ګڼونپوهنه

(د اعداد تیوري)

Nummbertheory

$$k = n \ (\mathrm{mod}\ m)$$

smakhan1946@gmail.com

Ketabton.com

لیکوىکی: جورج کوننبرویر

ژباړی: ډاکتر ماخان (میرزي) شینواری

(c) ketabton.com: The Digital Library

دلوي څښتن په نامه

په دې هیله، چې په دې لیکنو او ژباړو به مې زموږ د بې وزلي او له پوهې پاتې ملت - په ما د پوهنې لپاره د لګښت - لپاره د پوهنې په لور داسې لږ ونډه اخستې وي.

کتاب پیژندنه

د کتاب نوم: ګیونیپوهنه

لیکونکی: پرفیسور جورج ګوتنبرونر

ژباړی : ډاکتر ماخان،، میرې،، شینواری

د خپریدو لړی ....

خپرندوی: د افغانستان کلتوري ودې ټولنه

جرمني

چاپ کال ۲۰۱۲

د ژباړي بریښنا پته : smakhan1946@gmail.com

چاپ چارې

چاپ ته یې د هر چمتو هیوادوال مرسته په سترګو منل کیږي

.

(c) ketabton.com: The Digital Library

پښتو مو ژبه او شمیرپوهنه پرې ساده ده

د ژباړې مننه

(c) ketabton.com: The Digital Library

نیولیک

د ژباړي سریزه
د لیکونکي سریزه
- د... خویونه ۱
د.. د ا کسیومونو سیستم ۱
د طبیعي اعدادو ځای انځورونه ۸
-۲- په ... وېشوړوالی ۱۴
پروېشوني (مقسوم علیه) 3۱
د اویکلید یا اقلیدس له مخې ټاکل ۱۸
خورا غټ ګډ پروېشونی ۲۸
۳ - لومړني ګڼونه ۳۲
نور خویونه ۳۸
(د خ غ ګ او خ ک ګ زیاتځلي - - ۴۲
۴ ـ کونګروانځ **۵۱**
د کونګروانځ سره شمېرنه ۵۱
د پروېشنوړوالي قوانین ۵۸
پاتې ټولګي **۶۳**

(c) ketabton.com: The Digital Library

د پاتې ټولګې کړی یا ـــ رینګ ۶۷

۵ - الجبري کونګروانڅ ۷۵

د کرښیزو کونګروانڅو حلوړوالی ۷۵

سیمولتان کونګروانت ۸۱

الجبري کونګروانت ۸۷

۶ -د حلونوو عملي شمېرنه ۸۹

د الجبري کونګرواینڅو دحلونو ګڼون یا تعداد ۹۸

- لومړني پاتې ټولکي کروپونه ۱۰۱

د أبل ګروپ ۱۰۱

د $\varphi(m)$ شمېرنې ته ۱۰۳

د اویلر جمله ۱۱۰

د $(\mathbb{Z}_m^*,\cdot)$ جوړښت ۱۱۶

د حقیقیي اعدادو g ـــادیکي ودیزیینه ۱۲۶

ټولزه ودیزیینه ۱۲۶

کله $\alpha \in \mathbb{Q}^+$ دوه g ـــادیکي انځورونه لري؟ ۱۳۳

کوم $\alpha \in \mathbb{Q}^+$ یوه پای g ـــادیکي انځورونه لري؟ ۱۳۵

(c) ketabton.com: The Digital Library

پریودیکي وده ۱۳۸

ځانګړی حالت: سوچه پریودیکي وده ۱۴۵

ټولیز حالت: نه سوچه – پریودیکي وده ۱۴۹

۸ - N-م توان ۱۵۰

په ځانګړي حالت بیرته اړول ۱۵۰

د... د حل لپاره تګلار ۱۵۳

د حل ساده متودونه ۱۵۸

ځانګړی حالت ۱۵۸

د $x^n \equiv a(2^k), k \geq 3$ لپاره د حل متودونه ۱۶۵

څلوریز پاتې(که غواړئ: مربع باقیمانده) ۱۶۹

ځانګړی حالت ۱۶۹

څلوریز پاتې(که غواړئ: مربع باقیمانده ۱۷۴

ځانګړی حالت ۱۷۴

لژندر-سومبول ۱۷۹

ساده خویونه: ۱۸۰

د ګاوس لیما یا جملګۍ ۱۸۶

د Legendre-Symbo لپاره د څلورۍ – یا ... ۱۹۶

جاکوبي سومبول ۲۰۱

ځانګړي حالتونه ۲۰۵

(c) ketabton.com: The Digital Library

د ژباړي سريزه

ګرانو لوستونکو!

د ليکونکي سريزه راوړل شوې هلته اړين څه شته دی، خو زه غواړم دومره يادونه وکړم، چې ګڼونپوهنه يا د اعادو تيوري يو له بنسټيزو درسونو څخه ګڼل کيږي، چې ما يې ډېر وخت د يوې داسې ليکنې لټه کوله. ښه دی، دا مې يو ډېرښه سکريپټ پيدا کړ او بيا دا د ويانا د پوهنتون هم دی، چې ما هلته درس ويلی. دا په ګوته کوم، چې د ويانا پوهنتون کې ډېر ښه او مشهور ګڼونپوهان تير شوي او لا هم شته.

دا ما له دې امله هم اړينه وبلله، چې زما په اند دا درس د افغانستان پوهنتونونو کې نه شته. هيله ده، چې دابه د ګرانو هيوادوالوپه ګټه وخوري.

په دې هيله هم،چې ګڼونپوهنه به دپه درسي پروګرام کې خوندي شي.

ستاسو ماخان

سريزه:

(c) ketabton.com: The Digital Library

په هغه وخت کې ګاوس ګڼونپوهنه یا د عددونو تیوري د ماتماتیک د ملکې(پاچاګۍ) په نوم ونوموله. د دې لپاره چې د شمیرپوهنې په دې ساحې ښه وپوهیږو، مختلفې پیلونې – همداسې مخ ته تللې لکچرونه وړاندې کیږي.

ګڼونتیوري د ډېرو داسې ساده بریښیدونکو پرابلمونو، ښوونه او یا د هغوې تضاد تر څیړنې لاندې نیسي، چې تر نن ورځې پورې دا پاتې دي یا نه دي شوی، او د پوره پام کونې له مخې خورا سخت مخ ته لیدل شوي دي. د وخت په تیریدو سره دې د ګڼونپوهنې دې خویونو یو د شمیر پوهنې تیوري ودې خورا ستر د تغذیې ورشو موندله، چې د خپل دسڅیلین دپولې زیاته ور اخواته رسیدونکې ده. په دې اړوند دې دا هم په ګوته شوې وي، چې د ساده پرابلمونو یو ډکی(حجم) شتون لري، د کومې له مخې چې هر څوک په خوښه ازمایلی شي([Guy94] وګورئ).

، د ګڼونتیوری یوه غټه معنا ، چې د دې ساحې یا ورشو د یوه قهرمان څخه نږدې ۳۰۰ نا روښانه کلونو وروسته حل شوې: د فرمات Fermat ګومان چې په ښه توګه د ، ،،لوی فرمات Der große Fermat ،،تر نامه لاندې نوم یا شهرت لري.

که څه هم عملي کارونه یا استعمال یې د ۱۹۹۴ د اندریو ا و ریچارد تیلور جملې څخه په سختۍ لیدل کیږي، بیاهم ګڼونپوهنه سیده یا په همدې وخت کې په ماډرن شمیرپوهنه کې غوره رول لري. په دې اړونده سړی فقط د بیلګې په توګه کریپتوګرافي ته خپل پام اړوي، چیرته چې د خبرونو د کود (شفر)څخه وازونه ، د نورو تر څنګ خورا لوی لومړنیو ګڼونو ته اړتیا پیښیږي.

په ۶/۳ برخه کې لنډ دې پرابلم ته پام شوی دی، دګڼونپوهنې د بنسټیز د استعمالوړوالي دې دلته اانتظار نه کیږي، ځکه چې بنسټیزه تیوري، نه مګر د هغې استعمال د دې سکریپت په ککره کې ځای لري. علاقمند لوستونکی دې په دې هکله نورو د ګڼونتیوري زیاتو کتابونو لوستلو ته راوبلل شي. دا مخ ته پرته لیکنه د ویانا پوهنتو کې د ۲۰۰۰ او ۲۰۰۱ ژمي سمستر لپاره لکل شوې. بنسټیزې پوهنې یې له وړاندې – یا مخنیونه نه ده، مګر ښه خو ده، چې د الجبري جوړښت او کلیمو سره بلدتیا شتون ولري. لکچر پروفیسر میچ او اړونده تمرینونه یې ډاکتر شویزنګایر مخ ته بیول. دا سکریپت د لکچر په لیکنو ولاړ دی او د تکمیل ادعا نه کوي.

جورج ګوتنبرونر اپریل ۲۰۰۲

(c) ketabton.com: The Digital Library

د $(\mathbb{Z},+,\cdot,\leq)$ خویونه

د $\mathbb{Z}$ لپاره اکسیومسیستمونه Axiomensystemen

د $(\mathbb{Z},+,\cdot,\leq)$ لپاره یو ممکنه اکسیوم دی:

لومړی: اکسیوم،، + ،، پوره کوي : $a,b\in\mathbb{Z}\Rightarrow a+b\in\mathbb{Z}$ او :

الف::

اسوشیاتیو قانو $a+(b+c)=(a+b)+c\ \forall a,b,c\in\mathbb{Z}$

ب-

$\exists\, 0\in\mathbb{Z}\ (,,Null``):a+0=0+a=a\ \forall a\in\mathbb{Z}$ (بې اغیزه یا ناپیلی توکی)

پ –

$\forall a\in\mathbb{Z}\exists -a\in\mathbb{Z}:a+(-a)=(-a)+a=0$ (په ښت یا معکوس توکی)

ت -
$a+b=b+a\ \forall a,b\in\mathbb{Z}$ (کموتاتیو یا د بدلېدو قانون)

دویم : ضرب ،، . ،، پوره کوي $a,b\in\mathbb{Z}\Rightarrow a\cdot b^1\in\mathbb{Z}$ او:

الف-

$a\cdot(b\cdot c)=(a\cdot b)\cdot c\ \forall a,b,c\in\mathbb{Z}$(اسوشیاتیو قانون)

ب –

(c) ketabton.com: The Digital Library

$\exists\, 1 \in \mathbb{Z}, 1 \neq 0, („Eins“)$ د $1 \cdot a = a \cdot 1 = a \ \forall a \in \mathbb{Z}$ (بي اغيزه يا ناپيلی توکی)

پ-

$a \cdot b = b \cdot a \ \forall a, b \in \mathbb{Z}$ (کموتاتيو يا د بدلېدو قانون)

ت-

$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \ \forall a, b, c \in \mathbb{Z}$)ديستريبوتيو قانون)

دريم: نسبت و نظم „$\leq$`` ته باور لري:

الف ـ $a \leq a \ \forall a \in \mathbb{Z}$ رفلکسيويي

ب . $a \leq b, b \leq a \Rightarrow a = b \ \forall a, b \in \mathbb{Z}$ انتيسيومتري.

پ ـ $a \leq b, b \leq c \Rightarrow a \leq c \ \forall a, b, c \in \mathbb{Z}$ ترانزيتيو.

ب ـ $\forall a, b \in \mathbb{Z} : a = b \vee a \leq b \vee b \leq a$

ټ ـ $a \leq b, c \in \mathbb{Z}$ په خوبنه $\Rightarrow a + c \leq b + c \ \forall a, b \in \mathbb{Z}$

ث ـ $a \leq b, c \in \mathbb{Z}, c > 0 \Rightarrow a \cdot c \leq b \cdot c \ \forall a, b \in \mathbb{Z}$

څلوم- برخدېری $\mathbb{N} = \{a \in \mathbb{Z} \mid a > 0\}$ پوره منظمه ده، دا په دې معنا چې د $\mathbb{N}$ هره ناتش برخدېرۍ A کوچنی توکی لري. (نو: $A \neq \emptyset \Rightarrow \exists\, a_0 \in A : a_0 \leq a, \ \forall a \in A$)

يادونه ۱.۱.۱ د جمعې يا زياتون د څلور خويونو لپاره $(\mathbb{Z}, +)$ يو ابل گروپ جوړوي، د ضرب د خويونو سره په گډه د $(\mathbb{Z}, +, \cdot)$ سره په اړوند د يوه

کموتاتيو رينگ څخه غږيږو، د يوې(واحد) توکي سره.

(c) ketabton.com: The Digital Library

د اکسیومونو $3a-3d$ سره په ګډه $(\mathbb{Z},\leq)$ یو توتالمنظمه ډېرۍ(،،ځنځیر،،) جوړوي.. که ټول اکسیومونه $1-3$ باور ولري، نو دا بی یو منظم رینګ(کړی) دی(بېلګه: $(\mathbb{Z},+,\cdot,\leq)$)

یادونه ۱ . ۱ . ۲ سرې کړی شي وښايي: $(R,\oplus,\odot,\preceq)$ یو په خوښه الجبري جوړښت دی، هغه چې د ا پورته له ۱ تر ۴ اکسیومونه پوره کوي، نو دا بیا په روښانه توګه [1.1] برابر دی له $(\mathbb{Z},+,\cdot,\leq)$ سره.

ترې لاس ته راوړنه: په $(\mathbb{Z},+,\cdot,\leq)$ کې باور لري:

$$a\leq b, c<0 \Rightarrow bc\leq ac. \quad (1.1)$$

ښوونه:

$$c<0 \quad \overset{3e}{\Rightarrow} \quad c+(-c)<0+(-c)\overset{1b}{=}-c\Rightarrow 0<-c. \quad (1.2)$$

$$a\leq b \quad \overset{3f}{\Rightarrow} \quad a\cdot(-c)\leq b\cdot(-c)\overset{UE}{\Rightarrow}-(ac)\leq-(bc)\overset{3e}{\Rightarrow} \quad (1.3)$$

$$\overset{3e}{\Rightarrow} \quad -(ac)+(bc)\leq-(bc)+(bc)=0\overset{3e}{\Rightarrow} \quad (1.4)$$

$$\overset{3e}{\Rightarrow} \quad (ac)-(ac)+(bc)\leq(ac)+0\Rightarrow \quad (1.5)$$

$$\Rightarrow \quad bc\leq ac. \quad (1.6)$$

(c) ketabton.com: The Digital Library

جمله ګی۱ . ۱ . ۴ له $(\mathbb{Z},+,\cdot,\leq)$ څخه د $\leq$ لپاره باور لري:

$$a \leq b \Leftrightarrow a=b \ \vee \ b=a+n \ (n\in\mathbb{N}). \qquad (1.7)$$

ښوونه: $(\Leftarrow)$

$$b=a+n, n\in\mathbb{N} \Rightarrow b-a=n \Rightarrow b-a>0 \Rightarrow b>a \Rightarrow a<b. \qquad (1.8)$$

$(\Rightarrow)$

$$a\leq b \overset{3e}{\Rightarrow} a+(-a)\leq b+(-a) \Rightarrow 0\leq b-a \qquad (1.9)$$

$$\Rightarrow b-a=0 \vee b-a>0 \Rightarrow b=a \vee b-a\in\mathbb{N} \qquad (1.10)$$

$$\Rightarrow n:=b-a \Rightarrow b=a+n \quad \text{د } n\in\mathbb{N}. \text{ سره} \qquad (1.11)$$

لاس ته راوړنه۱ . ۱ . ۵ : $\cdots -2<-1<0<1<2 \ \cdots$

جمله ګی ۱ . ۱ . ۶ : د$\mathbb{N}$ لپاره د اندکشن اصول باور لري، دا په دې معنا چې $\exists\, \emptyset \neq A\subseteq\mathbb{N}$ د لاندې سره:

1. $1\in A$,
2. $n\in A \Rightarrow n+1\in A$,

نو باور لري $A=\mathbb{N}$.

