Мисол. 26=4·6+2 => (26; 4)=(4; 2)=2.

a ва b натурал сонларнинг ЭКУБни куйидаги усул билан топиш Евклид алгоритми дейилади:

Фараз килайлик a сон b га булинмасин. У холда a ни b га колдикли буламиз ва куйидаги системани хосил киламиз:

$$\begin{cases} a=bq_1+r_1\ (0<r_1<b), \\ b=r_1q_2+r_2\ (0<r_2<r_1), \\ r_1=r_2q_3+r_3\ (0<r_3<r_2), \\ - - - - - - - - - - - - - - \\ r_{n-2}=r_{n-1}q_n+r_n\ (0<r_n<r_{n-1}), \\ r_{n-1}=r_nq_{n+1}\ . \end{cases} \qquad (1)$$

Бу системада $r_n<r_{n-1}<r_{n-2}<...<r_2<r_1<b$ эканлиги равшан. (1) системадаги нолдан фаркли энг охирги колдик булган r_n сон a ва b сонларнинг ЭКУБ булади.

Хакикатан,

$$\begin{cases} a=bq_1+r_1=>(a;b)=(b,\ r_1), \\ b=r_1q_2+r_2=>(b;r_1)=(r_1;r_2), \\ r_1=r_2q_3+r_3=>(r_1;r_2)=(r_2;r_3), \\ - - - - - - - - - - - - - - - - - \\ r_{n-2}=r_{n-1}q_n+r_n=>(r_{n-2};r_{n-1})=(r_{n-1};r_n), \\ r_{n-1}=r_nq_{n+1}=>(r_{n-1};r_n)=r_n \end{cases} \qquad (2)$$

булиб, (2) дан $(a;b)=(b;r_1)=(r_1;r_2)=...=(r_{n-1};r_n)=r_n$, яъни $(a;b)=r_n$ келиб чикади.

Мисол . 148 ва 135 сонларнинг ЭКУБ топилсин.

Ечиш. 148=135·1+13,

135=13·10+5,

13= 5·2+3,

5=3·1+2,

3=2·1+1,

2 =1·2.

Демак, нолдан фаркли энг охирги колдик, 1 булгани учун (148; 135)=1 булади.

Теорема. d сон a ва b сонларнинг ЭКУБ булиши учун d умумий булувчи a ва b сонларнинг хар кандай умумий булувчисига булиниши зарур ва етарли.

I. Зарурлиги. (a⋮b)=d ва k сон a ва b ларнинг ихтиёрий умумий булувчиси булсин. d⋮k эканлигини исбот килайлик.

$$\begin{cases} a=bq_1+r_1=>r_1=a-bq_1=>r_1:k, \\ b=r_1q_2+r_2=>r_2=b-r_1q_2=>r_2:k, \\ - - - - - - - - - - - - - - - - - - - \end{cases}$$

$$r_{n-2}=r_{n-1}q_n+r_n=>r_n=r_{n-2}-r_{n-1}q_n=>r_n:k,$$

яъни $r_n=d$ булиб, $d\vdots k$ булади.

II. Етарлилиги. d сон a ва b сонларнинг умумий булувчиси булиб, у a ва b ларнинг ихтиёрий умумий булувчиси k га булинсин, яъни $d\vdots k$ булсин. $(a\vdots b)=d$ эканлигини исбот килайлик.

Фараз килайлик $(a; b)\neq d$. У холда $(a; b)=m$ булсин. Бу ерда $m>d$ булади. Лекин берилганга кура d:m булиши керак. Аммо бунинг булиши мумкин эмас, яъни $m>d$ эди. Демак, фаразимиз нотўғри экан. У холда $(a; b)=d$ булади.

Теорема. Агар $(a_1,a_2,...a_n,)=d$ булиб, $(a_1,a_2,)=d_2$, $(d_2,a_3)=d_3$, ...,$(d_{n-1};a_n)=d_n$ булса , у холда $d_n=d$ булади.

Исботи. Теоремани исбот килиш учун $d:d_n$ ва $d_n:d$ эканлигини курсатиш лозим.

$(d_{n-1};a_n)=d_n => d_{n-1}\vdots d_n$, $a_n\vdots d_n$;

$(d_{n-2};a_{n-1})=d_{n-1}=> d_{n-2}\vdots d_{n-1,}$ $a_{n-1}\vdots d_{n-1;}$

Демак, $(a_{n-1};d_{n-1})\wedge(d_{n-1}:d_n)=>a_{n-1}\vdots d_n$ булади.

$(d_{n-3};a_{n-2})=d_{n-2}=>d_{n-3}\vdots d_{n-2},a_{n-2}\vdots d_{n-2}$;

Демак, $(a_{n-2};d_{n-2})\wedge(d_{n-2}:d_{n-1})=>a_{n-2}\vdots d_{n-1}$ булади.

У холда $(a_{n-2}: d_{n-1)})\wedge(d_{n-1};d_n)=>a_{n-2}\vdots d_n$ келиб чикади. Ш[у жараённи давом эттирсак $a_n\vdots d_n$, $a_{n-1}\vdots d_n$, ... ,$a_2\vdots d_n$, $a_1\vdots d_n$ га эга буламиз. Демак, d_n сон a_1, a_2,...,a_n сонларнинг умумий булувчиси экан. У холда $d\vdots d_n$ келиб чикади.

$a_1\vdots d$ ва $a_2\vdots d$ булгани учун d сон a_1 ва a_2 сонларнинг умумий булувчиси булиб, $d_2\vdots d$ булади.

$a_3\vdots d$ ва $d_2\vdots d$ булгани учун d сон a_3 ва d_2 сонларнинг умумий булувчиси булиб $d_3\vdots d$ булади. Шу жараённи давом эттириб энг охирида $d_n\vdots d$ муносабатга эга буламиз. Демак, $d\vdots d_n$ ва $d_n\vdots d$ булиб, улардан $d_n=d$ эканлиги келиб чикади.

Таъриф. Агар k сон $a_1,a_2,...,a_n$ сонларга булинса, у холда k сон $a_1,a_2,...,a_n$ сонларнинг умумий булинувчиси (карралиси) дейилади.

k соннинг умумий булинувчилари чексиз куп булиши мумкин. Уларнинг ичида энг кичиги энг кичик умумий булинувчи (ЭКУК) дейилади ва уни $[a_1,a_2, ..., a_n]$ куринишда белгиланади.

Мисол. [12; 18]=36.

Теорема. $a_1,a_2,...,a_n$ сонларнинг умумий булинувчиси булган m сони бу сонларнинг ЭКУК булиши учун бу сонларнинг хар кандай умумий булинувчисининг m га булиниши зарур ва етарли.

I. Зарурлиги. $[a_1,a_2,...,a_n]=k$ дейлик. m сон a_1, a_2, ..., a_n сонларнинг ихтиёрий умумий булинувчиси булсин ва у бу сонларнинг хар кандай бошка умумий булинувчиларига булинсин. Исбот килиш керак m нинг ЭКУК эканлигини. m ни k га колдикли буламиз, яъни $m=kq+r$ $(0<r<k)$. $m\vdots a_i$ $(I=\overline{1,n})$, $k:a_i$ $(i=\overline{1,n})$. $r=m-kq=>r\vdots a_i$ $(i=\overline{1,n})$. Демак, r сон a_i сонлар учун умумий булинувчи экан. Лекин $r<k$ ва $r\vdots a_i$ $(i=\overline{1,n})$ эканлигидан r=0 келиб чикади. Шунинг учун $m=kq$, яъни $m\vdots k$ булади.

II. Етарлилиги. m сон a_i сонларнинг ихтиёрий умумий булинувчиси булиб, у бу сонларнинг хар кандай бошка умумий булинувчисини булсин. У холда m сон ЭКУК булган к ни булади, яъни $k\vdots m$ келиб чикади

Демак, $m\vdots k$ ва $k\vdots m$ булгани учун k=m келиб чикади.

Теорема. a ва b натурал сонлар булганда $[a;b]=\dfrac{ab}{(a;b)}$ тенглик уринли.

Бу теоремани исботи [1,2] да берилган.

Агар $[a_1a_2,...,a_n]=m$ булиб, $[a_1;a_2]=m_2$,$[m_2;a_2]=m_3$,...,$[m_{n-1};\ a_n]=m_n$ булса, у холда $m_n=m$ булади.

Мисол. 1. 12 ва 18 сонларнинг ЭКУКни топинг.

Ечиш. $[12; 18]=\frac{12\cdot 18}{(12;18)}=\frac{12\cdot 18}{6}=36$, [12;18]=36.

2. 12, 18, 24 сонларнинг ЭКУКни топинг.

Ечиш.

[12; 18] =36, [36; 24]=?

$[36;24]=\frac{36\cdot 24}{(36;24)}=\frac{36\cdot 24}{12}=72$, [36; 24] =72

Демак, [12, 18, 24]=72 булади.

Текшириш саволлари

1. Иккита сонинг ЭКУБ деб нимага айтилади?
2 .n та соннинг ЭКУБ кандай топилади?
3. Иккита соннинг ЭКУК деб нимага айтилади?
4. n та соннинг ЭКУК кандай топилади?
5. Узаро туб сонлар деб нимага айтилади?
6. Евклид алгаритимини тушунтириб беринг.

Таянч тушунчалар

1. Туплам.
2. Натурал, бутун сонлар ва .улар устида амаллар.
3. Булувчи, булинувчи.
4. Колдикли булиш.
5. Туб сонлар.

6,7-маърузалар

Чекли занжир касрлар ва уларнинг хоссалари (2 соат)

Режа:

1. Узлуксиз занжир каср.
2. Чекли занжир каср.
3. Рационал сонни чекли занжир касрга ёйиш.
4. Муносиб касрлар ва уларнинг хоссалари.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси. II кисм. Т.: Укитувчи. 1995 й. (16-22-бетлар).
2. Куликов Л.Я. Алгебра и теория чисел. М.: Высш.шк. 1972 г. (стр.380-385).

