TÜRKMENISTANYŇ BILIM MINISTRLIGI

MAGTYMGULY ADYNDAKY TÜRKMEN DÖWLET UNIWERSITETI

B. Kömekow, O. Annaorazow, H. Geldiýew, A. Öwezow

Sanlar nazaryýeti

Ýokary okuw mekdepleriň talyplary üçin okuw kitaby

Türkmenistanyň Bilim ministrligi tarapyndan hödürlenildi

Aşgabat – 2010

B. Kömekow, O. Annaorazow, H. Geldiýew, A. Öwezow

Sanlar nazaryýeti. – Aşgabat, 2010

Okuw kitabynda Sanlar nazaryýeti dersiniň esasy düşünjeleri beýan edilýär.Köpsanly mysallar işlenip görkezilýär. Bu kitapdan talyplar we matematika mugallymlary peýdalanyp bilerler.

Giriş

Mälim bolşy ýaly ylmy-tehniki progresiň häzirki pajarlap ösýän döw-ründe matematikany çuňňur öwrenmekligiň zerurlygy öňkä garanyňda has artdy. Bu okuw kitbynda Sanlar nazaryýetiniň esasy düşünjeleri beýan edilýär. Okuw kitaby Sanlar nazaryýeti dersi boýunça okuw maksatnamalaryna doly gabat gelýär. Getirilýän nazary maglumatlary berkitmek üçin köp sanly anyk mysallar işlenip görkezilýär. Okuw kitaby matematika hünärini ele alýan talyplara niýetlenendir.

1.Bölünijilik häsiýetleri.

Sanlar nazarýeti bitin sanlaryñ (ine bir bitin (+) bolman , bitin (-) sanlaryñ hem-de 0-l sanlaryñ) häsiýetlerini öwrenmek bilen meşgulanýan matematikanyñ bölümidir. Eger-de a san başga bir b sana $(b \neq 0)$ galyndysyz bölünýän bolsa , oña b sana kratny diýilip aýdylýar we bu fakyt a/b (b/a ýa-da a:b) görnüşde belgilenýär. Şeýlelikde a san b sana kratny bolan halatynda käbir q san bar bolup , a=b˙q deñlik ýerne ýetýändir. Bu ýagdaýda q sana a-ny b sana bölenmizde ýetýän paý diýlip aýdylýar. Indi subut etmesi kyn bolmadyk indiki tasyklamalary getireliñ .

1.a b sana kratnyý bolanda , b san bolsa, s sana kratnyý bolanda , a san s sana kratnydyr .

2. a +b +…+s=0 p+q+…+t deñlikde haýsy hem bolsa , bir goşulyjydan başgasy k sana bölünýän bolsa , onda şol goşulyjy hem bu k sana bölünýändir.

Hakykatdan hem bu tassyklamalaryñ 1-njisiniñ subudy a=bq we b=s˙r gatnaşyklardan a=bq=s(r˙q)=st deñligiñ gelip çykýanlygyndan 2-njisiniñ subudy bolsa, eger-de bu deñlikde p goşulyjydan galanlary k sana kratnyý bolan halatlarynda $a=a_1 \cdot k$, $b=b_1 \cdot k$,…, $s=s_1 \cdot k$, $q=q_1 \cdot k$, …, $t=t_1 \cdot k$. deñliklerden $p=a+b+\ldots+s-q-\ldots-t=a_1 \cdot k+b_1 \cdot k+\ldots+s_1 \cdot k-q_1 \cdot k-\ldots-t_1 \cdot k=k(a_1+b_1+ +\ldots+s_1-q_1-\ldots-t_1)=k \cdot m$. Bolýandygyndan gelip çykýandyr.

Galyndyly bölmegiñ algaritimi (algorifmi) diýilip atlandyrylýan indiki tassyklama dogrudyr.

Teorema: Islendik a sany polažitel b sanyñ üsti bilen ýeketäk usulda a=b˙q+r $0 \leq r < b$ (1) görnüşde añladylýandyr. Hakykatdan hem şeýle görnüşdäki ýazgynyñ biriniñ b˙q köpeltmek hasyly a-dan uly bolmadyk b sanyñ kratnylarynyñ ulusyna deñ diýip alsak , alynjakdygy düşnüklidir . Bu ýazgynyñ ýeketäkdigini subut etmek üçin bolsa , tersinden guman ederis.

Goý 1-nji ýazgydan başgada $a=b \cdot q_1+r_1$ $0 \leq r_1 < b$ (2) 2-nji ýazgy bardyr diýip guman edeliñ . Onda olaryñ 1-njisinden 2-njisini tarapma-tarap , aýyryp , $0=b(q-q_1)+(r-r_1)$ (3) 3-nji deñligi alarys . Bu deñligiñ çep tarapynyñ (0-lyñ) hem-de sag tarapynyñ 1-nji goşulyjysynyñ b sana kratnydyklaryna görä, ýokarda subut edilen tasyklamadan sag tarapynyñ 2-nji goşulyjysynyñ hem b sana kratny bolmalydygyny alarys. Ýöne talaba görä, $r-r_1$ tapawut ine 0-a deñ bolan halatynda b sana kratny bolar . Diýmek $r-r_1=0$ bolmalydyr . Onda (3)-nji deñlikden $b(q-q_1)=0$ deñlik alynyp , $q-q_1=0$ bolmalydygy alynar. Şeýlelikde (1) we (2) ýazgylardaky $q=q_1$ $r=r_1$ gatnaşyklary kanagatlandyrýan sanlardyr. Bu diýildigi (1) we (2) deñlikleriñ birmeñzeşdiklerini añladýar. Teorema subut edildi.

(1) formuladaky q sana a-ny b sana bölenimizdäki doly däl paý , r sana bolsa bu bölünmekdäki galýan galyndy diýilip , aýdylýar. Mysal işlenende a sana (+) bolanda q sany tapmak üçin ýetmezi bilen , a san (-) bolan halatynda -a sany

b sana artykmajy bilen q we r sanlary tapýarlar.

2. Iñ uly umumy bölüji.

Biz geljekde sanlaryñ diñe (+) bölüjilerine seretjekdiris . Eger-de a san b sana kratny bolsa , biziñ bilşimize görä b san onuñ bölüjisidir. Eger-de käbir s san a we b sanlaryñ ikisiniñ hem bölüjisi bolsa , onda oña bu sanlaryñ umumy bölüjisi diýip aýdylýar. a we b sanlaryñ umumy bölüjileriniñ iñ ulysyna ol sanlaryñ iñ uly umumy bölüjisi diýlip aýdylýar,we ol (a,b) görnüşde belgilenýär.

Eger-de iki a we b sanlaryñ iñ uly umumy bölüjisi 1-e deñ bolsa , onda olara özara ýönekeý sanlar diýilýär. Mysal üçin: (9,8)=1 bolanlygyna görä 9 we 8 sanlar özara ýönekeýdirler .

$a_1, a_2, \ldots, a_n$ sanlara jübüt-jübütden (ýa-da ikibir) ýönekeý diýilýär. Eger-de olaryñ islendik iki sanysy özara ýönekeý sanlar bolsalar. Başgaça aýdanyñda $\forall 1 \le i \ne j \le n$ nomer üçin $(a_i, a_j)=1$ sanlaryñ iñ uly bölüjisi 1-e deñ bolsa) sanlaryñ berlen toplumuna , jübüt-jübütden ýönekeý sanlar diýilýär . Mysal üçin : 8,12,15 sanlar jübüt-jübütden ýönekeý däldirler sebäbi (12,15) =3 (8,12)=4 bolýandyrlar.

Ýokardaka meñzeşlikde özara ýönekeýlik düşünjesi 2-den köp sandaky sanlar üçin hem kesgitlenändir. Ýagny $(a_1,a_2,\ldots,a_k)=1$ (sanlaryñ iñ uly umumy bölüjisi 1-e deñ bolsa) onda bu sanlara özara ýönekeý diýip aýdylýar. Mysal üçin: Ýokarda berlen 8,12,15 sanlar özara ýönekeýdirler. Hakykatdan hem ol sanlaryñ iñ uly umumy bölüjisi 1-e deñdir .

Kesgitlemelerden görnüşi ýaly berlen sanlar . Jübüt-jübütden ýönekeý bolsalar , onda olaryñ özara ýönekeý bolçakdyklary düşnüklidir . Ýöne iki sany san üçin özara ýönekeýlik hem-de jübüt-jübütden ýönekeýlik düşünjeleri gabat gelýändirler.

Indi 2 sany sanyñ umumy bölüjileri üçin dogry bolan käbir häsiýetleri belläp geçeliñ .

1) Eger-de a san b sana kratnyý bolsa , onda a we b sanlaryñ umumy bölüjileriniñ toplumy b sanyñ bölüjileriniñ toplumy bilen gabat gelýändir we hususan (a,b)=b deñlik dogrudyr. Hakykatdan hem a sanyñ b sana kratnydygyna görä , (a b-he galyndysyz bölünýän bolsa,) b-niñ her bir bölüjisi a sany hem bölýändir. Onda b sanyñ her bir bölüjisi a we b sanlar üçin umumy bölüjidir hem-de tersine a we b sanlaryñ her bir umumy bölüjisi b sanyñ bölüjisidir. Diýmek a we b sanlaryñ umumy bölüjileriniñto plumy bilen b sanyñ bölüjileriniñ toplumy gabat gelýändirler. Hususan bu toplumlaryñ iñ uly elementleri bolan (a,b) we b sanlar özara deñdirler. (a we b sanlaryñ iñ uly umumy bölüjisi).

2)Eger-de a=bq+s bolsa , onda a we b sanlaryñ umumy bölüjileriniñ toplumy bilen b we s sanlaryñ umumy bölüjileriniñ toplumy gabat gelýär. Hususan (a,b)=(b,s) (a bilen b-niñ iñ uly umumy bölüjisi b bilen s-iñ iñ uly umumy bölüjisi deñdir.) Hakykatdan hem bölüjiligiñ ýokarda öwrenilen häsiýetlerinden a bilen b-niñ umumy bölüjisine s san hem bölünýändir. 2-nji bir tarapdan b-niñ

hem-de s-niñ umumy bölüjisine şol häsiýete görä , a san hem bölünýändir . Diýmek , a we b sanlaryñ umumy bölüjileriniñ toplumy bilen b we s sanlaryñ umumy bölüjileriniñ toplumy gabat geländirler. Şeýlelikde bu toplumlaryñ iñ uly elementleri bolan (a,b) we (b,s) sanlar özara deñdirler.
a we b sanlaryñ iñ uly umumy B-sini tapmak üçin Ýewklid algaritmi ady bilen belli indiki düzgünden peýdalanmak mümkindir.

Goý a we b (+) sanlar bolsun (0-a deñ däl , 0-dan uly , 0-la deñ bolsada (-) sanlar bolmasyn) onda galyndyly bölmegiñ algaritiminden peýdalanyp olaryñ birini beýlekisine , Mysal üçin : a sany b sana bölüp alarys. $a=bq_1+r_1$ soñra $0 \le r_1 < b$ $r_1 \ne 0$ hasap etmek bilen b-ni r_1-iñ üsti bilen ýokardaka meñzeşlikde añladalyñ . $b= r_1 q_2+r_2$ $0 \le r_2 < r_1$.
Eger-de $r_2 \ne 0$ bolsa, r_1-i galyndyly bölmegiñ algaritiminden peýdalanyp r_2-niñ üsti bilen añladarys. $r_1 = r_2 q_3 + r_3$ $0 \le r_3 < r_2$ $r_3 \ne 0$ bolanda şu prosesi dowam etmek bilen ahyr soñunda bölünmäniñ galyndysyz ýerine ýetýän ýagdaýyna eýe bolarys.(çünki bu yzygiderli bölünmelerdäki $r_1,r_2,r_3,\dots$ galyndylar birsyhly kiçelýärler . Şeýlelikde olaryñ (-) bolup bilmeýändiklerine görä , tükenikli gezek bölünmelerden soñ , galyndysyz bölünmä eýe bolunar).

$$r_1 = r_2 q_3 + r_3, \quad r_{k-2} = r_{k-1} q_k + r_k$$
$$0 \le r_k < r_{k-1.} \quad r_{k-1} = r_k q_{k+1}$$

galyndysyz bölünýär.

Şeýle usul bilen tapylan, iñ soñky 0-dan tapawutly r_k galyndy a we b sanlaryñ iñ uly umumy bölüjisidir . Muny subut etmek üçin ilki bilen r_k –nyñ a we b sanlaryñ umumy bölüjisi bolýandygyny soñra onuñ bu a we b sanlaryñ islendik umumy bölüjisine galyndysyz bölünýändigini (kratnydygyny) görkezmelidir.
Hakykatdan hem soñky deñlikden r_{k-1} sanyñ r_k-a kratnydygyna görä, öñ ýanyndaky deñlikden r_{k-2} we r_{k-1} sanlaryñ hem r_{k-a} sana bölünýändiklerini , başgaça aýdanyñda r_k-nyñ r_{k-1} we r_{k-2} sanlaryñ umumy bölüjisidigini taparys. Onda şu pikir ýöretmeleri dowam etmek bilen alynan deñliklerde ýokarlygyna hereket edip , r_1 we r_2 sanlaryñ hem , şeýle hem b we r_1 sanlaryñ , ahyr soñunda a we b sanlaryñ umumy bölüjisi bolup , r_k sanyñ hyzmat edýändigini göreris.
Indi käbir d san a we b sanlaryñ iñ uly umumy bölüjisi bolsa , onda ol b we r_1 sanlaryñ hem iñ uly umumy bölüjisidir . 3-nji deñlikden onuñ r_1 we r_2 sanlaryñ hem iñ uly umumy bölüjisidigini şu pikir ýöretmeleri alnan deñliklerde ýokardan aşaklygyna dowam etmek bilen d sanyñ r_{k-2} we r_{k-1} r_{k-1}-iñ r_k galynda kratnydygyna görä bolsa , şol umumy bölüjiniñ r_k-nyñ özi bilen gabat gelýändigini taparys.
Indi netijeler añsatlyk bilen alynýandyrlar.
1) a we b sanlaryñ umumy bölüjileriniñ toplumy a we b sanlaryñ iñ uly umumy bölüjisiniñ bölüjileriniñ toplumy bilen gabat gelýändir.
2) Bu iñ UUB-i Ýewklidiñ algaritimindäki iñ soñky 0-dan tapawutly r_n galynda deñdir.

Indiki tassyklamalar añsatlyk bilen subut edilýändirler.

Teorema:

1) Islendik m(+) san üçin (a·m,b·m)=m(a,b)
2) Eger-de b=(a,b) (delta a bilen b sanlaryñ UUB-sine deñ bolsa) onda
$\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{(a,b)}{\delta}$ deñlik dogrudyr. Hususan $\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=\frac{(a,b)}{(a,b)}=1$ iñ UUB-si.

<u>Subudy:</u> Ýewklid algaritimindäki yzygiderli bölünmelerde ähli deñlikleri m sana köpeltsek şol gatnaşyklar a·m, b·m, r_1·m, r_2·m, r_n·m köpeltmek hasyllary üçin alynarlar . Bu diýildigi täze alnan gatnaşyklardaky iñ soñky 0-a deñ bolmadyk galyndynyñ m·r_n köpeltmek hasylyna deñdigini añladýar. Bu diýildigi a·m we b·m köpeltmek hasyllarynyñ iñ UUB-siniñ m·r_n sana deñdigini ,Ýagny $(a\cdot m,b\cdot m)=r_n\cdot m=m(a,b)$ deñligiñ dogrudygyny añladýandyr. Teoremanyñ tassyklamasynyñ 2-nji böleginiñ subudyny almak üçin indiki gatnaşyklaryñ dogrudyklaryny görmek ýeterlikdir.

$$(a,b)=\left(\delta\cdot\frac{a}{\delta},\delta\frac{b}{\delta}\right)=\delta\left(\frac{a}{\delta},\frac{b}{\delta}\right)\qquad\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{(a,b)}{\delta}.$$

Iñ UUB-jiniñ indiki häsiýetleri sanlar nazaryýetiniñ meseleleri öwrenilende ähmiýetli ulanyşlary eýedirler.

<u>Teorema:</u> Eger-de $(a,b)-1$ *onda* $(as,b)=(s,b)$ iñ UUB-sine deñdir.
Hakykatdan hem (as,b) kesgitlemä görä as we b sanlaryñ UB-leriniñ iñ ulysydyr. Onda as we b sanlaryñ UB-siniñ as we b·s sanlaryñ hem UB-si bolýandygyna görä,onda bu köpeltmek hasyllarynyñ iñ UUB-si (as,bs)=s(a,b)=s bolýandygyna görä s san hem as we b sanlaryñ her bir UB-sine bölünýändir . Diýmek bu UB –ji s we b sanlar üçin hem UB-i bolup hyzmat edýändir. Şeýlelikde as we b sanlaryñ UB-leriniñ toplumy , s we b sanlaryñ UB-leriniñ toplumyny berýändir . 2-nji bir tarapdan s we b sanlaryñ her bir UB-si a·s-ni hem bölýändir. Onda ol as we b sanlar üçin UB-dir . Şeýlelikde as we b sanlaryñ UB-leriniñ toplumy s we b sanlaryñ UB-leriniñ toplumy bilen gabat gelýändir. Onda bu toplumlaryñ iñ uly elementleri özara deñdirler.

<u>Teorema:</u> Eger-de (a,b)=1 bolsa, hem-de as we b sana bölünýän bolsa , onda s san b sana bölünýändir.

<u>Subudy:</u> as köpeltmek hasylynyñ b sana kratnylygyndan hem-de s b köpeltmek hasylynyñ hem b sanakratnylygyndan b sanyñ as we bs köpeltmek hasyllary üçin UB-ji bolup hyzmat edýänligini has dogrusy ol köpeltmek hasyllarynyñ UB-sidigini görýäris . Onda ýokarda getirlen tassyklamadan (as,bs)=s (a,b)=s sanyñ b sana bölünýändigine eýe bolarys .

<u>Teorema:</u> $a_1,a_2,\ldots,a_n$ sanlaryñ her biri $b_1,b_2,\ldots,b_m$ sanlaryñ her biri bilen özara ýönekeý bolsa , onda $(a_1a_2\ldots a_n,b_1b_2\ldots b_n)=1$ olaryñ köpeltmek hasyllary hem ýönekeýdir.