ښوونه:وي دې $\emptyset\neq A\subseteq\mathbb{N}, A$ په خوښهد دواړو خویونو سره ورکړ شوې، ښایو:

(c) ketabton.com: The Digital Library

$A = \mathbb{N}$ (د $(\mathbb{Z}, +, \cdot, \leq)$ اکسیومونو په مرسته)

نیسو $A \neq \mathbb{N}$. راوړو

$$T := \mathbb{N} \setminus A = \{x \in \mathbb{N} \mid x \notin A\}, \qquad (1.12)$$

له دې امله $T \neq \emptyset$. د اکسیم4 له مخې T یو کوچنی توکی $n_0 \in T$ لري.. دی $n_0 \neq 1$ ، ځکه چې د A خوی1 له مخې:

$$1 \notin T = \mathbb{N} \setminus A. \Rightarrow 1 \in A, \qquad (1.13)$$

د1.1.4 پسې $n_0 > 1$ لرو ، داسې چې د3e پسې باور لري:

$$n_0 - 1 \in \mathbb{N} \text{ نو } n_0 - 1 > 1 - 1 = 0, \quad (1.14)$$

(د $\mathbb{N}$ تعریف وګورئ) د

$$n_0 - 1 < n_0 \ (n_0 = (n_0 - 1) + 1 \overset{1.1.4}{\Rightarrow} n_0 - 1 < n_0), \quad (1.15)$$

له امله او داچې $n_0 \in T$ د T کوچنی توکی دی، لرو:

$$n_0 - 1 \notin T. \qquad (1.16)$$

له دې امله $n_0 - 1 \in A$ باور لري (پام: $n_0 - 1 \in \mathbb{N}$). له دې سره د A د 2 خوي له امله ، داسې چې هم $(n_0 - 1) + 1 \in A$ د ی، دا په دې معناچې $n_0 \in A$. تضاد.

(c) ketabton.com: The Digital Library

جملګی۱ . ۱ . ۷: (د پاتې سره وېش) که $a \in \mathbb{Z}, b \in \mathbb{N}$ وي، نو ګڼونه یا عددونه (یواځني تاکلي) $q, r \in \mathbb{Z}$ شتون لري د $a = bq + r$ سره د $0 \leq r < b$ سره.

ښوونه: وي دې

$$M := \{n \in \mathbb{N}_0 \mid n = a - bx \quad x \in \mathbb{Z}\}. \qquad (1.17)$$

وښایه: $M \neq \emptyset$

که $a \geq 0$ وي ، نو دی

$$n := a - b \cdot 0 = a \in \mathbb{N}_0, \qquad (1.18)$$

پس $n \in M$ ، که $a < 0$ وی ، نو $0 < -a$ او له $a \leq b$ څخه د 3f له مخې لاس ته راځي

$$1 \cdot (-a) \leq b \cdot (-a), \qquad (1.19)$$

دا په دې معنا ، چې

$$-a \leq -(ba) \overset{3g}{\Rightarrow} a + (-a) \leq a + (-ba), \quad (1.20)$$

دا په دې معنا، چې $0 \leq a - b \cdot a$ ، له دې سره $a - ba \in \mathbb{N}_0$ او $n = a - ba \in M$ دی(د 3d له مخې بل امکانات نه شته).

د له مخې دا ډېری یو کوچنی توکی r لري r : ، داپه دې معنا، چې $r \in \mathbb{N}_0$ او

(c) ketabton.com: The Digital Library

$$r = a - b \cdot x_0 \text{ für ein } x_0 \in \mathbb{Z}; \qquad (1.21)$$

له دې سره لاس ته راځي

$$a = b \cdot x_0 + r, \text{ چېرته چې } 0 \leq r. \qquad (1.22)$$

نور غواړو وښايو: $r < b$

نیسو $r \geq b$ ([3d](#))، د [1.1.4](#) پسې $x_0 < x_0 + 1$ باور لري، له دې سره $-(x_0+1) < -x_0$، د $b > 0$ له امله د[3f](#) پسې لرو:

$$-(x_0+1)b < -x_0 b \overset{3e}{\Rightarrow} a - (x_0+1)b < a - x_0 b = r; \qquad (1.23)$$

باور لري

$$a = bx_0 + r \overset{r<b}{\leq} bx_0 + b = b(x_0+1), \qquad (1.24)$$

نو لاس ته راځي: $a - b(x_0+1) \leq 0$، له دې سره

$$a - (x_0+1)b \in M. \qquad (1.25)$$

تضاد، ځکه چې r په M کې کوچنی ګڼ یا عدد دی.

بېلګه 1.1.8 : $a = -42, b = 32$

اجازه نه لري، ځکه چې $r = -10 < 0$ دی. $-42 = 32 \cdot (-1) + (-10)$

د پاتې سره وېشدی، ځکه چې $0 \leq r = 22 < b = 32$ دی. $-42 = 32 \cdot (-2) + 22$

(c) ketabton.com: The Digital Library

د پښني یادونه:

...غوره [1.1]

سړی هم وایي ،،تر ایزومورفي پورې،، .

د طبیعي ګڼونو یا –اعدادو ځای انځورونه

لکه $273 = 2 \cdot 10^2 + 7 \cdot 10^1 + 3 \cdot 10^0$ ، له دې سره

$$0 \leq 2 < 10, 0 \leq 7 < 10, 0 \leq 3 < 10$$

جملګی1.2.1 : وي دې $a \in \mathbb{N}, b \in \mathbb{N}, \ b \geq 2$ ، نو یواځنی ټاکلی ګڼ یا عدد؛ $n \geq 0, a_i \in \mathbb{N}_0$ شتونلری د لاندې سره:

$$a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0, \qquad (1.26)$$

د کوم سره چې $a_n > 0, \ 0 \leq a_i < b \ (i = 1, \ldots, n)$

ښوونه:

شتون :

که $a < b$ وي، نو $a = a_0$ ، د کوم سره چې $n = 0, a_0 = a < b$ راکوي.

وي دې $a \geq b$. د وېش له امله د پاتې سره راکوي:

$$a = bq_1 + a_0, 0 \leq a_0 < b, \qquad (1.27)$$

$$q_1 = bq_2 + a_1, 0 \leq a_1 < b, \qquad (1.28)$$

(c) ketabton.com: The Digital Library

$\vdots$ (1.29)

$$q_i = bq_{i+1} + a_i, 0 \leq a_i < b. \quad (1.30)$$

وښایه : $q_i \geq 0 \ (i = 1, 2, \ldots)$ د پورا ایندکشن له لارې:

$i = 1$:

نیسو $q_1 < 0$ ، نو باور لري

$$a = bq_1 + a_0 < b \cdot 0 + a_0 = a_0 < b, \quad (1.31)$$

- تضاد یا مخامخوالی!

$i \to i + 1$:

نیسو $q_{i+1} < 0 \Rightarrow q_{i+1} \leq -1$ ، داسې چې

$$q_{i+1} + 1 \leq -1 + 1 = 0, \quad (1.32)$$

نو

$$q_i = bq_{i+1} + a_i < bq_{i+1} + b = b(q_{i+1} + 1) \leq b \cdot 0 = 0 \quad (1.33)$$

- تضاد!

باور لري: $q_i \geq q_{i+1} \ (i = 1, 2, \ldots)$. ځکه چې:

$$q_i = bq_{i+1} + a_i \geq bq_{i+1} \overset{b \geq 2, q_{i+1} \geq 0}{\geq} 2q_{i+1} \geq q_{i+1}. \quad (1.34)$$

له دې سره $q_1 \geq q_2 \geq \cdots$ دی $q_{i+1} > 0$ ، نو $q_i > q_{i+1}$ دی .

(c) ketabton.com: The Digital Library

د ډېرۍ یا سټ $M := \{q_i \mid q_i > 0\}$ لپاره باور لري، $M \neq \emptyset$ ، نو یو کوچنی توکی $q_n \in M$ شتون لري. پسې لاس ته راځی $q_{n+1} = 0$. له دې سره :

$$q_n = bq_{n+1} + a_n = a_n, \quad (1.35)$$

دابه دې معنا چې $a_n = q_n > 0$ ، د په ځېږ اینوونې له لارې لاس ته راوړو:

$$\begin{aligned} a &= bq_1 + a_0 = b(bq_2 + a_1) + a_0 = q_2b^2 + ba_1b - a_0 = \cdots \\ &= q_nb^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0 \ (q_n = a_n > 0). \end{aligned}$$

یواځیوالی:

نیسو، چې دوه مختلفې انځورونې شتون لري. وي دې

$$a = a_nb^n + \cdots + a_1b + a_0 = \bar{a}_mb^m + \bar{a}_{m-1}b^{m-1} + \cdots + \bar{a}_1b + \bar{a}_0, \quad (1.36)$$

د $n \geq m,\ a_n > 0,\ 0 \leq a_i < b\ \forall i,\ \bar{a}_m > 0,\ 0 \leq \bar{a}_j < b\ \forall j$ سره .

له دې امله: $a_0 - \bar{a}_0 = bq$ د یوه $q \in \mathbb{Z}$ لپاره ، د $0 \leq \bar{a}_0 < b$ له امله باور لري

$$-b < -\bar{a}_0 \leq 0 \overset{0 \leq a_0 < b}{\Longrightarrow} -b < a_0 - \bar{a}_0 < b. \quad (1.37)$$

که $q > 0$ وي، نو $q \geq 1$ دی او د $b > 0 : a_0 - \bar{a}_0 = bq \geq b \cdot 1 = b$ له امله ، تضاد.

(c) ketabton.com: The Digital Library

که $q < 0$ وي، نو $q \leq -1$ دی او د
$b > 0 : a_0 - \bar{a}_0 = bq \leq (-1)b = -b$ له امله تضاد .

نو باید $q = 0$ باور ولري، له دې سره $a_0 - \bar{a}_0 = b \cdot 0 = 0$ او $a_0 = \bar{a}_0$. له دې امله باور لري:

$$a_n b^n + \cdots + a_1 b = \bar{a}_m b^m + \cdots + \bar{a}_1 b; \qquad (1.38)$$

د b سره لنډوني له لارې لاس ته راځي:

$$a_n b^{n-1} + \cdots + a_2 b + a_1 = \bar{a}_m b^{m-1} + \cdots + \bar{a}_2 b + \bar{a}_1. \; (1.39)$$

په ورته توګه لاس ته راځي: $a_1 = \bar{a}_1, a_2 = \bar{a}_2, \cdots, a_m = \bar{a}_m$ ، داسې چې په تولیزه توګه راکوي:

$$a_n b^{n-(m+1)} + \cdots + a_{m+1} = 0 \; (n \geq m) \qquad (1.40)$$

که $n > m$ وی له $a_n > 0, b > 0 \Rightarrow$ سره وی ، نو لاس ته ترې راځي: کینه لور له صفر لویه ده، تضاد.

له دې امله باید $n = m$ باور ولري، او $a_0 = \bar{a}_0, a_1 = \bar{a}_1, \ldots, a_m = \bar{a}_m.$ هم. □

پیژند (تعریف)1.2.2 : پورتنی د $a \in \mathbb{N}$ یواځنی انځورونه د$b \in \mathbb{N}, \; b \geq 2$ له لارې د a ځای انځورونه بلل کیږي نسبت بنسټ b ته، سومبولیک

(1.41)	$a = (a_n, a_{n-1}, \ldots, a_1, a_0)_b.$

(c) ketabton.com: The Digital Library

که $b = 10$ وي، نو له دیکادیکي *dekadischen* یا لسمیزې انځوروني غږیږو، د $b = 2$ سره له بینار یا دوه ییزې انځوروني غږیږو. که $b > 0$ وي، نو سرې لیکي $A = 10, B = 11, \ldots$ (د دې لپاره چې له 10 خخه یې توپیر وکړای شو).

یادونه1.2.3 : د a ځای انځورونه نسبت $b \geq 2$ ته کېدی شي د [1.2.1](#) د شووني په بنسټ و ټاکل شي[1.2] .

$$a = q_1 b + a_0 \quad 0 \leq a_0 < b \;\Rightarrow\; a_0 \text{ ټاکلی.} \qquad (1.42)$$

$$q_1 = q_2 b + a_1 \quad 0 \leq a_1 < b \;\Rightarrow\; a_1 \text{ ټاکلی.} \qquad (1.43)$$

q2=q3b+a2 0<u><</u>a2<b =>a2 ټاکلی : (1.44)

بېلګه1.2.4 : وي دې $a = 731,\ b = 10$ ، غوښته: دa انځورونه ، $731 : 10 = 73 + 1$ نو

$$\left.\begin{array}{rcll} 731 & = & 73 \cdot 10 + 1 & 0 \leq 1 < 10 \;\Rightarrow a_0 = 1 \\ 73 & = & 7 \cdot 10 + 3 & 0 \leq 3 < 10 \;\Rightarrow a_1 = 3 \\ 7 & = & 0 \cdot 10 + 7 & 0 \leq 7 < 10 \;\Rightarrow a_2 = 7 \end{array}\right\} \Rightarrow 731 = (731)_{10}. \qquad (1.45)$$

بېلګه 1.2.5 : وي دې $a = 367, b = 2$ ، غوښتنه یا ثبوت: دa بینار-یا دوه ییزه انځورونه $367 = 183 \cdot 2 + 1 = \cdots$ سرې داسې لیکي :

367 : 2	183 : 2	91 : 2	45 : 2	22 : 2	11 : 2	5 : 2	2 : 2	1 : 2	0
1	1	1	1	0	1	1	0	1	

(c) ketabton.com: The Digital Library

$\Rightarrow 367 = (101101111)_2$.

ازماېښت:

$1 \cdot 2^0 + 1 \cdot 2^1 + 9 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 +$
$1 \cdot 2^6 + 0 \cdot 2^7 + 1 \cdot 2^8 = 367$.

په $\mathbb{Z}$ کې تړونه Teilbarkeit in $\mathbb{Z}$

لاندې برخه(خورا غټ ګډ پروېشونی = ggT)

- پروېشوني او $\mathrm{ggT}(a,b)$ (مقسوم علیه او) یا

د اوکلید له مخې د ggT تاکنه

د

$a_1, a_2 \ldots, a_n \in \mathbb{Z}$

خورا غټ ګډ پروېشونی(بزرګترین مقسوم علیه مشترک)

Georg Gutenbrunner 2002-10-04

پر وېشونی او خورا غټ ګډ پروېشونی $\mathrm{ggT}(a,b)$

پېژند(تعریف) 2.1.1 : وي دې $a \in \mathbb{Z}$ ، سرې وایي $b \in \mathbb{Z}$ a وېشي، که د یوه $q \in \mathbb{Z}$ لپاره باور ولري $a = b \cdot q$.

(c) ketabton.com: The Digital Library

سومبولیک : $b \mid a$ ، b د a پروېشوني بلل کیږي، q د b پوره کېدونکې یا کمپلمنتار پروېښوني بلل کیږي. که b د a پروېشوني (مقسوم علیه) نه وي، نو لیکو $b \nmid a$.