Таъриф. Ушбу

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \ldots \\ \ldots + \cfrac{b_k}{a_k}}} \qquad (1)$$

($a_i(i=\overline{0,k}),b_j(j=\overline{1,k})$ бутун сонлар) курининшдаги ифода узлуксиз занжир каср дейилади. Агар (1) да $b_1=b_2= \ldots =b_k=l$, a_0-бутун сон, a_1, a_2, ...,a_k-натурал сонлар булиб $a_k>1$ булса, у холда ушбу

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots \\ + \cfrac{1}{a_k}}} \qquad (2)$$

ифодани чекли занжир каср дейилади.

a_0, a_1,a_2, ..., a_k сонлар чекли занжир касрнинг элементлари дейилади, (2) ни кискача (a_0, a_1, a_2, ...,$a_к$) ёки $a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_к}$ курининшларда хам белгиланади.

Теорема. Хар кандай рационал сон чекли занжир касрга ёйилади ва бу ёйилма ягона булади.

Исботи. $\frac{m}{n}$ ($n\geq 1$) рационал сон берилган булсин. m ни n га колдикли буламиз ва Евклид алгоритмидан фойдаланамиз, яъни

$$\begin{cases} m=nq_1+r_1 \ (0<r_1<n), \\ n=r_1q_2+r_2 \ (0<r_2<r_1), \\ r_1=r_2q_2+r_3 \ (0<r_3<r_2), \\ \text{-- -- - - - - - - - - - -} \\ r_{k-2}=r_{k-1}q_k+r_k \ (0<r_k<r_{k-1}), \\ r_{k-1}=r_kq_{r+1} \end{cases} \qquad (3)$$

системага эга буламиз. (3) даги тенгликларнинг хар икки кисмини мос равишда n, r_1 , r_2...,r_{k-1},r_k ларга кетма-кет булиб куйидаги тенгликларни хосил киламиз:

$$\begin{cases} \frac{m}{n} = q_1 + \frac{r_1}{n}, \\ \frac{m}{n} = q_2 + \frac{r_2}{r_1}, \\ \frac{r_1}{r_2} = q_3 + \frac{r_3}{r_2}, \\ \text{.....} \\ \frac{r_{k-2}}{r_{k-1}} = q_k + \frac{r_k}{r_{k-1}}, \\ \frac{r_{k-1}}{r_k} = q_{k+1}. \end{cases} \qquad (4)$$

(4) системадаги тенгликлардан

$$\frac{m}{n} = q_1 + \frac{r_1}{n} = q_1 + \frac{1}{\frac{n}{r_1}} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_{k+1}}}},$$

$$\frac{m}{n} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_{k+1}}}} \quad (q_{k+1}>1) \qquad (5)$$

ифодани хосил киламиз. (5) ифода $\frac{m}{n}$ (n≥1) рационал соннинг чекли занжир касрга ёйилмаси булади. Бу ёйилманинг ягоналигини исботлашни мустакил иш учун ажратамиз.

(5) да куйидаги 3 хол булиши мумкин:

1. m>n булса, $q_1>0$ булади;
2. m<n булса, $q_1=0$ булади;
3. m<0 булса, $\frac{m}{n}$ нисбатни $\frac{m}{n} = -t + \frac{r_1}{r}$ (t>0) куринишда ёзиб оламиз.Бу ерда $\frac{r_1}{r}$ ту²ри мусбат каср сон булади. Натижада $\frac{m}{n} = -t + \frac{r_1}{r} = \overline{(-t, q_2, q_3, \ldots, q_{k+1})}$ ёйилма хосил булади.

Хар кандай бутун сонни бир булакли узлуксиз каср деб караш мумкин.

Масалан, 5=(5). $\frac{1}{a}$ (a > 1) курнишдаги касрни икки булакли узлуксиз каср деб караш мумкин.

Агар (5) ифодада $q_{k+1}>1$ булса, у холда $\frac{m}{n}$ рационал соннинг чекли занжир касрга ёйилмаси ягона булади. Агар (5) да $q_{k+1}>1$ шарт куйилмаган булса, у холда $q_{k+1}=(q_{k+1}-1)+\frac{1}{1}$ тенгликка асосан $\left(\overline{q_1, q_2, q_3, \ldots, q_{k+1}}\right) = \left(\overline{q_1, q_2, \ldots, q_{k+1}-1,1}\right)$ ёзиш мумкин. Бу тенгликнинг унг томонидаги ёйилма булаклар сони билан чапдаги ёйилма булаклари сони тенг эмас.

Мисол. $\frac{55}{16}$ сонини чекли занжир касрга айлантиринг.

Ечиш. $55=16\cdot3+7,$
$16=7\cdot2+2,$
$7=2\cdot3+1,$
$2=1\cdot2+0.$

Демак, $\frac{55}{16} = 3 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2}}}$ булади.

$T = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots + \cfrac{1}{a_n}}}$ булсин.

$A_0=a_0$ деб олайлик. У холда буни нолинчи тартибли муносиб каср дейилади.

$A_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$ – биринчи тартибли муносиб каср дейилади.

$A_2 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$ – иккинчи тартибли муносиб каср дейилади.

.....

$A_n=T$ эса n-тартибли муносиб каср дейилади.

$A_0 = \frac{a_0}{1} = \frac{P_0}{Q_0}$ деб белгилайлик. У холда $P_0=a_0$, $Q_0=1$ хосил булади;

$A_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{P_1}{Q_1}$ десак, у холда $P_1=a_0a_1+1, Q=a_1$ хосил булади;

$A_2 = a_0 + \dfrac{1}{a_1 + \dfrac{1}{a_2}} = \dfrac{P_2}{Q_2}$ - иккинчи тартибли муносиб каср;

.....

$A_n=T=\dfrac{P_n}{Q_n}$ n- тартибли муносабат каср.

Шу йул билан

$$P_0,P_1,P_2,... \quad (6)$$

$$Q_0,Q_1,Q_2,... \quad (7)$$

кетма-кетликларни хосил киламиз. Бу кетма-кетликлардан куйидаги рекуррент формулаларни хосил киламиз:

$$P_k=P_{k-1}a_k+P_{k-2}, \quad (8)$$

$$Q_k=Q_{k-1}a_k+Q_{k-2}. \quad (9)$$

Теорема. $A_k = \dfrac{P_k}{Q_k}\left(k = \overline{0,n}\right).$ (10)

(10) тенгликни математик индукция принципи асосида исбот киламиз.

1. к=0 булсин. У холда $A_0=\dfrac{a_0}{1} = \dfrac{P_0}{Q_0}$ булиб, (10) муносабат тўғри булади.

2. Фараз килайлик (10) тенглик k учун тўғри булсин. Унинг *k+1* учун тўғрилигини исбот килайлик.

Исботи. $A_{k+1} = a_0 + \dfrac{1}{a_1 + ... + \dfrac{1}{a_{k+1}}}, A_k = a_0 + \dfrac{1}{a_1 + ... + \dfrac{1}{a_k}}$

$$A_k = \frac{P_k}{Q_k} = \frac{P_{k-1}a_k + P_{k-2}}{Q_{k-1}a_k + Q_{k-2}}.$$

$$A_{k+1} = \frac{P_{k-1}(a_k + \frac{1}{a_{k+1}}) + P_{k-2}}{Q_{k-1}(a_k + \frac{1}{a_{k+1}}) + Q_{k-2}} = \frac{P_{k-1}(a_k a_{k+1} + 1) + a_{k+1} \cdot P_{k-2}}{Q_{k-1}(a_k a_{k+1} + 1) + a_{k+1} \cdot Q_{k-2}} =$$

$$= \frac{P_{k-1}a_k a_{k+1} + P_{k-1} + P_{k-2}a_{k+1}}{Q_{k-1}a_k a_{k+1} + Q_{k-1} + Q_{k-2}a_{k+1}} = \frac{P_{k-1}a_k + \frac{P_{k-1}}{a_{k+1}} + P_{k-2}}{Q_{k-2}a_k + \frac{Q_{k-1}}{a_{k+1}} + Q_{k-2}} =$$

$$= \frac{P_k + \frac{P_{k-1}}{a_{k+1}}}{Q_k + \frac{Q_{k-1}}{a_{k+1}}} = \frac{P_k a_{k+1} + P_{k-1}}{Q_k a_{k+1} + Q_{k-1}} = \frac{P_{k+1}}{Q_{k+1}},$$

$$A_{k+1} = \frac{P_{k+1}}{Q_{k+1}}$$

Демак, (10) муносабат уринли экан.

$\frac{P_k}{Q_k} - k -$тартибли муносиб каср дейилади. $P_к$-к–тартибли муносиб касрнинг сурати ,Q_k –к- тартибли муносиб касрнинг махражи дейилади.

$P_{-2}=0$, $P_{-1}=1$, $Q_{-2}=1$,$Q_{-1}=0$ деб белгилайлик. Лекин уларнинг узи маънога эга эмас. Юкоридаги тушунчалардан куйидаги жадвални тузамиз:

k	-2	-1	0	1	2	...	n-1	n
A_k	-	-	a_0	a_1	a_2	...	a_{n-1}	a_n
P_k	0	1	P_0	P_1	P_2	...	P_{n-1}	P_n
Q_k	1	0	Q_0	Q_1	Q_2	...	Q_{n-1}	Q_n

Бу жадвалда хоналар (8) ва (9) формулалар оркали тулдирилади.

Мисол. $\frac{a}{b} = 2 + \frac{1}{1} + \frac{1}{1} + \frac{1}{3} + \frac{1}{1} + \frac{1}{2}$ булса, $\frac{a}{b}$ ни топинг.

Ечиш. $a_0=2$,$a_1=a_2=a_4=1$, $a_3=3$, $a_5=2$, a=?, b=?

k			0	1	2	3	4	5
$a_к$			2	1	1	3	1	2
$P_к$	0	1	2	3	5	18	23	64
Q_k	1	0	1	1	2	7	9	25

Бу жадвалдан куринадики, $\frac{P_5}{Q_5} = \frac{64}{25}$ эканлиги. Шу сабабли a=64, b=25 булиб, $\frac{a}{b} = \frac{64}{25}$ булади.

Теорема.

$$P_кQ_{k-1}-P_{k-1}Q_k=(-1)^{k-1} \qquad (11)$$

тенглик к нинг хар кандай кийматида ту²ри булади.

(11) тенгликнинг ростлигини математик индукция принципи асосида исбот киламиз.

1. k=l булсин. У холда $P_1Q_0-P_0Q_1=(a_0a_1+1)\cdot 1-a_0a_1=1=(-1)^{1-1}$ булиб, (11) муносабат рост булади.