<u>Subudy:</u> Hakykatdan hem ýokarda subut edilen tassyklamalardan indiki deñlikleriñ añsatlyk bilen alynýandygyny görmek kyn däldir. $\forall k$ *nomer*
üçin $(a_1a_2...a_n,b_k)=(a_2a_3...a_n,b_k)=(a_3...a_n,b_k)=...=(a_n,b_k)=1$
2-nji bir tarapdan $A=a_1\cdot a_2\cdot\ldots\cdot a_n$ belgiläp
$(b_1b_2...b_m,A)=(b_2b_3...b_m,A)=(b_3...b_m,A)=...=(b_m,A)=1.$

Eger-de 2-den köp sandaky sanlaryñ iñ UUB-sini tapmaklyk talap edilýän bolsa, onda ol 2 sany sanyñ iñ uly UUB-sini tapmaklyga syrykdyrylyp , hasaplanýar. Hakykatdan hem eger-de $a_1,a_2,\ldots,a_n$ sanlaryñ iñ UUB-sini tapmaly bolsa ilki bilen $(a_1,a_2)=d_2$ (olaryñ ilkinji 2-siniñ iñ UUB-sini tapýarys) d_2-ni tapýarys, soñra $(d_2,a_3)=d_3$ we şuña meñzeşlikde dowam etmek bilen ahyr soñunda $(d_{n-2},a_{n-1})=d_{n-1}$ tapyp, $(d_{n-1},a_n)=d_n$ d_n-san tapylar . Bu d_n san berlen sanlaryñ IUUB-sidir. Ýagny $d_n=(a_1,a_2,\ldots,a_n)$.

3. Ýönekeý sanlar

1 den uly bolan her bir bitin sanyñ iñ azyndan 2 sany bitin bölüjisi bardyr. Hakykatdan hem ol sanlaryñ her biri hiç bolmanda 1-e we özüne bölünýändir. Eger-de 1-den uly bitin sanyñ bölüjileriniñ sany 2-den köp bolmasa, ýagny ol **diñe** özüne hem-de 1-e bölünýän bolsa, onda oña **ýönekeý san** diýip aýdýar. Tersine ýagdaýda ýgny 1-den uly sanyñ 1 we özünden başgada (+) bölüjisi bar bolsa, onda oña **düzme san** diýip aýdýär.

T1. 1-den uly sanyñ 1-den tapawutly iñ kiçi bölüjisi ýönekeý sandyr.

C hakykatdan hem goý q 1-den uly a sanyñ 1-den tapawutly iñ kiçi bölüjisi bolsun. Eger-de bu san düzme bolsa, ol $1<q_1<q$ deñsizligi kon-ýan käbir q_1 bölüjä eýe bolar. Bu ýagdaýda a san q sana kratny bolmak bilen onuñ her bir q_1 bölüjisine hem kratnydyr. Bu diýildigi ýokarda aýdanymyza ters bolan ýagny a sanyñ 1-den tapawutly iñ kiçi bölüjisiniñ q sandygy hakykatdaky gümanymyza ters bolan ýagdaýa getirer. Şeýlelikde q-nyñ düzmedigi hakyndaky eden çaklamamyz nädogrydyr.

$$a=q\cdot a_1 = q_1 (t\cdot a_1)=q_1\cdot a_2$$
$$q=q_1\cdot t$$

T2. A düzme sanyñ iñ kiçi 1-den tapawutly bölüjisi $\sqrt{a}$-dan uly däldir. C hakykatdan hem goý a düzme sanyñ 1-den tapawutly iñ kiçi bölüjisi q bolsun. Onda $a=a_1\cdot q$ deñlik käbir a_1 bitin san bilen ýerne ýetýändir. Edilen talaba görä, (q-nyñ 1-den tapawutly iñ kiçi bölüjidigine görä) $a_1\geq q$ bolmalydyr. Şeýlelikde $a=a_1\cdot q\geq q\cdot q=q^2$ deñsizlige eýe bolarys. Ýa-da bu ýerde $q^2\leq a$ ýa-da başgaça $q\leq\sqrt{a}$ deñliklige eýe bolarys.

Eratosfen gözenegi.

Ilki bilen sanlaryñ tükeniksiz köpdügini belläliñ. Hakykatdan hem islendik k sany $p_1, p_2,\ldots, p_n$ ýönekeý sanlar üçin olaryñ arasynda saklanmaýan başgada bir ýönekeý sanyñ bardygyny görkezsek, onda k sanyñ erkindigine görä, ýönekeý sanlaryñ t-siz kökdügini añladýan subutnama bolardy. $p_1, p_2,\ldots p_k +1$ sanyñ iñ kiçi 1-e deñ bolmadyk natural bölüjisi $p_1, p_2,.., p_k$ sanlaryñ arasynda saklanmaýan käbir ýönekeý sandyr. Bu diýildigi islendik k sany ýönekeý san üçin başga bir ýönekeý sany hem görkezmek mümkindigini añladýär. Indi **eratosfen gözenegi** diýilip atlandyrylýan düzgünden peýdalanyp käbir N natural sandan uly bolmadyk, ýönekeý sanlaryñ tablisasyny düzmekligi öwreneliñ munuñ üçin ilki bilen bu N sandan uly bolmadyk ähli natural sanlary ýazyp çykýarys.

1, 2, 3, 4, 5, 6, 7, 8,…, N (1)

bu san hatarynda duran 1-den uly iñ kiçi san 2-dir. Ol diñe 1-e we özüne bölünýär. Diýmek bu san ýönekeýdit. (1)-nji san hatarynda ikiniñ özüne geçmän 2-ä kratny bolan ähli bitin sanlary çyzyp çykýarys (bçünki olaryñ natural bölüjileriniñ sany 2-den köpdür) we şoña göräde olar düzme sanlardyr. 2-den soñ çyzylman galan sanlaryñ içinde iñ kiçisi 3-dür. Ol diñe 1-e we özüne bölünýär. Şoña görä-de ol ýönekeýdir. Şeýlelikde 3-iñ özüne degmän oña kratny bolan sanlaryñ ählisini çyzyp çykýarys. 3-den soñky çyzylman galan sanlaryñ arasynda iñ kiçisi 5-dir. Ol 2-ä we 3-e bölünmeýär (eger bölünen bolsady, onda ol çyzylardy). Şoña görä-de, diñe 1-e we özüne degmän bu sanhatarynyñ 5-e kratny bolan ähli sanlaryny çyzyp çykýarys. Şu prosessi dowam edýäris. Şeýle usul bilen, p ýönekeýden kiçi bolan ähli ýönekeýleriñ kratnylary çyzylyp çykylandan soñ, p2-dan kiçi bolan ähli çyzylmadyklar, ýönekeýdirler. Hakykatdan hem p2-dan kiçi bolan her bir a düzme san $\sqrt{a}$ -dan uly bolmadyk özüniñ iñ kiçi ýönekeý bölüjisiniñ kratnysy hökmünde çyzgylardy.

$\sqrt{a}$ (≤p) şeýlelikde

1) p ýönekeý sanyñ kratnylaryny çyzmaklygy p2-dan başlamaly.

2) N-den uly bolmadyk ýönekeý sanlaryñ tablisasyny düzmek -den uly bolmadyk ähli ýönekeý sanlaryñ kratnylaryny çyzyp çykanymyzdan soñ tamam bolýar.

4. Iñ kiçi umumy kratny.

a we b sanlaryñ 2-sinede bölünýän sana bu sanlaryñ umumy kratnysy diýilip aýdylýar. Umumy kratnylaryñ iñ kiçi (+) –ne berlen sanlaryñ iñ kiçi umumy kratnysy diýilýär. a we b sanlaryñ iñ kiçi umumy kratnysy köpleniç [a,b] görnüşinde belgilenýär . Mysal üçin: 5 we 6 sanlaryñ iñ KUK-sy 30 [5,6]=30 . Biz geljekde diñe (+) sanlaryñ umumy kratnylaryna seretjekdiris. Ilki bilen a bilen b sanlaryñ UK-laryny tapalyñ.

Indiki tassyklama dogrydyr.

T1. Islendik biten a san P ýönekeý san bilen ýa özara ýonekeýdir ýa-da P sana bölünýändir.

C. bu tassyklamanyñ subudyny almak üçn (a, P) (sanlaryñ iñ UUB-si) ýa 1-e deñ ýa-da P-deñ

$(a,p)=\begin{cases}1\\p\end{cases}$ a bilen özara ýönekeý bolanlarynda (a,p sana bölünmese)

a san p sana bölünse

T2. egerde birnäçe köpeldijileriñ köpeltmek hasyly p ýönekeý sana bölýnýän bolsa onda köpeldejileriñ hiç bolmanda biri bu sana bölünýändir C hakykatdan hem köpeltmek hasylynyñ köpeldijileriniñ her biri subut edilen geçen tassyklama görä, a P san bilen özara ýönekeýdir ýa-da P sana bölünýändir. Eger-de köpeldijileriñ ählisi hem P ýönekeý sana bölünýän bolsa onda köpeldijileriñ hiç bolmanda biri bu sana bölünýändir C hakykatdan hem köpeltmek hasylynyñ köpeldijileriniñ her biri subut edilen geçen tassyklama görä, a P san bolsa özara ýönekeýdir ýa-da P sana bölünýändir. Eger-de köpeldijileriñ ählisi hem P san bilen özara ýönekeý bolsalar, onda olaryñ köpeltmek hasyly hem P san bilen özara ýönekeýdir (öñden bilşimize görä, (a,b) özara ýönekeý bolup, a·c b sana bölünse, onda c san b sana bölünýändir). Şeýlelikde köpeltmek hasylynyñ köpeldijileriniñ hiç bolmanda biri P sana bölünýändir. Teorema subut edildi.

T3 1-den uly islendik bitin sany köpeldijileriñ tertibini hasaba almanyñda ýeketäk hasyly görnüşinde añlatmak mümkindir.

C Goý a 1-den uly a>1 islendik bitin san bolsun. Onda biziñ bilşimize görä, onuñ 1-den tapawutly iñ kiçi bölüjisi käbir P_1 ýönekeý sandyr. Onda käbir a_1 san bar bolup, $a=p_1 \cdot a_1$ deñlik ýerne ýetýändir. Egerde $a_1>1$ diýsek, onda onuñ 1-den tapawutly iñ kiçi bölüjisi p_2 ýönekeý san bilen, käbir a_2 san tapylyp, $a_1=p_2 \cdot a_2$ deñlik ýerne ýetýändir. Eger-de $a_2>1$ bolsa, onda şu prosesi dowam etdirmek bilen ahyr soñunda käbir $a_n=1$ paý bolan ýagdaýyna ýagny $a_{n-1}=p_2$ – ýönekeý san bolan ýagdaýyna geleris. Şeýlelikde bu alnan deñlikleri biri-birinde ornuna goýmak bilen

$$a=p_1 \cdot a_1=p_1 \cdot p_2 \cdot a_2=p_1 \cdot p_2 \cdot p_3 \cdot a_3= \ =p_1 \cdot p_2 \cdot p_3 \ldots p_n$$

añlatma eýe bolarys. Bu deñlikdäki pi sanlar ýönekeý sanlardyr. Indi sanyñ ýönekeý köpeldijilere bu dagytmasynyñ köpeldijileriñ tertibini hasaba almanyñda ýeketäkdigini görkezeliñ. Goý a san ýçin $a=p_1 \cdot p_2 \ldots p_n$ (1) añlatmadan başgada käbir $a=q_1 \cdot q_2 \ldots q_s$ (2) bu sanyñ qi ýönekeý köpelijilere dagytmakdan $p_1 \cdot p_2 \ldots p_n=q_1 \cdot q_2 \ldots q_s$ (3) deñlik alnar.

Bu deñligiñ sag tarapynyñ q_1 sana bölünýändigine görä, onuñ çep tarapynyñ hem şol sana bölünjekdigi düşnüklidir. Bu ýagdaýda deñligiñ çep tarapyndaky köpelijileriñ hiç bolmanda biriniñ bu q_1 sana bölünmelidigi ýokarda subut edilen tassyklamadan gelip çykýandyr. Kesgitlilik üçin goý p_1 köpeliji q_1-e bölünsin diýeliñ. Bu ýagdaýda p_1 köpelijiniñ hem ýönekeýdigine görä, onuñ q_1 ýönekeý köpeliji bilen deñligiñ alynar. Ýagny p1=q1 şeýlelikde (3) deñligiñ iki tarapyny hem p1=q1 sana bölmek bilen $p_2 \cdot p_3 \ldots p_n=q_2 \cdot q_3 \cdot q_s$ (4) deñligi alarys. Bu deñlikden onuñ sag tarapynyñ q_2-ä bölünýändigine görä, onuñ çep tarapyndaky köpeltmek hasylynyñ köpelijileriniñ hiç bolmanda biriniñ mü/n: p_2-niñ bu sana bölünmelidigi alynar. Bu diýişedigi $p_2=q_2$ deñligi añladardy. Ýene-de (4) deñligiñ iki tarapyny hem $p_2=q_2$ sana bölmek bilen şu prosesi dowam etdireris we ony birnäçe gezek gaýtalanymyzdan soñ s>n bolan ýagdaýynda $1=q_{n+1} \ldots . q_s$ deñlik alynar. s<n $p_{s+1} \ldots p_n=1$ ýöne ýönekeý sanyñ kesgitlemesine görä, soñky ýazylan deñlik mümkin däl deñlikdir. Hiç bir ýönekeý sanlaryñ köpeltmek

hasyly 1-e deñ bolan (1) we (2) ýönekeý köppeldijilere a sanyñ dürli görnüşdäki dagytmalary bardygy hakyndaky aýdan gümanymyzyñ nädogrydygyny añladýar. Başgaça aýdanyñda 1-den uly islendik a sany ýeketäk usul bilen ýönekeý köpeldijileriñ köpeltmek hasyly görnüşinde (1) deñlikdäki ýaly edip añlatmak mümkindir (eger-de köpeldijileriñ tertibini hasaba almanyñda) ýöne (1) dagytmada käbir ýönekeý sanyñ birnäçe gezek gaýtalanmagy mümkindir. Eger-de bu dagytmadaky p_1, p_2,..,p_n ýönekeý köpeldijileriñ arasyndaky dürlüleri p_1, p_2,…, p_k we olaryñ bu deñlikdäki gaýtalanyşlaryny (kratnylyklaryny) degişlilikde α_1, α_2,…, α_k (α_1+ α_2 + +α_k=n) diýsek, (1) deñlikden a sanyñ ýönekeý köpelijilere **kanonik dagytmasy** diýilip atlandyrylýar $a = p_1^{\alpha_1} p_2^{\alpha_2} ....p_k^{\alpha_k}$ deñligi alarys. Teorema subut edildi.

a sanyñ ýönekeý köpeldijilere kanonik dagytmasyndaky α_1, α_2,… αk sanlara p_1, p_2, …,p_k ýönekeý köpeldijileriñ **degişli kratnylyklary** diýip aýdylýär.

T4. Goý $a = p_1^{\alpha_1} p_2^{\alpha_2} ....p_k^{\alpha_k}$ - a k d a sanyñ ýönekeý köpeldijilere kanonik dagytmasy bolsun. Onda a sanyñ ähli bölüjileri bilen $a = p_1^{\beta_1} p_2^{\beta_2} ....p_k^{\beta_k}$ (*)-bu ýerde $0 \leq \beta_i \leq \alpha_i$, $i = 1,\overline{k}$ görnüşdäki sanlaryñ ähli si we diñe şolar hyzmat edýändirler.

i=1,k 1 bilen k-nyñ arasyndaky ähli bahalary üçin ýerne ýetýändir.
C hakykatdan hem goý α a sanyñ bölüjisi bolsun. Onda, käbir q san bar bolup a=d·q deñlik ýerne ýetýändir. Şeýlelikde soñky deñlikden d sanyñ ähli ýönekeý bölüjileriniñ a sanyñ hem olaryñ d sandaky kratnylyklaryndan az bolmadyk kratnylyklary bilen bölüjileridikleri gelip çykýandyr. Bu diýildigi d sanyñ (*) görnüşdäki kanonik dagytma eýe bolmalydygyny añladýar. Tersine her bir (*) görnüşdäki kanonik dagytma eýe bolan a sanyñ bölüjisidigi düşnüklidir.

Sanlar nazaryýetinde ulanylýan funksiýalar.

5. [x] we {x} funksiýalary.

k. [x] fisy ähli hakyky sanlar köplerinde kesgitlenen b/n, x-den uly bolmadyk iñ uly bitin sany añladýandyr. We ol bitin bölegi diýen atlandyrylýan f-dyr. Mü/n: [7, 4]=7, [5, 2]=5, [0, 9]=9, [-2, 31]=-3.

{x} f-sy hem ähli hakyky sanlar köplüginde kesgitlenen b/n, {x}=x-[x] (x=[x]+{x}) deñlige görä, kesgitlenilýän drob bilen diýilip atlandyrylýän f-ýadyr. Mysal: {x}= x2,3-[x2,3]

{2, 3}=0,3(=2, 3-[2, 3]=0,3)

{-5, 4}=-5,4-(-6)=-5, 4+6=0,6.

Bitin hem-de drob bölekleri d-n atlandyrylýan bu f-ýalr sanlar nazarýetinde ähmiýetli br-ýalardyr. Mü/n: bitin bölegi diýlen f-ýa bilen indiki tassyklamada gabat gelýäris.

T1. n! Köpeltmek hasylyna p ýönekeý sanyñ girýän derejesi $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\dots$ jemi deñdir.

C. Hakykatdan hem n! Köpeltmek hasylyndaky köpelijileriñ arasynda p sana kratnylarynyñ sany $\left[\frac{n}{p}\right]$ sana deñdir. Bu köpelijileriñ arasynda p2 kratnylarynyñ sany $\left[\frac{n}{p^2}\right]$ sana deñ galar.

Bu soñky köpelijileriñ arasynda p3-e kratnylarynyñ sany bolsa, $\left[\frac{n}{p^3}\right]$ sana deñdir we ş. meñ. Şeýle usul bilen alnan sanlaryñ jemi bolsa gözlenilýän derejäki (n!-a girýän p ýönekeý sanyñ cerejesini) derýändir. Çünki

n! Köpeltmek hasylynyñ her bir pm+1 derejä kratny bolmadyk, ýöne pm kratny bolan, köpelijisi görkezlen usulda p, p2,…, pm derejelere kratny hökümiňde ylaýyk m gezek hasaplanýandyr. Teorema subut edildi.

Multiplikatiw funksiýalar.

K1. Multiplikatiw f-ýa d-n,

1) θ(a) (tetafunksiýa0 ähli bitin (+) sanlary köplüginde kesgitlenen bolup, busanlaryñ hiç bolmanda birinde o-la deñ bolmadyk baha kabul edýän b/sa;

2) Islendik (a1, a2)=1 bolan, a1 we a2 sanlar üçin θ(a1·a2)=θ(a1)·θ(a2) şerti könýan bolsa, tetefunksiýasyna aý-ýar θ(a).

Multiplikatiw f-ýalaryñ iñ sadalarynyñ biri θ(a)=as bu ýerde s – islendik hakyky ýa-da kompleks san, görnüşde kesgitlenilýän f-ýa hyzmat edip biler.