د1 پروېشوني د $\mathbb{Z}$ یوونونه یا واحدونه بلکیږي(دا فقط $\{1, -1\}$ دي).

یادونه 2.1.2 : هر ګڼ یا عدد $a \in \mathbb{Z}$ پروېشوني $1, -1, a, -a$ لري، داسې په نامه ساده(نا اصلي) پروېشوني. که نور پروېشوني شتون ولري، نو دا اصلي پروېشوني بلل کیږي.

لېما جمله ګوتې 2.1.3:

1. $b \mid a \Rightarrow b \cdot c \mid a \cdot c \;\forall c \in \mathbb{Z}$.
2. $bc \mid ac, c \neq 0 \Rightarrow b \mid a$.
3. $a \mid b, b \mid c \Rightarrow a \mid c$.
4. $a \mid b, b \neq 0 \Rightarrow |a| \leq |b|$.
5. $a \mid b, b \mid a \Rightarrow a = \pm b$ (also)نو $|a| = |b|$.)
6. که $a_1, \ldots, a_n, b \in \mathbb{Z}$ وي، د $b \mid a_1, \ldots, b \mid a_n$ سره، نو باور لري $\forall c_1, \ldots, c_n \in \mathbb{Z}$:

$$b \,\Bigg|\, \sum_{i=1}^{n} c_i a_i \; . \qquad (2.1)$$

ښونه:

(c) ketabton.com: The Digital Library

ad 4

د $a \mid b = a \cdot q$ لپاره $= |a| \cdot |q|, q \neq 0\ q \in \mathbb{Z} \Rightarrow |b|$ پرته له دې, $b = 0$,

نو $|q| \geq 1$ او $|b| = |a| \cdot |q| \geq |a|$ ($|a|$ هم > 0 پرته له دې, $b = 0$).

ad 5

$a \mid b \Rightarrow b = aq, b \mid a \Rightarrow a = br$
$\Rightarrow$ Ist $a = 0$,

نو له دې$b = 0$ لاس ته راځي. که $b = 0$ وي، نو$a = 0$ هم . که a او b د صفر سره برابر نه وي:

$|a| \leq |b|$ او $|b| \leq |a|$ ، له دې سره $|a| = |b|$ دی، داپه دې معناچې $a = \pm b$ دی .

ad 6

$a_1 = bq_1, \ldots, a_n = bq_n \ (q_i \in \mathbb{Z})$

$$\Rightarrow \sum_{i=1}^{n} a_i c_i = \sum_{i=1}^{n} (bq_i) c_i = b \underbrace{\sum_{i=1}^{n} q_i c_i}_{\in \mathbb{Z}} \Rightarrow b \Big| \sum_{i=1}^{n} a_i c_i \ \forall c_i \in \mathbb{Z}. \quad (2.2)$$

لاس ته راوړنه2.1.4 : هر $a \in \mathbb{Z}, a \neq 0$ ، پای ډېرې پروېشوني b لري، ځکه چې د(4) 2.1.3 پسي باور لري: $|b| \leq |a|$ ، نو $-|a| \leq b \leq |a|$ ، له دې امله

(c) ketabton.com: The Digital Library

$$b \in \{-|a|, -|a|+1, \ldots, |a|-1, |a|\}, \quad (2.3)$$

دا فقط پای ډېر دي.

مګر : $a = 0$ ټول ګڼونه یا ټولعددونه د پروېشونو په څېر لري: $0 = b \cdot 0 \ \forall b \in \mathbb{Z}$
، دا په دې معنا چې a ناپای ډېر پروېشوني لري.

پسې راتلنه یا لاس ته راوړنه 2.1.5 : د $a \in \mathbb{N}$ $(\Rightarrow a \neq 0)$ د زیاتیزو یا مثبتو
پروېشونو د ټاکلو له امله کېدی شي سړی ځان په هغه د $1 \leq b \leq \sqrt{a}$ سره رابند یا
محدود کړي.

ځکه چې : که q د $a \neq 0$ یو پروېشونی وي د $q > \sqrt{a}$ سره او
$a = qr \ (r \in \mathbb{Z})$ وي، نو دی $r < \sqrt{a}$ ، ځکه چې :

$$r \geq \sqrt{a} \Rightarrow a = qr \geq q\sqrt{a} > \sqrt{a}\sqrt{a} = a \quad (2.4)$$

- تضاد! له دې سره r پورره کېدونکې پروېشوني ده د $r \leq \sqrt{a}$ سره.

بېلګه 2.1.6 : $a = 80$ ، ټول پروېشوني غوښتونوي دي. د $\sqrt{80} < 9$ له امله ټول
زیاتیز یا مثبت پروېشوني b دې د $1 \leq b \leq \sqrt{80} < 9$ سره وټاکل شي:

$$1, 2, 4, 5, 8; 80, 40, 20, 16, 10. \quad (2.5)$$

له دې سره ټول پروېشوني دي:

$$\pm 40, \pm 80 \ \pm 1, \pm 2, \pm 4, \pm 5, \pm 8, \pm 10, \pm 16, \pm 20,$$

(c) ketabton.com: The Digital Library

پېژد(تعريف) 2.1.7: وي دې $a,b \in \mathbb{Z}$، نو $c \in \mathbb{Z}$ د a,b ګډ پروبېښونی بلل کيږي، که $c \mid a$ او $c \mid b$ وي .

ياودونه2.1.8 : که $a \in \mathbb{Z}, a \neq 0$ وي، نو دa [2.1.4](#) پسې يا له مخې فقط پای ډېر پروبېشوني لري. که $b \in \mathbb{Z}$ په خوښه وي، نو a او b فقط پای ډېر پروبېشوني لري. د اکسيوم [3d](#) له مخې $\mathbb{Z}$ توتالي (ټول يا بېخي) منظم دی، يعني د a,b ګډ پروبېشونی يو خورا لوي توکی دی. نو سېرى کېږى شي تعريف کړي:

پېژند يا تعيف2.1.9 : (خورا غټ ګډ پروبېشونی يا بزرګترين مقسوم عليه Greatest comon divisor) وي دې $a,b \in \mathbb{Z}$ ، نه دواړه صفر، نو $\mathrm{ggT}(a,b)$ (انګرېزي يې gcd(a,b)) د ټولو ګډ پروبېشونو خورا لوی(يعني تر ټولو لوي) دی . دا يواځنی ټاکلی دی. دی، که $\mathrm{ggT}(a,b)=1$ وي، نو a,b نسبي لومړني يا پريم بلل کيږي يا پروبېش پردېِ(ګډ اصلي پروبېشونی نه لري).

يادونه 2.1.10 : که $a,b \in \mathbb{Z}$ دواړه صفر نه وي. نو کېدی شي سړی د $\mathrm{ggT}(a,b)$ ټاکلو لپاره په زياتيزو يا مثبتو ګډو پروبېشونو ځنونه محدود کړي، ځکه چې 1 يو ګډ پروبېشونی دی، يعني باور لري:

$$\mathrm{ggT}(a,b) \geq 1$$

بېلګه2.1.11 : $a=12, b=-8$

$a: 1,2,3,4,6,12;\ b: 1,2,4,8$ د زياتيز پروبېشنونې له دې لاس ته راځي ګډ مثبت پروبېشوني دي:

$$1,2,4 \Rightarrow \mathrm{ggT}(a,b)=\mathrm{ggT}(12,-8)=4$$

(c) ketabton.com: The Digital Library

د اویکلید یا اقلیدس له مخې د ggT ټاکنه

جمله 2.2.1 : د اویکلید الګوریتم (Algorithmus [1] [2.] Euklidische) وي دې $a, b \in \mathbb{N}$ او بې له ټولیزو بندیزونو $b \leq a$. که $b \mid a$ وي، نو ږدو $r_0 = b$، که $b \nmid a$ باور لري، ځکه چې که د وېش له لارې د پاتې سره $q_i, r_i \in \mathbb{Z}$ سرې په لاندې توګه ټاکي:

$$
\begin{aligned}
a &= q_0 b + r_1, && 0 \leq r_1 < b \\
b &= q_1 r_1 + r_2, && 0 \leq r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, && 0 \leq r_3 < r_2 \\
&\vdots \\
r_{m-1} &= q_m r_m + r_{m+1}, && 0 \leq r_{m+1} < r_m \\
&\vdots
\end{aligned}
$$

نو کوچنی $n \in \mathbb{N}_0$ شتون لري د $r_{n+1} = 0, r_n \neq 0$ سره او $r_n = \mathrm{ggT}(a, b)$ باور لري .

ښوونه : که $b \mid a$ وي، نو باور لري

$$r_0 = b = \mathrm{ggT}(a, b), r_1 = r_{0+1} = 0 \qquad (2.6)$$

(c) ketabton.com: The Digital Library

د $a = b \cdot q_0 + r_1$ لپاره.

وي دې $b \nmid a$، نو $a = q_0 b + r_1, 0 \le r_1 < b$ باور لري د $r_1 \neq 0$ سره. د جوړښت له مخې باور لري

$$r_1 > r_2 > \cdots > r_i > r_{i+1} > \cdots . \qquad (2.7)$$

وي دې $M := \{r_i \mid r_i > 0\}$، نو $M \neq \emptyset$ دی، ځکه چې $r_1 \neq 0$، له دې سره $r_1 \in M$. د پوره نظم اصولو له مخې (Axiom 4) په M کې یو کوچنی توکی شتون لري: r_n. نو باور لري:

$$r_n > 0 \ (r_n \in M) \quad \text{und} \quad r_{n+1} = 0 \ (0 \le r_{n+1} < r_n). \qquad (2.8)$$

وښایی : $r_n = \mathrm{ggT}(a, b)$

- $r_n \mid a, b$ اخرنی مساوات یا برابرون دی:

$r_{n-1} = q_n r_n (+ r_{n+1}),$	(2.9)

نو $r_n \mid r_{n-1}$. له اخر د مخه مساوات دي:

$r_{n-2} = q_{n-1} r_{n-1} + r_n,$	(2.10)

نو $r_n \mid r_{n-1}, r_{n-2}$

(c) ketabton.com: The Digital Library

- که په ورته توګه مخ ته لاړ شو، نو ترې لاس ته راځي

$r_n \mid r_2, r_n \mid r_1, r_n \mid b$ او له دې امله

$r_n \mid q_0 b + r_1 = a \Rightarrow r_n \mid a, b.$	(2.11)

$r_n = \mathrm{ggT}(a, b)$

t دې په خوښه يو د a, b مثبت پروېشونی وي. نو د لومړي مساوات څخه لرو :

$r_1 = a - q_0 b \overset{2.1.3(6)}{\Rightarrow} t \mid r_1;$	(2.12)

له 2 مساوات :

$r_2 = b - r_1 q_1 \Rightarrow t \mid r_2,$	(2.13)

او همداسې پسې، تر

$$t \mid r_{n-1}, t \mid r_n \overset{2.1.3(4)}{\Rightarrow} |t| \leq |r_n|. \qquad (2.14)$$

t مثبت، $\Rightarrow t \leq r_n \Rightarrow r_n$ مثبت له دې لاس ته راځي $\mathrm{ggT}(a, b)$. غټ ګډ پروېشونی دی.

يادونه 2.2.2 : که د اعدادو يو (يا دواړه) $a, b \in \mathbb{Z}$ د صفر کوچني وي، نو د اوکليد الګوريتم دې په $|a|$ همداسې په $|b|$ باندې وکارول شي، ځکه چې

موږ د a, b د مثبت پروېشونو پيداکېدل غواړو (پام $\mathrm{ggT}(a, b) \geq 1$).

بېلګه2.2.3 : $a = 97, b = -44$ ، نو باور لري : $|b| = 44 \leq 97 = a$ ، نو لاس ته راځي:

(c) ketabton.com: The Digital Library

$$97 = 44 \cdot 2 + 9 \quad 0 \le 9 < 44$$

$$44 = 9 \cdot 4 + 8 \quad 0 \le 8 < 9$$

$$9 = 8 \cdot 1 + 1 \quad 0 \le 1 < 8$$

$$8 = 1 \cdot 8 \qquad \Rightarrow \mathrm{ggT}(97, -44) = \mathbf{1}$$

پېژند یا تعریف2.2.4 : (کرښیز کمپرزېشن یا – یوځای اینسوونه) : وي دې $a, b \in \mathbb{Z}$ ، نو یو $c \in \mathbb{Z}$ د a, b کرښیز کمپوزېشن بلل کیږي، که $c = xa + yb$ وي د ځانګړو $x, y \in \mathbb{Z}$ سره.

که c, d د $a, b \in \mathbb{Z}$ کرښیز ښیز کمپوزېشنونه وی، په دې پسي $\alpha c + \beta d,$ ، $\forall \alpha, \beta \in \mathbb{Z}$.

هم کرښیز کمپوزېشن دی..

جمله 2.2.5 : (اوکلید) که وي $a, b \in \mathbb{Z}$ ، نه دواړه صفر، نو $\mathrm{ggT}(a, b)$ د a, b : یو کرښیز کمپوزېشن دی، د ټاکلو $x, y \in \mathbb{Z}$ لپاره. $\mathrm{ggT}(a, b) = xa + yb$

ښوونه:

لومړی $b > 0$: نو $0 < b \le a$ ، یعني $a, b \in \mathbb{N}$ ، داسې چې د اوکلید الګوریتم 2.2.1 سره باور لري:

(c) ketabton.com: The Digital Library

$\mathrm{ggT}(a,b) = r_n, r_{n+1} = 0, r_0 = b \quad b \mid a.$;	(2.15)

دويم . له دې سره باور لري

$$r_{n-2} = q_{n-1}r_{n-1} + r_n, \ldots, a = q_0 b + r_1$$

داپه دې معنا چې r_1 د a, b کمپوزېشن دی	$r_1 = a - q_0 b,$ نو
داپه دې معنا چې r_2 د a, b کمپوزېشن دی	$\Rightarrow r_2 = b - q_1 r_1,$
داپه دې معنا چې r_n د a, b کمپوزېشن دی	$\cdots \Rightarrow \underbrace{r_n}_{\mathrm{ggT}(a,b)} = r_{n-2} - q_{n-1}r_{n-1},$

.1 $\Rightarrow \mathrm{ggT}(a,b) = xa + yb$

د $x, y \in \mathbb{Z}$ د ټاکلو یا معلومو لپاره .

.2 $b = 0$: $d = \mathrm{ggT}(a,b) = a = 1 \cdot a + 0 \cdot b$

.3 $b < 0$: نو $-b > 0$ دی او له ۱ . حالته باو لري
$\mathrm{ggT}(a,b) = x \cdot a + y \cdot (-b)$

(c) ketabton.com: The Digital Library

(که غوښتوني ويa له $-b$ سره بدله کړی، که $a < -b$ باور ولري) . که $r_0 = b$ وي، نو $b \mid a$ او $\mathrm{ggT}(a,b) = 0 \cdot a + 1 \cdot b.$ باور لري.

□

یادونه 2.2.6 : ښوونه ښېرته جوړختیزه ده، دا یو متود راکوي د $x, y \in \mathbb{Z}$ تاکلو لپاره په $\mathrm{ggT}(a,b) = xa + yb$ کي، داسي چي د اوکلید الگوریم څخه پاتي افاده کوو یا وایو له مخ ته تیرو د کرښیز کمپوزیشن لویو څخه او په لاندي راتلونکي مساوات کي يي ځاېه ځایو کوو.