2. Фараз килайлик (11) муносабат к учун рост булсин. (11) нинг к+1 учун рост эканлигини исбот килайлик, яъни $P_{k+1}\,Q_k - P_kQ_{k+1} = (-1)^k$ булишини исбот килайлик

Исботи. $P_{k+1}Q_k-P_kQ_{k+1}=(P_ka_{k+1}+P_{k-1})Q_k-P_k(Q_ka_{k+1}+Q_{k-1})=$

$=P_kQ_ka_{k+1}+P_{k-1}Q_k-P_kQ_ka_{k+1}-P_kQ_{k-1}=-(P_kQ_{k-1}-P_{k-1}Q_k)=$

$=-(-1)^{k-1}=(-1)^k=(-1)^{k+1-1}$.

Демак, (11) тенглик $\forall k \in N$ булган рост экан.

Теорема. $A_к = \frac{P_к}{Q_k}$ муносиб касрнинг сурати билан махражи узаро туб, яъни $(P_к;Q_к)=1$ булади.

Исбот. Фараз килайлик $(P_к;Q_k) \neq d$ булиб $d>1$ булсин.

У холда $P_к:d, Q_k:d$ булади. Булиниш муносабати хоссаларига кура $P_к\ Q_{k-1}:d, P_{k-1}Q_k:d$ муносабатларни эътиборга олсак (11) тенгликдан $(P_кQ_{k-1}-P_{k-1}Q_k):d$ яъни

$(-1)^{л-1}$:d булиб, бу муносабат эса факат d=1 булганда уринли булади. Демак, $(P_к;Q_k)=1$ булади.

Бу теоремадан куринадики, $\frac{P_к}{Q_k}$ муносиб каср кискармас каср эканлиги.

$\frac{a}{b}$ рационал сон занжир касрга $\frac{a}{b} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + ... + \frac{1}{a_n}$ куринишда ёйилган булсин. $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, ..., \frac{P_n}{Q_n}$ кискармас каср булиб, $\frac{a}{b} = \frac{P_n}{Q_n}$ булади. $(a;b)=1$ ва $\frac{a}{b} = \frac{P_n}{Q_n}$ эканлигидан $P_n=a$, $Q_n=b$ хосил булади.

Текшириш саволлари.

1. Узлуксиз каср деб нимага айтилади?
2. Чекли занжир каср деб нимага айтилади?
3. Рационал сонни чекли занжир касрга ягона йул билан ёйишни баён этинг.
4. Муносиб касрлар хакида тушунча беринг?
5. Муносиб касрлар хакидаги теоремаларни баён этинг?
6. Чекли занжир касрларга мисоллар келтиринг?

Таянч тушунчалар

1. Рационал сонлар ва улар устида амаллар
2. Евклид алгоритми.

8-маъруза

Систематик сонлар ва улар устида амаллар (2соат)

Режа:

1. Санок системалари.
2. Систематик сонлар.
3. Систематик сонлар устида амаллар.
4. Бир санок системасидан бошка санок системасига утиш.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси. I кисм. Т.: Укитувчи. 1993 й. (36-47-бетлар).

3. Куликов Л.Я.Алгебра и теория чисел. М.: Высш. шк. 1972 г. (стр.385-389).

Урта мактаб, академик лицей, касб-хунар коллежлари математикасидаги барча хисоблашлар унлик санок системаси асосида урганилади.

Унлик санок системасидан бошка 2, 5, 7, 12, 60, ... санок системалари хам мавжуд. Бу санок системаларининг барчаси битта умумий йуналиш асосида курилади ва куйидаги теорема уринли:

Теорема. m>1 натурал сон булиб, M={0, 1, 2, ..., m-1} туплам берилганда хар кандай a натурал сон учун ушбу

$$a=a_0+a_1m+a_2m^2+...+a_nm^n=a_0m^0+a_1m^1+...+a_nm^n$$
$$(a_i\in M, i=\overline{1,n}, a_n\neq 0) \qquad (1)$$

ёйилма мавжуд ва ягонадир.

Теореманинг исботи [1, 2] да берилган.

Таъриф. a натурал соннинг (1) куриниши a ни m нинг даражалари буйича ёйиш дейилади.

m=10 булсин. У холда

$$m=a_n10^n+a_{n-1}10^{n-1}+...+a_1\cdot 10+a_0 \ (0\le a_i\le 9,\ i=\overline{0,n-1},\ 1\le a_n\le 9) \qquad (2)$$

булади.

(2) ни кискача $m=\overline{a_n a_{n-1}...a_1a_0}$ куринишда хам ёзилади.

Мисол. $27346=20000+7000+300+40+6=2\cdot 10^4+7'\cdot 10^3+$
$+3\cdot 10+4.10+6.$

Агар g≥2 ихтиёрий натурал сон булса, хар кандай m натурал сон учун юкоридаги теоремага кура ушбу

$$m=a_ng^n+a_{n-1}g^{n-1}+...+a_1g+a_0 \ (0\le a_i\le g-1, I=\overline{0,n-1}, 1\le a_n\le g-1) \qquad (3)$$

тенгликни ёза оламиз. (3) да $a_0,a_1,...,a_n$ лар m соннинг ракамлари дейилади. (3) ни кискача

$$m=\overline{a_n a_{n-1}...a_1a_0}_g \qquad (4)$$

куринишида ёзиш мумкин.

Таъриф. (3) куринишидаги сон асоси g га тенг булган систематик сон дейилади (бундай сондаги турли ракамларнинг сони g га тенг).

$$a=\sum_{i=0}^{\infty}a_ig^i \quad (0\le a_i<g) \qquad (5)$$

$$b=\sum_{i=0}^{\infty}b_ig^i \quad (0\le b_i<g) \qquad (6)$$

сонларни кушиш амалини карайлик.

c=a+b ни g лик санок системасида ёзайлик.

$$a=a_0+a_1g+a_2g^2+...+a_rg^r+... \qquad (7)$$
$$b=b_0+b_1g+b_2g^2+....+b_rg^r+... \qquad (8)$$

булгани учун

$$c=(a_0+b_0)+(a_1+b_1)g+(a_2+b_2)g^2+...+(a_i+b_i)g^i+(a_{i+1}+b_{i+1})\cdot$$
$$\cdot g^{i+1}+...+(a_r+b_r)g^r+...$$

булади. Иккинчидан ихтиёрий с соннинг g нинг даражалари буйича

$$c=c_0+c_1g+c_2 g^2+...+c_rg^r+... \quad (10)$$

каби ёйилмаси мавжуд ва ягона.

(9) ва (10) дан куринадики, с сон икки хил ёйилмага эга эканлиги. Бу икки ёйилма умуман устма-уст тушмай колиши хам мумкин. Бошкача айтганда куйидаги икки хол булиши мумкин:

1. $(a_i+b_i< g) => (a_i+b_i=c_i)$ $(i=0,1,2,...)$.

2. $(a_k+b_k\geq g)=>(c_k=d_k)$.

Бу ерда d_k^сон a_k+b_k ни g га булгандаги колдик. Демак, иккинчи холда c_k коэффициент учун a_k+b_k йи²индини g га булгандаги колдик, олинар экан. Бу холда $a_k+b_k=d_k+g$ тенглик уринли булганидан (9) ёйилмадаги k ва k+1 хадлар куйидагича булади:

$$(a_k+b_k)g^k+(a_{k+1}+b_{k+1})g^{k+1}=(d_k+g)g^k+(a_{k+1}+b_{k+1})g^{k+1}=$$
$$=d_kg^k+(a_{k+1}+b_{k+1}+1)g^{k+1}.$$

Лекин a_{k+1} ва b_{k+1} лар c_{k+1} коэффициентни аникловчилардир. Бошкача айтганда, $a_k+b_k\geq g$ булса, k+1 коэффициентга 1 бирлик кушилар экан.

Мисол. 342_5 ва 134_5 сонларнинг йи²индисини топинг.

1+1=2, 1+2=3, 1+3=4, 1+4=10 $(0+1\cdot5)$, 3+1=4, 3+2=10, 3+3=11 $(1+1\cdot5)$, 4+4=13 $(8_{10}=3\cdot5^0+1\cdot5)$ булгани учун $342_5+134_5=1031_5$, булади.

Айириш амали бир хонали сонларни айириш, кушиш амали асосида бажарилади.

g асосли ихтиёрий a ва b сонларни купайтириш купхадни купхадга купайтириш каби бажарилади.

Исталган системада ёзилган сонларни булиш худди g=10 булган холдаги булишдек бажарилади.

Бизга g асосда ёзилган m сони берилган булсин, яъни $m=\overline{a_n a_{n-1}...a_{0_g}}$ *булсин.* Шу сонни бошка h асосли системада ёзайлик. Айтайлик бу сон h асосли системада $m=\overline{b_p b_{p-1}...b_1 b_{0_h}}$ *кури*нишда ёзилган булсин.

$$m=a_ng^n+a_{n-1}g^{n-1}+...+a_1g+a_{0,}$$
$$m=b_pg^p+b_{p-1}g^{p-1}+...+b_1g+b_0.$$

Максадимиз $b_{0,}$ b_1,b_2,...,b_p ракамларни топиш. Бунинг учун аввало h ни g асосда ёзиб оламиз. У холда

$m=(b_ph^{p-1}+b_{p-1}h^{p-2}+...+b_1)h+b_0=q_1h+b_0$,

$m=q_1h+b_0$ $(0\leq b_0<h)$ тенгликдан b_0 топилади.

$q_1=(b_ph^{p-2}+b_{p-1}h^{p-3}+...+b_2)h+b_1=q_2h+b_1$,

$q_1=q_2h+b_1(0\leq b_1<h)$ тенгликдан b_1 топилади.

Шу жараённи давом эттириб, энг сунгида $q_p=q_{p+1}h+b_p$ $(0\leq b_p<h)$ тенгликдан b_p топилади. Демак, m соннинг h асосли системадаги b_0,b_1, ...,b_p ракамларини топдик.

Мисол. 3724_8 сонни 11 лик системада ёзинг.