Ýokary getirýän kesgitlemeden görnüş ýaly θ(a) multiplikatiw f-ýasynyñ θ(1)=1 şerti kan-ýandygyny görmekañsatdyr. Hakykatdan hem egerde a0 bitin (+) san bolup, θ(a0)≠0 bolsa kesgitlemeden θ(a0)= θ(a0·1)= θ(a0)·θ(1) deñlik alynyp, bu ýerden θ(1)=1 bolmalydygyny taparys. Deñligiñ iki tarapyny hem (θ(a0)≠0 sana bolýäris) 1= θ(a0·1)= $1=\frac{\theta(a_0)}{\theta(a_0)}=\theta(a_E\cdot 1)=\frac{\theta(a_0)\theta(1)}{\theta_1(a_0)}$

Mundan başgada islendik iki sany θ1(a) we θ2(a) multiplikatiw f-ýalaryñ θ(a)= θ1(a)·θ2(a) köpeltmek hasylynyñ hem multiplikatiw f-dygyny subut etmek añsatdyr. Dogrudanda θ(a) ähli bitin (+) sanlar köplüginde kesgitlenip, θ(1)=1 bölendygy düşnüklidir (tetanyñ bir nokatdaky bahasy bir bolýandygy bu, diýildigi multiplikatiwligiñ bir şerti ýerine ýetýär) ikinji bir tarapdan islendik |a1, a2|=1 şerti kan-ýan a1 we a2 sanlar üçin

θ(a1·a2)=θ1(a1·a2)·θ2(a1·a2)=θ1(a1)·θ1(a2)·θ2(a1)·θ2(a2)= θ(a1)·θ(a2) soñky alnan deñlik multiplikatiwligiñ ikinji şertiniñ hem ýerne ýetýändigini görkezýär. Diýmek islendik iki sany multiplikatiw f-ýalaryñ köpeltmek hasyly hem multiplikatiwdir.

T1. Goý θ(a) multiplikatiw f-ýa, $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_k^{\alpha_k}$ - a sanyñ ýönekeý köpeldijilere dagytmagy bolsun, onda $\sum\limits_{d/a}$ a sanyñ ähli a bölüjükleri boýunça

$$\sum_{d/a}\theta(d) = \left\{1+\theta(p_1)+\theta(p_1^2)+\ldots+\theta(p_1^{\alpha_1})\right\}\cdot$$

$$\cdot\left\{1+\theta(p_2)+\theta(p_2^2)+\ldots+\theta(p_2^{\alpha_2})\right\}\cdot\ldots$$

alynýan jemi belgilesek, $\left\{1+\theta(p_k)+\theta(p_k^2)+\ldots+\theta(p_k^{\alpha k})\right\}$

deñlik dogrudyr (a=1 bolan halatynda bu deñligiñ sag tarapyny 1-e deñ d-n hasap edýäris). Subudy: tassyklanan tojdestwony subut etmek üçin sag tarapyndaky skobkalary alýarys. Onda $\theta(p_1^{\beta_1})\cdot\theta(p_2^{\beta_2})\cdot\ldots\cdot\theta(p_k^{\beta_k}) = \theta(p_1^{\beta_1}\cdot p_2^{\beta_2}\ldots p_k^{\beta_k})$ bu ýerde $0 \le \beta i \le \alpha i$ $i=1,\overline{k}$.

funksiỳasynyň kesgitlemesinden $\theta_1(p_i) = -\theta(p_i) = \mu(p_i)\cdot\theta(p_i)$ *hem – de* $\theta_1(p_i^s) = \mu(p_i^s)\cdot$ $\cdot\,\theta(p_i^s) = o, \quad s > 1$

gatnaşyklara eỳe bolỳandygymyzy nazara alsak taparys.

$$\sum_{d\backslash a}\mu(d)\cdot\theta(d) = \left\{1+\theta_1(p_1)+\ldots+\theta\left(p_1^{\alpha_1}\right)\right\}\cdot\left\{1+\theta_1(p_2)+\ldots+\theta\left(p_2^{\alpha_2}\right)\right\}\cdot$$

$$\cdot\left\{1+\theta(p_k)+\ldots+\theta\left(p_k^{\alpha_k}\right)\right\} = (1-\theta(p_1))\cdot(1-\theta(p_2))\cdot\ldots\cdot(1-\theta(p_k))$$

H.1 $$\sum_{d\backslash a}\mu(d) = \begin{cases} 1, & a = 1 \quad bolanda \\ 0, & a > 1 \quad bolanda \end{cases}$$

Bu netijäniň subudyny almak ü $\sum\limits_{d\backslash a}\mu(d) = \left\{\begin{matrix} 1, & a = 1 & bolanda \\ 0, & a > 1 & bolanda \end{matrix}\right\}$ çin subut edilen teoremada $\theta(a) = 1$ diỳip,hasap etmak ỳeterlikdir.

H.2 $$\sum_{d\backslash a}\frac{\mu(d)}{d} = \left\{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)\right\}; \qquad a > 1$$

Bu tassyklamanyň subudyny almak üçin subut edilen teoremada $\theta(a)\frac{1}{a}$ diỳip saỳlap, almak ỳeterlikdir.

T.1 Goỳ bitin (+) $\delta = \delta_1, \delta_2, ..., \delta_n$ sanlara hakyky ỳa-da kompleks bolan, $f = f_1, f_2, ..., f_n$ sanlar degişli bolsun, onda S' bilen δ-nyň 1-e deň, δ-nyň d sana kratnylaryna degişli bolan f-leriň jemini belgilesek bahalaryna degişli bolan f-leriň bahalarynyň jemini S_d bolan bolsa,

$S' = \sum \mu(d) \cdot S_d$ deňlik dogrudyr. Bu ỳerde jem δ -laryň hiç bolmanda birini bölỳän ähli d natural bölüjiler boỳunça alynỳadyr.

$$S' = f_1 \sum_{d \backslash \delta_n} \mu(d) + f_2 \sum_{d \backslash \delta_2} \mu(d) + ... + f_n \sum_{d \backslash \delta_n} \mu(d)$$

S.Belgilemelere görä

bolup, şol bir α natural bölüjä, eỳe bolan çlenleriň ählisi bir

deňlik dogry ỳere toplap, hem-de olarda bar bolan umumy $\mu(d)$ köpelijini skopkanyň daşyna çykarsak, skopkanyň içinde galỳan aňlatma ỳokarda belgilenen, S_d - d natural bölüjä eỳe bolan ähli $\delta -$ lara degişli f-leriň jemine deňdir. Bu diỳildigi teoremanyň tassyklamasyny aňladỳar.

6. Eỳler funksiỳasy.

K.1 Eỳler funksiỳasy $\varphi(a)$ ähli bitin (+) a sanlar üçin kesgitlenen bolup, 0,1,2,….,a-1 (1) sanlaryň arasynda a san bilen özara ỳönekeỳleriň sanyny aňladỳar.

Mysal: $\varphi(1) = 1$ $\varphi(2) = 1$ $\varphi(3) = 2$ $\varphi(4) = 2$ $\varphi(5) = 4$

Indiki teorema adalatlydyr.

Goỳ, $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ a sanyň ỳönekeỳ köpelijilere dagytmasynyň kanonik görnüşi bolsun. Onda

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_k}\right) \qquad (2) \qquad ya - da$$

$$\varphi(a) = \left(p_1^{\alpha_i} - p_1^{\alpha_1 - 1}\right) \cdot \left(p_2^{\alpha_1} - p_2^{\alpha_2 - 1}\right) \cdot ... \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \qquad (3)$$

hus, usan $\varphi\left(p^\alpha\right)$ *bolanda,*

$$\varphi\left(p^\alpha\right) = p^\alpha - p^{\alpha - 1} = p^{\alpha - 1}(p - 1), \qquad \varphi(p) = p - 1, \qquad p$$

Islendik p ỳönekeỳ $\alpha > 1$ (α birden uly natural sanlar üçin)dogrudyr .
Subudy. Mỳobus funksiỳasy üçin ỳokarda subut edilen belli teoremada δ *we* f sanlary şeỳle saỳlap alalyň .Goỳ x (1) –nji sanlar sistemasyndan ähli elementleri özüne baha deregine kabul edỳän bolsun , hem-de bu ỳagdaỳda $\delta = (x, a)$ we f=1 oňa degişli edeliň . Onda şol teoremadaky S' ululuk $\delta = (x, a)$ sanlaryň bire deňleriniň sanyny aňladardy. S_d -d sana kratny bolan $\delta = (x, a)$-laryň sany .

Şeỳlelikde ỳokarda aỳdylanna görä ,(x,a) sanyň d sana kratny bolmaklarynyň zerur şertiniň bu sanlaryň her biriniň d sana kratny bolmalydyklaryna görä a san d sana galyndysyz bölünmelidigini nazara alsak bu ỳagdaỳda s_d ululyk x -leriň d sana kratnylarynyň sanyny aňladardy. Ỳa-da başgaça aỳdanyňda $\frac{a}{d}$ sana deň bolar.

$$\varphi(a) = \sum_{d \backslash a} \mu(d) \frac{a}{d}$$

Şeỳlelikde

$$\sum_{d \backslash a} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right)$$

dogry bolan deňligi nazara alsak, teoremanyň subudyny alarys. Subut edilen teoremadan $\varphi(a)$ Eỳler funksiỳasynyň multiplikatiw funksiỳa bolỳandygyny görmek kyn däldir.
Hakykatdan hem . Eger-de $(a_1, a_2) = 1$bolsalar, onda alnan formula görä , $\varphi(a_1, a_2) = \varphi(a_1) \cdot \varphi(a_2)$

7. Deňeşdirmeleriň käbir aýratyn häsiýetleri .

1).deňeşdirmeleriň iki tarapynyň umumy bölüjisi modul bilen özara ýönekeý bolsa onda deňeşdirmeleriň iki tarapyny hem bu umumy bölüjä bölmek mümkindir.

Hakykatdan hem goý, $a \equiv b(mod \quad m)$ bilen
$a = a_1 d, \quad b = b_1 d, \qquad we \qquad (d,m) = 1$ bolsun.
Onda şerte görä $a - b = d(a_1 - b_1)$ tapawut m-e galyndysyz bölünýändir. Bize öňden belli bolşuna görä , bu ýagdaýda $a_1 - b_1$ m modula galyndysyz bölünmelidir . Bu diýildigi belli bolan teoremadan $a_1 \equiv b_1(mod \ m)$ deňeşdirmä eýe bolarys.
2). Deňşdirmäniň ki arapyny hem onuň modulyny hem şol bir sana köpeltmek mümkindir. Ÿagny eger-de $a \equiv b(mod \ m)$ bolsa onda islendik k san üçin $a \cdot k \equiv b \cdot k(mod \quad mk)$ ýerine ýetýändir.

Hakykatdan hem $a \equiv b(mod \quad m)$ gatnaşykdan a=b+mt t-bitin san gatnaşygy alarys. bu deňligiň iki tarapyny hem k sana köpeltmek bilen $a \cdot k = b \cdot k + mk \cdot t$ deňlige eýe bolarys.
Bu ýerden belli teoremadan peýdalanyp $a \cdot k \equiv b \cdot k(mod \quad mk)$ deňeşdirmäni taparys.
3). Deňeşdirmäniň iki tarapyny hem , hem-de onuň modulnyň hem olaryň islendik umumy bölüjisine bölmek mümkindir . Hakykatdan hem eger-de $a \equiv b(mod \quad m)$ bilen $a = a_1 d,\ b = b_1 d,\ m = m_1 d$ bolsalar onda bize belli bolan tassyklamadan alynýan (a=b+mt) $a_1 d = b_1 d + m_1 d \cdot t$ deňligiň iki tarapyny hem d sana bölmek bilen $a_1 = b_1 + m_1 t$ bolmalydygyny ýa-da başgaça aýdanyňda $a_1 \equiv b_1(mod \quad m_1)$ bolýandyklaryny alarys.
4). Ege-de a we b sanlar birnäçe modullara görä deňeşdirerlikli bolsalar, onda olar b modullaryň iň kiçi umumy kratnysyna görä hem deňeşdirerliklidirler.

Hakykatdan hem eger-de
$a \equiv b(mod \quad m_1), a \equiv b(mod \quad m_2), \ldots, a \equiv b(mod \quad m_k)$
bolsa, bize belli bolan teoremadan a-b tapawudyň $m_1, m_2, \ldots, m_k$ modullara galyndysyz bölünmelidigi gelip çykýandyr. Onda bu tapawut modullaryň iň kiçi umumy kratnysyna hem bölüner . Bu diýildigi a we b sanlar modullaryň iň kiçi umumy $m_1, m_2, \ldots, m_k$
kratnysyna görä täze alynýan aňlatma öňki bilen m modula görä

5). Eger-de deňeşdirme m modula görä ýerne ýetýän bolsa , onda ol bu modulyň islendik bölüjisine görä hem ýerine ýetýändir.

Hakykatdan hem eger-de $a \equiv b(\mathrm{mod}\ m)$ bolsa onda a-b tapawut m modula görä galyndysyz bölünýändir. Onda ol tapawut m sanyň islendik d bölüjisine hem galyndysyz bölünýändir. Bu diýildigi $a \equiv b(\mathrm{mod}\ d)$ deňeşdirme dogrudyr.
6). Eger-de deňeşdirmäniň haýsy hem bolsa bir tarapy hem-de modul käbir sana bölünýän , bolsalar, onda ol sana deňeşdirmäniň beýleki tarapy hem bölünýändir.

Bu häsiýeti subut etmek üçin $a \equiv b(\mathrm{mod}\ m)$ deňeşdirmeden gelip çykýan $a = b + mt$ t-bitn san deňligiň çep tarapy a we onuň 2-nji goşulyjysy mt köpeltmek hasylynyň käbir c sana bölünýändiginden , sag tarapynda 1-nji goşulyjysy b-niň hem bu sana bölünmelidigini hasaba almak ýeterlikdir.
7). Eger-de $a \equiv b(\mathrm{mod}\ m)$ bolsa, $(a,m) = (b,m)$ bolýandyr.

Bu häsiýetiň dubudy üçin şerte görä , a=b+mt t-bitin san bolýandygyny , hem-denlemäni bu ýagdaýda a we m sanlaryň UB-jileriniň toplumy bilen b we m sanlaryň UB-jileriniň toplumynyň gabat gelýänliginden hem-denlemäni bu ýagdaýda hususan $(a,m)=(b,m)$ bolýanlygyndan peýdalanmak ýeterlikdir.

8) Eger-de

$$a_0 \equiv b_0(\mathrm{mod} \quad m), a_1 \equiv b_1(\mathrm{mod} \quad m), \ldots, a_n \equiv b_n(\mathrm{mod} \quad m)$$

$$x \equiv y(\mathrm{mod} \quad m)$$

bolsalar onda

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv b_0y^n + b_1y^n + b_1y^{n-1} + \ldots + b_{n-1}y +$$
$$+ b_n(\mathrm{mod} \quad m)$$

deňeşdirme dogrudyr.

8. Aýyrmalaryň doly sistemasy.

m modula görä deňedirerlikli sanlar bu modul boýunça sanlaryň klasyny emele getirýändirler. Şolbir klasa degişli bolan sanlaryň ählisiniň bu modula bölünende deň galynda eýedikleri bellidir. Eger-de $mq+r$ ýazgyda q ähli mümkin bolan bitin sanlardan bahalar alsa onda bu klasyň (m-e bölünende r galynda eýe bolan sanlaryň klasynyň) ähli sanlaryny almak mümkindir.

$$-4 = 5(-1)+1 \qquad\qquad -9 = 5\cdot(-2)+1$$

Şeýlelikde her bir klasyň sanlarynyň m modula bölünende bir meňzeş galynda eýediklerini nazara alsak hem-de $mq+r$ ýazgyda r galyndynyň $0,1,2,\ldots,m-1$ bahalara eýe bolmak mümkinçiligini (çünki galyndyly bölmegiň algoritminden $0 \le r < m$ bolandygyna görä) nazara alsak m modula görä sanlaryň ähli mümkin bolan klaslarynyň sanynyň m-e deňdigini alarys sanlaryň m modula görä klasynyň her
bir sanyna onyň bu klasyň galan sanlaryna görä aýyrmasy diýip aýdylýar. Her klasyň sanlarynyň $mq+r$ görnüşdäki ýazgysyna $q=0$ bolan halatynda alynýan r sana (bu klasyň sanlaryny m modula bölenimizde galýan r galynda) bu klasyň iň kiçi (-) bolmadyk aýyrmasy diýip aýdylýar.

M modula göra sanlaryň klaslaryndan bir- birden san (aýyrma) alynyp düzülen m sany sanlaryň sistemasyna bu m modula görä aýyrmalaryň doly sistemasy diýip aýdylýar.

Adatça m modula görä aýyrmalaryň doly sistemasyna derek $0,1,2,\ldots,m-1$ sanlaryň sistemasy alynyp, lo iň kiçi (-) bolmadyk aýyrmalarň doly sistemasy diýip atlandyrylýar.

Absalýut iň kiçi aýyrma diýip- klasyň absalýut ululygy boýunça iň kiçi ρ aýyrmasyna aýdylýar.

Eger-de sanlar klasynyň ähli sanlary $mq+r$ görnüşinde aňladylýan bolup, $r < \frac{m}{2}$ bolsa $\rho = r$ bolýnadyr. Eger-de $r > \frac{m}{2}$ bolsa onda

$\rho = r - m$ görnüşinde kesgitlenýändir. Şeýle hem $r = \frac{m}{2}$ bolanda ρ deregine ýa $\frac{m}{2}$ ýa-da $\frac{m}{2} - m = -\frac{m}{2}$ san alynýandyr. Şeýlelikde absolýut iň kiçi aýyrmalaryň doly sistemasy deregine m täk bolanda

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

Eger-de m jübüt bolanda ,

$$-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2} \quad ya-da \quad -\frac{m}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1 \text{ hatar}$$

alynýandyr.

Mysal üçin: 9 modula görä , iň kiçi (-)bolmady ayrmalaryň doly sistemasy 0,1,2,…,8 hatar bu modula görä , absalýut iň kiçi aýymalaryň dol sistemasy bolup,

-4,-3,-2,-1,0,1,2,3,4 hatar hyzmat edýändir.

Edil şuňa meňzeşlikde

0,1,2,3,4,5,6,7 hatar 8 modula görä , iň kiçi (-) bolmadyk aýyrmalaryň doly sistemasy

-3,-2,-1,0,1,2,3,4 ýa-da -4,-3,-2,-1,0,1,2,3, atarlaryň islendik birini 8 modula görä bsalýut iň kiçi aýyrmalaryň doly sistemasy deregine almak mömkindir.

Subut edilmesi kyn bolmadyk indiki tassyklamalary belläp geçeliň .

T.1 m modul boýunça ikibir-ikibir deňeşdirerlikli bolmadyk islendik m sany sanlaryň toplumy m modula görä aýyrmalaryň doly sistemasyny emele getirýändirler.