بېلګه 2.2.7 : $a = 111, b = 39$ ، نو دی $b = 39 \leq 111 = a$ ، داسي چي د2.2.1 سره باور لري:

$$
\begin{aligned}
111 &= 2 \cdot 39 + 33 & 3 &= 33 - 5 \cdot 6 \\
39 &= 1 \cdot 33 + 6 & &= 33 - 5(39 - 33) = 6 \cdot 33 - 5 \cdot 39 \\
33 &= 5 \cdot 6 + 3 & &= 6(111 - 2 \cdot 39) - 5 \cdot 39 \\
6 &= 2 \cdot 3. & &= 6 \cdot 111 - 17 \cdot 39
\end{aligned}
$$

.

بېلګه 2.2.8 : د $\mathrm{ggT}(a,b)$ د تاکلو لپاره ، که a او b د یوې اووښتوني یا متحولې په واک کي وي یا تابع وي.

غواړو پیدا کړو:

(c) ketabton.com: The Digital Library

$$d := \mathrm{ggT}(2k-1, 9k+4) \ (k \in \mathbb{Z}).$$

د $d \mid 2k-1, d \mid 9k+4$ له امله ، په ځانګړې توګه باور لري:

$$b \mid 9(2k-1) + (-2)(9k+1) = -17. \quad (2.16)$$

(x, y داسې ټاکل سوي دي، چې له هغې سره اووښتوني یا متحوله لرې کیږي، دا زیات وخت ممکن دی، ځکه چې $d = xa + yb$ د $\forall x, y \in \mathbb{Z}$).

له دې سره باور لري: $d = 1$ یا $d = 17 \ (d > 0)$. د کوم $k \in \mathbb{Z}$ لپاره $d = 17$ دی؟

که $d = 17$ وي ، نو دا په دې معنا چې $17 \mid 2k-1, 17 \mid 9k+4$ ، یعنې $2k - 1 = 17 \cdot t$ د $t \in \mathbb{Z}$ یوه لپاره، له دې امله $k = \frac{1}{2}(17t+1)$.

له دې امله باید t ناجوړه یا طاق وي(پرته له دې $k \in \mathbb{Z}$ دی)، یعنې $t = 2n-1, n \in \mathbb{Z}$. له دې نمله :

$$k = \frac{1}{2}(17(2n-1)+1) = \frac{1}{2}(34n-16) = 17n-8. \quad (2.17)$$

برعکس یا په څټ: که د یوه $n \in \mathbb{Z}$ لپاره $k = 17n - 8$ وي، نو بلاور لري:

$$2k - 1 = 34n - 16 - 1 = 34n - 17 = 17(2n-1)$$

دا په دې معنا چې $17 \mid 2k-1$.

$$9k + 4 = 9 \cdot 17n + 4 - 72 = 17(9n-4)$$

(c) ketabton.com: The Digital Library

دا په دې معناچي $17 \mid 9k+4$.

له دې امله باور لري: $d=17 \Leftrightarrow k=17n-8, n\in\mathbb{Z}$ په خوښه، $d=1$ پرته له دې له 2.2.5 څخه لاس ته راوړنې.

کورولار یا جملګی2.2.9 : وي دې $a,b\in\mathbb{Z}$ ، نه دواړه صفر، نو باور لري:

1. $d=\mathrm{ggT}(a,b) \Rightarrow \mathrm{ggT}(\frac{a}{d},\frac{b}{d})=1$
2. $t\mid a, t\mid b$ د $\mathrm{ggT}(\frac{a}{t},\frac{b}{t})=1$ سره ، نو دی $\mathrm{ggT}(a,b)=|t|$.
3. $m\in\mathbb{Z}, n\neq 0$ ، نو $\mathrm{ggT}(a\cdot m, b\cdot m)=|m|\cdot\mathrm{ggT}(a,b)$

ثبوونه: ad 1:

د2.2.5 له مخې باور لري: $d=xa+yb$ د تاکلو $x,y\in\mathbb{Z}$ لپاره، یعنې $d\cdot 1=d(x\frac{a}{d}+y\frac{b}{d})$ ، داسې چې باور لري ($d\neq 0$) $1=x\frac{a}{d}+y\frac{b}{d}$.

وي دې $t\geq 1$ په خوښه د $t\mid\frac{a}{d}, t\mid\frac{b}{d}$ سره، نو د 2.1.3(6) له مخې: $t\mid 1$،

دا په دې معنا چې $|t|\leq 1$ ، یعنې $t\leq 1$ ، له دې سره $t=1$. نو $\mathrm{ggT}(\frac{a}{d},\frac{b}{d})=1$.

ad 2:

له $\mathrm{ggT}(\frac{a}{t},\frac{b}{t})=1$ د:2.2.5 سره د معلومو $\alpha,\beta\in\mathbb{Z}$ لپاره راکوي $1=\alpha\frac{a}{t}+\beta\frac{b}{t}$ ، یعنې $t=\alpha a+\beta b$. د وړاندنیونو(فرضیو) وروسته $|t|$ د a,b یو ګډ پروېشونی دی. وي دې $s\geq 1, s\mid a, s\mid b$ په خوښه، نو د :2.1.3 له مخې $s\mid t$ باورلري، داسې چې $|s|\leq|t|$ دی، دا په دې معنا چې $s\leq|t|$.

یعنې $\mathrm{ggT}(a,b)=|t|$ دی.

(c) ketabton.com: The Digital Library

ad 3:

د 1 له مخې د $d = \operatorname{ggT}(a, b)$ لپاره باور لري، چې $\operatorname{ggT}(\frac{a}{d}, \frac{b}{d}) = 1$، د $d \mid a, b$ له امله د 2.1.3 پسې لاس ته راځي $md \mid ma, mb$، له دې سره لاس ته راځي $\operatorname{ggT}(\frac{a}{d}, \frac{b}{d}) = \operatorname{ggT}(\frac{ma}{md}, \frac{mb}{md}) = 1$، د 2 پسې لاس ته راځي

$$|md| = \operatorname{ggT}(ma, mb)$$

داپه دې معنا چې . $|m| \cdot d = |m| \operatorname{ggT}(a, b) = \operatorname{ggT}(ma, mb).$.

یادونه 2.2.10 : که $\frac{a}{b} \in \mathbb{Q}$ وي(ریښتوني یا راشنل)، نو د تولو : $d = \operatorname{ggT}(a, b)$ لپاره $\frac{\frac{a}{d}}{\frac{b}{d}} = \frac{a}{b}$ باور لري. د 2.2.9(1) له مخې باور لري: $\operatorname{ggT}(\frac{a}{d}, \frac{b}{d}) = 1$، دا په دې معنا چې $\frac{1}{b}$ کېدی شي په $\frac{c}{d}$ بڼه د $\operatorname{ggT}(c, d) = 1$ سره ولیکل شي (c, d حتی یواځني ټاکلي دي).

Korollar (جمله، چې د بنوول شوې جملې څخه لاس ته راځي کورولار بلل کیږي) :2.2.11

وي دې $a, b \in \mathbb{Z}$، نه دواړه صفر، نو باور لري: $d \in \mathbb{N}$ ګڼ یا عدد تیک هلته خرا غټ پروېشونی(لنډ:خ غ پ ggT = gcm) $\operatorname{ggT}(a, b)$ دی، که

(1) $d \mid a, d \mid b$.

(2) $c \mid a, c \mid b$ ($c \in \mathbb{Z}$) په خوښه $c \in \mathbb{Z}$) له دې لاس ته راځي c|d.

(c) ketabton.com: The Digital Library

ښوونه:

$(\Rightarrow)$

دی $d = \text{ggT}(a,b)$ ، نو باور $d \mid a, d \mid b$ لري، دا په دې معنا چې (1) باور لري، وي دې c د a,b په خوښه پروېشونی، نو له $d = xa + yb \ (x, y \in \mathbb{Z}$ لاس ته راځي (جمله [2.2.5](#)دې وکتل شي)، چې $c \mid d$ دی([2.1.3](#)) ، دا په دې معناچې(2) باور لري.

$(\Leftarrow)$

د (1) له مخې d د a,b ګډ پروېشونی دی. وي دې $c \in \mathbb{Z}, c \geq 1$ په خوښه د a,b پروېشونی، نو د (2) له مخې لاس ته راځي $c \mid d$ ، دا په دې معنا چې د[2.1.3](#) پسې $|c| \leq |d|$ دی ، له دې سره $c \leq d$. يعنې d د a,b خورا غټ ګډ پروېشونی(بزرګترين مقسوم عليه مشترک؟) دی

□

جمله2.2.12 : (ښسټيزه lemma (مرستندوی جمله چې د ښوونې يا ثبوت په جريان کې په کار راځي)) وي دې $a, b, c \in \mathbb{Z}, a \neq 0, \text{ggT}(a,b) = 1$ ، نو د $a \mid b \cdot c$ له مخې لاس ته راځي ،چې $a \mid c$ دی.

ښوونه : له $\text{ggT}(a,b) = 1$ لاس ته راځي

(2.18)	$1 = xa + yb$

(c) ketabton.com: The Digital Library

د څه یا ټاکلو $x, y \in \mathbb{Z}$ لپاره. له دې امله لاس ته راځي

$$c = xca + ybc. \quad (2.19)$$

دا چې د وړاندنیوني $a \mid bc, a \mid a$ څخه باور لري $\overset{2.1.3}{\Rightarrow} a \mid c.$ □

دپیښي یادون: اوکلید د200-365 ز ک څخه له مخه.

د $a_1, a_2 \ldots, a_n \in \mathbb{Z}$

خورا غټ ګډ پروېشونی $a_1, a_2 \ldots, a_n \in \mathbb{Z}$

پېژند یا تعریف :

لومړی : $a_1, \ldots, a_n \in \mathbb{Z}$ دې وي، نو $b \in \mathbb{Z}$ د $a_1, \ldots, a_n$ ګډ پروېشونی بلل کیږی، که $b \mid a_i, i = 1, \ldots, n$ باور دلري.

دویم : د ټول خورا غټ ګډ پروېشونی (نسبت $\leq$ ته) د $\operatorname{ggT}(a_1, \ldots, a_n)$ سره په نخښنه کیږي. که ټول $a_i = 0$ صفر نه وي، نو $a_i \neq 0$ هر یو فقط پای ډېر پروېشوني لري، یعنې هم پای ډېر ګډ پروېشوني. د دوي تر منځ یو خورا غټ شتون لري.

دریم : که $\operatorname{ggT}(a_1, \ldots, a_n) = 1$ وي، نو $a_1, \ldots, a_n$ نسبي لومړني(وروسته به دا پروېش پردي وبلل شي) بلل کیږي.

څلورم : $a_1, \ldots, a_n$ جوړه(حفت) نسبيي لومړني ګنونه یا عددونه بلل کیږي، که $\operatorname{ggT}(a_i, a_j) = 1$ وي د ټولو $\forall i \neq j$ لپاره.

یادونه 2.3.2 : له جوړه نسبي لومړنیو څخه لومړني لاس ته راځي. برعکسونه یا په

(c) ketabton.com: The Digital Library

څېړ کېدنه يې باور نه لري:

$$\mathrm{ggT}(1,2,4)=1, \mathrm{ggT}(2,4)=2$$

دا په دې معنا چې $(1,2,4)$ نسبي لومړني مګر نه جوړه لومړني ګڼونه دي.

جمله2.3.3 : وي دې $a_1,\ldots,a_n\in\mathbb{Z}$ ، نه ټول صفر او $d=\mathrm{ggT}(a_1,\ldots,a_n)$. نو باور لري:

$d=\sum_{i=1}^{n}x_ia_i$	(2.20)

د څه يا ځنو $x_i, i=1,\ldots,n$ لپاره.

ښوونه : وي دې

$M:=\{c_1a_1+\cdots+c_na_n\in\mathbb{Z}\mid c_i\in\mathbb{Z}\ i=1,\ldots,n\},$	(2.21)

نو $M\neq\emptyset$ او $i\neq j)$ د باور لري $a_i\in M, i=1,\ldots,n\ (c_i=1, c_j=0$
لپاره. د $a_i\in M$ له امله هم $-a_i\in M$ باور لري، که $a_i\notin\mathbb{N}$ وي،
نو $-a_i\in\mathbb{N}$ باور لري ، دا په دې معناچې هم M طبيعي يا پيداېښتي ګڼونه يا عددونه لري. د $\mathbb{N}$ د ټولنظم له مخې په M کې د ټولو طبيعي اعدادو ډېرۍ يا سټ يو خوا کوچنی توکی d^* لري، دا په دې معناچې

$d^*=x_1a_1+\cdots+x_na_n$	(2.22)

د ځنو $x_1,\ldots,x_n\in\mathbb{Z}$ لپاره . وښايی: $d^*=d=\mathrm{ggT}(a_1,\ldots,a_n)$:

(c) ketabton.com: The Digital Library

د پاتې سره د a_i وېشنه په d^* له لارې راکوي:

$a_i = q_i d^* + r_i, 0 \leq r_i < d^*;$	(2.23)

نو $r_i = a_i - q_i d^*$ او $r_i \in M$ د $a_1, \ldots, a_n$ کرښيز کمبينيشن دی، همداسي a_i ، په تعقيب کمښت يا تفريق هم. له دې سره له $0 \leq r_i < d^* : r_i = 0.$ څخه لرو. يعني:

$$a_i = q_i d^* \quad \text{und} \quad d^* \mid a_i \ \forall i = 1, \ldots, n. \ (2.24)$$

وي دې $t \geq 1$ د $a_1, \ldots, a_n, t$ يو په خوښه ګډپروېشونی، نو t هر کرښيز کمبينيشن وېشي يعني دا لاندې هم

$$t \mid x_1 a_1 + \cdots + x_n a_n = d^*; \ (2.25)$$

له دې سره د 2.2.11 پسې لرو، چې $d^* = \mathrm{ggT}(a_1, \ldots, a_n) = d.$

□

د $d = \mathrm{ggT}(a_1, \ldots, a_n)$ د تاکلو لپاره تلنلار:

د $n = 2$ لپاره: د اويکليد الګوريتم، جمله 2.2.1 .

د $d \geq 1$ له امله کېدی شي سرې تول $a_i > 0$ ونيسي(فرض کړي)(پرته له دې مطلق ارزښت، a_i ، چې صفر دي،(لرې)پرېږدي). سرې اوس د $a_1, \ldots, a_n$ لاندې

(c) ketabton.com: The Digital Library

هغه خورا کوچنی لټوي، دا دې بې له تولیزو بندیزونو a_1 وي(کېدی شي نمره بدل شي). د پاتې سره د $a_2, \ldots, a_n$ وېش د a_1 له لارې راکوي:

$$a_i = q_i a_1 + r_i, 0 \leq r_i < a_1 \;\; i = 2, \ldots, n. \quad (2.26)$$

وښایي:

$$d = \text{ggT}(a_1, \ldots, a_n) = d' = \text{ggT}(a_1, r_2 \ldots, r_n)$$

وي دې

$$d := \text{ggT}(a_1, \ldots, a_n), d' := \text{ggT}(a_1, r_2 \ldots, r_n); \quad (2.27)$$

نو باور لري $d \mid a_1, \ldots, a_n$ ، یعنې $d \mid a_1$ ، او له $r_i = a_i - q_i a_1$ لاس ته راځي $d \mid r_i \;\; (i = 2, \ldots, n)$ ، دا په دې معناچې d د $a_1, r_2, \ldots, r_n$ یو ګډ پروېشونی دی. d' خورا لویه ده له دې لاس تخ راځي $\Rightarrow d \leq d'$

برعکس یا په خټ باور لري: d' $a_1, d' \mid r_i \;\; (i = 2, \ldots, n)$ وېشي،، یعنې داسې لاس ته راځي $a_i = q_i a_1 + r_i : d' \mid a_i \;\; (i = 2, \ldots, n)$ (د لیما یا جملګۍ 2.1.3 پسې)، یعنې d' د $a_1, \ldots, a_n$ ګډپروېشونی دی. d خورا لوی دی له دې لاس ته راځي $\Rightarrow d' \leq d \overset{3b}{\Rightarrow} d = d'.$.