Ечиш. g=8, h=ll. Аввало 11 ни 8 асосда $ll=13_8$ куринищда ёзиб оламиз. Кейин куйидагиларни бажарамиз:

$3724_8 \mid 13_8$

$26_8 \quad 266_8$

112_8

102_8

104_8

102_8

$2_6 = 2_{11}$

$266_8 \mid 13_8$

$26_8 \quad 20_8$

$6_8 = 6_{11}$

$20_8 \mid 13_8$

$13_8 \quad 1_8 = 1_{11}$

$5_8 = 5_{11}$

Демак, $3724_8=1562_{11}$ булар экан.

Текшириш саволлари

1. Санок системалари хакида тушунча беринг.
2. Систематик сон деб нимага айтилади?
3. Систематик сонлар устида амалларга доир мисоллар келтиринг.
4. Бир санок системасидан бошка санок системасига утишга доир мисол келтиринг.

Таянч тушунчалар

1. Унли санок, системаси ва улар устида амаллар.
2. Соннинг унли асосдаги ёйилмаси.

9,10-маърузалар

Бутун сонлар халкасида таккосламалар ва уларнинг хоссалари (4 соат)

Режа

1. Таккосламанинг таърифи.
2. Таккосламанинг содда хоссалари.
3. Мисол.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси.II кисм. Т.: Укитувчи. 1993 й. (51 - 55-бетлар).
2. Куликов Л.Я. Алгебра и теория чисел. М.: Высш.шк. 1972 г. (стр.397-399).

Айтайлик Z-бутун сонлар халкаси булиб, $m \geq 1$ натурал сон булсин.

Таъриф. Агар Z халкага тегишли a ва b сонларни m натурал сонга булганда хосил булган колдиклар бир хил булса, ёки a-b айирма m га булинса, ёки $a=b+mq$ тенглик уринли булса, у холда **a ва b** сонлар m модуль буйича таккосланади дейилади ва уни $a \equiv b(\mathrm{mod}\, m)$ куринишда белгиланади.

Мисол. $15 \equiv 3(\mathrm{mod}\, 4)$, $5 \equiv -3(\mathrm{mod}\, 4)$, $20 \equiv 0(\mathrm{mod}\, 5)$.

Таккосламалар куйидаги хоссаларга эга:

1^0. Таккослама эквивалент бинар муносабат.

Бу хоссанинг исботи [1]да келтирилган.

2^0.Бир хил модулли таккосламаларни хадма-хад кушиш (айириш) мумкин.

Исботи. $a \equiv b(\text{mod} m)$, $c \equiv d(\text{mod} m)$ таккосламалар берилган булсин. Булардан $a=b+mq_1$, $c=d+mq_2$ тенгликларни ёза оламиз. Уларни хадма-хад кушиб (айириб) $a \pm c=(b \pm d)+m(q_1 \pm q_2)$ тенгликка эга буламиз. Бу эса $a \pm c \equiv (b \pm d) (\text{mod } m)$ демакдир.

Бу иш n та $a_1 \equiv b_1(\text{mod } m)$, $a_2 \equiv b_2(\text{mod } m),...,a_n \equiv b_n (\text{mod } m)$ таккосламалар учун хам бажарилади, яъни $a_1 \pm a_2 \pm ... \pm a_n \equiv (b_1 \pm b_2 \pm ... \pm b_n) (\text{mod } m)$ таккосламани хосил киламиз.

Натижа. Таккосламанинг бир кисмидаги сонни унинг иккинчи кисмига карама-карши ишора билан утказиш мумкин.

Бу натижанинг исботи [1] да келтирилган.

Натижа. Таккосламанинг ихтиёрий кисмига модулга каррали сонни кушиш мумкин.

Бу натижанинг исботи [1] келтирилган.

3^0. Бир хил модулли таккосламаларни хадма-хад купайтириш мумкин.

Бу хоссанинг исботи [1, 2] да келтирилган.

Натижа. Таккосламанинг икки кисмини (модулни узгартирмай) бир хил натурал даражага кутариш мумкин.

Бу натижанинг исботи [1] да келтирилган.

4^0. Модулни узгартирмаган холда таккосламанинг икки кисмини бир хил бутун сонга купайтириш мумкин.

Бу хоссанинг исботи [1] да келтирилган.

5^0.Агар $x \equiv y(mod\ m)$ булса, у холда ихтиёрий бутун коэффициентли $f(x)=a_0x^n+a_1x^{n-1}+... +a_{n-1}x+a_n$, $f(y)=a_0y^n+a_1y^{n-1}+...+a_{n-1}y+a_n$ купхадлар учун $f(x)=f(y) (mod\ m)$ таккослама уринли булади.

Бу хоссанинг исботи [1] да келтирилган.

6^0.Агар бир вактда $a_i=b_i (mod\ m)(i=\overline{1,n})$ ва $x= y (mod\ m)$ таккосламалар уринли булса, у холда

$a_0 x^n+a_1 x^{n-1l}+...+a_{n-1}x +a_n = b_0 y^n + b_1 y^{n-1} +...+$

$+b_{n-1} y+b_n(mod\ m)$ таккослама уринли булади.

Исботи. $x= y(mod\ m)$ булгани учун 3-хоссанинг натижасига кура

$$x^n \equiv y^n (\text{mod } m),$$
$$x^{n-1} \equiv y^{n-1} (\text{ mod } m),$$
$$. . . . . .$$
$$x \equiv y (\text{mod } m),$$
$$1 \equiv 1 (\text{mod } m)$$

таккосламаларни хосил киламиз. Берилганга кура

$$a_0 = b_0 (\text{mod } m),$$
$$a_1 \equiv b_1 (\text{mod } m),$$
$$. . . . . .$$
$$a_n \equiv b_n (\text{mod } m)$$

булиб, мос равишда бу таккосламаларни юкоридаги таккосламалар билан хадма-хад купайтириб, кейин кушилса теоремадаги исбот килиш керак булган таккослама хосил булади.

Натижа. Таккосламада катнашувчи кушилувчини узи билан тенг колдикли булган иккинчи сонга алмаштириш мумкин.

Бу натижанинг исботи [1] да келтирилган.

7^0. Таккосламанинг икки кисмини модуль билан узаро туб булган купайтувчига кискартириш мумкин.

Бу хоссанинг исботи [1, 2] да келтирилган.

8^0. Таккосламанинг икки кисмини ва модулини бир хил мусбат сонга купайтириш, таккосламанинг икки кисми ва модули умумий купайтувчига эга булса, у

холда бу таккосламанинг икки кисми ва модулини бу умумий купайтувчига булиш мумкин.

Бу хоссанинг исботи [1, 2] да келтирилган.

9^0. Агар таккослама бир неча модуль буйича уринли булса, у холда бу таккослама шу модулларнинг энг кичик умумий булинувчиси буйича хам уринли булади.

Бу хоссанинг исботи [1] да келтирилган.

10^0. Агар таккослама бирор m модуль буйича уринли булса, у холда бу такдослама модулнинг ихтиёрий булувчиси буйича хам уринли булади.

Бу хоссанинг исботи [1, 2] да келтирилган.

11^0. Таккосламанинг бир кисми ва модулининг ЭКУБ билан унинг иккинчи кисми ва модулининг ЭКУБ узаро тенг булади.

Исботи. $a\equiv b(\mathrm{mod}\ m)<=>a=b+mt$ ёки $a-mt=b$ булади. $(a;m)=d$, $(b;m)=d_1$ ва $a=da_1$, $m=dm_1$ булсин. У холда $a-mt=da_1-\ -dm_1t=b$ тенгликнинг чап кисми d га булинишидан b нинг хам d га булиниши келиб чикади.

Демак, d сон b ва m сонларнинг умумий булувчиси экан. У холда $d_1 \vdots d$ булади. $m=d_1m_2$, $b=d_1b_1$ булсин.

У холда $a=b_1d_1+m_2d_1t$ тенгликдан $a \vdots d_1$ келиб чикади, яъни d_1 сон a ва m сонларнинг умумий булувчиси эканлиги келиб чикади. У холда $d \vdots d_1$ муносабат уринли. Демак, $d_1 \vdots d$ ва $d \vdots d_1$ булганидан $d_1=d$ келиб чикади.

Мисол. 1. Агар n ток сон булса, у холда $n^2-1\equiv 0 \pmod 8$ таккосламанинг уринли эканлигини курсатинг.

Ечиш. n ток сон булсин, у холда n-1 ва n+1 сонлари кетма-кет келувчи жуфт сонлар булади. Агар улардан бири 2 га каррали булса, у холда иккинчиси 4 га каррали булади. У холда уларнинг купайтмаси 8 га булинади, яъни

$$(n-1)(n+1)=n^2-1\equiv 0 \pmod 8$$

таккослама уринли булади.

3. $3^{14}\equiv -1 \pmod{29}$ таккосламанинг ту²ри эканлигини текширинг.

Текшириш. $3^{14}=(3^3)^4 \cdot 3^2=27^4 \cdot 3^2 \equiv (-2)^4 \cdot 3^2=144\equiv$

$\equiv -1 \pmod{29}$, яъни $3^{14}\equiv -1 \pmod{29}$ ту²ри таккослама булади.

Текшириш саволлари

1. Таккослама деб нимага айтилади?
2. Таккосламага доир мисоллар келтиринг.
3. Таккосламанинг содда хоссаларини баён этинг.
4. Таккосламанинг хоссаларига доир мисоллар келтиринг.

Таянч тушунчалар

1. Бутун сонлар халкаси.
2. Булиниш муносабати.
3. Эквивалент муносабат.
4. Даражага кутариш.
5. Купхад ва унинг киймати.

11 – маъруза

Эйлер функцияси.Эйлер ва Ферма теоремалари (2соат)

Режа:

1. Модуль буйича чегирмаларнинг тула системаси.
2. Модуль буйича чегирмаларнинг келтирилган системаси.
3. Эйлер функцияси таърифи.
4. Эйлер функциясининг хоссалари.
5. Эйлер функциясини хисоблаш формулалари.
6. Эйлер теоремаси.
7. Ферма теоремаси.
8. Мисол.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси.II кисм. Т.: Укитувчи. 1995 й. (56-67-бетлар).

2. Куликов Л.Я. Алгебра и теория чисел. М.: Высш. шк.1979г. (стр.399-409).

Барча бутун сонларни m≥l натурал сонга булганда 0, 1, 2, ..., m-1 колдиклар хосил булади. Бундай х*ар* бир колдикка бутун сонларнинг бирор синфи мос келади.