T.2 Eger-de (a,m)=1 hem-de x m modula görä aýyrmalaryň doly sistemasyndan bahalar alýan bolsa, onda ax+b ýazgydan (bu ýerde b islendik bitin san) alynýan bahalar hem m modula görä aýyrmalaryň doly sistemasyny emele getirýändirler.

9. Aýyrmalaryň getirlen sistemasy .

Bize belli bolşuna görä , şol bir klasa degişli sanlaryň m modul bilen IUUB-leri gabat gelýändir. Bizi modul bilen özara ýönekeý sanlaryň klaslary gyzyklandyrjakdyr. Şeyle klaslaryň hersinden bir san alnyp ,düzülen sanlaryň sistemasyna berlen modula görä aýyrmalaryň doly sistemasy diýlip aýdylýar. Adatça aýyrmalaryň m modula görä , getirlen sistemasyny bu modula görä , iň kiçi (-) bolmadyk aýyrmalaryň 0,1,2,…,m-1 doly sistemasyndan bölüp alýarlar. Başgaça aýdanyňda bu sanlar hataryndaky sanlaryň m modul bilen özara ýönekeýlerini saýlap alýarlar. Kesgitlemeden görnüşi ýaly m modula

görä aýyrmalaryň getirlen sistemasyndaky sanlaryň sanynyň $\varphi(m)-e$ deň blakdygy düşniklidir.
T.1 m modul boýunça, deňeşdirerlikli bolmadyk m modul bilen özara ýöneleý blan islendik $\varphi(m)$ sany sanlar bu modula görä, aýyrmalaryň getirlen sistemasyny düzýändirler.

10. Ewklid algoritminiñ üznüksiz droblar bilen baglanşygy.

Goý α islendik hakyky san bolsun q_1 bilen α-dan uly bolmadyk iñ uly bitin sany belgiläliñ. Onda bitin bolmadyk α san üçin $\alpha = q_1 + \frac{1}{\alpha_2}$ $\alpha_2>1$ deñlik dogrudyr. Edil şuña meñzeşlikde bitin bolmadyk $\alpha_2, \alpha_3, \ldots \alpha_{s-1}$ sanlar üçin hem taparys.

$$\alpha_2 = q_2 + \frac{1}{\alpha_3} \qquad \alpha_3 = q_3 + \frac{1}{\alpha_4} \qquad \alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s}$$

$$\alpha_3>1 \qquad \alpha_4>1 \qquad \alpha_s>1$$

Bu toplan deñliklerden añlatmalary öñýanyndaky deñlikde ornyna goýmak bilen α san üçin $\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{.....q_{s-1} + \cfrac{1}{\alpha_3}}}}$ dogry bolan añlatma eýe bolarys.

Eger-de α san irrasional bolsa, onda α_s-leriñ hem her biri irrasional sandyr (çünki rasional α_s-de α sanyñ özi hem rasional bolardy). Hem-de, bu bolmeler prosesi tükeniksiz dowam eder. Eger-de α san rasional bolsa ýagny başgaça aýdanyñda ol (+) maýdalawnyjy bolan $\alpha = \frac{a}{b}$ görnüşinde gysgalmaly drob görnüşli san bolsa, ýokarda getirlen bölünmeler tükenikli bolup, olary Ewklid algoritminden peýdalanyp, ýerne ýetirmek mümkindir. Hakykatdan hem $a=b\cdot q_1+r_2$, $\alpha = \frac{a}{b}$ bolanlygy üçin iki tarapynam b bölmeli $\frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \cfrac{1}{\cfrac{b}{r_2}}$

$$\alpha = \frac{a}{b} = q_1 + \cfrac{1}{\cfrac{b}{r_2^{-2}}} \qquad r_2.$$

$$b=r_2q_3+r_3 \qquad \frac{b}{r_2} = q_2 + \cfrac{1}{\cfrac{r_2}{r_3}}$$

$r_2=r_3q_3+r_4$ $\qquad \frac{r_2}{r_3}=q_3+\frac{1}{\frac{r_3}{r_4}}$

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

Şeýlelikde rasional α san üçin $\alpha=\frac{a}{b}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_2+....\cfrac{1}{q_n}}}$ deñlige eýe bolarys.

α – sany üznüksiz droba dagydylanda emele gelýän q_1, q_2,… sanlara **doly däl paýlar** diýilip aýdylýär (α san rasional bölanda olar Ewklid algoritmindäki doly däl paýlardyr). Bu ýagdaýda $\delta_1=q_1$, $\delta_2=q_1+\frac{1}{q_2}$, $\delta_3=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3}}$ droblara bolsa **golaýlaşýän droblar** diýip aýdylýär.

11. Bir näbellili deňeşdirerlikler umumy düşünjeler.

Bir näbellili deňeşdirerlikler /has dogrusy "deňeşdirerlilikler"diỳilmeli /umumy görnüşde aşakdaky ỳaly ỳazylỳar:

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

$f(x)\equiv 0(\mathrm{mod}\, m)$ (1)

$a_0, a_1,\dots,a_n$ bitinsanlardyr.

Eger a_0 + m onda n deňeşdirerligiň görkezijisi diỳilỳär. (1) deňeşdirerligi çözmek-bu onuň kanagatlandyrỳan hemme bitin x-leri tapmak diỳmekdir.Ỳöne,eger $x_1$onuň bir çözüwi bolsa,ỳagny $f(x_1)\equiv 0(\mathrm{mod}\, m)$ onda deňeşdirerlikleriň häsiỳetine görä, (1) deňeşdirerligi m modul boỳunça x_1 bilen deňeşdirerli hemme x sanlar hem $x\equiv x_1(\mathrm{mod}\, m)$ kanagatlandyrỳarlar,ỳagny m modul boỳunça x_1-iň girỳän klasyndaky hemme aỳrylmalar ony ((1) gatnaşygy)kanagatlandyrỳarlar.((1) deňeşdirerligiň çözüwi bolỳarlar).

Şonuň üçin (1) deňeşdirerligiň çözüwi diỳip aỳratyn bir san alynman, eỳsem m modul boỳunça berlen deňeşdirerligi kanagatlandyrỳan sanlaryň bütin klasy hasap edilỳär.(Käwagt ỳönekeỳlik we amatlylyk üçin aỳratyn sanlara hem deňeşdirerligiň çözüwi diỳip atlandyrarys we olara diňe berlen modul boỳunça özara deňeşdirerli däl bolanda,ỳagny olar dürli klaslara degişli bolanda dürli çözüwde ỳaly gararys).

m modul boỳunça aỳrylmalaryň doly sistemasyndan (1) deňeşdirerligi näçesi kanagatlandyrỳan bolsa , hut şonçada çözüw klaslary bolỳar.(Bu klaslaryň wekilleri –(1) deňeşdirerligi kanagatlandyrỳan aỳrylmalardyr).

Diỳmek , m modul boỳunça doly sistemanyň aỳrylmalarnyň üstünde gös-göni synag edip,(1)deňeşdirerligi kanagatlandyrỳanlaryny saỳlap bileris , saỳlanan aỳrylmalaryň kömegi bilen hem çözüw klaslaryny talap bolar.

Çözüwleri şeỳle tapmak usulyna saỳlama metody diỳilỳär.

Mysal 1. Deňeşdirerligi çözmeli:

$$x^2 - x + 2 \equiv 0(\mathrm{mod}\,7)$$

Hasaplamany ỳeňilleşdirmek üçin 7 modul boỳunça absolỳut ululygy boỳunça iň kiçi aỳrylmalary alalyň:

$0,\ \pm 1,\ \pm 2,\ \pm 3.$

Ỳekän-ỳekän barlap göreliň:

X=0, $2 \equiv 0$ (mod 7)

X=-1, $(-1)^2-(-1)+2 \equiv 4 \equiv 0$(mod 7)

X=1, $1^2-1+2 \equiv 2 \equiv 0$ (mod 7)

X=-2, $(-2)^2-(-2)+2 \equiv 8 \equiv 1 \equiv 0$ (mod 7)

X=2, $2^2-2+2 \equiv 4 \equiv 0$ (mod 7)

X=-3, $(-3)^2-(-3)+2 \equiv 14 \equiv 0$ (mod 7) (*)

X=3 $3^2-3+2 \equiv 8 \equiv 1 \equiv 0$ (mod 7)

Şeýlelikde,berlen deňeşdirerligi diňe x=-3 kanagatlandyrýar.Şonuň űçin bu deňeşdirerligiň diňe bir çözűwi bar .

$x \equiv -3$(mod 7)

Ỳa-da $x \equiv 4$ (mod 7)

Mysal 2.

$$3x^4 + 2x^2 - 1 \equiv 0(\mathrm{mod}\,5)$$

5 modul boýunça aýrylmalaryň doly sistemasy: $0, \pm 1, \pm 2$.

Bularyň içinde deňeşdirerligi x=-2 we x=2 kanagatlandyrýarlar,diýmek onuň 2-i çözűwi bar;

$x \equiv -2 \equiv 3(\mathrm{mod}\,5)$

$x \equiv 2(\mathrm{mod}\,5)$

Mysal 3.

$$3x^2 + x - 1 \equiv 0(\mathrm{mod}\,5)$$

5 modul boýunça aýrylmalaryň doly sistemasy: $0,\pm1,\pm2$.

Aýyrmalaryň űstűnde geçirýän synaglarymyzyň hiç biri berlen deňeşdirerligi kanagatlandyrmaýar:

$x = o$ $\quad 3 \cdot 0^2 + 0 - 1 \equiv -1 \equiv 0(\mathrm{mod}\,5)$

$x = -1$ $\quad 3(-1)^2 + (-1) - 1 \equiv 1 \equiv 0(\mathrm{mod}\,5)$

$x = 1$ $\quad 3 \cdot 1^2 + 1 - 1 \equiv 3 \equiv 0(\mathrm{mod}\,5)$

$x = -2$ $\quad 3(-2)^2 + (-2) - 1 \equiv 9 \equiv 4 \equiv 0(\mathrm{mod}\,5)$

$x = 2$ $\quad 3 \cdot 2^2 + 2 - 1 \equiv 13 \equiv 3 \equiv 0(\mathrm{mod}\,5)$

Şeýlelikde ,berlen deňeşdirerligi hiç bir çözűwi ýok.

Deňeşdirerligi islendik bitin san kanagatlandyrýan bolsa, onda olar ýaly deňeşdirerliklere tozdestwolaýyn diýilýär. Tozdestwalaýyn deňeşdirerlige mysal edip Fermanyň kiçi teoremasynyň netijesini almak bolar:

$x^p - x \equiv 0 \pmod p$

Bu deňeşdirerlik islendik bitin x űçin ýerine ýetýär.

Elbetde , hemme koeffisiýenti m sana kratny /ýagny,

$a_i = mt_i, i=\overline{0,n}$)bolan deňeşdirerlik hem

$f(x) \equiv 0 \pmod m$

tozdestwolaýyndyr.

Konkret deňeşdirerlige olaryň umumy häsiýetlerini ulanyp,daşky görnűşi dűrli deňeşdirerliklere alyp bileris,olaryň hemmesi –deňgűýçlilikler,mysal űçin /mysal.3/

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

Ỳa-da $2x^2 - x + 6 \equiv 0 \pmod 5$

deňgűýçlilikler , çűňki biz aşakdaky iki deňeşdirerligiň tapawudyny aldyk :

$$5x^2 + 5 \equiv 0 (\mathrm{mod}\, 5)$$
$$3x^2 + x - 1 \equiv 0 (\mathrm{mod}\, 5)$$
$$2x^2 - x + 6 \equiv 0 (\mathrm{mod}\, 5)$$

Häsiýetleri hűşgärlik bilen dogry ulanmaly, bolmasa ýalňyşlyklara getirilýär , Meselem, $3x^2 + x - 1 \equiv 0 (\mathrm{mod}\, 5)$

bu ýerden, aýdaly,

$$6x^2 + 2x - 2 \equiv 0 (\mathrm{mod}\, 5)$$

dogrudyr /çep we sag bölegini 2-ä köpeltdik,çűňki

$(2,5)=1$

Emma eýäm

$$15x^2 + 5x - 5 \equiv 0 (\mathrm{mod}\, 5)$$

deňeşdirerlik indi tozdestwolaýyn deňeşdirerlikdir,ony biz çözűw bolmadyk

$$3x^2 + 1 \cdot x - 1 \equiv 0 (\mathrm{mod}\, 5)$$

deňeşdirerligiň indi bölegini hem 5-e köpeldip aldyk ,bu bolsa nädogry , çűňki 5 modul bilen özara ýönekeý däl.

(1)deňeşdirerligi f(x)=my iki näbellili kesgitsiz /diofant/deňleme bilen çalşyryp bileris. Tersine geçmek hem mümkin . Bu fakty soň ulanarys.

Gönükme.

Saýlama metody bilen deňeşdirerlikleri çözmeli:

33.
1) $2x^3 + 3x - 5 \equiv 0 (\mathrm{mod}\ 7)$
2) $x^2 + x - 2 \equiv 0 (\mathrm{mod}\ 5)$
3) $7x^2 - 5x + 1 \equiv 0 (\mathrm{mod}\ 7)$
4) $4x^3 - 7x^2 + 10 \equiv 0 (\mathrm{mod}\, 11)$
5) $x^3 - x + 1 \equiv 0 (\mathrm{mod}\, 13)$

12. Birinji derejeli deňeşdirerlikler.

Bir näbellili birinji derejeli deňeşdirerligi umumy görnüşde /azat çleni ters alamaty bilen sag bölege geçirip / şeýle ýazarys:

$$ax \equiv b(\text{mod}\, m) \qquad (1)$$

(1) deňeşdirerligiň çözüwi hakyndaky meseläni barlamyzda , m modul bilen a koeffisiýentiň özara baglanyşygynyň täsiriniň boljakdygyny aňşyrmak bolýar.

Ilki (1) gatnaşygy (a,m)=1 şert bilen çäklendireris.

1) Eger indi x m modul boýunça doly sistemadaky aýrylmalaryň bahalaryny alyp çykanda, ax çyzykly formanyň hem doly sistemadaky aýrylmalaryň hemmesiniň bahalaryny alýandygyny ýatlalyň

2) (1) deňeşdirerligiň çözüwleriniň sany,doly sistemadaky(1)gatnaşygy kanagatlandyrýan aýrylmalarynyň sanyna deňdir (v bap ,N1)

Şeýlelikde , 1) we 2)pikirýöretmelerden x-iň doly sistemadan alnan bir we diňe bir bahasynda ax b bilen deňeşdirerli bolýar.

Diýmek (a,m)=1 şertde (1) deňeşdirerligiň bir çözüwi bolýär:

$$x \equiv x_1(\text{mod } m)$$

ýa-da $x = x_1 + mt, t = 0, \pm 1, \pm 2, ...$

Bu çözüwi saýlama metody bilen tapyp bolar.

Mysal

$$7x \equiv 5 \ (\text{mod } 8)$$

8 modul boýunça aýrylmalaryň doly sistemasy

$0, \pm 1, \pm 2, \pm 3, 4.$

Aýrylmalaryň üstünde synag geçirip

$$X = 3 \ (\text{mod } 8)$$

çözüwi tapýarys.

2.2. Goý indi (a,m)=d > 1 bolsun.

Bu halda iki ýagdaýyň bolmagy mümkin : 1)b d, 2)b/d.

1)b d ýagdaýda (1) deňeşdirerligiň çözüwi bolup bilmez,çüňki deňeşdirerligiň häsiýetine görä , onuň çep hem sag bölekleri modul bilen şol bir iň uly umumy bölüjä(U.U.B)eýe bolmaly.

Mysal.

$6x \equiv 5(\text{mod } 9)$ deňeşdirerligiň çözüwi ýokdyr, çüňki(6,9)=3,emma 5 3. Tersine,eger (b,m)=d>1, a d bolsa, /mysal, $5x \equiv 6(\text{mod } 9)$,onda bu heniz deňeşdirerligiň çözgütsizdigine aňlatman eýsem, eger deňeşdirerligiň çözüwi bar bolaýsa, onda bu çözüw ax d şerti kanagatlandyrmalylygyny aňladýar. /Bu hem öz gezeginde çözülişi eňilleşdirmäge kömek berýär./

2. Goý indi ikinji ýagdaý ýerine ýetsin : b/d (şerte görä-dä (a,m)=d) Onda , elbetde,

$a=a_1d$, $b=b_1d$ we $m=m_1d$ (2)

indi (1) deňeşdirerlik $a_1dx=b_1d(\text{mod } m_1d)$

ýa-da $a_1x=b_1(\text{mod } m_1)$ (3)

/Deňeşdirerlikleriň häsiýetine görä onuň iki bölegini we moduly umumy köpeldijä bölüp bilýäris/

(3)deňeşdirerlikde $(a_1,m_1)=1$,onda (3)çözütli bolup, onuň bir çözüwi bardyr:

$$x=x_1(\text{mod } m_1) \qquad (4)$$

(4) çözüwde x_1 sana $m_1$modul boýunça iň kiçi otrisatel däl aýrylma ýaly garap, şol öňki m_1 modul boýunça aşakdaky aýrylmalar bir klasa girýärler:

$\ldots,x_1-m_1,x_1,x_1+m_1,\ldots,x_1+(d-1)m_1,\ldots$(5)

m modul boýunça bolsa (5) hatardaky sanlar bir çözüw bolman, eýsem olar 0,1,2,…,m-1hatarda /bular m modul boýunça aýrylmalaryň doly sistemasyny guryar we diýmek , dürli klaslara degişli bolýar/ näçesi bar bolsa,şonça-da (1) deňeşdirerligiň m modul boýunça dürli çözüwleri bolar. (5) hataryň içinde aşakdaky sanlar:

$x_1, x_1+m_1,x_1+2m_1,\ldots,x_1+(d-1)m_1$ (6)

0,1,2,…,m-1

hataryň içinde doly ýerleşýärler

diýmek, iň ulusy

ýöne eýýäm (6) hatarda

d san bar.Şeýlelikde , (1) deňeşdirerligiň d dürli çözüwi bar.

Aýdylanlary ýygnap,teorema aldyk:

ax=b(mod m) (1)

deňeşdirmek üçin

1) Eger (a,m)=1 bolsa , çözüwi bar, özem ýeke-täkdir.
2) Eger (a,m)=d>1 bolsa, onda a) b d ýagdaýynda çözüwi ýok. b) b/d ýagdaýynda hem d çözüwi bar.