یادونه : په پام کې دې وي: د دې تلنلار سره ګڼونه یا غددونه تل کوچني کیږي($0 \leq r_i < a_1$) او د امکان په حالت کې حتی کمیږي(کېدی شي $r_i = 0$ وي).

بېلګه 2.3.5 : $d = \text{ggT}(721, 613, 114)$.

(c) ketabton.com: The Digital Library

$a_1 = 114$ ، وېش له پاتې سره :

$$721 = 6 \cdot 114 + 37, 0 \leq 37 < 114$$

,

$$613 = 5 \cdot 114 + 43, 0 \leq 43 < 114$$

.

له دې سره: $d = \mathrm{ggT}(114, 37, 43)$.

$\tilde{a}_1 = 37$ ، وېش له پاتې سره:

$$114 = 4 \cdot 37 + 3, 0 \leq 3 < 37$$

,

$$43 = 1 \cdot 37 + 6, 0 \leq 6 < 37$$

.

له دې سره: $d = \mathrm{ggT}(37, 3, 6)$.

$\tilde{\tilde{a}}_1 = 3$ ، وېش له پاتې سره:

$$37 = 12 \cdot 3 + 1, \cdots \Rightarrow d = 1$$

.

۳ - لومړني ګڼونه(اعداد) Primzahlen

لومړني ګڼونه$\mathbb{P}$

(c) ketabton.com: The Digital Library

Die Menge der Primzahlen $\mathbb{P}$

بنسټونه *Grundlagen*

پېژند(تعریف) 3.1.1 : یو طبیعي ګڼ یا عدد p لومړنی بلل کیږي، که هغه فقط ساده پروېشوني ولري، دا په دې معنا، چې فقط $\pm 1, \pm p$ پروېشوني دي.

د ټول لومړنیو اعدادو ډېرۍ د $\mathbb{P}$ سره په نخښه کوو.

جمله : (اویکلید) ناپای ډېر لومړني ګڼونه شته.

ښوونه: نیسو، چې $p_1, \ldots, p_n$ ټول لومړني اعداد دي چې شتون لري. جوړوو

$$N := p_1 \cdots p_n + 1. \quad (3.1)$$

ترڅېرني نیسو

$$M := \{q \in \mathbb{N} \mid q > 1 \text{ او } q \mid N\}, \quad (3.2)$$

نو $M \neq \emptyset$ دی، ځکه چې $N \in M$ (په ساده توګه $N > 1, N \mid N$). د ټول نظم اصولو سره یو خورا کوچنی توکی q شتونلري، دا په دې معنا، چې $q > 1$ او $q \mid N$. وښایې: q یو لومړنی عدد دی:

وي دې $t > 1$ د $t \mid q$ سره، نو د 2.1.3 پسي لاس ته راځی، چې $t \mid N \Rightarrow t \in M$. له $t \leq q$ ، q د $M \Rightarrow t = q$ خورا کوچنی توکی دی.

یعني q لومړنی ګڼ دی، له نیوني څخه لاس ته راځي: $\exists j : q = p_j$. له دې سره $q \mid N \ (q \in M)$ باولري او په ساده توګه :

(c) ketabton.com: The Digital Library

$$p_j \mid p_1 \cdots p_n \overset{2.1.3}{\Rightarrow} p_j \mid N - p_1 \cdots p_n = 1 \Rightarrow p_j \leq 1, \quad (3.3)$$

- تضاد□

د ټول لومړنيو اعدادو ټاکل، چې $\leq n$ دي ($n \in \mathbb{N}$ ورکړ شوی): د اراتوستنس[3.1] *Eratosthenes* غلبېل :

تر له 1 تر n پورې ټول ګڼونه وليکه، که ټول لومړني $\leq \sqrt{n}$ اعداد پېژندل شوي وي، نو سرې دې د ټولو دې لومړنيو ګڼونو په دېرواره کربنه راکاږي (تر پخپله لومړني $\leq \sqrt{n}$ عدد پورې)، اوس فقط لومړني ګڼونه پاتې دي.

بېلګه 3.1.3 : ټول له ≤ 50 لومړني عددونه وټاکی. د $\sqrt{50} < 8$ او $2, 3, 5, 7$ له امله ټول لومړني < 8 عددونه لاس ته راځي(≤ 50 جوړه اعداد کېدی شي تر 2 پورې لري شي):

$2, 3, 5, 7, \not{9}, 11, 13, \not{15}, 17, 19, \not{21}, 23, \not{25}, \not{27}, 29, 31, \not{33}, \not{35},$

$37, \not{39}, 41, 43, \not{45}, 47, \not{49}$

ټول اعداد چې کربنه په راکښل شوې نه ده لومړني اعداد دي او ≤ 50 دي.

يادونې 3.1.4 :

لومړی: د دې لپاره چې ايا يو عدد پريم دی، که نه، يوه اغيزمنه – يا اقتصادي تلنلار نه شته(لږ تر لږه تر اوسه، وګوری[Gut02b, Rie94])، کارونه يا استعماليې په کريپتولوژي Kryptologie کې کيږي.

(c) ketabton.com: The Digital Library

دویم: د لومړنیو ګڼونو جمله:

که $\pi(x)$ د لومړنیو ګڼونو $\leq x\ (x \in \mathbb{N})$ ګڼون یا تعداد وي ، نو باور لري

(3.4)	$\pi(x) \sim \frac{x}{\ln x}$

دریم: د لویې $x \in \mathbb{N}$ لپاره

نږدې:

$$\pi(100) \sim 178; \pi(1000) \sim 1247; \pi(10000) \sim 9360$$

څلورم : لومړني اعداد په طبیعي اعدادو کط ډېر نامنظم خواره دي، له یوې خوا یو په بل پسې لومړني ګڼونه شتون لري، چې د هغو کمښت 2 دی، داسې په نامه د لومړنیو اعدادو غبرګوني: (اټکل کیږي، چې ناپای ډېر د لومړنیو اعدادو غرګوني شتون لري، د دې لپاره [HL22], [Gut02a] وګورئ).

له بلې خوا د دوه لومړنیو اعدادو ترمنځ په خوښه لویې تشیاوې شتون لري:وي دې $n \in \mathbb{N}$ ، نو $(n+1)! \quad +(n+1)$ $(n+1)!+2, \dots,$ ګڼونه همدا اوس n یو په بل پسې اعداد دي، چې لومړني اعداد نه دی، ځکه چې:

که $g = (n+1)! + k$ د $2 \leq k \leq n+1$ سره وي، نو باور لري

$k \mid k, k \mid (n+1)!$ له دې لاس ته راځي $\overset{2.1.3}{\Rightarrow} k \mid g$ ، کوم ته چې

(c) ketabton.com: The Digital Library

او $k \neq 1\ (2 \leq k)$ $k \neq g\ (g = (n+1)! + k > k)$ (د اعدادو پرلپسي.

کېدی شي لا له پخوا رامنځ ته شي، لکه د $n = 4$ لپاره $24 - 27$ دی دا همدا

اوس یوه تشیا ده، لکه چي غوښتل مو چېرته چي $27 \ll (4+1)! + 2$ دی).

پنځم : د دیریښلیت Dirichlet[3.2] جمله : که $a, b \in \mathbb{N}$ وي د $\text{ggT}(a, b) = 1$ سره، نو ډېری دا لاندي خوندي لري

$$\{ak + b \mid k = 1, 2, \ldots\} \quad (3.5)$$

ناپای ډېر لومړني اعداد. (د اریتمیتیکي پروګرشن لپاره د لومړنیو اعدادو جمله، ثبوت یې ډېره پېچلې ده!)

د $\{4k + 1 \mid k = 1, 2, \ldots\}$ لپاره ، همداسي $\{4k + 3 \mid k = 1, 2, \ldots\}$ لپاره لږ څه وروسته ښایو(جمله 9.2.8 همداسي جمله 3.1.10 وګورئ).

شپږم: د $2^{2^n} + 1 (n \in \mathbb{N})$ بڼي عدد د فرمات عدد *Fermat'sche Zahl*[3.3] بلل کیږي، د $n = 0, 1, 2, 3, 4$ لپاره په رېښتوني لومړني اعداد دي:
$3, 5, 17, 257, 65.537$
.

له دې پسي چا نور د فرمات اعداد بیدا نه کړل. تر اوسه معلومه نه ده، چي ایا پای او که ناپای ډېر فرمات ګڼونه شتون لري. د فرمات کوچنی عدد، چي تراوسه یې څوک ترتیبولی نه شي F_{33} دی.

(c) ketabton.com: The Digital Library

اوم : يو د $2^n - 1 \ (n \in \mathbb{N})$ بڼي عدد د مرزن عدد *Mersenne'sche Zahl*[3.4] بلل کيږي. د دې ډول ټول اعداد لومړني اعداد نه دي. دلته هم روښانه نه ده، چې ايا پای ډېر مرزن ګڼونه شتون لري. دا تراوسه خورا ستر لومړنی عددد مرزن عدد دی، داسي نامېز $p = 2^{13.466.917} - 1$.

اتم: د ګولدباښ ګومان : هر جوړه عدد له څلور سره برابر يا ترې لوی وي د دوه لومړنيو اعدادو د زياتون يا جمعي په څېر انځورېږ دی. (د بېلګي په توګه $4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, \ldots$). د عدد 1742 په هکله ګومان کېدی شي نه تراوسه وښوول شي او نه رد شي.

جمله3.1.5 : که $a_1, \ldots, a_n \in \mathbb{Z}$ وي او p يو لومړنی عدد د $p \mid a_1 \cdots a_n$ سره وي، نو لږ تر لږه p د ضريبونن يا څلوونو $a_i, 1 \le i \le n$ څخه يو وېشي.

ښوونه: د n پسي ايندکشن:

$n = 1$:ساده دی.

$n \to n + 1$:

وي دې $p \mid a_1 \cdots a_n a_{n+1}$ ، باور لري $p \mid a_{n+1}$ ، نو وښوول شو. پرته له دې: نو $p \nmid a_{n+1}$ $\mathrm{ggT}(p, a_{n+1}) = 1$ دی، داسي چې د بنسټيزې جملګی[2.2.12] څخه لاس ته راځي، چي $p \mid a_1 \cdots a_n$. د ايندکشن د نيوني يا فرضيي څخه لاس ته راځي $p \mid a_i$ د $1 \le i \le n$. لپاره.

□

(c) ketabton.com: The Digital Library

لاس ته راوړنه3.1.6 : د $n = 2$ لپاره باور لري: د p $a_1 \cdot a_2$ یو پروپښونی دی، p لومړنی ګڼ له دی لاس ته راځي $p \mid a_1 \vee p \mid a_2 \vee p \mid a_1, a_2$. په ځتوالی یا

معکوسوالی هم باور لري: که g یو طبیعي عددد وی د،،

$g \mid a_1 \cdot a_2 \ (a_1, a_2 \in \mathbb{Z})$ سره، نو تل دواړه $g \mid a_1 \vee g \mid a_2 \vee$ لاس ته راځي،،

، نو g بیا یو لومړنی ګڼ دی.

ښوونه: نیسو، چې g لومړنی عدد نه دی، نو g بیا اصلي پروپشوني لري، دا په دې معنا چې $g = a \cdot b$ ، چېرته چې $1 < a < g, 1 < b < g$ دي . نو باور لري: $g \mid a \cdot b$ ، یعني د نیوني له مخې $g \mid a \vee g \mid b$. که $g \mid a$ وي، نو د $a \mid g \ (g = a \cdot b)$ سره لاس ته راځي، چې $g = \pm a$ - تضاد.

که $g \mid b$ وي، نو په ورته توګه لاس ته راځي $g = \pm b \Rightarrow g$ ، چېg باید لومړنی وي.

□

نور خویونه Weitere Eigenschaften

جمله 3.1.7 : (لومړني ضریبتوته ونه یا په لوړنیو ضریبونو توټه کونه) هر طبیعي عدد $n > 1$ کېدی شي په یواځني ډول د لومړنیو عددونو دضرب په څېر ولیکل شي(دا په دې معنا ، چې لومړني ګڼونه د $\mathbb{N}$ ضربیي جوړښتخښتې دي).

ښوونه:

شتونوالی:

(c) ketabton.com: The Digital Library

په n پسې د (ټولیز شوي) ایندکشن Induktion له لارې:

: $n = 2$

ساده

: $n-1 \to n:$

ښايو: جمله د $2,3,\ldots,n-1$ لپاره ټیک ده.

نسیده، نیسو چې$\exists k : 2 \leq k \leq n-1$ ، کوم چې د لومړنیو ګڼونو یا عددونوضرب نه دی. وي دې k_0 د دوی ترمنځ خورا کوچنی عدد. نو k_0 لومړنی عدد نه دی. یعنې که باور ولري $k_0 = a \cdot b$ ، چېرته چې $a < b < k_0$ ، له دې سره لاس ته راځی:

a او b هر یو د لومړنیو ګڼونو ضرب دی، له دې امله k_0 هم د لومړنیو ګڼونو ضرب دی – تضاد!

وښايي: n د لومړنیو عددونو ضرب نه دی.

که n لومړنی عدد وي، نو موږ کار تمام کړ.

که n لومړنی عدد نع وي، نو$n = cd$ باور لري د $1 < c, d < n$ سره. د پورته پام کوني څخه جمله د c, d لپاره ټیک ده، دا په دې معنا چې c, d هر یو د لومړنیو عددونو ضرب دی، یهنې هم $n = c \cdot d$.

یواخېوالی یا یواځنوالی:

وي دې $n > 1$ او

(3.6)	$n = p_1 \cdots p_r = q_1 \cdots q_s$

(c) ketabton.com: The Digital Library

د کومو سره چې $p_i, q_j \in \mathbb{P}, r \leq s$. د $p_1 \mid p_1 \cdots p_r$ له امله لاس ته راځي $p_1 \mid q_1 \cdots q_s$ ، د 3.1.5 پسې لرو $p_1 \mid q_i$ (p_1 لومړنی عدد) د لږ تر لږه یوې i لپاره د $1 \leq i \leq s$ سره ، له دې امله $p_1 = \pm 1$ یا $p_1 = \pm q_i$ (q_i لومړنی عدد) ، یعنې $p_1 = q_i$ (p_1 لومړنی عدد دی، یعنې > 1) . د نمره بدلون سره کېدی سرې لاس ته راوړي: $p_1 = q_1 \ (q_i \rightarrow q_1)$. له دې سره لاس ته راځی

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \Leftrightarrow p_2 \cdots p_r = q_2 \cdots q_s; \quad (3.7)$$

په ورته توګه‌مخ ته ځو، تر $p_r = q_r, 1 = q_{r+1} \cdots q_s$ پورې.