Таъриф. m га булинганда r га тенг бир хил колдик берадиган бутун сонлар туплами m модуль буйича чегирмалар синфлари дейилади ва уни $\bar{r}$ каби белгиланади.

Масалан, m=3 булса,

$\bar{0}$={..., -6, -3, 0, 3, 6, ...},

$\bar{1}$={..., -5, -2, 1, 4, 7, ...},

$\bar{2}$={..., -4, -1, 2, 5, 8, ...}

чегирмалар синфлари булади.

Таъриф. Чегирмалар синфининг ихтиёрий элементи шу синфнинг чегирмаси дейилади.

Таъриф. m модуль буйича тузилган хар бир чегирмалар синфидан эркинлик билан биттадан элемент олиб тузилган тупламга m модуль буйича чегирмаларнинг тула системаси дейилади.

Масалан, m=3 булганда 0, 1, 2; -1, -5, 6; 0, -4,4;... системалар 3 модуль буйича чегирмаларнинг тула системаси булади.

Синфнинг битта чегирмаси m модуль билан узаро туб булса, у холда бу синфнинг барча элементлари хам m модуль билан узаро туб булади.

Таъриф. m модуль билан узаро туб булган барча чегирмалар синфидан эркинлик билан биттадан чегирма олиб тузилган туплам чегирмаларнинг m модуль буйича келтирилган системаси дейилади.

Масалан, m=3 булса, у холда 1, 2; -1, 7; -5, 8, ... системалар З модуль буйича чегирмаларнинг, келтирилган системаси булади.

m модуль буйича чегирмаларнинг келтирилган системасидаги элементлар сонини аниклаш учун Эйлер функцияси деб аталувчи φ(m) функциядан фойдаланамиз.

Таъриф. Агар куйидаги иккита шарт бажарилса, у холда φ(m) сонли функция Эйлер функцияси дейилади:

1. φ(1)=1.

2. φ(m) функция m дан кичик ва m билан узаро туб булган натурал сонлар сони.

Мисол. m=10 булса, у холда φ(10)=4 булади, яъни 1 дан 10 гача ва 10 билан узаро туб булган натурал сонлар сони 4 та булади.

Таъриф. Натурал сонлар тупламида аникланган f функция учун (m; n)=1 булганда f(m·n)=f(m)·f(n) тенглик бажарилса, у холда f функцияга мультипликатив функция дейилади.

Теорема. Эйлер функцияси мультипликатив функция булади.

Бу теореманинг исботи [1, 2] да келтирилган.

φ(m) Эйлер функциясини хисоблаш формулалари куйидагилардан иборат:

1. m=p туб сон булса, у холда φ(p)=p-1 булади.

2. m= p^{α} (p-туб сон, α-натурал сон) булса, у холда φ(p^{α})= $=p^{\alpha-1}\cdot(p-1)$ булади.

3. m= $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_к^{\alpha_к}$ булса, у холда

$$\varphi(m)=\varphi\left(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}\right)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$$

булади.

Бу формулаларнинг хосил булиши [1,2] да берилган.

Мисол. φ(540) ни топинг.

Хакикатдан, φ(540)=φ($2^2\cdot3^3\cdot5$)=540(1-$\frac{1}{2}$) (1-$\frac{1}{3}$)(1--$\frac{1}{5}$)=144, φ(540)=144 булади.

Теорема (Эйлер теоремаси). Агар (a; m)=1 булса, у холда $a^{\varphi(m)}\equiv1(\mathrm{mod}m)$ таккослама уринли булади.

Бу теореманинг исботи [1, 2] да келтирилган.

Теорема (Ферма теоремаси). Агар а сон р туб сонга булинмаса, у холда $a^{p-1}\equiv1$ (mod m) таккослама уринли булади.

Бу теореманинг исботи [1, 2] да келтирилган.

Мисол. 1) m=10, a=7 булса, у холда φ(10)=4 булиб $7^4\equiv1(\mathrm{modl0})$ булади.

2) m=7, a=10 булса, у холда φ(7) = 6 булиб, $10^6\equiv1(\mathrm{mod}7)$ булади.

Текшириш саволлари

1. Модуль буйича чегирмаларнинг тула системаси деб нимага айтилади?
2. Модуль буйича чегирмаларнинг келтирилган системаси деб нимага айтилади?
3. Эйлер функцияси деб нимага айтилади?
4. Мультипликатив функция деб нимага айтилади?
5. Эйлер функцияси кандай хоссаларга эга?
6. Эйлер функциясини хисоблаш формулаларини ёзиб беринг.
7. Эйлер теоремасини баён этинг.
8. Ферма теоремасини баён этинг.

Таянч тушунчалар

1. Барча бутун сонлар туплами.
2. Таккосламалар.
3. Колдикли булиш.
4. Узаро туб сонлар.

12,13–маърузалар

Биринчи даражали ва туб модуль буйича юкори даражали таккосламалар (4 соат)

Режа:

1. Бир номаълумли таккосламалар хакида тушунчалар.
2. Бир номаълумли биринчи даражали таккосламалар ва уларни ечиш усуллари.

3. Туб модулли юкори даражали таккосламалар.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси.II кисм. Т.: Укитувчи. 1995 й. (67-76-бетлар).

2. Куликов Л.Я. Алгебра и теория чисел. М.: Высш. шк. 1979 г. (стр.409-413).

Коэффициентлари бутун сонлардан иборат $f(x)= a_0 x^n+ +a_1\cdot \cdot x^{n-1} ...a_{n-1}x+a_n$ купхад берилган булсин.

Таъриф. Ушбу

$f(x)\equiv 0(modm)$ (a_0 сон m га булинмайди, $a_i\in Z$, $m\geq 1$) (1)

куринишдаги таккосламани бир номаълумли n- даражали таккослама дейилади.

Таъриф. Агар x=c булганда

$$f(c)\equiv 0(modm) \quad (2)$$

таккослама туғри булса, у холда c сон (1) таккосламани каноатлантиради дейилади.

Теорема. Агар c сон (1) таккосламани каноатлантирса, у холда $\bar{c}$ чегирмалар синфига тегишли ихтиёрий сон хам (1) таккосламани каноатлантиради.

Исботи. Берилишига кура $f(c)\equiv 0$ (modm) туғри таккосламадир.

$\forall b\in \bar{c}$ булсин. У холда $b\equiv c(modm)$ булиб, таккосламалар хоссасига кура $f(b)\equiv f(c)$ булади.Бунда $f(c)\equiv 0(modm)$ эканлигини эътиборга олсак, $f(b)\equiv 0(modm)$ келиб чикади. Демак, $\bar{c}$ синфга тегишли ихтиёрий b сон хам таккосламанинг ечими булар экан.

Таъриф. Агар c сон (1) таккосламани каноатлантирса, у холда $\bar{c}$ чегирмалар синфи (1) таккосламанинг ечими дейилади.

m модуль буйича барча чегирмалар синфи $\bar{0},\bar{1},\bar{2},...,\overline{m-1}$ булади. Демак, m модулли таккосламани каноатлантирувчи сонларни 0,1,2,..., m-1 сонлар ичидан кидириш лозим.

Мисол. $x^3 - 2x+ 6\equiv 0(mod\ 11)$ таккосламани ечинг.

Ечиш. 11 модуль буйича чегирмалар синфлари $\bar{0},\bar{1},\bar{2},...,\overline{10}$ булади. Берилган таккосламани каноатлантирувчи сонларни 0, 1, 2, ..., 10 сонлар ичидан кидириш керак.

$f(0)\equiv 0(modll)$, $f(l)\equiv 0(modll)$, $f(2)\equiv 0(modll)$, $f(3)\equiv 0(mod11)$, $f(4)\equiv 0(modll)$, $f(6)\equiv 0(modll)$, $f(7)\equiv 0(modll)$, $f(8)\equiv 0(modll)$, $f(9)\equiv (mod11)$, $f(10)\equiv (modll)$ таккосламаларнинг хеч бири туғри таккослама эмас. Лекин $f(5)\equiv 0(mod11)$ таккослама туғри таккослама булади. Демак, 5 сон берилган таккосламани каноатлантиради. Шунинг учун $\bar{5}$ синф бу таккосламанинг ечими булади.

Таъриф. Ечимлари туплами устма-уст тушган таккосламаларни тенг кучли таккосламалар дейилади.

Агар (1) таккосламанинг икки кисмига ихтиёрий купхад кушилса ёки хар икки кисмини m модуль билан узаро туб булган k сонга купайтирилса, ёки икки кисми ва модулини k натурал сонга купайтирилса, у холда хосил булган таккослама берилган таккосламага тенг кучли булади.

Таъриф. Ушбу

$$ax\equiv b(modm)\ (a,b\in Z,\forall m\in N) \quad (3)$$

куринишдаги таккосламага бир номаълумли биринчи даражали таккослама дейилади.

Теорема. Агар (a;m)=1 булса, у холда (3) таккослама ягона ечимга эга булади.

Исботи. Эйлер теоремасига кура $a^{\varphi(m)}\equiv 1(modm)$ таккослама уринли. (3) таккосламанинг икки кисмини $a^{\varphi(m)-1}$ га купаитириб $a^{\varphi(m)}x\equiv ba^{\varphi(m)-1}(modm)$ таккосламага эга буламиз. Бунда $a^{\varphi(m)}\equiv 1(modm)$ эканлигини эътиборга олсак,

$$x \equiv ba^{\varphi(m)-1} (\mathrm{mod} m) \qquad (4)$$

ечимга эга буламиз (Бу ечимнинг ягоналигини мустакил равишда исботланг).

(3) нинг ечимини (4) оркали топиш (3)ни Эйлер усулида ечиш дейилади.

Мисол. $5x \equiv 3 (\mathrm{mod} 8)$ таккосламани ечинг.

Ечиш. (5; 8)=1. Шу сабабли бу таккослама ягона ечимга эга. Бу ечимни Эйлер усулида топайлик. $\varphi(8)=4$. У холда (4) га кура

$x \equiv 3 \cdot 5^{4-1} (\mathrm{mod} 8)$, $x \equiv 3 \cdot 5^3 (\mathrm{mod} 8)$, $x \equiv 3 \cdot 125 (\mathrm{mod} 8)$, $x \equiv 3 \cdot 5 (\mathrm{mod} 8)$, яъни $x \equiv 7 (\mathrm{mod} 8)$.