Mysal

15x=25(mod 55)

Deňeşdirerligiň iki bölegini we moduly 5-e bölüp

3x=5 (mod 11)

alarys.Saýlama metody bilen

x=9(mod 11)

taparys.Ýa-da x=9+11t, t=0, ±1,±2,... Başlangyç deňeşdirerligiň bäş çözüwi bolup, olar

x=9, 9+11, 9+2 11, 9+3 11, 9+4 11 (mod 55)

ýagny, x=9,20,31,42,53 (mod 55)

2.3 Koeffisiýentleri özgertmek metody bilen birinji derejeli deňeşdirerlikleri çözmek mümkin: Deňeşdirerlikleriň häsiýetlerni ulanyp, deňeşdirerligiň sag bölegini näbelli x-iň koeffisiýentine bölüner ýaly edip, koeffisiýentlerni özgertmege synanşylýar. Bu özgertmeler esasan aşakdakylardyr:

Koeffisiýentleri absolýut ululygy boýunça iň kiçi aýrylmalar bilen çalşyrmak, a koeffisiýente bölüner ýa-ly edip, sag bölegni modula kratny sanlary goşmak çep we sag böleklerniň umumy bölüjileri bolar ýa-ly edip başga deňeşdirerli sanlara geçmek we ş.m.

Özgertmäni a-yň , ýa-da b-yň , ýa-da ikisiniň hem üstünde geçirmek mümkin.

Ýene-de , (b,m)=d>1 bolanda çözülişiň eňilleşýändigini belläpdik, bu ýagdaýda täze näbellä geçmek hem amatlylyk döredip biler.

Koeffisiýentleri özgertmek metody diýlip aýdylsa-da , deňeşdirerligiň, çözüwini kesgitli öwürmeli, ammalary yzygider ýerne ýetirilip alynaýmaýar. Her bir konkret

Mysal çözülende esasy ýaraglary /umuman matematiklere gerek sypatlary/-aşyrmagy endigi we hasaplaýyş ukybyny ulanmaly bolýar. Her halatda hem /esasan hem modul 0 diýen uly bolmanda / bu metoda netijeli metod ýaly garamak mümkin.

Mysalar.

$29x=1(\text{mod } 17)$

$(29-17)x=1\ (\text{mod } 17)$

$12x=1$ /ýalňyşlyga ýa-da düşniksizlige getirmeýan bolsa modulyny gaýtalap ýazyp durarys/.

$12x=1+17=18,$

$2x=3,\ \ 2x=3+17=20$

ýagny $2x=20\ (\text{mod } 17)$

ýa-da $x=10\ (\text{mod } 17)$

2. $5x=6\ (\text{mod } 9),\qquad (6,9)=3$

5x hem 3-e bölünmelidir, $5x/3$,ýöne 5 3 onda $x/3$

Diýmek çözüwi 3,6 sanlary barlamak bilen taparys:

$5.3=6\ (\text{mod } 9)\ \ 6=6(\text{mod } 9)\qquad x=3(\text{mod } 9)$

Iki mysalda hem ýeketäk çüňki

1) $(29,17)=1$ we 2) $(5,9)=1$.

2) mysalda $(6,9)=3$ bolany üçin $x=3y$ bilen çälşyryp bolardy,

onda $5\ 3y=6\ (\text{mod } 9)$

$5y=2(\text{mod } 3)$

$2y=2(\text{mod } 3)\qquad y=1(\text{mod } 3)$

$3y=3(\text{mod } 3\ 3)$

$x=3(\text{mod } 9)$

3. $21x+5=0\ (\text{mod } 29);\qquad (21,29)=1$

$(21+29)x=-5(\text{mod } 29)$

$50x=-5\ (\text{mod } 29)$

$10x=-1=28(\text{mod } 29)$

$10x=28+8\ 29=28+232=260(\text{mod } 29)$

$x=26\ (\text{mod } 29)$

4. $8x=27\ (\text{mod } 12)$

$(8,12)=d=4;\ \ 20/4$

$2x=5\ (\text{mod } 3)$

$(2+3)x=5(\text{mod } 3)$

$5x=5\ (\text{mod } 3)$

$x=1(\text{mod } 3)$

Diýmek ,8x=20(mod 12)deňeşdirerligiň çözüwleri
X=1, 1+3, 1+2 3, 1+3 3 (mod 12)
X=1, 4, 7, 10 (mod 12)
4-çözüwi bar.
5. Goỳ,

111x=81 (mod 447)

(111,447)=d=3 we 81/3

Sonuň üçin

37x=27 (mod 149)

deňeşdirerligi çözmeli bolỳarys. /Başdaky deňeşdirerligiň 3 çözüwi bolar/. Bu deňeşdirerligi çözmek umuman aňsat däl. Saỳlama matody bilen çemeleşsek. 0,1,2,…,148 aỳrylmalary ỳekän-ỳekän synagdan geçirjek bolsak köp wagt gerek , koeffisiỳentlerini özgertmek metodyny bolsa nähili we nädip ulanmalydygyny görmek kyn /uly tejribe , ennik we aňlylyk gerek/

2.4. Eỳler teoremasyny ulanyp,birinji derejeli deňeşdirerlikleri çözmek otnositel kyn däl.

Goỳ bize (1) deňeşdirerlik berlen bolsun

ax=b (mod m) (1)

(a,m)=1 hasap etmek bolar /bolmasa ol şol ỳagdaỳa, getirlerdi, ỳokarky mysalda (111,447)=d=3, ỳöne eỳỳäm

37x=27 (mod 149)

deňeşdirerlikde (37,149)=1 we biz soňkyny çözmeli /.
(a,m)=1 bolany üçin, Eỳler teoremasy esasynda

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

Indi (1) deňeşdirerligi aşakdaky ỳäly ỳazmak mümkin

$$ax \cdot 1 \equiv b \cdot a^{\varphi(m)} (\operatorname{mod} m)$$

bu ỳerden

$$x \equiv ba^{\varphi(m)-1} (\operatorname{mod} m)$$

Seỳlelikde (1) deňeşdirerligiň çözüwini aňsatlyk bilen tapỳarys. Mysalarda garaliň.

1.
$$2x \equiv 5(\operatorname{mod} 7)$$
$$(2,7) = 1, \varphi(7) = 6$$
$$x \equiv 5 \cdot 2^{\varphi(7)-1} (\operatorname{mod} 7) \equiv 5 \cdot 2^{6-1} (\operatorname{mod} 7) \equiv$$
$$\equiv 5 \cdot 2^5 \equiv 5 \cdot 32 \equiv 160 \equiv 6(\operatorname{mod} 7)$$
$$x \equiv 6(\operatorname{mod} 7)$$

3. $37x \equiv 27($

2.
$$37x \equiv 27(\operatorname{mod} 149), (37,149) = 1$$
$$\varphi(149) = 148$$
$$x \equiv 27 \cdot 37^{\varphi(149)-1} (\operatorname{mod} 149)$$
$$x \equiv 27 \cdot 37^{147} (\operatorname{mod} 149)$$

Seỳlelikde , bu deňeşdirerligiň çözüwini aňsatlyk bilen tapdyk. Yöne çözüwiň şu görnüşde göwnimiz suw içmeỳär, çözüwini şu görnüşde galdyryp, biz doly kanagatlanyp bilmeris. Tygşytsyzlyk ,çemesizlik indi $27 \cdot 37^{147}$, sanyň /aỳrylmanyň/ ululygy bilen ỳüze çykỳar.Islendik çözüwi-berlen modul boỳunça iň kiçi /absolỳut ululygy boỳunça ỳa-da otrizatel däl ululygy boỳunça/aỳrylmanyň kömegi bilen aňlatmaga çalyşỳarys.
Su deňeşdirerligiň "oňat"çözüwi

$$X=41 \text{ (mod 149)}$$

Bolmaly,/diỳmek,

$$27 \cdot 37^{147} \equiv 41 (\text{mod} 149)$$

Aỳdylanlardan aşakdaky netijä gelỳäris:
Eỳler teoremasyny ulanyp, deňeşdirerligiň çözüwi aňsat tapylỳan hem bolsa , çözüwini aňladỳan aỳrylmanyň köp halatlarda uly bolỳanlygy zerarly çemesizlik döreỳär.

2.5. Birinjiderejeli deňeşdirerlikleriň zynjyr droblarynyň kömegi bilen çözülişleri.

Goỳ bize (1) deňeşdirerlik berlen bolsun

$$ax=b \text{ (mod m)} \qquad (1)$$

$$(a,m)=1 \text{ we } a>0$$

talap edỳäris. /şeỳle bolmanda şu ỳagdaỳlara getirip bolỳanlygy düşniklidir/. m/a gysgalmaỳan drobi zynjyr drobyna dargadalyň,
onuň golaỳlanỳan droblaryny adatdaky ỳaly $\delta_k = \dfrac{p_k}{\theta_k}$ bilen belläliň .

m/a rasional drob, şonuň üçin iň soňky golaỳlanỳan droby $\dfrac{p_n}{\theta_n}$ bolsa,

Onda deregine ỳazyp bolỳar we bu ỳerden
Ya-da
(7)deňeşdirerligiň iki bölegini hem $(-1)^{n-1}b$ sana köpeldip alarys:
Soňky deňeşdirerligi başlangyç (1) bilen özara deňeşdirip , onuň çözüwi bolỳar diỳip netijä gelỳäris.
Seỳlelikde , (1)deňeşdirerligiň (9) çözüwini tapmakda esasy mesele m/a rasional sanyň iň soňkyň öň ỳanyndaky golaỳlanỳan drobynyň sanowjysyny (p_{n-1}) hasaplamakdyr.
(1) deňeşdirerligiň ỳeke-täk çözüwi bar, onda (9) şol ỳalňyş çözüw bilen gabat gelmeli.

Mysallar.
Oň doly işlenilmän goỳlan 5-nji mysala garalyň.

$$111x=81 \text{ (mod 447)}$$

$$(111,447)=d=3, \quad 81/3$$

$$37x=27 \text{ (mod 149)}$$

$$\frac{m}{a} = \frac{149}{37} = 4 + \frac{1}{37}$$

n=2, P_1=4

$$x \equiv (-1)^{2-1} \cdot 4 \cdot 27 \equiv -108 \equiv 41(\bmod 149)$$

Indi başlangyç deňeşdireligiň çözüwleri:

d=3; $x \equiv 41, 41+1\cdot 149, 41+2\cdot 149(\bmod 447)$

$x \equiv 41, 190, 339(\bmod 447)$

$$380x \equiv 236(\bmod 1232)$$

$$(380,1232) = d = 4; 236/4$$

$$95x \equiv 59(\bmod 308)$$

$$\frac{308}{95}$$

Şeỳlelikde , $P_{n-1}=P_4=107$

Ýa-da $x \equiv (-1)^4 \cdot 107 \cdot 59(\bmod 308)$

$x \equiv 6313 \equiv 153(\bmod 308)$

Onda başdaky deňeşdirerlik üçin

$$x \equiv 153; 153+1\cdot 308; 153+2\cdot 308; 153+3\cdot 308(\bmod 1232)$$

$$x \equiv 153; 461; 769; 1077(\bmod 1232)$$

Bir näbelli birinji derejeli deňeşdirerlikleri zynjyr droblarynyň kömegi bilen çözmeklik – bu esasy metoddyr.

Gönükmeler.

34. Saỳlama metody bilen deňeşdirerlikleri çözmeli:

1)$11ч \equiv 15(ьщв 36)$; 2)$7x \equiv 9(\bmod 10)$

3)$10ч \equiv 15(\bmod 35)$; 4)$6x \equiv 27(\bmod 12)$

35.koeffisiýentleri özgertmek metody bilen deňeşdirerlikleri çözmeli:

1) 13x=10(mod 11) 2)19x=12(mod 35)

3) 16x=31(mod 31) 4)7x=5(mod 24)

36.Eýler teoremasyny ulanyp deňeşdirerlikleri çözmeli:

1)13x=3(mod19); 2)27x=7(mod58)

37. Zynjyr droblarynyň kömegi bilen deňeşdirerlikleri çözmeli:

1) 213x=137(mod 516); 2) 186x=374(mod 422)

3)129x=321 (mod 471); 4)67x=64 (mod 183)

13. Iki näbellili birinji derejeli kesgitsiz deňlemeleri çözmek.

3.1.Birinji derejeli iki näbellili kesgitsiz deňleme

ax+by=c (1)

görnüşde bolup, (a,b-nuldan tapawutly bitin sanlar,C-islendik bitin san),muny kanagatlandyrýan x-iň we y-iň diňe bitin bahalar bar bolsa , olara kesgitsiz (1) deňlemäniň çözüwleri diýlip, deňlemäniň özüne bu ýagdaýda – bitin sanlarda çözgütli diýilýär.

Ters ýagdaýda –(1) kesgitsiz deňleme bitin sanlarda çözgütsiz diýlip aýdylýar.

a we b koeffiziýentlere özara ýönekeý sanlar ýaly garamak mümkin,eger ol beýle bolmasa , onda

$$(a,b)=d>1$$

we $a=a_1d$, $b=b_1d$

(1) deňleme hem

$$(a_1x+b_1y)d=c \quad (2)$$

görnüşde geçirdi we onuň bitin çözüwleriniň bolmagy diňe c/d ýerine ýetende mümkin . /Eger C azat çlen d köpeldijä bölünmese , onda (2) bitin sanlarda çözgütsizdigi aýdyň/ c/d şertden $c=c_1d$ gelýär we (2)-ni

$$(a_1x+b_1y)d=c_1d$$

Ýa-da $a_1x+b_1y=c_1$ (1_1)

ýazyp bolýar,ýöne indi $(a_1,b_1)=1$

3.2. Ilki c=0 ýagdaýa garaliň,onda (1) deňleme

$$ax+by=0 \quad (3)$$

görnüşe geçer. Soňkyny x görä çözüp alarys:

(4)

Bu ýerden x bitin bahalary diňe y galyndysyz a sana bölünende alynýändygy görünýär. Onda a sana kratny bitin y ululygy

$$y=at \quad (5)$$

görnüşde ýazyp bolar, t erkin bitin sanlary kabul edýär.

(5)-den y-iň bahasyny (4) gatnaşykda goýup

(6)

x-iň bahasyny alarys.

(6),(5) gatnaşyklary ýygnap

$x=-bt$, $y=at$, $t=0,\pm 1,\pm 2,\dots$

(2) deňlemäniň hemme bitin çözüwlerini görkezýän formulalary alýarys.

Goý indi $c\neq 0$ we $(a,b)=1$,

Ýagny $ax+by=c$

Ýa-da $ax=c-by$

$$ax\equiv c \pmod b \quad (7)$$

Soňky deňeşdirerligi çözip (ol çözgütlidir,çüňki(a,b)=1) alarys:

$$x\equiv x_1 \pmod b$$

ýa-da $x=x_1+bt$, $t=0,\pm 1,\pm 2,\dots$

degişli bahalarny kesgitlemek üçin:

$$a(x_1+bt)+by=c$$

bu ýerden $by=c-ax_1-abt$

ýa-da $y=\dfrac{c-ax_1}{b}-at, t=0;\pm 1,\dots$

$y_1=\dfrac{c-ax_1}{b}$ -bitin san bolmagy zerur,ol x_1-e degişli y-iň hususy bahasy bolýar.

Şeýlelikde,(1) kesgitsiz deňlemäniň umumy çözüwi aşakdaky görnüşde bolar:

38. Kesgitsiz deňlemeleri bitin sanlarda çözmeli.

1)$17x-16y=31$; 2)$11x+16y=156$.

39. ax+by=c göniň üştünde abssissalary a_1 we a_2 bolan nokatlaryň bolan arasynda ýatan bitin nokatlaryň sanyny tapmaly./Bitin nokatlar diýip koordinatalary bitin bolan nokatlara aýdylýär/.

1)8x-13y+6=0, a_1=-100, a_2=150

2)7x+29y=584, a_1=-20, a_2=160

14. Birinji derejeli deňeşdirerlikleriň sistemasy.

Bir näbellili birinji derejeli deňeşdirerlikleriň sistemasynyň aşakdaky ýaly ýazarys:

$$\alpha x \equiv b_1 (\mathrm{mod}\, m_1)$$
$$.......\alpha x \equiv b_k (\mathrm{mod}\, m_k)$$

Sistemany çözmek diýmek, ony kanagatlandyrýan x-iň hemme bitin bahalaryny tapmak diýmekdir. X-iň şeýle bahalarynyň bolmagy üçin, deňeşdirerlikleriň her haýsynyň aýratynlykda çözgütli bolmagy zerur /ýöne, elbetde,ýeterlik däldir /

Şonuň üçin her haýsy aýratynlykda çözgütli bolan deňeşdirerlikleriň sistemasyna garamak ýeterlikdir:

Sistemalar bilen iş salyşylanda , ilkinji nobatda bileleşiklilik kesgitlenilýär. Eger deňeşdirerlikleriň sistemasy bileleşikli bolsa /ýagny bitin sistema çözgitli bolsa/, onda indi onuň çözüwi gözlenilýär.

4.2. Modullary özara goşa-goşadan ýönekeý ýagdaýynda ,

Ýagny $(m_i,m_j)=1$, i=j

Bolanda,deňeşdirerlikleriň sistemasy mydama bileleşişli bolýar /sebäbini şu punkda-da,umumy ýagdaýa garalanda-da degişli ýerinde görkezeris/.

Eger (2) sistemadaky deňeşdirerlikleriň hemmesinde sag bölegini şol bir x_0 san bilen aňladyp bilsek , ýagny

Onda(v bap,N1.1.3. b)) (2_1) sistema

(3) $x \equiv x_0 (\mathrm{mod}[m_1, m_2, ..., m_k]) \equiv x_0 (\mathrm{mod}\, m_1, m_2, ..., m_k)$

deňeşdirerlik bilen deňgüýçli . Diýmek, gözlenilýän çözüw:

(3) $x = x_0 + mt, t = 0, \pm 1, ...; M = m_1 \cdot m_2, ..., m_k$ (4) bolar.

Garalýan ýagdaýda,ýagny hemme

$(m_i,m_j)=1$ i=j

bolanda,suratlandyrlan x_0 sany mydama tapmak mümkin.

Munuň üçin M moduly aşakdaky görnüşlerde ýäzylan

$M=(m_1)\ m_2m_3,\dots,m_k=m_1\,(m_2)\ m_3\dots m_k=\dots=m_1\ m_2\dots(m_k)$

Ýa-da $M=m_1M_1=m_2M_2=\dots=m_kM_k$

M_1köpeltmek hasyly m_1 moduldan özge hemme modullary özünde saklaýar, M_2 – m_2-den özge modullary saklaýan we ş.m.