که $s > r$ وی نو باور لري چې q_{r+1} بنی خوا وېشي: $q_{r+1} \mid 1$ ،یعنې $q_{r+1} \leq 1$ ، و q_{r+1} ته تضاد چې لومړنی عدد دی له دې لاس ته راځي $\Rightarrow s = r$ او له دې سره $p_i = q_i, 1 \leq i \leq r$.

یادونه 3.1.8 : که $g \in \mathbb{Z}$ وي د $g < -1$ سره، نو $-g > 1$ دی او د 3.1.7 پسې $-g = p_1 \cdots p_r$ د ځنو ، یواځنیو، لومړنیو ضزیبونو لپاره، یعنې $g = -p_1 \cdots p_r$.

یادونه 3.1.9 : که د $n > 1,$ د لومړنیو ضریبونو توته کونه سره یوځای کړو

$$n = p_1 \cdots p_r \quad (3.8)$$

مساوي ععدونه سره یوځای کړو، نو د لومړنیو عددونو توان لاس ته راځی، یعنې

(c) ketabton.com: The Digital Library

(3.9)	$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \alpha_i \in \mathbb{N}.$

که دا دلته نه شتون لرونکو لومړنیو عددونه د p $p^0 := 1$ له لارې پوره کړو، نو سرې لیکلی شي:

$$n = \prod_{p \in \mathbb{P}} p^{\alpha_p} \quad (3.10)$$

(د ټول لومړنیو عددونو ضرب، فقې پای ډېر $\alpha_p \neq 0$!). له دې سره $1 = \prod_{p \in \mathbb{P}} p^0$ هم لیکلی شو. یعنې د په ټولیزه توګه د ټول $g \in \mathbb{Z}, g \neq 0$ لپاره باور لري :

$$g = \pm \prod_{p \in \mathbb{P}} p^{\alpha_p} \qquad (\alpha_p \in \mathbb{N}_0). \quad (3.11)$$

جمله 3.1.10 (دیریښلیت) د $4k + 3 \; (k = 0, 1, \dots)$ بڼې ناپای ډېر لومړني ګڼونه شتون لرى، دا به دې معنا ، چې د $\{3, 7, 11, 15, 19, \dots\}$ عدونو په ډېرئ کې ناپای ډېر لومړني عددونه شتون لرى..

ښوونه: نیسو چې په دې ډول ډېر لومړني عددونه شتون لري، چې د $p_1, \dots, p_s$ سره یې سرې په نخښه کولی شي. سرې جوړوي

$$N := p_1^2 \cdots p_s^2 + 2; \qquad (3.12)$$

(c) ketabton.com: The Digital Library

د نیونې یا فرضیې له مخې د ځنو $k_i \in \mathbb{N}_0\ (i = \mathbf{1}, \dots, s)$ لپاره $p_i = 4k_i + 3$ باور لري، یعني

(3.13	$p_i^2 = (4k_i + 3)^2 = 16k_i^2 + 24k_i + 9 = 4k + 1$

د یوه k لپاره. له دې امله $(4k+3)(4l+3) = 4m+1$ د یوه $m \in \mathbb{N}$ لپاره.

له دې امله $N := p_1^2 \cdots p_s^2 + 2$ بڼه $(4n+1) + 2 = 4n+3$ لري.

وې دې $N = q_1 \cdots q_r$ د $N \in \mathbb{N}\ (N > 1)$ په لومړنیو ګڼونو ټوټه ونه. نه ټول q_i د بڼې $4k+1$ دي(ځکه چې بیا به N هم له دې بڼې وی). له دې امله q_j ، $1 \leq j \leq r$ یو شتون لري د بڼې $q_j = 4k+3$ سره(د پاتې سره وېشنه راکوي: $0 \leq a < 4$ ، یعني $q_j = 4 \cdot k + a$.

مګر $4k+0$ او $4k+2$ لومړني عددونه نه دي . $4k+1$ که همدا اوس ترې دباندې دی. 2 د ضریب په حیث نه رامنځ ته کیږي، ځکه چې $N = 4k+3$ ناجوړه دی).

لاس ته راځي: $q_j = p_i$ د یوه $i\ (1 \leq i \leq s)$ لپاره چېرته چې لرو $q_i \mid N$ او

$$q_j = p_i \mid p_1^2 \cdots p_s^2 \Rightarrow q_j \mid N - p_1^2 \cdots p_i^2 \cdots p_s^2 = 2, \quad (3.14)$$

یعني $q_j \leq 2$ - تضاد ($q_j = 4k + 3 \geq 3$).

(c) ketabton.com: The Digital Library

□

د ggT او kgV ترمنځ اړیکې(د خ غ ګ او خ ک ګ زیاتځلي - -

جمله3.2.1 : وي دې $a=\prod_{p\in\mathbb{P}} p^{\alpha_p}$ ، $b=\prod_{p\in\mathbb{P}} p^{\beta_p}$ ، نو باور لري

$$\mathrm{ggT}(a,b)=\prod_{p\in\mathbb{P}} p^{\min(\alpha_p,\beta_p)}. \quad (3.15)$$

ښوونه: ښايو: وی دی $x=\prod_{p\in\mathbb{P}} p^{\rho_p}, y=\prod_{p\in\mathbb{P}} p^{\sigma_p}$ ، نو باور لري:

$$x\mid y \Leftrightarrow \rho_p\le\sigma_p\ \forall p\in\mathbb{P}$$

$(\Rightarrow)$ يا له ذدې لاس ته راځي

$$x\mid y\Rightarrow y=x\cdot z$$
،

د $z=\prod_{p\in\mathbb{P}} p^{\tau_p}$ سره په لومړنيوضريبونو توټه کوني په حيث، يعنې

$$\prod_{p\in\mathbb{P}} p^{\rho_p+\tau_p}=\left(\prod_{p\in\mathbb{P}} p^{\rho_p}\right)\left(\prod_{p\in\mathbb{P}} p^{\tau_p}\right)=xz=y=\prod_{p\in\mathbb{P}} p^{\sigma_p}. \quad (3.16)$$

په لومړنيوضريبونو توټه کوني د يواخيوالي په بنسټ لاس ته راځيعددونو په

$$\rho_p+\tau_p=\sigma_p\ \forall p\in\mathbb{P}; \quad (3.17)$$

(c) ketabton.com: The Digital Library

د 1.1.4 پسې لاس ته راځي $\rho_p \leq \sigma_p \ \forall p \in \mathbb{P}$.

$(\Leftarrow)$

$\rho_p \leq \sigma_p \ \forall p \in \mathbb{P}$ ، نو د1.1.4 پسې باور لري:

$$\sigma_p = \rho_p + \tau_p \ \ \tau_p \in \mathbb{N}_0 \ \forall p \in \mathbb{P}. \quad (3.18)$$

وي دې $z := \prod_{p \in \mathbb{P}} p^{\tau_p}$ ، نو لاس ته راځي:

$$xz = \left(\prod_{p \in \mathbb{P}} p^{\rho_p}\right)\left(\prod_{p \in \mathbb{P}} p^{\tau_p}\right) = \prod_{p \in \mathbb{P}} p^{\rho_p + \tau_p} = \prod_{p \in \mathbb{P}} p^{\sigma_p} = y, \quad (3.19)$$

يعنې $xz = y \Rightarrow x \mid y$.

وي دې $d := \mathrm{ggT}(a, b)$ او $d = \prod_{p \in \mathbb{P}} p^{\gamma_p}$ ، د $d \mid a, b$ له امله باور لري $\gamma_p \leq \alpha_p, \beta_p \ \forall p \in \mathbb{P}$. له دې سره $\gamma_p \leq \min(\alpha_p, \beta_p)$. برعکس له

$$\min(\alpha_p, \beta_p) \leq \alpha_p, \beta_p \ \forall p \in \mathbb{P}, \quad (3.20)$$

څخه لاس ته راځي، چې عدد $c := \prod_{p \in \mathbb{P}} p^{\min(\alpha_p, \beta_p)}$ عددونه a, b ويشي، د جملې2.2.5 او جملګی یا کورولار 2.2.11 څخه $c \mid d$ لاس ته راځي، دا په دې معن،

(c) ketabton.com: The Digital Library

چې $\min(\alpha_p, \beta_p) \leq \gamma_p \; \forall p \in \mathbb{P}$. يعني د اکسيوم 3b سره لاس ته راځي $\gamma_p = \min(\alpha_p, \beta_p) \; \forall p \in \mathbb{P}$.

له دې سره د لومړنيوضريبونو يواځيوالي سره لاس ته راځي، چې $c = d$ ، دا په دې معنا، چې

$$\mathrm{ggT}(a, b) = \prod_{p \in \mathbb{P}} p^{\min(\alpha_p, \beta_p)}. \; (3.21)$$

بېلګه 3.2.2 : وي دې $a = 2^2 \cdot 3^4 \cdot 5^2, b = 2^3 \cdot 3^2 \cdot 7^3$ ، نو د نا شتونو لومړنيو ګڼونو د پوره کېدنې له امله د 0 اکسپننت له لارې باور لري:

$$a = 2^2 3^4 5^2 7^0, b = 2^3 3^2 5^0 7^3$$

$$\Rightarrow \mathrm{ggT}(a, b) = \prod_{p \in \mathbb{P}} p^{\min(\alpha_p, \beta_p)} = 2^2 3^2 5^0 7^0 = 2^2 3^2. \; (3.22)$$

کورولار يا جمګې3.2.3 :

لومړی :

وي دې $a_i \in \mathbb{N}, sei \;\; a_i = \prod_{p \in \mathbb{P}} p^{\alpha_{i,p}}, \;\; i = 1, \ldots, n$ د لومړنيوضريبونو توټه کونه، نو باور لري

$$\mathrm{ggT}(a_1, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{\min\limits_{1 \leq i \leq n} (\alpha_{i,p})}. \; (3.23)$$

(c) ketabton.com: The Digital Library

دويم : وي دې $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}, b = \prod_{p\in\mathbb{P}} p^{\beta_p}$ ، نو باور لري

$\mathrm{ggT}(a_1, \ldots, a_n) = 1 \Leftrightarrow \min(\alpha_p, \beta_p) = 0 \; \forall p \in \mathbb{P}.$	(3.24)

تعريف3.2.4 : وي دې، نو $v \in \mathbb{Z}$ د a, b ګډ ډېرځله (مضرب مشترک)بلل کيږي، که $a \mid v$ او $b \mid v$ وي(داپه دې معناچې $v = xa = yb$ د ځنو $x, y \in \mathbb{Z}$ سره).

يادونه3.2.5 : $a \cdot b$ او $|a| \cdot |b|$ هر يو د a, b ګډ ډېرځله دي، دا په دې معنا، چې هم کميز او هم زياتيز يعنې منفي او مثبت ګډ ډېرواره يا ګډ ډېرځله شتون لري.

که د a, b د ټول مثبتو ګډ ډېرځلو ډېرۍ په پام کې ونيسو، نو دا ډېرۍ د پورته يادونو په بنسټ هم تشه نه ده، دا د اکسيم 4 په بتسټ هم دا ډېرۍ کوچنۍ توکی لري. نو کړی شو تعريف کړو:

پيژند(تعيف)3.2.6 : وي دې $a, b \in \mathbb{Z}$ ، دواړه د ضفر سره نابرابر، نو د a, b د ټولو مثبتو خورا کوچنيو ګډ زياتځلو د $\mathrm{kgV}(a, b)$ سره په نخښه کوو.

که له دې ګڼونو يو صفر وي، يا دواړه، نو تعريفوو $\mathrm{kgV}(a, b) := 0$.

يادونه3.2.7 : شرايط (مثبت) مهم دي، ځکه چې پرته له دې بايد نه دی، چې خورا کوچنی ګډ زياتځله شتون ولري. وي دې $a = 2, b = 3$ ، نو ټول $v = -6, -12, -18, \ldots$ د a, b ګډ پرويشوني دي.

جمله3.2.8 : $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ ، $b = \prod_{p\in\mathbb{P}} p^{\beta_p}$ دې ورکړ شوي وي، نو باور لري

(c) ketabton.com: The Digital Library

$$\mathrm{kgV}(a,b)=\prod_{p\in\mathbb{P}} p^{\max(\alpha_p,\beta_p)}. \quad (3.25)$$

ښوونه: وي دې $v=\prod_{p\in\mathbb{P}} p^{\max(\alpha_p,\beta_p)}$ ، نو $v>0$ دی. له

(3.26)	$\alpha_p,\beta_p \le \max(\alpha_p,\beta_p)$

امله د جملې 3.2.1 ښوونه پسې باور لري، چې

(3.27)	$a \mid v, b \mid v.$

که $c=\prod_{p\in\mathbb{P}} p^{\gamma_p}$ د a,b يو ګډ زياتځله وي(c په خوښه، زياتيز)، نو له $a \mid c,$ $b \mid c:$ $\alpha_p \le \gamma_p, \beta_p \le \gamma_p$ او $\max(\alpha_p,\beta_p) \le \gamma_p \ \forall p \in \mathbb{P}$ لاس ته راځي.

يعني باور لري: $v \le c$ ، دا په دې معنا، چې ($v>0$ ، $c>0$) د ليما(5)2.1.3 له لارې دي. نو له دې سره v د a,b خورا کوچنی ګډ زياتځله دی، يعني

$$\mathrm{kgV}(a,b)=\prod_{p\in\mathbb{P}} p^{\max(\alpha_p,\beta_p)}$$

بېلګه 3.2.9 : وي دې $a=2^3 3^2 5, b=2^2 3^3 7$ ، نو

$$a=2^3 3^2 5^1 7^0, b=2^2 3^3 5^0 7^1$$

(c) ketabton.com: The Digital Library

$$\Rightarrow \mathrm{kgV}(a,b) = 2^3 3^3 5^1 7^1 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$$

کورولار (جمله گۍ)3.2.10 : وي دې $a, b \in \mathbb{Z}$ ، $v \leq 0$ ، نو $\mathrm{kgV}(a,b)$ ټيک هلته دی، که وي

1. $a \mid v, b \mid v$
2. له $a \mid c, b \mid c \Rightarrow v \mid c$

د $a_1, \ldots a_n$ لپاره په ټوليزه توگه:

تعريف 3.2.11 : وي دې $a_1, \ldots, a_n \in \mathbb{Z}$ ، نو $v \in \mathbb{Z}$ د $a_1, \ldots, a_n$ يو گډ زياتځله بلل کيږي، که $a_i \mid v, i = 1, \ldots, n$.

وي دې $a_i \neq 0, i = 1, \ldots, n$ ، نو دا د ټول مثبتو خورا کوچنيو گډزياتځله د $\mathrm{kgV}(a_1, \ldots, a_n)$ سره په نخښه کوو (شتون و حالت $n = 2$ ته ورته مدلل وړ دی)

که لږ تر لږه يو $a_i = 0$ وي، نو سرې تعريفوي $\mathrm{kgV}(a_1, \ldots, a_n) := 0$.

يادونه3.2.12 : د $\mathrm{kgV}(a_1, \ldots, a_n) = \mathrm{kgV}(|a_1|, \ldots, |a_n|)$ له امله کېدی شي دا حالت په باندې $a_1, \ldots, a_n \in \mathbb{N}$ محدود شي.