Текшириш. x=7 булсин. У холда $5 \cdot 7 \equiv 3 (\mathrm{mod} 8) <=> 35-3 = 32:8$, яъни $35 \equiv 3 (\mathrm{mod} 8)$ таккослама ту²ри. Демак,7 сон берилган таккосламани каноатлантиради.У холда 7 сон билан таккосланувчи барча сонлар берилган таккосламани каноатлантиради, яъни $x \equiv 7 (\mathrm{mod} 8)$ ёки $\overline{7}$ ечим экан.

(3) таккосламани ечишнинг Эйлер усулидан бошка синаш, коэффициентларини узгартириш усули, чекли занжир касрдан фойдаланиш усуллари хам мавжуд. Бу усуллар [1, 2] да берилган.

Теорема. Агар (a; m)=d булиб, b сон d га булинмаса, у холда (3) таккослама ечимга эга эмас.

Исботи. Фараз килайлик (3) таккослама $x \equiv \alpha (\mathrm{mod} m)$ ечимга эга булсин. У холда $a\alpha \equiv b (\mathrm{mod} m)$ таккослама ту²ри булади, яъни $a\alpha \equiv b+mq$ булиб, бундан $a\alpha - mq = b$ тенгликни ёза оламиз. $a \vdots d$ булгани учун $a\alpha \vdots d$ ва $m \vdots d$ булгани учун $mq \vdots b$ булиб, $(a\alpha - mq) \vdots d$, яъни $b \vdots d$ келиб чикади. Бунинг булиши мумкин эмас, чунки бу берилган шартга зиддир. Демак, (3) таккослама ечимга эга эмас экан.

Мисол. $12x \equiv 11 (\mathrm{mod} 8)$ таккосламада (12; 8)=4 булиб, 11 сон 4 га булинмайди. Демак, берилган таккослама ечимга эга эмас.

Теорема. Агар (3) таккосламада (a; m)=d булиб, b сон d га булинса, у холда (3) таккослама сони d га тенг булган ушбу

$$\overline{\alpha},\ \overline{\alpha + \frac{m}{d}}, \ldots, \overline{\alpha + \frac{(d-1)m}{d}} \qquad (5)$$

ечимларга эга булиб, бундаги α ечим $\frac{a}{d}x \equiv \frac{b}{a} (\mathrm{mod} \frac{m}{d})$ таккосламанинг ягона ечими булади.

Бу теореманинг исботи [1, 2] да делтирилган.

Энди туб модулли юкори даражали таккосламаларни карайлик. 9,10-маърузалардаги таккосламаларнинг, 10-хоссасига асосан, хар кандай мураккаб модулли таккосламаларни хар доим туб модулли таккосламаларга келтириш мумкин. Туб модулли таккосламалар устида иш курайлик.

Таъриф. Агар $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$, $a_i \in Z$, p-туб сон, a_0сон p га булинмаса, у холда ушбу

$$f(x) \equiv 0 (\mathrm{mod}\ p) \qquad (6)$$

таккосламага туб модулли п-даражали бир номатьлумли таккослама дейилади.

Теорема. Агар (6) таккосламада a_0 бош коэффициент p га булинмаса, у холда (6) таккослама бош коэффициента 1 га тент булган бошка бир таккосламага тенг кучли булади.

Исботи.a_0сон p га булинмаса $\Leftrightarrow (a_0, p)=1$. У холда

$$a_0\, y \equiv 1 (\mathrm{mod} p) \qquad (7)$$

таккослама ягона ечимга эга булади. (7) ни каноатлантирувчи сонлардан бири y_0 булсин, яъни $a_0\, y \equiv 1 (\mathrm{mod} p)$ ту²ри таккослама булсин. (1) нинг хар икки кисмини y_0 га купайтириб,

$$(a_0y_0)x^n + (a_1y_0)x^{n-1} + \ldots + (a_ny_0) \equiv 0 (\mathrm{mod} p) \qquad (8)$$

таккосламага эга буламиз. (8) нинг чап кисмидаги коэффициентларни р модуль билан таккосланувчи сонлар билан куйидагича алмаштирайлик:

$a_0y_0 \equiv 1(\text{mod}p)$, $a_1y_0 \equiv b_1(\text{mod}p)$, $a_2y_0 \equiv b_2(\text{mod}p)$, ... , $a_ny_0 \equiv \equiv b_n(\text{mod}p)$. У холда $x^n+b_1 x^{n-1} +...+b_n =0(\text{mod } p)$, яъни бош коэффициенти 1 га тенг булган таккосламага эга буламиз.

Теорема. Агар f(x) ва g(x) коэффициентлари бутун сонлардан иборат купхадлар булса, у холда

$$f(x) \equiv 0(\text{mod } p), \quad (7)$$

$$f(x)-(x^p-x)g(x) \equiv 0(\text{mod}p) \quad (8)$$

таккосламалар тенг кучли булади.

Исботи. Фараз килайлик x_0 сон (7) ни каноатлантирсин, яъни

$$f(x_0) \equiv 0(\text{mod}p) \quad (9)$$

булсин. Ферма теоремасига асосан ихтиёрий а сон учун $a^p-a \equiv 0(\text{mod}p)$ таккослама ту²ри булади. Бунда $a \equiv x_0$ булса, у холда

$$x_0^p- x_0 \equiv 0(\text{mod}p) \quad (10)$$

таккослама ту²ри булади. (10) нинг хар икки кисмини $g(x_0)$ га купайтириб

$$(x_0^p - x_0)g(x_0) \equiv 0(\text{mod}p) \quad (11)$$

таккосламага эга буламиз. (9) дан (11) ни айириб

$$f(x_0)-(x_0^p-x_0)g(x_0) \equiv 0(\text{mod}p) \quad (12)$$

таккосламани хосил киламиз. Бу эса x_0 сон (8) ни каноатлантиришини курсатади.

Айтайлик x_0 сон (8)ни каноатлантирсин, яъни (12) муносабат уринли булсин. У холда (12) га (11) ни куйиб (9)ни хосил киламиз. Бундан куринадики, x_0 сон (7) ни каноатлантириши. Демак, (7) ва (8) таккосламалар тенг кучли экан.

Бу теоремадан фойдаланиб куйидаги теорема исботланади:

Теорема. Даражаси n (n>p) булган р туб модулли таккослама даражаси р-1 дан катта булмаган таккосламага тенг кучли булади.

Бу теореманинг исботи [1] да келтирилган.

Теорема. Туб модулли n-даражали таккослама ечимлари сони n тадан ортик эмас.

Бу теореманинг исботи [1, 2] да келтирилган.

Текшириш саволлари

1. Бир номаълумли n-даражали таккослама деб нимага айтилади?
2. Таккосламанинг ечими деб нимага айтилади?
3. Тенг кучли таккосламалар деб нимага айтилади?
4. Биринчи даражали бир номаълумли таккослама деб нимага айтилади?
5. Бир номаълумли биринчи даражали таккосламаларнинг ечимлари мавжудлиги хакидаги теоремаларни баён этинг.
6. Бир номаълумли биринчи даражали таккосламаларни кандай ечиш усулларини биласиз?
7. Туб модулли n-даражали таккослама деб нимага айтилади?
8. Туб модулли n-даражали таккосламаларга тегишли теоремаларни **баён** этинг.
9. Туб модулли n -даражали таккослама ечимлари сони кандай булади?

Таянч тушунчалар

1. Таккосламалар ва улар устида амаллар.
2. Туб ва мураккаб модуллар.
3. Купхад ва улар устида амаллар.

14,15 ° маърузалар

Соннинг курсаткичи. Туб модуль буйича бошлан²ич илдизлар (4 соат)

Режа:

1. Модуль буйича сонга тегишли курсаткич (соннинг модулга кура курсаткичи).
2. Курсаткичга тегишли синфларнинг мавжудлиги ва сони.
3. Модуль буйича бошлан²ич илдиз.
4. Туб модуль буйича бошлан²ич илдизнинг мавжудлиги.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси. II кисм. Т.: Укитувчи. 1995 й. (85-93-бетлар).
2. Куликов Л.Я. Алгебра и теория чисел. М.: Высш.шк. 1979 г. (стр. 413 – 416).

Эйлер теоремасига кура (a; m)=1 булганда $a^{\varphi(m)} \equiv 1(\mathrm{mod} m)$ таккослама уринли эди. Бу таккосламанинг^икки кисмини k натурал даражага кутариб

$A^{k\varphi(m)} \equiv 1(\mathrm{mod} m)$ таккосламани хосил киламиз. $k\varphi(m)=\gamma$ булсин. У холда $a^{\gamma} \equiv 1(\mathrm{mod} m)$ таккослама уринли. Бу таккосламани каноатлантирувчи энг кичик γ натурал сон мавжуд. Уни δ оркали белгилайлик, яъни $\delta = \min\gamma$ булсин.

Таъриф. Агар (a; m)=1 булганда $a^{\delta}=1(\mathrm{mod} m)$ таккослама уринли булса, у холда δ сон a соннинг m модулга кура курсаткичи ёки m модуль буйича a сонига тегишли курсаткич дейилади.

Бу таърифга кура хар доим $\delta \le \varphi(m)$ булади.

Мисол. m=5 модуль буйича 4 сонига тегишли булган курсаткични топинг.

$4=4(\mathrm{mod}5)$, $4^2=1(\mathrm{mod}5)$. Демак, 4 сон 5 модуль буйича 2 курсаткичга тегишли булади.

Соннинг модулга кура курсаткичи куйидаги хоссаларга эга:

1^0. Бирор m модуль буйича тузилган битта синфнинг чегирмалари шу модуль буйича бир хил курсаткичга тегишли булади.

Бу хоссанинг исботи [1] да келтирилган.

2^0. Агар (a; m)=1 булганда $a^{\delta} \equiv 1(\mathrm{mod} m)$ булса, у холда $a^0, a^1, \ldots, a^{\delta-1}$ сонлар системаси m модуль буйича узаро таккосланмайди.

Бу хоссанинг исботи [1, 2] да келтирилган.

Натижа. Агар $\delta=\varphi(m)$ булса, у холда $a^0, a^1, \ldots, a^{\delta-1}$ система m модул буйича чегирмаларнинг келтирилган системасини ташкил килади.

Бу натижанинг исботи [1] да келтирилган.