Onda $(M_1,m_1)=(M_2,m_2)=\dots=(M_k,m_k)=1$

Şonuň üçin

Deňeşdirerlikler ýerine ýeter ýaly $M_1,M_2,..,M_k$ sanlary tapmak mümkin /olar häzirlikçe bize belli däl, ýöne şeýle sanlaryň barlygyny tassyklaýarys, çüňki $(M_i,m_i)=1$;
Eýler, Ferma teoremalaryny ýatlaň /
Edil şol sebäbäplere görä
$M_2,M_2=1$;modul boýunça galanlary bolsa $(m=m_2)$
m_k modul boýunça galanlary bolsa
Şeýlelikde
Bu ýerden hem

(4)

Indi ýokarda agzalan häsiýetlere eýe bolan x_0 sany aşakdaky formula boýunça gurup bileris:

(5)

Hakykatdan-da, (4) zerarly (5)-den

Soňkylaryň üsti bilen (2) sistemamyz (2_1) sistema geçýär,$(2)_2$-iň çözüwi bolsa, eýýäm belleşimiz ýaly:

(6)

Ýene bellemeli faktymyz-bu M_i we M_i sanlaryň
b_i sana bagly däldigidir. Şonuň üçin (2) sistemadaky deňeşdirerlikleriň sag bölekleri ütgeýände, degişli x_0 aňlatmalary (5) gatnaşygynda b_i-leri täze bahalary bilen çalşyryp alynýar.

1. 4-e,5-e we 7-ä bölenimizde galyndysy degişlilikde
3,4,5 deň bolan 200 we 500 sanlaryň arasynda ýerleşen sanlary tapmaly.

Çözülişi:

Şerte görä:
$(4,5)=(4,7)=(5,7)=1$
$M=4\ 5\ 7=140=4\ 35=5\ 28=7\ 20$
$M_1=35;\ \ M_2=28;\ \ M_3=20$

$X_0=35\ 3\ 3+28\ 7\ 4+20\ 6\ 5=1699,$
$200<x=1699+140t<500$
$x_1=1699-140\ 10=299,$
$x_2=299+140=439;$
299, 439.

4.3. Umumy ýagdaýda (2) sistemadaky deňeşdirerlikleriň modullaryny çäklendirmeýäris. (2) sistema çözgütli bolanda , ony kanagatlandyrýan sanlar berlen $m_1,m_2,\ldots,m_k$ modullaryň K.Y.K-yna deň bolan $M[m_1,m_2,..,m_k]$modul boýunça aýrylmalaryň klasyny emele getirýär.

(2) sistemanyň birinji deňeşdirerligini kanagatlandyrýan san aşakdaky görnüşde bolar:

$x=b_1+m_1t_1$ (6)

Bularyň içinde (2) sistemnyň hem ikinji deňeşdirerligini kanagatlandyrýanlary
$m_1t_1=b_2(\text{mod } m_2)$ (7)
şerti ýerine ýetirmeli we diňe şolar bolmaly.
$m_1t_1=b_2-b_1(\text{mod } m_2)$
Eger $(m_1,m_2)=d$ we b_2-b_1 d bolsa , onda (7) deňeşdirerligiň çözüwi ýok we, diýmek, (2) deňeşdirerlikler sistemasy bileleşikli däl ($(m_1,m_2)=1$ bolsa, deňeşdirerlik çözgütli bolardy, indiki deňeşdirerlikler hakynda hem şuny aýtmak bolýar, hut şunuň üçin modullar goşa-goşadan ýönekeý bolanda , sistema bileleşikli bolýar). (7) deňeşdirerligiň çözgütli bolmagy üçin
Indi bolany üçin , soňky deňeşdirerligiň çözüwi bar, ol çözüw:
Ýa-da t_2-islendik bitin san. Şeýlelikde, sistemanyň birinji we ikinji deňeşdirerliklerini kanagatlandyrýan baha (6) we soňky gatnaşyklara seret)
Ýa-da
Bu ýerde $x_2=b_1+m_1t_1$ onda
Şeýle pikirýöretmäni üçünji deňeşdirerlige geçemezde-de ,soňra-da dowam edip, eger sistema çözgütli bolsa $M=[m_1,m_2,..,m_k]M$ modul boýunçä ony kanagatlandyrýan aýrylmalaryň klasyna (2) sistemanyň çözüwi diýip aýdarys.

Gönükmeler
40.Aşakdaky şertleri ýerine ýetirýän 1000-deň kiçi natural sanlary tapmaly:
1) 3-e, 5-e, 8-e bölemizde , galyndylary degişlilikde
2, 4, 1 deň . 2) 15-e, 14-e, 11-e bölemizde, galyndylary degişlilikde 11 , 3 , 5 deň.
41. Deňeşdirerlikleriň sistemasyny çözmeli:
$$\begin{cases} x \equiv 13(\text{mod}\,14) \\ x \equiv 6(\text{mod}\,35) \\ x \equiv 25(\text{mod}\,45) \end{cases}$$

42.
$$x \equiv b_1(\text{mod}\,8)$$
$$x \equiv b_2(\text{mod}\,9)$$
$$x \equiv b_3(\text{mod}\,13)$$
Sistemanyň çözüwiniň umumy görnüşini ýazyň.

Ýokary derejeli deňeşdirerlikler.

15. Ýönekeý modul boýunça ýokary derejeli deňeşdirerlikler.

1.1. Ýokary derejeli deňeşdirerligi barlamak , olary has ýönekeýleşdirmek olaryň moduly ýönekeý san bolanda aňsat we amatly bolýar.

Şeýlelikde, goý bize
$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n=0\ (\text{mod } p) \quad (1)$$
deňeşdirerlik berlen bolsun, a_0 p

Ilki bilen $a_0,a_1,\ldots,a_n$ koefiziýentleri absolýut ululygy boýunça iň kiçi aýrylmalar bilen çalşyrmak mümkin, ýene esasy zadyň biri-ýokary koefiziýenti bire deňläp bolýar /çüňki

$a_0a=1$ (mod p)

/şeýle a bardyr, Ferma teoremasyny ýatlaň/

Aşakdaky teoreme deňeşdirerlikleri has düýpli sadalaşdyrýar:

Teorema

(1) deňeşdirerlik derejesi (p-1)-den ýokary bolmadyk deňeşdirerlik bilen deň güýçli.

Subuty.

Ferma teoremasy esasynda $x^p - x=0$ (mod p), onda we R(x) derejesi ýokary däl.

Diýmek, f(x)=R(x) (mod p) (2)

Soňkydan teoremanyň tassyklamasy gelip çykýar.

Praktikada f(x) köp çleni x^p-x ululyga bölüp durmaýarlarda , hem bir x^m(m>p) ululyk x^r ululyga getirilýär we

$$r \le p-1$$

$$m = (p-1)k + r, 0 \le r \le p-1$$

$$x^p \equiv x(\mathrm{mod}\, p)$$

tozdestwolaýyn deňeşdirerligiň 2-i bölegini hem

ululyklara köpeldip, yzygider zynjyr boýunça alarys:

Şeýlelikde

Mysal.

Aşakdaky deňeşdirerligi

$x^9-2x^8+3x^7-2x^5+2x^4+x+8=0$ (mod 5)

derejesi 4-den ýokary bolmadyk deňeşdirerlige getirmeli.

(2) formulany alaliň :

$x-2x^4+3x^3-2x+2x^4+x+3=0$ (mod 5)

$3x^3+3=0$ (mod 5); $x^3+1=0$ (mod 5)

1.2. Indi (1) deňeşdirerligiň çözüwleriniň maksimal sany hakynda näme aýdyp bolar?

Teorema

Ýönekeý modul boýunça n-ji derejeli deňeşdirerligiň çözüwleriniň sany n-den artyk bolmaz.

Deňlemeler bilen iş salşylansoň , bu teoemany tassyklamasy anyk ýaly görünmegi mümkin. Ýöne beýle "anyklyk"ähtibarsyzdyr, çünki düzümli modul boýunça n-ji derejeli deňeşdierlikleriň çözüwiniň sany n-den köp bolup biler.

Ýokarky teoremada-da , geljekde-de biz $n<p-1$ diýip alarys /deňeşdirerlikler üçin bu ýagdaýa elmydama getirlip bolýar/.

Eger x_1 (1) deňeşdirerligiň çözüwi bolsa, ýagny

$$f(x_1)=0 \pmod p$$

onda $f(x)=(x-x_1)f_1(x)+f(x_1)$

tozdestwo Bezu teoremasy boýunça alynýar we $f_1(x)$ köpçlen /derejesi n-1, ýokary koeffiziýenti a_0 $f(x_0)$ san , ol P modula bölünýär, diýmek

$$f(x)=(x-x_1)f_1(x)(\mathrm{mod}\ p) \quad (4)$$

Ýa-da $(x-x_1)f_1(x)=0 \pmod p$ (5)

Eger x_2 $f_1(x)=0(\mathrm{mod}\ p)$ deňeşdirerligiň çözüwi bolsa ,

$$f_1(x)=(x-x_2)f_2(x) \pmod p$$

ýa-da $(x-x_1)f_2(x)=0 \pmod p$ (6)

ýazyp bilerdik, (5) gatnaşygy göz öňünde tutup

$$f(x)=(x-x_1)(x-x_2)f_2(x)=0 \pmod p$$

Umuman

Eger indi $f_k(x)=0 \pmod p$ deňeşdirerligiň çözüwi ýok bolsa, onda $x_1,x_2,\ldots,x_k$-dan özge $f(x)=0 \pmod p$ deňeşdirerligiň hem çözüwi ýokdyr,çünki eger

Hem bolmaly $(x-x_i)$ p , $i=1,k$, bu bolsa $f_k(x)$ hakynda aýdanymyzda garşy gelýar.Şeýlelikde, bu ýagdaýda (1) deňeşdirerligiň $k<n$ çözüwi bar.

(1) deňeşdirerligiň bardy-geldi n çözüwi $x_1,x_2,\ldots,x_n$ bolaýsa onda tozdeýstwolaýyn deňeşdirerlik alarys:

$$f(x)=a_0(x-x_1)(x-x_2)\ldots(x-x_n)=0 \pmod p \quad (8)$$

Bu gatnaşyk hem (1) deňeşdirerligiň çözüwi n-den artyk däldigini görkezýär

Teorema doly subut edildi.

/moduly düzümli san bolanda, (8) ýa-ly tozdestwolaýyn deňeşdirerligiň alynmagy hökmäny däl, mysal üçin

$$x^2+3x+2=0 \pmod 6$$

deňeşdirerligiň 4-t çözüwi bar:

$$x=1;\ 2;\ 4;\ 5 \pmod 6$$

Elbetde, köpçleni algebraýik köpeldijilere dargatmak bilen modul boýunça köpeldijilere dargatmak şol bir zat däl, birinjiden elmydama 2-ji /hatda düzümli modul boýunçada / gelip çykýan, tersine tassyklamak, umuman nädogry /7/, /8/ gatnaşyklarda käbir x_i –leriň gabat gelmekleri hem mümkindir.

Teorema 3.

Ýokary çleniniň koeffisiýenti 1 bolan ($a_0=1$), $n<p$ derejeli deňeşdirerligiň

$$f(x)=0(\mathrm{mod}\ p)$$

n sany çözüwi x^p-x ikiçleniň f(x) köpçlene bölünende alynýan galyndyň hemme koeffiziýentleri P sana kratny ýagdaýynda we diňe şeýle ýagdaýda bolýar.

Subuty.

Paýy g(x) we galyndysy r(x) bolan algebradan belli tozdestwany ýazaliň.

$x^p - x = f(x)\, g(x) + r(x)$

ýa-da $r(x) = x^p - x - f(x)\, g(x)$

Bitin koeffiziýentli g(x) derejesi p-n , r(x) galyndynyň derejesi (n-1)-dan uly bolmaýar. /dereje diýlende dereje görkezjisini gözöňünde tutýarys/

Goý f(x)=0 (mod p) deňeşdirerligiň n çözüwi bar bolsa , onda $x^p - x = 0 \pmod p$ tozdestwolaýyn ýerine ýetýändigi zerarly /Fermanyň Kiçi teoremasynyň netijesi/ r(x)=0 (mod p) deňeşdirerlik hem n çözüwe eýe bolýar, derejesi bolsa <n-1, diýmek, onuň hemme koefisiýenti p sana kratny bolmaly, ýogsam öňki teorema garşy gelinerdi. Şeýlelikde, teoremanyň

Zerurlyk şertini görkezdik "…we diňe şeýle ýagdaýda bolýar"/. Ýeterlik şertde (r(x) galyndyň hemme koefisiýentleri p sana kratny ýagdaýynda")

$f(x)\, g(x) = 0 \pmod p$

deňeşdirerlik tazdeýstwolaýyn ýerine ýetýär, ýagny p çözüwi bar, ýöne onuň her bir çözüwi

$f(x) = 0 \pmod p, \qquad g(x) = 0 \pmod p$

deňeşdirerlikleriň bolmanda birini kanagatlandyrýar, diýmek soňkylaryň çözüwleriniň sany $n_1 + n_2 > p$, $n_2 < p - n$ göz öňünde tutsak $n_1 > n$, ýöne f(x)=0 (mod p) deňeşdirerligiň çözüwiniň sany n-den artyk bolup bilmeli däl /öňki teorema esasynda/, şonuň üçin $n_1 = n$

Teorema doly subut edildi.

2 we 3 teoremanyň netijesi hökmünde täze teoremany formulirläp bileris:

Teorema.

$f(x) = 0 \pmod p \qquad (1)$

deňeşdirerligiň çözüwiniň sany n-den artyk bolsa, onda f(x) köpçleniň hemme koýefisiýentleri p sana kratnydyr.

(p modulyň ýönekeý sandygyny ýatýan çykarmaly däl.)

1.3. Wilson teoremasy.

Eger p ýönekeý san bolsa, onda

$$(p-1)! + 1 = 0 \pmod p \qquad (10)$$

Subuty.

$X^{p-1} = 1 \pmod p$ /Ferma teoremasyna seret/

Deňeşdirerlik p-1 çözüwe eýe /bu çözüwleriň iň kiçi aýrylmalary 1,2,…,p-1.

Onda (8) gatnaşyk esasynda

$X^{p-1} - 1 = (x-1)(x-2)\dots(x-(p-1)) \pmod p$

X=0 bolanda /azat çlen/

$-1 = (-1)^{p-1} 1\ 2\ \dots\ (p-1) \pmod p$

p-täk ýönekeý san bolanda (p-1 –jübüt)

$(p-1)! + = 0 \pmod p$

bolar. P=2 bolanda (10) gatnaşygyň dogrulygy gös-göni görünýär .

Şeýlelikde, Wilson teoremasy subut edildi.
Eger (p-1)!+1 san galyndysyz p sana bölünýän bolsa /ýagny (10) gatnaşyk ýerine ýetýän bolsa/, onda P ýönekeý sandyr.

Gönükme

43. Deňeşdirerlikleri mümkingadar ýönekeýleşdirmeli /derejesini peseltmeli, koeffiziýentleri absolýut ululygy boýunça kiçeltmeli,ýokary çleniniň koeffiziýetini bir etmeli/:

1) $34x^{10}-29x^{7}+6x^{6}+43x^{4}-19x+37=0$ (mod 5)
$75x^{17}-62x^{12}-53x^{11}-20x^{8}-24x^{6}+13x-27=0$ (mod 7)

44 Berlen modul boýunça köpçleni köpeldijilere dargatmaly:
x^3+11x^2+8x+3; m=23 modul boýunça

45. 1) $x^3+x-3=0$ (mod5) deňeşdirerligiň 3 çözüwi barmy?
($x^5-x=(x^3+x-3)\times q(x)+r(x)$, r(x)-hemme koefisiýenti 5-e bölünýärmi?
2) $x^5-3x^4+2x^3+x^2-3x+2=0$ (mod7) deňeşdirerligiň näçe çözüwi bar?

46. $f(x)=x^4-15x^3+4x^2+4x-15=0$ (mod29)
f(-1)=0 (mod29), f(2)=0 (mod29) belli f(x) köpçleni çyzykly (29 modul boýunça)
köpeldijilere dargadyp, çözüwlerini tapmaly.

17. Düzümli modul boýunça ýokary derejeli deňeşdirerlikler.

2.1. Düzümli modul boýunça deňeşdirerlikleri çözmeklik, ýönekeý modul boýunça
deňeşdirerlikleri çözmeklige getirilýändigini görkezeliň.

Teorema;
Goý f(x)=0 (modM) (1)
deňeşdirerligiň düzümli M moduly goşa-goşadan ýönekeý köpeldijileriň köpeltmek
hasylyna deň bolsun:
$M=m_1\times m_2\times\ldots\times m_k$, $(m_i,m_j)=1$, $i\neq j$ onda (1) deňeşdirerlik

$$\begin{cases} f(x)=0(\bmod m1) \\ f(x)=0(\bmod m2) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f(x)=0(\bmod mk) \end{cases} \quad (2)$$

deňeşdirerlikleriň sistemasy bilen deňgüýçlidir.

2) M modul boýunça (1) deňeşdirerligiň N sany çözüwi bolup, (2) sistemadaky her bir
deňeşdirerligiň degişli modullary boýunçä $n_1, n_2, \ldots, n_k$ çözüwleri bolsa, onda

$$N=n_1\times n_2\times\ldots\times n_k$$

Subuty.
Eger käbir M modul boýunça deňeşdirerlik bar bolsa, onda ol modulyň islendik bölüjisi boýunça hem dogrudyr.