کورولار(حمله گۍ)3.2.13 : وي دې $a_1, \ldots, a_n \in \mathbb{Z}, a_i = \prod_{p \in \mathbb{P}} p^{\alpha_{i,p}}$ په لړمړنی ضريب توټه کونه، نو باور لري ($a_i \neq 0 \ \forall i$) :

(c) ketabton.com: The Digital Library

(3.28)	$$\mathrm{kgV}(a_1,\ldots,a_n)=\prod_{p\in\mathbb{P}} p^{\max\limits_{1\le i\le n}(\alpha_{i,p})}.$$

د ggT او kgV (خ غ پ او خوک ز)د اړیکې په هکله بالاخره لاندې جمله معلومات راکوي:

جمله 3.2.14 : وي دې $a_1,\ldots,a_n\in\mathbb{N}$ او په نخښه کړه $A_i:=\frac{a_1\cdots a_n}{a_i}$، $(i=1,\ldots,n)$. نو باور لري:

(3.29)	$$\mathrm{kgV}(a_1,\ldots,a_n)\cdot\mathrm{ggT}(A_1,\ldots,A_n)=a_1\cdots a_n.$$

ښوونه : وي دې $a_i=\prod\limits_{p\in\mathbb{P}} p^{\alpha_{i,p}}, i=1,\ldots,n$. نو باور لري

$$A_i=\prod_{p\in\mathbb{P}} p^{\sum\limits_{j\neq i}\alpha_{j,p}}, i=1,\ldots,n$$

او

$$\mathrm{ggT}(A_1,\ldots,A_n)=\prod_{p\in\mathbb{P}} p^{\min\limits_{1\le i\le n}(\sum\limits_{j\neq i}\alpha_{j,p})},\quad (3.30)$$

$$\mathrm{kgV}(a_1,\ldots,a_n)=\prod_{p\in\mathbb{P}} p^{\max\limits_{1\le i\le n}(\alpha_{i,p})},\quad (3.31)$$

$$a_1\cdots a_n=\prod_{p\in\mathbb{P}} p^{\sum\limits_{i=1}^{n}\alpha_{j,p}}.\quad (3.32)$$

وي دې $\alpha_{i_0,p}=\max\limits_{1\le i\le n}(\alpha_{i,p})$ ، نو باور لري $\alpha_{i,p}\le\alpha_{i_0,p}, i=1,\ldots,n$ یعني

$-\alpha_{i_0,p}\ \le\ -\alpha_{i,p}$ او

(c) ketabton.com: The Digital Library

$$\sum_{j=1}^{n}\alpha_{j,p}-\alpha_{i,p}\geq\sum_{j=1}^{n}\alpha_{j,p}-\alpha_{i_0,p}, \quad (3.33)$$

دا په دې معنا، چې $\sum_{j\neq i}\alpha_{j,p}\geq\sum_{j\neq i_0}\alpha_{j,p}, i=1,\ldots,n$ ،

نو $\min_{1\leq i\leq n}(\sum_{j\neq i}\alpha_{j,p})=\sum_{j\neq i_0}\alpha_{j,p}$. له دې سره:

$$\mathrm{kgV}(a_1,\ldots,a_n)\,\mathrm{ggT}(A_1,\ldots,A_n)=\prod_{p\in\mathbb{P}}p^{\alpha_{i_0,p}+\sum_{j\neq i_0}\alpha_{i_0,p}}= \quad (3.34)$$

$$=\prod_{p\in\mathbb{P}}p^{\sum_{i=1}^{n}\alpha_{i,p}}=a_1\cdots a_n. \quad (3.35)$$

جملگی3.2.15 : دا یو امکان دی ، چې د لویو گڼو یا عددونو $\mathrm{kgV}(a_1,\ldots,a_n)$ لپاره و شمېرو ($=\frac{a_1\cdots a_n}{\mathrm{ggT}(A_1,\ldots,A_n)}$ ، چېرته چې $\mathrm{ggT}(A_1,\ldots,A_n)$ د وېش له لارې د پاتې سره شمېرل کیږي).

بېلگه 3.2.16: $\mathrm{kgV}(6,8,15)=?$ ؟

(عددونه ډېر کوچني دي، دلته په لومړنیو ضریبونو ټوټه کونه ښه ده)

$$A_1=a_2a_3=120, A_2=a_1a_3=90, A_3=a_1a_2=48\Rightarrow$$

$$\Rightarrow\mathrm{ggT}(A_1,A_2,A_3)=\mathrm{ggT}(120,90,48)=6\Rightarrow$$

(c) ketabton.com: The Digital Library

$$\Rightarrow \mathrm{kgV}(6,8,15) = \frac{6 \cdot 8 \cdot 15}{6} = 120.$$

لاس ته راوړنه3.2.17 :

$n = 2, a_1, a_2 \in \mathbb{N};\ \mathrm{kgV}(a_1, a_2)\,\mathrm{ggT}(A_1, A_2) = a_1 a_2$ دا په دې معنا، چې

$\mathrm{kgV}(a_1, a_2)\,\mathrm{ggT}(a_1, a_2) = a_1 a_2$ ، نو لاس ته راځي:

$$\mathrm{kgV}(a_1, a_2) = a_1 a_2 \Leftrightarrow \mathrm{ggT}(a_1, a_2) = 1, \quad (3.36)$$

دا په دې معنا، چې د دوه ګڼونو a_1, a_2 خورا کوچنی ګډزیاتځله تیک هلته د هغو ضرب دی، که دا یو بل ته نسبي لومړني عددونه وي.

یادونه3.2.18 : په ټولیزه وګه: که $a_1, \ldots, a_n \in \mathbb{N}$ وي، نو $\mathrm{kgV}(a_1, \ldots, a_n) = a_1 \cdots a_n$ تیک هلته دی، که $a_i, i = 1, \ldots, n$ جوړه یو بل ته نسبي لومړني عددونه وي. (ښوونه د لومړنیو فاکتورونو ټوټه کوني سره کیږي)

کونګروانځ Kongruenzen

د کونګروانځ سره شمېرنه Rechnen mit Kongruenzen

که $a \in \mathbb{Z}, m \in \mathbb{N}$ وي، د پاتې سره وېش راکوي:

$$a = qm + r, 0 \leq r < m; \quad (4.1)$$

(c) ketabton.com: The Digital Library

یعني $a-r=qm$ ، دا به دې معنا، چې $m \mid a-r$.

بیژند(تعریف)4.1.1 : که وي $a,b \in \mathbb{Z}, m \in \mathbb{N}$ په خوښه، نو a,b کونګروانځ مودولو m بلل کیږي، که $m \mid a-b$ ، سومبولیک یا لیکندود $a \equiv b(m)$.

بېلګه 4.1.2 : $6 \equiv 24(9)$ ، ځکه چې $9 \mid 24-6=-18$

$14 \equiv -1(5)$ ، ځکه چې $5 \mid 14-(-1)=15$.

لیما 4.1.3 : که وي $a,b \in \mathbb{Z}, m \in \mathbb{N}$ ، نو a,b تیک هلته کونګروانت مودولو m دي، که m د له لارې د پاتې سره په وېش کې دا یو د بل پاتې برابر دي.

ښوونه : وي دې $a=qm+r, 0 \le r < m$ او $b=q'm+r', 0 \le r' < m$

(د پاتې سره وېش). ښایو: $a \equiv b(m) \Leftrightarrow r=r'$

$(\Leftarrow)$

$r=r'$:

(4.2) $$a-b=(qm+r)-(q'm+r')=(q-q')m+\underbrace{(r-r')}_{=0},$$

دا په دې معن، چې $m \mid a-b$ ، له دې $a \equiv b(m)$ باور لري.

(c) ketabton.com: The Digital Library

$(\Rightarrow)$

$a \equiv b(m)$:

$m \mid a-b=(q-q')m+(r-r') \overset{2.1.3}{\Rightarrow} m \mid r-r',$ (4.3)

وي، نو له $|r-r'| \leq 0$ باور لري . که $m=|m| \leq |r-r'|$ یعني
لاس ته راځي، چې $0 \leq r' < m$ ، $0 \leq r < m,$

$0 \leq r < m, -m < -r' \leq 0,$ (4.4)

نو لرو $-m < r-r' < m$ ، دا په دې معنا، چې $|r-r'| < m$ ـ تضاد!

له دې سره لاس ته راځي $|r-r'|=0$ ، یعني $r=r'.$.

یادونه : د,, $\equiv$ `` له لارې په $\mathbb{Z}$ د $m \in \mathbb{N}$ لپاره یو ورته اړیکي ، په خوښه مګر
کره ټاکلي، تعریف دي:

لومړی : (

1. (Reflexivität هندارونه) $a \equiv a(m)\ \forall a \in \mathbb{Z}$ ځکه,
چې $m \mid a-a=0$,
2. (Symmetrie سیوتري)
$a \equiv b(m) \Rightarrow m \mid a-b \Rightarrow m \mid b-a \Rightarrow b \equiv a(m)$
,
3. (Transitivität).

(c) ketabton.com: The Digital Library

$$a \equiv b(m), b \equiv c(m) \Rightarrow m \mid a-b, m \mid b-c$$

$$\overset{2.1.3}{\Rightarrow} m \mid (a-b)+(b-c) = a-c \Rightarrow a \equiv c(m)$$

ختی لا ډېر باور لري ($\equiv$ د $+$ او $\cdot$ سره زعموړ دی، د ،،کونګروانځ ،،کلمه دې پع الجبر کې پرتله شي)

لېما 4.1.5 : وي دې $a, b, c, d \in \mathbb{Z}, m \in \mathbb{N}$ په خوښه. نو باور لري

1. $a \equiv b(m), c \equiv d(m) \Rightarrow a+c \equiv b+d(m)$,
2. $a \equiv b(m), c \equiv d(m) \Rightarrow a \cdot c \equiv b \cdot d(m)$,
3. $a \equiv b(m), t \mid m \Rightarrow a \equiv b(|t|)$,
4. $a \equiv b(m), k \in \mathbb{Z}, k \neq 0 \Rightarrow ka \equiv kb(|k|m)$,
5. $ka \equiv kb(m)$ für ein $k \in \mathbb{Z}, d = \text{ggT}(k,m) \Rightarrow a \equiv b(\frac{m}{d})$,
6. $a \equiv b(m), a \equiv b(n), n \in \mathbb{N} \Rightarrow a \equiv b(\text{kgV}(m,n))$.

ښوونه:

1. $a \equiv b(m), c \equiv d(m) \Rightarrow m \mid a-b, m \mid c-d^{2}$

$l \overset{2.1.3}{\Rightarrow} m \mid (a-b)+(c-d) \Rightarrow (a+c) \equiv (b+d)(m)$

(c) ketabton.com: The Digital Library

$$a \equiv b(m), c \equiv d(m) \Rightarrow m \mid a-b, m \mid c-d \overset{2.1.3}{\Rightarrow} m \mid (a-b)c = ac-bc$$

$$m \mid (c-d)b = cb-db$$

,

$$\Rightarrow m \mid (ac-bc)+(cd+db) = ac-bd \Rightarrow ac \equiv bd(m)$$

.

$$a \equiv b(m) \Rightarrow m \mid a-b \Rightarrow t \mid a-b \Rightarrow a \equiv b(|t|)$$

.

$$a \equiv b(m) \Rightarrow m \mid a-b \Rightarrow km \mid k(a-b) = ka-kb \Rightarrow ka \equiv kb(|k|m)$$

$$ka \equiv kb(m) \Rightarrow m \mid ka-kb \Rightarrow k(a-b) = m \cdot s$$

1. لپاره $s \in \mathbb{Z}$ يوهد

$$\Rightarrow \frac{k}{d}(a-b) = \frac{m}{d} \cdot s \frac{m}{d} \Big| \frac{k}{d}(a-b), \qquad (4.5)$$

د کورولار يا جملګی(1)2.2.9 له امله باور ري:

$\operatorname{ggT}\left(\frac{m}{d}, \frac{k}{d}\right) = 1,$	(4.6)

نو د بنستيزې ليما 2.2.12 څخ لاس ته راځي:

$\frac{m}{d} \Big\| a-b \Rightarrow a \equiv b\left(\frac{m}{d}\right).$ $a \equiv b(m), a \equiv b(n)$	(4.7)

(c) ketabton.com: The Digital Library

(4.8)	$\Rightarrow m \mid a-b, n \mid a-b,$

دا په دې معنا، چې $a-b$ د m, n ګډ ډېرځله دی

(4.9)	$\Rightarrow \mathrm{kgV}(m,n) \mid a-b \Rightarrow a \equiv b(\mathrm{kgV}(m,n)).$

لومړی :

$$a \equiv b(m), c \in \mathbb{Z} \Rightarrow a+c \equiv b+c(m), ac \equiv bc(m)$$

$\equiv$ ، دا په دې معنا، چې د ترنو یاکارونو یا عملیو سره زغوړ دی(د ورته اړیکو یا کونګروانځ اړیکو په هکله دتر مخه تېر ي یادونې4.1.4 وکورئ) .

دویم :

$$a_i \equiv b_i(m), i=1,\ldots,k \Rightarrow a_1+\cdots+a_k \equiv$$
$$\equiv b_1+\cdots+b_k(m), a_1\cdots a_k \equiv b_1\cdots b_k(m)$$

(ښوونه د ایندکشن له لارې) .

دریم :

$$a_1=\cdots=a_k=a, b_1=\cdots=b_k=b \Rightarrow a^k \equiv b^k(m)\ \forall k \in \mathbb{N}$$

$a \equiv b(m), f(x)=c_0+c_1x+\cdots+c_kx^k$ د $c_i \in \mathbb{Z}$ سره، نو باور لري

$$f(a) \equiv f(b)(m)$$

(c) ketabton.com: The Digital Library

څلورم :

$$ka \equiv kb(m), \mathrm{ggT}(k,m) = 1 \Rightarrow a \equiv b(m)$$

(مګر له $4 \cdot 4 \equiv 4 \cdot 2(4)$ لاس ته نه اځي $3 \equiv 2(4)$!!!) .

پنځم :

$$ka \equiv kb(m), k \mid m \overset{4.1.5(5)}{\Rightarrow} a \equiv b\left(\frac{m}{|k|}\right)$$

شپږم :

$$a \equiv b(m), a \equiv b(n), \mathrm{ggT}(m,n) = 1 \Rightarrow a \equiv b(m \cdot n)$$

اوم :

$a \equiv b(m), m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ په لومړنيو ضريبونو ټوټه کونه

$$\Rightarrow a \equiv b(p_1^{\alpha_i}) \forall i = 1, \ldots, k$$

(ځکه چې $p_i^{\alpha_i} \mid m$)

اتم :

$a \equiv b(p_i^{\alpha_i}), i = 1, \ldots, k, p_i$ مختلف لومړني ګڼونه

(c) ketabton.com: The Digital Library

$$\Rightarrow a \equiv b(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) : a \equiv b(m)$$

د پروېشنوړوالي قوانينTeilbarkeitsregeln

هر يا يوه يا بل د پروېشنوړ قوانين پېژني. د دې قوانينو څخه زيات يې به روښانه ت وګه د لاندې جملې په بنسټ ولاړ دي.