3^0. a сон m модуль буйича δ курсаткичга тегишли булса, у холда $a^{\gamma} = a^{\gamma_1}(\mathrm{mod} m)$ таккослама уринли булиши учун $\gamma \equiv \gamma_1(\mathrm{mod}\delta)$ таккосламанинг уринли булиши зарур ва етарли.

Бу хоссанинг исботи [1, 2] да келтирилган.

Натижа. $\gamma=0(\mathrm{mod}\delta)$ булганда ва факат шу холдагина $a^{\gamma}=1(\mathrm{mod} m)$ таккослама уринли булади.

Натижа. a соннинг m модуль буйича δ курсаткичи $\varphi(m)$нинг булувчиси булади.

Мисол. 11 модуль буйича 7 сон тегишли булган курсаткични топиш учун $\varphi(11)=10$ булганидан 1,2,5,10 курсаткичларни текшириш етарли.

Натижа. Агар а сон m модуль буйича δ курсаткичга тегишли булса, у холда a^k сони шу модуль буйича $\frac{\delta}{(\delta;к)}$ курсаткичга тегишли булади.

Натижа. Агар (δ;k)=1 булса, у холда а сон δ курсаткичга тегишли булади.

Бу хосса ва юкоридаги натижаларнинг исботи [1,2] да келтирилган.

Таъриф. Агар (a,m)=1 булиб, δ=φ(m) булса, у холда а сон m модуль буйича бошлан²ич илдиз дейилади.

φ(m) нинг узидан бошка хамма булувчиларини топганимизда, бу булувчилардаги ихтиёрий а сон булганда a^{α} сон учун $a^{\alpha}\neq1(modm)$ булса, у холда а сон m модуль буйича бошлан²ич илдиз булади.

Мисол. a=5, m=54 булсин. У холда $\varphi(54)=\varphi(2*3^3)=54(1-\frac{1}{2})(1-\frac{1}{3})=18$, φ(54)=18 булиб, 18 нинг узидан бошка натурал булувчилари 1, 2, 3, 6, 9 булади.

$5\neq 1(mod54)$, $5^2\neq 1(mod54)$, $5^3\neq 1(mod54)$, $5^6\neq 1(mod54)$,

$5^9\neq 1(mod54)$.

Демак, 5 сони 54 модуль буйича бошлан²ич илдиз экан.

m=p - туб сон булсин. У холда φ(p)=p-1 булиб, а соннинг даражаси p-1 булса, а бошлан²ич илдиз булади. Бунда p-1 нинг узидан бошка хамма булувчиларини топиб, кейин синаб куриш лозим.

Масалан, p=11 булсин. У холда φ(11)=10 булиб, 10 нинг узидан бошка натурал булувчилари 1, 2, 5 булади. 11 билан узаро туб булган 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 сонларини оламиз. Бу сонлар 11 модуль буйича чегирмаларнинг келтирилган системасини ташкил этади.

$2\equiv 2(mod11)$

$2^2\equiv 4(mod11)$,

$2^5\equiv 10(mod11)$,

Демак, 2 сон 11 модул буйича бошлан²ич илдиз экан.

$3\equiv 3(mod11)$,

$3^2\equiv 9(mod11)$,

$3^5\equiv 1(mod11)$,

Демак, 3 сон 11 модуль буйича бошлан²ич илдиз эмас экан.

4,5,6,7,8,9,10 сонларнинг хам 11 модуль буйича бошлан²ич илдиз ёки бошлан²ич илдиз эмас эканлигини шу йул билан текшириб курилади. Баъзи модулга кура бошлан²ич илдиз булмаслиги мумкин.

Масалан, m=5 булса, φ(15)=8 булиб, курсаткичи 8 га тенг булган сон мавжуд эмас.

Бошлан²ич илдизлар факатгина m=2, 4, p^{α}, $2p^{\alpha}$ (p-ток туб сон, $\alpha\geq 1$ натурал сон) сонлар учун мавжуд булади. Бошлан²ич илдизлар бевосита хисоблаш усулида топилади.

Лемма. p-туб сон булиб, δ сон p-1 соннинг булувчиси булсин, у холда p модуль буйича чегирмаларнинг келтирилган синфлар системасида δ курсаткичга тегишли синфлар сони φ(δ) та булади.

Бу лемманинг исботи [1, 2] да келтирилган.

Мисол. 17 модуль буйича 4 сони тегишли булган курсаткични топинг ва 17 модуль буйича курсаткичга тегишли булган келтирилган чегирмалар системасини тузинг.

Ечиш. p=17 булгани учун p-1 =16 булиб, 16 нинг барча натурал булувчилари 1, 2, 4, 8, 16 булади. 4 нинг даражаларини текширамиз.

$4 \equiv 4(\mathrm{modl}7)$, $4^2 \equiv 6(\mathrm{mod}17)$, $4^4 \equiv 1(\mathrm{mod}17)$. Демак, 4 сон 17 модуль буйича 4 курсаткичга тегишли экан.

Энди 17 модуль буйича курсаткичга тегишли булган сонларни излаймиз. Юкоридаги леммага асосан бундай сонлар сони $\varphi(4)=2$ та булади. 1,3 система 4 модуль буйича чегирмаларнинг келтирилган системаси булади.

Демак, биз излаган сонлар 4^1, 4^2, яъни 4, 16 булади.

Теорема. p туб модуль буйича тузилган p-1 соннинг хар бир δ булувчиси $\varphi(\delta)$ та синфнинг курсаткичи булади. Хусусий холда $\varphi(p-1)$ та бошлан²ич илдизлар синфи мавжуд.

Бу теореманинг исботи [1, 2] да келтирилган.

Текшириш саволлари

1. Соннинг модулга кура курсаткичи деб нимага айтилади?
2. Соннинг модулга кура курсаткичи хоссаларини баён этинг?
3. Соннинг модулга кура курсаткичи хоссаларига мисол келтиринг.
4. Соннинг модуль буйича бошлан²ич илдизи деб нимага айтилади?
5. Бошлан²ич илдизнинг мавжудлиги хакида нимани биласиз?
6. Бошлан²ич илдизга мисол келтиринг?

Таянч тушунчалар

1. Таккосламалар ва уларнинг хоссалари.
2. Туб сонлар ва узаро туб сонлар.
3. Соннинг даражаси.
4. Эйлер функцияси ва уни хисоблаш формулалари.
5. Энг катта умумий булувчи.

16,17 ° маърузалар

Туб модуль буйича индекслар. Икки хадли таккосламалар
(4 соат)

Режа:

1. Соннинг модуль буйича индекси.
2. Индексларнинг хоссалари.
3. Икки хадли таккосламалар.
4. Индексларнинг тадбики.

Адабиёт

1. Назаров Р.Н., Тошпулатов Б.Т., Дусумбетов А.Д. Алгебра ва сонлар назарияси. II кисм. Т.: Укитувчи. 1995 и. (93-101-бетлар).

2. Куликов Л.Я. Алгебра и теория чисел. М.: Высш.шк. 1979 г. (стр. 417 - 421).

15-маърузада хар кандай p туб модуль буйича бошлан²ич илдиз мавжудлиги билан танишган эдик. Маълумки, g сон p туб модуль буйича бошлан²ач илдиз булса, у холда

$$g^0, g^1, g^2, \ldots, g^{p-2} \qquad (1)$$

сонлар катори шу p модуль буйича чегирмаларнинг келтирилган системасини ташкил килади. (1) кетма-кетликнинг хадлари p билан узаро туб булиб, улар p модуль буйича φ(p)= p-1 та синфнинг вакилларидан иборатдир. ^

Демак, (a; p)=1 булса, у холда (1) кетма-кетликда p^ модуль буйича a сон билан таккосланадиган ягона элемент топилади, яъни

$$g^{\gamma}=a(\text{mod } p) \qquad (2)$$

таккослама уринли булади.

Таъриф. Агар g сон p туб модуль буйича бошлан²ич илдиз булиб, (a; p)=1 булганда $g^{\gamma}=a(\text{mod } p)$ таккослама ту²ри булса, у холда $\gamma \geq 0$ бутун сон a соннинг p модуль буйича g асосга нисбатан индекси дейилади ва у $\gamma=\text{ind}_g a$ каби белгиланади.

Агар асос олдиндан берилган булса, a нинг индекси ind a оркали белгиланади. Юкоридаги тушунчаларга асосан, хар бир (a; p)=1 шартни каноатлантирувчи a сон, берилган асос буйича

$$0, 1, 2, \ldots p-2 \qquad (3)$$

сонларнинг биттаси билан аникланувчи индексга эга экан. Асоснинг узгариши билан индекс хам узгаради. Хар бир (a; p)=1 каноатлантирувчи a сони, g бошлан²ич илдиз буйича чексиз куп индексга эга булади. Бу индексларнинг барчаси $g^{\gamma} = g^{\gamma_1}(\text{mod} p)$ таккосламани каноатлантиради. Бу таккослама уринли булиши учун $\gamma \equiv \gamma_1(\text{mod } p-1)$ таккосламанинг бажарилиши зарур ва етарлидир.

Индекслар куйидаги хоссаларга эга:

1^0. $a \equiv b(\text{mod } p)$ <=> inda =indb.

Исботи. 1) $a \equiv b(\text{mod} p)$ берилган булсин. inda=indb эканлигини исботи килайлик.

r=inda <=> $g^r \equiv a(\text{mod } p) => g^r \equiv b(\text{mod } p)$<=>r=indb

Демак, inda=indb экан.

2) inda=indb берилган $a \equiv b(\text{mod } p)$ эканлигини исбот килайлик. inda=indb=r булсин. У холда $g^r \equiv a(\text{mod} p)$, $g^r \equiv b(\text{mod } p)$ булиб, ундан $a \equiv b(\text{mod } p)$ келиб чикади.

2^0. Агар (a;p)=1, (b;p)=1 булса, у холда ind(ab)=inda+ +indb(mod p-1) булади.

Исботи. ind(ab)=r деб белгилайлик.

Inda=r_1<=> $g^{r_1} \equiv a(\text{mod} p)$,

Indb=$r_2 \Leftrightarrow g^{r_2} \equiv b(\text{mod} p)$.