Bu ýerden (1) deňeşdirerligi kanagatlandyrýan her bir x (2) sistemany hem kanagatlandyrmalydyr.
Ikinji tarapdan deňeşdirerlik birnäçe modul boýunça ýerine ýetýän bolsa, onda ol deňeşdirerlik modullaryň iň kiçi umumy kratnysy (K.U.K) boýunça hem ýerine ýet-
melidir. Diýmek, (2) sistemany kanagatlandyrýan her bir x (1) deňeşdirerligi hem kanagatlandyrmaly.
Seýlelikde, (1)$\Leftrightarrow$(2).
Teoremanyň ikinji bölegini subut etmek hem kyn däl.
Eger $x=b_1$ (mod m_1), $x=b_2$ (mod m_2),…,$x=b_k$ (mod m_k) (3)
(2) sistemanyň bir çözüwi bolsa /elbetde, sistemadaky deňeşdirerlikleriň biri çözgütsiz
bolsa, bütin sistema hem çözgütsizdir, diymek, (1) deňşdirerlik hem çözgütsizdir/, onda $x \equiv x_0 \equiv M_1M`_1b_1+M_2M_2`b_2+\ldots+M_kM`_kb_k$ (mod M) hem (2) sistemanyň, hem (1) deňeşdirerligiň bir çözüwidir. Yone (2) sistemadaky birinji deňeşdirerligiň n_1 çözüwi
ikinji n_2 çözüwi we ş. m. K-njysy n_k çözüwi bar (şerte görä), diýmek, (3) görnüşdäki
sistemalaryň sany $n_1 \times n_2 \times \ldots \times n_k$ bolar, şonça-da x_0-yň bahalary bolar.
Seýlelikde, teorema doly subut edildi.
Mysal
Deňeşdirerligi çözmeli:
$f(x) \equiv x^4+2x^3+8x+9 \equiv 0$ (mod 35)
ýa-da $\begin{cases} f(x)=0(\text{mod}\,5) \\ f(x)=0(\text{mod}\,7) \end{cases}$ (4)
Saýlama metodyny ulanyp 1-nji deňeşdirerligiň iki çözüwi: $x \equiv 1; 4$(mod5) ikinjisininňki üç çözüwi: $x \equiv 3;5;;6$(mod7) barlygyny tapyp bileris. Diýmek, (4) sistemanyň $2 \times 3=6$ çözüwi bar. Olary tapalyň:

$$\begin{cases} x=b1(\text{mod}\,5) \\ x=b2(\text{mod}\,7) \end{cases}$$

Bu ýerde $b_1=1;4$, $b_2=3;5;6$, onda $M=35=7\times5=5\times7$ $M_1=7$; $M_2=5$
$7 \times M`_1 \equiv 1$ (mod5) $5M`_2 \equiv 1$ (mod7)
$M`_1=3$ $M`_2=3$
Diýmek, $x \equiv x_0 \equiv 7\times3\times b_1+5\times3\times b_2$ (mod35)
1) $b_1=1$, $b_2=3$; 2)$b_1=1$, $b_2=5$; 3)$b_1=1$, $b_2=6$; 4)$b_1=4$, $b_2=3$; 5)$b_1=4$, $b_2=5$; 6)$b_1=4$,$b_2=6$
$x \equiv 21\times1+15\times3$; $21\times1+15\times5$; $21\times1+15\times6$; $21\times4+15\times3$; $21\times4+15\times5$; $21\times4+15\times6$
ýa-da $x \equiv 66$; 96; 111;129; 159; 174; (mod35)
ýa-da $x \equiv 31$; 26; 6; 24; 19; 34 (mod35)

2.2 Arifmetikanyň esasy teoremasy esasynda

$M=p_1^{\alpha 1}\times p_2^{\alpha 2}\times\ldots\times p_k^{\alpha k}$ we $f(x)\equiv 0 \pmod{p_1^{\alpha 1}\times p_2^{\alpha 2}\times\ldots\times p_k^{\alpha k}}$

deňeşdirerligi barlamak we çözüwini tapmaklyk 2.1. punkt boýunça

$$f(x)\equiv 0 \pmod{p^{\alpha}} \qquad (5)$$

deňeşdirerligi barlamaga we çözüwini tapmaga getirilýär, soňky bolsa, umuman,

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

deňeşdirerlige getirilýär.

Hakykatdan-da, hem bir (5) deňeşdirerligi kanagatlandyrýan x_1 (6) deňeşdirerligi
hem kanagatlandyrmaly.

$f(x_1)/p^{\alpha}$ bolsa, elbetde $f(x_1)/p$. Goý, deňeşdirerligiň bir çözüwi $x\equiv x_1 \pmod{p}$ bolsun,

onda $x=x_1+pt_1$, t_1-bitin. (7)

Bularyň hemmesi (6) deňeşdirerligi kanagatlandyrýan, bularyň içinden

$$f(x)\equiv 0 \pmod{p^2}$$

deňeşdirerligi kanagatlandyrýanlaryny saýlamaly. Soňky deňeşdirerligiň çep bölegini Teýlor hataryna dargadalyň:

$$f(x)=f(x_1+pt_1)=f(x_1)+\frac{pt1}{1!}f`(x1)+\frac{(pt1)}{2!}f``(x1)+\ldots+\frac{(pt1)}{n!}f^{(n)}(x_n)$$

ýa-da $f(x_1)+pt_1f``(x)\equiv 0 \pmod{p^2}$ çünki, galan çlenlerinde $f^{(n)}(x_1)/k!$ bitin we her goşulyjynyň p^k, $k\geq 2$ köpeldijisi bar. Elbetde $f(x_1)/p$,

Sonuň üçin $\frac{f(x1)}{p}+f`(x1)t\equiv 0 \pmod{p}$

ýa-da $f`(x_1)t_1\equiv -\frac{f(x1)}{p} \pmod{p}$ (8)

Iki ýagdaýyň bolmagy mümkin:

1) $f^1(x_1)/p$, ýagny $f^1(x_1)\neq 0 \pmod{p}$
2) $f^1(x_1)/p$, ýagny $f^1(x_1)\equiv 0 \pmod{p}$

1) ýagdaýda (7) deňeşdirerligiň çözüwi bar.(5 bap, 2., 2.1.)

$$t_1\equiv t`_1 \pmod{p},\ t_1\equiv t`_1+pt_2,\ t_2=0,\pm 1,\ldots$$

Onda (7):

$$x=x_1+pt_1=x_1+p(t`_1+pt_2)=x_1+pt`_1+p^2t_2=x_2+p^2t_2$$

$$x\equiv x_2 \pmod{p^2}$$

Indi $f(x)\equiv 0 \pmod{p^3}$ deňeşdirerligiň çözüwüni gözlämuzde

$$f(x_2+p^2t_2)\equiv 0 \pmod{p^3}$$

ýa-da

$$f(x_2)+p^2t_2f`(x_2)\equiv 0 \pmod{p^3};\ f`(x_2)/p$$

$$f`(x_2)t_2\equiv -f(x_2)/p^2 \pmod{p}\ \ f(x_2)/p^2$$

ýazyp, $x=x_2+p^2(t`_2+pt_3)=x_2+p^2t`_2+p^3t_3$

ýa-da $x=x_3+p^3t_3$; $x\equiv x_3 \pmod{p^{\alpha}}$ alardyk. we ş. m.

$x \equiv x_\alpha \pmod{p^\alpha}$ çözüwe gelerdik.
2) Ýagdaýda, ýagny $f`(x_1)/p$ we (8)-iň sag bölegi p sana bölünmese, (8) çözgütsiz
(5 bap, 2., 2.2.) eger-de (8) gatnaşygyň sag bölegi p sana bölünse, onda (8) tojdeýstwolaýyn bolýar we

$$f(x) \equiv 0 \pmod{p^2}$$

çözüwe eýedir.
Mysal:
$f(x) \equiv 0 \pmod{3^3}$; $f(x)=2x^4+5x-1$; $f(x) \equiv 0 \pmod 3$ deňeşdirerligiň bar çözüwi bar
$x \equiv 1 \pmod 3$ /saýlama metodyny ulanyp tapsa bolýar/ $x=1+3t_1$

$$f(1)+3t_1 \times f`(1) \equiv 0 \pmod{3^2})$$

ýa-da $6+3t_1 \times 13 \equiv 0 \pmod{3^2}$; $f(1)=6$, $f`(1)=13$.

$$2+13t_1 \equiv 0 \pmod 3$$
$$13t_1 \equiv -2 \pmod 3$$
$$t_1 \equiv 1 \pmod 3$$

$t_1=1+3t_2$; $x=1+3t_1=1+3(1+3t_2)=4+9t_2$; $x=4+9t_2$; $x_2=4$

$$f(4)+9t_2 f`(4) \equiv 0 \pmod{3^3}$$
$$531+9t_2 \times 517 \equiv 0 \pmod{27}$$
$$59+517t_2 \equiv 0 \pmod 3$$
$$t_2 \equiv 1 \pmod 3),\ t_2=1+3t_3$$
$$x=4+9(1+3t_3)=13+27t_3$$
$$x \equiv 13 \pmod{27}.$$

Gönükmeler.
47. Deňeşdirerlikleri çözmeli:
1) $5x^4+2x^3-x+17 \equiv 0 \pmod{21}$
2) $2x^2-7x+6 \equiv 0 \pmod{55}$
48. Deňeşdirerlikleri çözmeli:
1) $x^3+2x+2 \equiv 0 \pmod{125}$
2) $x^4+4x^3+2x^2+2x+12 \equiv 0 \pmod{625}$

18. Ikinji derejeli deňeşdirerlikler

§1. Umumy düşünjeler we teoremalar.

1.1.Ikinji derejeli deňeşdirerlikleri umumy görnüşde

$$Ax^2+Bx+C \equiv 0 \pmod M \qquad (1)$$

ýaly ýazyp bolýar we ol

$$Ax^2+Bx+C=My$$

kesgitsiz deňleme bilen deňgüýçli.
(1) deňeşdirerligi mydama has ýönekeý görnüşe getirip bolýar:

$$x^2 \equiv a \pmod m \qquad (2)$$

Bu ýerde esasy ideýa-bitin koeffisiýentli doly kwadrata getirmek /elkbetde, modul hem käbir sana köpelip biler./

Aýdylanlary mysallarda görkezeliň:

1) $x^2-5x+16\equiv 0 \pmod{24}$,

ýa-da $4x^2-20x+64\equiv 0 \pmod{96}$,

$(4x^2-2\times 2\times 5\times x+25)+39\equiv 0 \pmod{96}$,

$(2x-5)^2+39\equiv 0 \pmod{96}$,

$y^2\equiv -39\equiv 57 \pmod{96}$,

$y^2\equiv 57 \pmod{96}$; $y=2x-5$.

Seýlelikde, indi biz

$$x^2\equiv a \pmod{m},\ (a,m)=1 \qquad (2)$$

görnüşdäki deňeşdirerliklere gararys we ol çözgütli bolsa, onda a ululyk m modul boýunça kwadratik aýrylma diýlip atlandyrylýar, eger (2) çözgütsiz bolsa, onda a
akwadratik aýrylma däl diylip atlandyrylýar.

Umuman $x^n\equiv a \pmod{m}$, $(a,m)=1$ bolanda, n derejeli aýrylma ýa n derejeli aýrylma däl hakynda gürrüň giderdi.

Seýlelikde, biz

$$x^2\equiv a \pmod{p}$$
$$x^2\equiv a \pmod{p^\alpha}$$
$$x^2\equiv a \pmod{2^\alpha}$$

deňeşdirerliklere gararys, bu ýerde p täk ýönekeý san. Yazylan deňeşdirerlikleriň birinjisi has wajyp, ony çözmäni öwrensek, galanlary ýa oňa getirilýär, ýa-da çözülişi
meňzeş bolýar.

1.2. Indi $x^2\equiv a \pmod{p}$ (3)

p ýönekeý we 2-den uly.

Eger a/p onda, elbetde, $x\equiv 0 \pmod{p}$ we bu ýönekeýje ýagdaýa geljekde garap durmarys: $(a,p)=1$.

Onda (3) çözüwini p modul boýunça getirilen sistemadaky aýrylmalaryň klaslarynyň
içinden gözlemeli bolýarys. Eger (3) deňeşdirerligiň bir çözüwi hökmünde $x\equiv x_1 \pmod{p}$ alsak, onda ikinji çözüwi $x\equiv -x_1 \pmod{p}$ bolar, çünki $(-x_1)^2=x_1^2$. Bu ikinji çözüw birinji çözüwden tapawutlydyr /ýagny başga klasa girýär/.

Tapawutlanmaýandyr diýip pikir etsek, onda $x_1\equiv -x_1 \pmod{p}$ ýa-da $2x_1\equiv 0 \pmod{p}$
bu ýerden $2x_1/p$. ýöne $(2,p)=1$ we $(x,p)=1$, ýagny 2 hem x_1 hem p sana bölünmeýär,
onda $2x_1$ hem p sana bölünmeli däl, ýagny bolmalysy $2x_1/p$, biz bolsa $x_1\equiv -x_1 \pmod{p}$
ýerine ýetýändir diýip $2x_1/p$ aldyk, bu mümkin däl, diýmek $x_1\equiv -x_1 \pmod{p}$
hem mümkin däl. Başga söz bilen aýdylanda, x_1 we $-x_1$ dürli klasyň aýrylmalary bol-

ýar.
Seýlelikde, eger (3) deňeşdirerlik çözgütli bolsa, onda balmanda onuň iki çözüwi bar, Yöne onuň ikiden artyk çözüwi hem bolup bilmez /derejesi 2, modula ýönekeý p/
(6 bap, 1., 1.2., teorema 2.)
Diýmek, (3) deňeşdirerlik ýa çözgütsiz, ýa-da çögütli we bu ýagdaýda onuň dos-dog
ry iki çözüwi bar, özem, eger bir çözüwi belli bolsa $x \equiv x_1 (\mathrm{mod}\ p)$, ikinjisini awtomati-
ki ýazyş bolýar: $x \equiv -x_1 (\mathrm{mod}\ p)$.
1.2.p modul boýunça aýrylmalaryň getirilen sistemasy /absolýüt ululygy boýunça iň
kiçi/

$$-\frac{p-1}{2},\ldots,-2,-1,1,2,\ldots,-\frac{p-1}{2} \qquad (4)$$

we (3) deňeşdirerligiň çözüwini tapmak üçin, ondaky x-iň deregine $1,2,\ldots,\frac{p-1}{2}$ san-
lary goýup barlamak ýeterlikdir. Sunlukda, onuň çep böleginde

$$1^2,2^2,\ldots,(\frac{p-1}{2})^2 \qquad (5)$$

sanlar alynýar. Bularyň biri /bolsa diňe biri, öňky punkta görä birden artyk bolmagy mümkin däl/, mysal üçin, k^2, p modul boýunça a bilen deňeşdirerli bolaýsa, (3) deňeşdirerligiň çözüwleri

$$x \equiv \pm k (\mathrm{mod}\ p)$$

bolar. Sol wagytda biz ýene has wajyp tassyklamany, yagny a sanyň p modul boýunça
(5) hatardaky sanlar bilen deňeşdirerli bolanyndaky ýagdaýynda we onuň (a ululygyň)
diňe şeýle ýagdaýynda (3) deňşdirerligiň çözgütli bolýanlygyny görýäris.
(Başga söz bilen: (5) hatardaky sanlar p modul boýunça kwadratik aýrylmalardyr)
Bularyň hemmesi dürli klaslara girýän kwadratik aýrylmalardyr. Tersinden pikir et-
sek, ýagny $1 \le k < l \le \frac{p-1}{2}$ üçin $k^2 \equiv l^2 (\mathrm{mod}\ p)$ diýsek, onda (3) deňeşdirerligiň 4 çözü-
wi bolup bilerdi.

$$x \equiv \pm k (\mathrm{mod}\ p), \quad x \equiv \pm l (\mathrm{mod}\ p)$$

bu bolsa mümkin däl. Diýmek, –

$$k^2 \equiv l^2 (\mathrm{mod}\ p)$$

diýmämiz ýalňyş, ýagny (5) hatardaky sanlar p modul boýunça dürli klaslara giryärler Seýlelikde, p modul boýunça dürli klaslara giryän kwadratik aýrylmalaryň sany $\frac{p-1}{2}$

bolýar; onda hut şonça($\frac{p-\alpha}{2}$ -sany) muktarda-da p modul boýunça kwadratik aý-
rylma däl bar (çünki p modul boýunça getirilen aýrylmalaryň sany p-1).

Mysal.

1. Moduly 13 bolan iň kiçi polojitel kwadratik aýrylmalar:

$$x^2 \equiv 1;\ 3;\ 4;\ 9;\ 10;\ 12;\ (\text{mod } 13).$$

onda kwadratik aýrylmalar däl sanlar:

$$2;\ 5;\ 6;\ 7;\ 8;\ 11.$$

($x^2\equiv1$; $x^2\equiv3$; $x^2\equiv4$; $x^2\equiv9$; $x^2\equiv10$; $x^2\equiv12$ (mod 13) we mysal üçin, $x^2\equiv10\equiv36$ (mod 13)
üçin çözüwi $x\equiv\pm6$ (mod 13): $x_1\equiv6$; $x_2\equiv-6\equiv7$ (mod 13). Emma $x^2\equiv2$ (mod 13) çözgüt-
sizdir we şonuň üçin 2 kwadratik aýrylma däl./

1.4.Eýler kriterisi

$$x^2\equiv a \ (\text{mod } p) \qquad (3)$$

çözgütlimi ýa-da çözgütsizmi /ýagny a kwadratik aýrylmamy ýa-da dälmi/-muny çalt
bilmek gerek bolýar.

a ululygyň((a,p)=1, (2,p)=1) öňki punktdaky (5)hataryň sanlary bilen p modul boýunça deňeşdirerlisi barmy ýa ýokmy-muny bilmek goýlan soraga jogap berýän hem bolsa, bu usul netijeli hasap edilmeýär.

Eýleriň tapan kriterisi örän wajyp:

1) a sanyň p modul boýunça kwadratik aýrylma bolmagy üçin aşakdaky şertiň ýeri-
ne ýetmegi zerur we ýeterlik.

$$a^{\frac{p-1}{2}}\equiv1 \ (\text{mod } p) \qquad (6)$$

2) a sanyň kwadratik aýrylma däl bahalary üçin we diňe şolar üçin

$$a^{\frac{p-1}{2}}\equiv-1 \ (\text{mod } p) \qquad (7)$$

gatnaşygy ýerine ýetýär. /Yagny (7) zerur we ýeterlik şertdir/

Subuty:

Ferma teoremasy esasynda

$$a^{p-1}\equiv1 \ (\text{mod } p),\ (a,p)=1$$

ýa-da

$$a^{p-1}-1\equiv0 \ (\text{mod } p)\equiv(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1)\equiv0 \ (\text{mod } p)$$

Bu ýerden $a^{p-1}-1/p$ onda, diýmek, bolmanda skopkalaryň biri p sana bölünmeli, ýöne skopkalaryň tapawudy 2-ä deň 2 bolsa p sana bölünmeýär: (2,p)=1. Bu diýilligi-skop-
kalaryň diňe biri p sana bölünýär /skopkalaryň ikisi hem p sana bölünende, olaryň tapawudy hem p sana bölünmeli bolardy/.

Goý a kwadratik aýrylma bolsun, onda ol (5) hatardaky sanlar bilen ýa olar bilen p modul boýunça deňeşdirerli sanlar bilen deňeşdirerli bolmaly, ýagny

$$a\equiv x^2 \pmod p),\ (x,p)=1 \qquad (8)$$

Bu ýerde

$a^{\frac{p-1}{2}}\equiv(x^2)^{\frac{p-1}{2}}\equiv x^{p-1}\equiv1 \pmod p$ (9) bolar ($x^{p-1}\equiv1 \pmod p$ Ferma teoremasy
esasynda) (9)-dan $a^{\frac{p-1}{2}}\equiv1 \pmod p$ (6) gatnaşygy aldyk, ýagny zerurlyk şert
(a kwadratik aýrylma bolanda (6) gatnaşyk ýerine ýetýär/ subut edildi.

Indi ýeterlik şerti subut edeliň.

((6) gatnaşyk ýerine ýetende, a kwadratik aýrylma bolýandygyny görkezeliň)

Ferma teoremasyndan:

($(x^2)^{\frac{p-1}{2}}\equiv$) $x^{p-1}\equiv1 \pmod p$, (x,p)=1 we (6) gatnaşykdan (9) gatnaşygy gelýär.
(9)-da $a^{\frac{p-1}{2}}\equiv(x^2)^{\frac{p-1}{2}} \pmod p$, (x,p)=1 hem bolansoň a-nyň kwadratik
aýrylmadygy görünýär, ýöne (9)-dan olaryň çözüwi $\geq\frac{p-1}{2}$ ýaly, emma (6) ýönekeý modully bola-
ny üçin $\frac{p-1}{2}$ derejesinden artyk çözüwe eýe bolup bilmez. Seýlelikde, (6) ýerine ýetende a kwadratik aýrylmadyr we onuň dos-dogry $\frac{p-1}{2}$ dürli bahasy /çözüwi/ bolar. /Mysal üçin 13 modul boýunça 1, 14, 27,… we ş. m. sanlara a-nyň bir bahasy
diýip düşünilýar, çünki $1\equiv14\equiv27\equiv\ldots \pmod{13}$. Onda a-nyň galan bahalary üçin /olar hem $\frac{p-1}{2}$ sany, çünki (a,p)=1, ýagny, kwadratik aýrylmalar däl bahalar üçin we diňe
şolar üçin

$$a^{\frac{p-1}{2}}+1/p \text{ ýa-da } a^{\frac{p-1}{2}}\equiv-1 \pmod p \qquad (7)$$

Eýler kriterisi doly subut edildi.

Mysallar.

1) $x^2\equiv5 \pmod{13}$, $5^{\frac{13-1}{2}}\equiv5^6 \pmod{13}$

$5^2\equiv25\equiv-1 \pmod{13}$, $5^6\equiv(5^2)^3\equiv(-1)^3\equiv-1 \pmod{13}$

Diýmek, 5 san 13 modul boýunça kwadratik aýrylma däl we $x^2\equiv5 \pmod{13}$ çözdütsiz-
dir.

2) $x^2 \equiv 5 \pmod{23}$; $5^{\frac{23-1}{2}} \equiv 5^{``}$ (mod 23)

$5^2 \equiv 25 \equiv 2$; $5^{``} \equiv (5^2)^5 \times 5 \equiv 2^5 \times 5 \equiv 160 \equiv 22 \equiv -1$

Bu ýagdaýda hem $x^2 \equiv 5 \pmod{23}$ çözgütsiz.

3) $x^2 = 12 \pmod{13}$

$$12^{\frac{13-1}{2}} \equiv 12^6 \equiv (-1)^6 \equiv 1(ьщв 13)$$

Diýmek $x^2 \equiv 12 (\mathrm{mod}\, 13)$ çözgütli we onuň iki çözüwi bolmaly

$x \equiv \pm 5 (\mathrm{mod}\, 13)$

Gönükme.

49. Eýlerkriterisini ulanyp, deňeşdirerlikleriň çözgütlidigini kesgitlemeli:

2) $x^2 = 11 \pmod{29}$ 2) $x^2 = 8 \pmod{37}$

3) $x^2 = 5 \pmod{41}$ 4) $x^2 = 6 \pmod{59}$

19. Lezandr simwoly.

2.1. Lezandr simwolyny girizeliň (a/p) /okalyşy: p boýunça a-yň simwoly, a simwolyň sanowjysy, p maýdalowjysy diýilýär/. galan üçin simwol kesgitlenýär. Eger p modul boýunça a kwadratik aýrylma bolsa (a/p)=-1

Indi Eýler kriterisini göz öňünde tutsak:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\ p) \quad (10)$$

2.2. Lezandr simwolyny käbir häsiýetlerini görkezeliň:

$a \equiv a_1 (\mathrm{mod}\ p)$

1. $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$ bolsa, onda (11)

Bu dogrydyr, çüňki a we a_1 şol bir wagtda ýa kwadratik aýrylmadyr, ýa-da kwadratik aýrylma däl ululykdyr.

2. $\left(\frac{1}{p}\right) = 1$, çüňki $1 = 1^2$ kwadratik aýrylmadyr.

3. $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$ Bu 2.1. (10) gatnaşykdan gelýär.

/Bu ýerden , ýönekeý p san 4m+1 görnüşde bolsa, -1 kadratik aýrylma bolýar; p=4m+3 görnüşde bolsa, -1 kwadratik aýrylma däl bolýar).

4. $\left(\frac{a \cdot b \ldots l}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ldots \left(\frac{l}{p}\right)$

hakykatdan hem

$$\left(\frac{a \cdot b \ldots l}{p}\right) \equiv (a \cdot b \ldots l)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \ldots l^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \ldots \left(\frac{l}{p}\right) (\mathrm{mod}\ p)$$

Bu ýerden hususan,

$$\left(\frac{a^2}{p}\right)=1;\left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right)$$

5. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$

Bu wajyp häsiýetini subutyny soň getireris.
Eger p=8m+1 görnüşde bolsa (8m+1 ýa-da 8m+7)
Onda jübü san diýmek, 2-kwadratik aýrylma. Eger p=8m+3 görnüşde bolsa (8m+3, 8m+5), onda
täk diýmek, 2-kwadratik aýrylma däl.
Mysal
1) x^2=2(mod 1097), p=1097=8m+1 görnüşde bolany üçin deňeşdirerlik çözgütli: 2-kw.aýrylma.
2) x^2=2(mod 1709); 1709=8m+5 görnüşde diýmek, deňeşdirerlik çözgütsiz: 2-kwadratik aýrylma däl.

5. Kwadratik aýrylmalaryň tüýsibirlik kanuny

P we g täk ýönekeý sanlar bolanda

Bu ýerden p-1/2 ýa-da g-1/2 sanlaryň iň bolmanda biri jübüt bolsa, ýagny p ýa-da g sanlaryň iň bolmanda biri 4m+1 görnüşde bolsa, onda görkeziji jübüt bolýar we (12)-den

Eger p-1/2 we g-1/2 sanlaryň ikisi hem täk bolsa, ýagny hem p, hem g 4m+3 görnüşde bolsa, onda p-1/2 g-1/2 görkeziji täk bolýar we şunuň üçin

5 we 6 häsiýetleri ulanmaga degişli mysallara garaliň.
Mysal 1.

x^2 =102 (mod 1097)

(102/1097) üçin Lejandr simwolyny hasaplap deňeşdirerligiň çözgütliligini kesgitläliň. 1097 – ýönekeý san, 102=2 3 17 onda

$$\left(\frac{102}{1097}\right)=\left(\frac{2}{1097}\right)\cdot\left(\frac{3}{1097}\right)\left(\frac{17}{1097}\right)$$

1) $\left(\frac{2}{1097}\right)=1,1097\equiv 1(mod\,8)$

2) $\left(\frac{3}{1097}\right)=\left(\frac{1097}{3}\right)=\left(\frac{2}{3}\right)=-1$

çüňki 1097=1(mod 4), soňra 5 häsiýet: 3=3(mod 8)

3) $\left(\frac{17}{1097}\right)=\left(\frac{1097}{17}\right)=\left(\frac{9}{17}\right)=\left(\frac{3^2}{17}\right)=1$

Diýmek, $\left(\frac{102}{1097}\right)=(+1)(-1)(+1)=-1.$

Berlen deňeşdirerlik çözgütsiz

2.3. Indi 5 we 6 häsiýetleri subut edeliň .

Aşakaky deňeşdirerliklere garalyň

(13)

Bu ýerde $P_1=\frac{p-1}{2}, \varepsilon_x r_x$ ax ululygyň absolýut ululygy boýunça iň kiçi aýrylmasy, $\varepsilon_x=\pm 1,$ diýmek, $r_1, r_2, \ldots, r_{p1}$, ululyklaryň her biri $1,2,\ldots,p_1$ sanlaryň diňe birine deň , onda

$1\ 2\ldots p_1=r_1\ r_2\ldots r_{p1}$

Indi (13) deňeşdirerlikleri biri-birine köpeldip we iň soňky ýazylany göz öňünde tutup alarys:

Ýa-da (14)

Indi

1) Eger bolsa

we aňlatma jübüt:

2) Eger-de bolanda bütin aňlatma täk bolýar.

1) ýagdaýda ax-iň kiçi otrisatel däl aýrylmasy ½ P-den kiçi – bu bolsa $\varepsilon_x=\pm 1$ diýildigi , 2) ýagdaýda ax-iň iň kiçi otrisatel däl aýrylmasy diýmek , absolýut ululygy boýunça iň kiçi aýrylmasy otrisatel, ýagny

E_x=-1

Aýdylanlardan

E_x=(-1)

We (14)-i göz öňünde tutsak: P_1

a-ny täk san hasap edip, soňky gatnaşykda käbir özgertmeleri amala aşyraliň

Bu ýerden

(15)

(16)-den a=1 bolsa

Indi 6 häsiýeti subut etmäge girişeliň

(15) we 6 häsiýetden

(16)

Goý indi $g-1/2=g_1$ g_x we py aňlatmalarda x we y sanlar biri-birine bagly bolman aşakdaky bahalary kabul etsin

$x=1,2,\ldots,p_1$; $y=1,2,\ldots,g_1$

Onda mümkin bolan goşa sanlar:

Ÿagny P_1g_1 sany goşa sanlar bolýar.

Bu goşa sanlaryň iki kompanenti özara deň bolmagy mümkin däl, ýagny x-iň we y-iň islendik bahasynda gx=py, çüňki (p,g)=(y,g)=1 bolany üçin py g . Onda gx<py deňsizligi ýerine ýetirýän /birinji komponenti kiçi bolan/ goşalaryň sanyny S_1 bilen we gx>py deňsizligi ýerine ýetirýän goşalaryň sanyny hem S_2 bilen belläp, $p_1g_1=S_1+S_2$ boljakdygyny görýäris.

/deňligiň iki bölegini hem (p/g) köpeltsek-(12) gatnaşyk /

2.4. Ležandr simwolyny umumylaşdyrýan Ÿakobi simwoly köp ýagdaüýlarda peýdaly bolýar.

Goý $P=p_1 p_2\ldots p_k$ ýönekeý köpeldijileri dargamasy bolsun , (a,P)=1 diýeliň .

Onda Ÿakobi simwoly aşakdaky ýaly kesgitlenýär:

Sag bölekdäki skopkalar –Ležandr simwollary. Hut Ležandr simwolynyň häsiýetlerini ulanyp, Ÿakobi simwolynyň häsiýetlerini görkezmek mümkin-olar daşky görnüşi boýunça edil Ležandr simwolynyňky ýaly. 3,5,6 häsiýetler subut edilende, jübüt derejesi bölünip çykarylýar.

Moduly düzümli ýagdaý

Goý bize $x^2=a \pmod p$ (1)

Berilsin, a>0, (a,p)=1

$f(x)=x^2-a$, $f(x)=2x$, eger indi $x=x_1 \pmod p$

$x^2=a \pmod p$ (2)

deňeşdirerligiň çözüwi bolsa, onda

$f(x_1)$ p (3)

Hakykatdan-da, (a,p)=1 we $(x_1,p)=1$, p-täk, şonuň üçin $(2x_1,p)=1$, diýmek, $2x_1$ p, ýagny

$f(x_1)$ p

Indi (1) deňeşdirerligi

$f(x)=x^2-a=0 \pmod p$

ýaly gorap, ony 6 bap, N2.2.2. ýaly çözeris. (3) zerarly onuň ýeke-täk çözüwi bar. Şeýlelikde, (2) deňeşdirerligiň her bir çözüwine (onuň bolsa çözüwi bar: $x\equiv\pm x_1(mod\, p)$) (1) deňeşdirerligiň diňe bir çözüwi degişli bolýar.

3.2. Indi $x^2=a \pmod 2$, a>0, (a,2)=1 (4) Bu ýerde $f(x_1)=2x_1$ 2-ä bölünýär we şonuň üçin 6 bap, N2,2.2 ýaly pikirýöretme geçýär. (4) deňeşdirerligi aşakdaky ýaly ýazyp

$(x^2-1)+1=a \pmod 2$ (5)

(a,2)=1 bolany üçin, eger soňky deňeşdirerlik çözgütli bolsa, onda (x,2)=1, diýmek, Ležandr simwolynyň 5 häsiýetine görä $x^2-1/8$

Şeýlelikde, (5) deňeşdirerligiň çözgütli bolmagy üçin, aşakdaky şertleriň ýerine ýetmegi zerur:

Eger $\alpha=2$ bolsa, $a=1 \pmod 4$ Eger-de $\alpha\geq 3$ bolsa, $a=1 \pmod 8$

$\alpha \le 3$ bolanda x^2=a (mod 2) deňeşdirerligi islendik täk san ýerine ýetirýär; we ýeke-täk çözüwi bar

x=1 (mod 2); x^2=a(mod 4) deňeşdirerligi iki çözüwi bar:

x=1; 3 (mod 4)

x^2=a (mod 8) deňeşdirerligiň dört çözüwi bar:

x=1,3,5,7 (mod 8) α =4;5;… bolanda täk sanlary

$x=\pm(1+4t_3)$ (6)

görnüşde ýazyp, olaryň haýsylarynyň x^2=a (mod 16), x^2=a(mod 32) we ş.m. deňeşdirerlikleri kanagatlandyrandygyny barlaýarys. Alynjak netije:

Gönükmeler

50. Çözüwleriniň sanyny tapmaly

1) x^2=5 (mod 73); 2) x^2=3(mod 73)

51. Deňeşdirerlikleriň çözgütliligini kesgitlemeli:

1) x^2=31 (mod 77); 2) x^2=20 (mod 171)

52. Ležandr simwolyny kesgitlemeli:

$$1)\left(\frac{165}{373}\right);2)\left(\frac{1015}{1621}\right);3)\left(\frac{230}{457}\right)$$

20. Görkezijiler, görkezijileriň häsiýetleri, asyl kökler.

1.1. Eger (a,m)=1 bolsa, onda

a^{γ} =1(mod m) (1)

deňeşdirerligi kanagatlandyrýan natural γ sanlar bardyr.

Hakykatdan-da, şeýle sanlaryň bolmanda birini Eýler teoremasy esasynda görkezilýär, ýagny $\varphi(m)$. (1) deňeşdirerligi $k \cdot \varphi(m)$ hem kanagatlandyrar. / K bitin san /-bu deňeşdirerligiň häsiýetinden gelýär.

Geljekde-de δ bilen belgilenýän (1) deňeşdirerligi kanagatlandyrýan γ-yň iň kiçi bahasyna m modul boýunça a degişli görkeziji diýip atlandyrarys. Diýmek,eger

$a^{\delta} \equiv 1(mod\, m)$ (2)

bolsa, $\delta \le \gamma$ çünki $a^{\gamma} \equiv 1(mod\, m) we 1 \le x < \delta$

bolanda, $a_x \equiv 1(mod\, m)$,

onda m modul boýunça δ görkezijä a degişli diýilýär.

Eger m modul boýunça $\varphi(m)$ görkezijä a degişli bolsa , ýagny $\delta = \varphi(m)$ bolsa a sana m modul boýunça asyl kök diýilýär. Bu ýerden, eger a ýonekeý p modul boýunça asyl kök bolaýsa , onda ol / a san / $\varphi(p) = p-1$ görkezijä degişli bolýar. Görkezijini tapmaga degişli mysallara garalyň.

1) 11 modul boýunça 2,3,4,5,6,7,8,9,10. A sanlaryň haýsy görkezijä degişlidigini tapalyň./ Hemme erde moduly 11 , gysgalyk üçin ony ýazyp durmarys /

1)$2^2= 4$; $2^3=8$; $2^4=16=5$; $2^5=32=10=-1$

$2^6=2^5*2=(-1)*2=-2=9$; $2^6=2^{4*}2^2=5*4=20=9$

Şeýle deňeşdirerligiň häsiýetlerini ulanyp , $2^{\delta}=1$ (mod 11) diňe $\delta=10$ bolanda ýerine etjekdigini birinji setirden görýäris :

$2^{10}=2^5*2^5=(-1)*(-1)=1(mod11)$; $\delta=10=\varphi(11)$

Diýmek , 2 biziň alan 11 modulymyz boýunçaasyl kök bolýar .

2) $3^2=9=-2$, $3^3=5$; $3^4=5*3=4$; $3^5=3^4*3=4*3=1$

$$3^5=1(mod11)$$

Bu ýagdaýda $\delta=5$.

3-lik 11 modul boýunça 5 görkezijä degişli

$4^2=5$; $4^3=9$; $4^4=3$; $4^5=4^4*4=3*4=1$; $\delta=5$.

E D E B I Ý A T

1. Türkmenistanyň Prezidenti Gurbanguly Mälikgulyýewiç Berdimuhamedow (gysgaça terjimehal). Aşgabat, Türkmen döwlet neşirýat gullugy, 2007. 128 sah.
2. Gurbanguly Berdimuhamedow. Türkmenistanda saglygy goraýşy ösdürmegiň ylmy esaslary. Aşgabat, Türkmen döwlet neşirýat gullugy, 2007. 96 sah.
3. Gurbanguly Berdimuhamedow. Garaşsyzlyga guwanmak, Watany, Halky söýmek bagtdyr. Aşgabat, Türkmen döwlet neşirýat gullugy, 2007. 44 sah.
4. Gurbanguly Berdimuhamedow. Eserler ýygyndysy. Aşgabat, Türkmen döwlet neşirýat gullugy, 2007. 416 sah.
5. Türkmenistanyň Prezidenti Gurbanguly Mälikgulyýewiç Berdimuhamedowyň Umumy milli “Galkynyş” Hereketiniň we Türkmenistanyň Demokratik partiýasynyň nobatdan daşary V gurultaýlarynyň bilelikdäki mejlisinde sözlän sözi. Aşgabat, Türkmen döwlet neşirýat gullugy, 2007. 48 sah.
6. Gurbanguly Berdimuhamedow. Türkmenistan – Saglygyň we ruhubelentligiň ýurdy. Aşgabat, Türkmen döwlet neşirýat gullugy, 2007. 175 sah.

7. Türkmenistanyň Prezidenti Gurbanguly Mälikgulyýewiç Berdimuhamedowyň daşary syýasaty. Wakalaryň hronikasy. Aşgabat, Türkmen döwlet neşirýat gullugy, 2007. 64 sah.
8. Türkmenistanyň Prezidenti Gurbanguly Mälikgulyýewiç Berdimuhamedowyň Ýurdy täzeden galkyndyrmak baradaky syýasaty. Aşgabat, Türkmen döwlet neşirýat gullugy, 2007. 133 sah.

9. Виноградов И.М. Основы теории чисел, Москва 1976.
10. Бухштаб А.А. Теории чисел, Москва 1964.
11. Оразов Г. Санлар теориясы, Окув голланмасы, 1989

Mazmuny

Baba Kömekow, Orazmämmet Annaorazow,
Hajymuhammet Geldiýew, Azatgeldi Öwezow

Sanlar nazaryýeti

Ýokary okuw mekdepleriň talyplary üçin okuw kitaby