Бу таккосламаларни хадма-хад курайтириб $g^{r_1+r_2}=ab(\text{mod} p)$ таккосламага эга буламиз. Бундан $r_1+r_2=\text{ind}(ab)$ келиб чикади. $r_1+r_2=r$ булиб, у холда ind(ab)=inda+indb (mod p-1) булади. Бу эса $r=r_1+ +r_2 \text{ (mod } p-1)$ демакдир.

Шу йул билан $\text{Ind}(a_1\ a_2....a_n) \equiv \text{inda}_1+\text{inda}_2+...+\text{inda}_n(\text{mod } p-1)$ таккослама исботланади.

Бу таккосламанинг исботи [1] да келтирилган.

3^0. Агар (a;p)=1 ва $\forall n \in N$ булса, у холда $\text{ind}(a^n) \equiv$

$\equiv n \cdot \text{inda}(\text{mod } p-1)$ таккослама уринли булади.

Исботи. $\text{ind}(a^n)=r_k$ деб белгилайлик.

inda=r <=> $g^r=a(\text{mod } p)$. Бу таккосламанинг икки кисмини n-натурал даражага кутарайлик. У холда $g^m \equiv a^n \text{ (mod } p)$ таккослама хосил булиб, бунда $\text{ind}(a^n)=r \cdot n$ булиб, $r_k=r \cdot n(\text{mod } p-1)$, яъни $\text{iad}(a^n) \equiv n \cdot \text{inda}(\text{mod } p-1)$ булади.

bx=a(mod p) таккдосламани каноатлантирувчи сонни $\frac{a}{b}$ куринишда белгилайлик.

4^0. $\text{ind}\left(\frac{a}{b}\right) \equiv \text{inda - indb}(\text{mod } p-1)$ таккослама уринли.

Исботи. bx= a(mod p) таккосламани олайлик ва унинг хар икки кисмини индекслайлик, яъни ind(bx)=inda(mod p-1) булсин. 2-хоссага кура бу таккосламани

indb+indx= inda(mod p-l) ёки indx=inda-indb(mod p-l) куринишда ёзамиз. Бу таккосламада $x=\frac{a}{b}$ десак, $\mathrm{ind}\left(\frac{a}{b}\right)\equiv$ inda-

-indb(mod p -1) таккослама келиб чикади.

5^0. ind1=0 , $\mathrm{ind}_g g=l$.

Исботи. $g^0\equiv 1(\mathrm{mod} p)$=> $\mathrm{ind}1\equiv 0(\mathrm{mod}\ p\text{-}1)$, яъни ind1=0 булади.

$g^1\equiv g(\mathrm{mod}\ p)$ => $\mathrm{ind}g\equiv 1(\mathrm{mod}\ p\text{-}1)$, яъни $\mathrm{ind}_g g=l$ булади.

Демак, индексларнинг хоссалари, логарифмлар хоссаларига ухшаш булар экан.

Мисол. g=2, p=11 буйича индекслар жадвалини тузинг.

Ечиш.

$2\equiv 2(\mathrm{mod}\ 11)$ => ind2 = 1,
$2^2\equiv 4(\mathrm{mod}11)$ => ind4 = 2,
$2^3\equiv 8(\mathrm{mod}11)$ =>ind8=3,
$2^4\equiv 5(\mathrm{mod}11)$ =>ind5=4,
$2^5\equiv 10(\mathrm{mod}11)$ =>ind10=5,
$2^6\equiv 9(\mathrm{mod}11)$ =>ind9=6,
$2^7\equiv 7(\mathrm{mod}11)$ =>ind7=7,
$2^8\equiv 3(\mathrm{mod}11)$ =>ind3=8,
$2^9\equiv 6(\mathrm{mod}11)$ =>ind6=9,
$2^{10}\equiv 1(\mathrm{mod}11)$ =>ind1=$10\equiv 0(\mathrm{mod}10)$.

Индекслар жадвали куйидагича булади:

a	1	2	3	4	5	6	7	8	9	10
Inda	10	1	8	2	4	9	7	3	6	5

Таъриф. Агар a сон m сонга булинмаса, у холда ушбу

$$ax^2+bx+c=0(\mathrm{mod}m) \qquad (4)$$

куринишдаги таккослама иккинчи даражали (квадратик) таккослама дейилади.

Таъриф. Агар a сон p туб сонга булинмаса, у холда ушбу

$$ax^n=b(\mathrm{mod}\ p)\ (\forall n\in N) \qquad (5)$$

куринишдаги таккосламани n-даражали икки хадли таккослама дейилади.

(5) нинг хар икки кисмини a га булиб, сунг индекслаб $n\cdot\mathrm{ind}x=\mathrm{ind}b-\mathrm{ind}a(\mathrm{mod}\ p\text{-}1)$ таккосламага эга буламиз.

(n; p-1)=d булсин. Бу таккослама ечимга эга булиши учун d нинг indb-inda айирмага булиниши зарур ва етарли. Агар бу шарт бажарилса, у холда бу таккослама, шу жумладан (5) таккослама хам d та ечимга эга булади.

Таъриф. Ушбу

$$x^2\equiv a(\mathrm{mod}\ m) \qquad (6)$$

куринишдаги таккосламани икки хадли квадратик таккослама дейилади.

Теорема. (4) куринишдаги таккосламани хар доим (6) куринишдаги m_1 модулли таккосламага келтириш мумкин.

Бу теореманинг исботи [1] да келтирилган (Бунда m_1 моудль m нинг булувчиси).

Таъриф. Агар (a;m)=1 булганда (6) таккослама ечимга эга булса, у холда a сон m модуль буйича квадратик чегирма, акс холда a сон m модуль буйича квадратик чегирмамас дейилади.

Таъриф. Агар (a;m)=1 булганда (5) таккослама ечимга эга булса, у холда а сон m модуль буйича n-даражали чегирма, акс холда а сон n-даражали чегирмамас дейилади.

Таъриф. Ушбу

$$x^2 \equiv a(\mathrm{mod} p) \quad ((a;p)=1,(2;p)=1) \qquad (7)$$

куринишдаги таккосламани ток туб модулли квадратик таккослама дейилади.

Агар (7) да а: р булса, у холда (7) таккослама x≡0(mod p) ечимга эга булади.

Агар (7) нинг ечими $\overline{x_1}$ синф булса, у холда унинг ечими

$-\overline{x_1}$ синф хам булади.

Бу мулохазаларнинг хакикатлиги [1] да келтирилган.

Теорема (Эйлер критерияси). Агар (а; р)=1 булиб,

$a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod} p)$ булса, у холда (7) таккослама иккита ечимга эга булади, $a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod} p)$ булса, у холда (7) таккослама ечимга эга булмайди.

Бу теореманинг исботи [1] да келтирилган.

(7) таккосламада р модуль етарлича катта сон булганда Эйлер критериясидан фойдаланиш унчалик кулай эмас. Бундай холда Лежавдр символидан фойдаланиш яхши натижа беради. (Лежавдр символи ва унинг хоссалари мустакил таълимда урганилади).

Мисол. $x^2 \equiv 3(\mathrm{mod} 11)$ таккосламанинг ечимга эга ёки ечимга эга эмас эканлигини аникланг.

Ечиш. Эйлер критериясидан фойдаланамиз.

$$3^{\frac{11-1}{2}} \equiv 3^5 \equiv 243 \equiv 1(\mathrm{mod} 11)$$

булгани учун берилган таккослама ечимга эга.

Индекслар ёрдамида таккосламаларни ечиш анча кулай хисобланади.

Мисол. $10x \equiv 7(\mathrm{mod} 23)$ таккосламани ечинг.

Ечиш. Ind10 + indx≡ ind7(mod 22)

Индекслар жадвали буйича indl0=l, ind7=21 ларни топиб, кейин $1+\mathrm{ind}x \equiv 21(\mathrm{mod} 22)$ ёки $\mathrm{ind}x \equiv 20(\mathrm{mod} 22)$ таккосламани хосил киламиз. Кейин антеъиндекслар жадвалидан фойдаланиб $x \equiv 3(\mathrm{mod} 23)$ топилади. Бу берилган таккосламанинг ечими булади.

2. $x^2 \equiv 8(\mathrm{mod} 23)$ таккосламани ечинг.

Ечиш. Бу мисолни хам 1-мисолдаги каби индексларнинг хоссаларидан фойдаланиб ечамиз.

$2\mathrm{ind}x \equiv \mathrm{ind}8(\mathrm{mod} 22)$,

$2\mathrm{ind}x \equiv 2(\mathrm{mod} 22)$,

$\mathrm{ind}x \equiv 1(\mathrm{mod} 11)$,

$\mathrm{ind}x \equiv 12(\mathrm{mod} 11)$,

$\mathrm{ind}x_1 \equiv 1(\mathrm{mod} 22)$,

$\mathrm{ind}x_2 \equiv 12(\mathrm{mod} 22)$,

$x_1 \equiv 10(\mathrm{mod} 23)$,

$x_2 \equiv 13(\mathrm{mod} 23)$,

яъни $\overline{x_1} = \overline{10}, \quad \overline{x_2} = \overline{13}$ ечим булади.

Текшириш. $10 \in \overline{10}$ олайлик. У холда $10^2-8=92 \vdots 23$ булади, $13 \in \overline{13}$ олайлик. У холда $13^2-8=161 \vdots 23$ булади.

Демак, $10^2 \equiv 8(\mathrm{mod} 23)$, $13^2 \equiv 8(\mathrm{mod} 23)$ таккосламалар ту²ри таккосламалар булади, яъни $\overline{x_1} = \overline{10}, \quad \overline{x_2} = \overline{13}$ синфлар берилган таккосламанинг ечимлари экан.

Текшириш саволлари

1. Соннинг модуль буйича индекси деб нимага айтилади?
2. Индекснинг кандай хоссаларини биласиз?
3. Индекснинг хоссалари логарифм хоссаларига ухшашми?
4. n-даражали икки хадли таккослама деб нимага айтилади?
5. n-даражали икки хадли такколамалар ечимлари сони n та буладими?
6. Туб модулли икки хадли квадратик таккослама ечимлари сони кандай булади?
7 Эйлер критериясини баён этинг.

Таянч тушунчалар

1. Таккослама ва унинг хоссалари.
2. Бошлан²ич илдиз.
3. Туб ва мураккаб сонлар.
4. Узаро туб сонлар.
5. Модуль буйича чегирмаларнинг келтирилган системаси.