جمله4.2.1 : $n = (a_k a_{k-1} \dots a_1 a_0)$ دې د $n \in \mathbb{N}$ ديکاديکي يا لسميزه انځوره وي. نو باور لري

1. $n \equiv a_0(2)$,
2. $n \equiv a_0 + \cdots + a_k(3)$,
3. $n \equiv a_0 + 10 \cdot a_1(4)$,
4. $n \equiv a_0(5)$,
5. $n \equiv (a_0 + 10a_1 + 10^2 a_2) - (a_3 + 10a_4 + 10^2 a_5) + - \cdots (7)$,

resp. (13),

6. $n \equiv a_0 + 10a_1 + 10^2 a_2(8)$,
7. $n \equiv a_0 + a_1 + \cdots + a_k(9)$,
8. $n \equiv a_0 - a_1 + a_2 - + \cdots + (-1)^k a_k(11)$.

ښوونه:

(c) ketabton.com: The Digital Library

لومړی: د $10 \equiv 0(2)$ له امله باور لري $10^i \equiv 0^i(2)\ \forall i \geq 1$ ، يعنې

$$n = a_0 + 10a_1 + \cdots + 10^k a_k \equiv a_0 + 0 \cdot a_1 + \cdots + 0 \cdot a_k(2) \Rightarrow n \equiv a_0(2). \quad (4.10)$$

دويم :

د $10 \equiv 1(3)$ له امله باور لري: $10^i \equiv 1^i(3)\ \forall i \geq 1$ ، يعنې

$$n = a_0 + 10a_1 + \cdots + 10^k a_k \equiv a_0 + 1 \cdot a_1 + \cdots + 1 \cdot a_k(3) \quad (4.11)$$

$$\Rightarrow n \equiv a_0 + a_1 + \cdots + a_k(3). \quad (4.12)$$

دريم :

د $10^2 \equiv 0(4)$ له امله باور لري $10^i \equiv 0^i(4)\ \forall i \geq 2$ ، يعنې

$$n = a_0 + 10a_1 + \cdots + 10^k a_k \equiv a_0 + 10a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_k(4) \quad (4.13)$$

$$\Rightarrow n \equiv a_0 + 10a_1(4). \quad (4.14)$$

څلورم د $10 \equiv 0(5)$ له امله باور لري $10^i \equiv 0^i(5)\ \forall i \geq 1$ ، يعنې

$$n = a_0 + 10a_1 + \cdots + 10^k a_k \equiv a_0 + 0 \cdot a_1 + \cdots + 0 \cdot a_k(5) \Rightarrow n \equiv a_0(5). \quad (4.15)$$

(c) ketabton.com: The Digital Library

پنځم :

1. د۱ - له امله

$$n = (a_0 + 10a_1 + 10^2a_2) + 10^3(a_3 + 10a_4 + 10^2a_5) + \quad (4.16)$$

$$+10^6(a_6 + 10a_7 + 10^2a_8) + \cdots \quad (4.17)$$

او $1001 = 10^3 + 1 = 7 \cdot 13$ باور لري: $10^3 \equiv -1(7, 13)$ ، نو هم

$(10^3)^i \equiv (-1)^i(7, 13)\ \forall i \geq 0$ ، داسې چې

$$n \equiv (a_0 + 10a_1 + 10^2a_2) + (-1)(a_3 + 10a_4 + 10^2a_5) + \quad (4.18)$$

$$(-1)^2(a_6 + 10a_7 + 10^2a_8) + \cdots (7, 13). \quad (4.19)$$

$10^i \equiv 0^i(8)\ \forall i \geq 3$

د $10^3 \equiv 0(8)$ له امله باور لري: ، نو

$$n = a_0 + 10a_1 + \cdots + 10^k a_k \equiv \quad (4.20)$$

$$\equiv a_0 + 10 \cdot a_1 + 10^2 \cdot a_2 + 0 \cdot a_3 + \cdots + 0 \cdot a_k(8) \quad (4.21)$$

(c) ketabton.com: The Digital Library

$$\Rightarrow n \equiv a_0 + 10a_1 + 10^2 a_2 (8). \qquad (4.22)$$

Modul 3 ($10 \equiv 1(9) \ldots$) ته ورته

له $10 \equiv -1(11)$ ا مله باور لري: $10^i \equiv (-1)^i (11) \ \forall i \geq 0$ ، نو

$$n = a_0 + 10a_1 + \cdots + 10^k a_k \equiv \qquad (4.23)$$

$$\equiv a_0 - a_1 + a_2 - + \cdots + (-1)^k \cdot a_k (11) \qquad (4.24)$$

$$\Rightarrow n \equiv a_0 - a_1 + a_2 - + \cdots + (-1)^k a_k (11). \qquad (4.25)$$

جمله ګې 4.2.2 : (پروېشنوڕ قوانين) که $n = (a_k \ldots a_0)_{10} \in \mathbb{N}$ وي، نو باور لري:

1. $2 \mid n \Leftrightarrow 2 \mid a_0$,
2. $3 \mid n \Leftrightarrow 3 \mid a_0 + \cdots + a_k$,
3. $4 \mid n \Leftrightarrow 4 \mid (a_1 a_0)_{10}$,
4. $5 \mid n \Leftrightarrow 5 \mid a_0$,
5. $7, 13 \mid n \Leftrightarrow 7, 13 \mid (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - + \cdots$,
6. $8 \mid n \Leftrightarrow 8 \mid (a_2 a_1 a_0)_{10}$,

(c) ketabton.com: The Digital Library

7. $9 \mid n \Leftrightarrow 9 \mid a_0 + \cdots + a_k$,

8. $11 \mid n \Leftrightarrow 11 \mid a_0 - a_1 + a_2 - + \cdots + (-1)^k a_k$.

ښوونه : د ښېلګي په توګه د دې لومړنيو درې راوړل شوي قوانين ښايو، نو ټول کېدی شي په ورته توګه وښوول شي.

$$2 \mid n \Leftrightarrow n \equiv 0(2) \qquad (4.26)$$

$$\Leftrightarrow^{1} a_0 \equiv n \equiv 0(2) \qquad (4.27)$$

$$\Leftrightarrow 2 \mid a_0. \qquad (4.28)$$

يادونه 4.2.3 : سرې کړی شي د معلومو پروېشقوانينو پسي وغزوي، که مودول نسبي لومړني وي.

لکه $m = 2, n = 3 \Rightarrow$

لاس ته راځي او

Etwa $m = 2, n = 3 \Rightarrow$ bzgl. 6 = bzgl. 2 und bzgl. 3 ($\mathrm{ggT}(2,3) = 1$).

Beispiel 4.2.4 $n = 97234382 \mid n$, da $2 \mid 8$; $3 \mid n$, da $3 \mid 36$; $4 \nmid n$, da $4 \nmid 38$; $5 \nmid n$, da $5 \nmid 8$; $6 \mid n$, da $2 \mid n, 3 \mid n \wedge \mathrm{ggT}(2,3) = 1$; $7 \nmid n$, da $7 \nmid (438 - 723 + 009) = -276$ $8 \nmid n$, da $8 \nmid 438$; $9 \mid n$, da

(c) ketabton.com: The Digital Library

$9 \mid 36$; $11 \nmid n$, da $11 \nmid (8-3+4-3+2-7+9) = 10$; $12 \nmid n$,
da $4 \nmid n$; . . .

پاتې ټولګي Restklassen

د4.1.3 له مخې باور لري: $a \equiv b(m)$ تیک هلته یا هلته او هلته، که د m سر د a
او b وېشني برابر پاتې ولري ($0 \leq r < m$) .

که ټول $a, b \in \mathbb{Z}$ د دې خویونو سره د یوې ډېرۍ په توګه سره یوځای کړو، نو سړی
داسي په نامه،، پاتې ټولګي،، لاس ته راوړي، فورمال د 4.1.4 پسي ،، $\equiv$ ،، په $\mathbb{Z}$
یو ورته اړیکه ده، یعني له دې سره د $\mathbb{Z}$ یو پارتیشن یا ټوټه کونه ورکړ شوې د پردیو
disjunkte ټولګیو $\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a(m)\}$ سره، داسې په نامه ورته ټولګي
Äquivalenzklassen ، دا په دې معنا، چې

1. $\overline{a} \neq \emptyset$,
2. $\overline{a} \cap \overline{b} = \emptyset \vee \overline{a} = \overline{b}$,
3. $\bigcup_{a \in \mathbb{Z}} \overline{a} = \mathbb{Z}$.

باور لري:

لومړی : د $\overline{a}$ څخه توکي بڼه $a + km$ لري(د $k \in \mathbb{Z}$ لپاره)، ځکه چې:

(c) ketabton.com: The Digital Library

د یوه $x \in \overline{a} \Leftrightarrow x \equiv a(m) \Leftrightarrow x - a = km$ $k \in \mathbb{Z} \Leftrightarrow x = a + km$ لپاره . له دې سره

$$\overline{a} = \{a + km \mid k \in \mathbb{Z}\} = a + m\mathbb{Z}$$ په خوښه

دویم : $\forall a \in \mathbb{Z} : \overline{a} = \overline{r}$ د کوم سره چې $r \in \mathbb{Z}$ په m باندې د a د وېشنې پاتې دی ($0 \le r < m$)، ځکه چې:

$$a = qm + r, 0 \le r < m \Leftrightarrow a - r = qm \Leftrightarrow$$

$$\Leftrightarrow m \mid a - r \Leftrightarrow a \equiv r(m) \Leftrightarrow \overline{a} = \overline{r}$$

.پېژند(تعریف)4.3.1 : وي دې $m \in \mathbb{N}$ په خوښه، نو ورته ــیا اکویوالنت ټولګی $\operatorname{mod} m$ یو پاتې ـټولګی$\operatorname{mod} m$ بلل کیږي. هر د$\overline{a}$ توکی د ټولګي $\overline{a}$ نماینده بلل کیږي. د ټول پاتې ټولګیو $\operatorname{mod} m$ ډېری د $\mathbb{Z}_m$ سره په نخښنه کیږي.

لیما 4.3.2 : د په خوښه $m \in \mathbb{N}$ لپاره باور لري: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$،
دا په دې معنا، چې $\mathbb{Z}_m$ m توکي لري.

ښوونه : که $\overline{a}$ په خوښه پاتې ټولګی وي، نو باور لري:

$$a = qm + r, 0 \le r < m, \quad (4.29)$$

(c) ketabton.com: The Digital Library

دا په دې معن، چې $0 \le r \le m-1$ ، دا په دې معناء چې زيات له زياته m مختلف پاتې ټولګي شتون لري.

که $\overline{r} = \overline{r'}, 0 \le r \le m-1, 0 \le r' \le m-1$ باور ولري، نو $r \equiv r'(m)$ باور لري ، په m باندې د r, r' د وېشني خخه r همداسي r' پاتې(که غواړی: باقي) پاتې کيږي، دا بايد د 4.1.3 پسي باور ولري: $r = r'$. برعكس: $r = r' \Rightarrow \overline{r} = \overline{r'}$. نو تيک m ټولګي شتون لري.

بېلګه4.3.3 : $m = 5 : \mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ ، څه:

$\overline{2} = \{2 + 5 \cdot k \mid k \in \mathbb{Z}\} = \{\ldots, -13, -8, -3, 2, 7, 12, \ldots\}$ ، نو په ځانګړې توګه

$$\overline{2} = \overline{17} = \overline{(-3)} = \cdots$$

پېژند (تعريف) 4.3.4: د $\mathbb{Z}$ يوه برخه ډېرى كومه چې له هر پاتې ټولګي ټيک يو توکی خوندي لري، نو پوره موډولو m پاتې سيستم بلل کيږي.

بېلګه4.3.5 : $m = 4, \mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}; \{0, 1, 2, 3\}$ يو پوره پاتې سيستم $\bmod 4$ دى، همداسي $\{4, -3, -2, 4\}$ يا $\{100, 99, 98, 97\}$.

ليما 4.3.6 : يوه برخډېرى $\{r_1, \ldots, r_m\} \subseteq \mathbb{Z}$ ټيک هلته يو پوره پاتې سيستم موډولو m دى، که $r_i \not\equiv r_j(m)\ \forall i, j = 1, \ldots, m : i \neq j$ وي.

ثبوونه:

(c) ketabton.com: The Digital Library

($\Rightarrow$)

که $\{r_1, \dots, r_m\}$ یو پوره پاتې سیستم وي، نو r_i، $i = 1, \dots, m$ په مختلفو پاتې ټولګیو $\bmod m$ کې پراته دي، نو باور لري $r_i \not\equiv r_j(m)$، $\forall i \neq j$.

($\Leftarrow$)

که باور ولري $r_i \not\equiv r_j \; \forall i \neq j$، نو r_i په مختلفو پاتې ټولګیو کې پراته دي، او ټول مختلف دي، نو $\{r_1, \dots, r_m\}$ یو پوره پاتې سیستم دی.

کورولار یا جمله ګی 4.3.7 : وې دې $\{r_1, \dots, r_m\} \subseteq \mathbb{Z}$ یو پوره پاتېسیستم مودولو m او $a, b \in \mathbb{Z}$ دې د $\text{ggT}(a, m) = 1$ سره وي، نو $\{ar_1 + b, \dots, ar_m + b\}$ هم یو پوره پاتې سیستم مودولو m دی.

ښوونه : نیسو چې $\exists i \neq j : ar_i + b \equiv ar_j + b(m)$، نو لاس ته رځي

$$ar_i \equiv ar_j(m), \quad (4.30)$$

او له دې سره د(4)4.1.6 له امله :

$$r_i \equiv r_j(m), \quad (4.31)$$

دا چې $\text{ggT}(a, m) = 1$ دی، نو تضاد ته ځو!

(c) ketabton.com: The Digital Library

نو له دې سره لاس ته راځي

$$ar_i + b \not\equiv ar_j + b \; \forall i \neq j, \quad (4.32)$$

او له 4.3.6 سره غوښتنه لرو.

جمله ګې4.3.8 : وي دې $\{r_1, \ldots, r_m\} \subseteq \mathbb{Z}$ يو پوره پاتې سيستم مودولو m ، $\{s_1, \ldots, s_n\} \subseteq \mathbb{Z}$ يو پوره پاتې سيستم مودولو n او $\mathrm{ggT}(m,n) = 1$ ، نو

$\{nr_1 + ms_1, \ldots, mr_m + ms_n\}$	(4.33)

$$\{nr_1 + ms_1, \ldots, mr_m + ms_n\} \quad (4.33)$$

يو پوره پاتې سيستم مودولو $m \cdot n$ دی.

ښوونه : نيسو، چې باور لري

$$nr_i + ms_j \equiv nr_k + ms_l (m \cdot n) \quad (4.34)$$

د ځنو $i \neq k$ همداسې $j \neq l$ لپاره يا دواړه. د $m \mid m \cdot n$ له امله لاس ته راځی:

$$nr_i + ms_j \equiv nr_k + ms_l (m), \quad (4.35)$$

له دې سره $nr_i \equiv nr_k (m)$.

له دې امله د لاس ته راوړنې پسې(4)4.1.6 لاس ته راځي: $r_i \equiv r_k (m)$ ځکه چې

$$\mathrm{ggT}(m,n) = 1 \quad \Rightarrow i = k$$

(c) ketabton.com: The Digital Library

د4.3.6 له مخي . له دې سره نيونه داسي ده:

$$nr_i + ms_j \equiv nr_i + ms_l(m \cdot n) \Rightarrow ms_j \equiv ms_l(m \cdot n), \quad (4.36)$$

نو $s_j \equiv s_l(n) \Rightarrow j = l$ دی دا د4.3.6له امله - تضاد دی □

د پاتې تولګي کړی یا -- رینګ $(\mathbb{Z}_m, +, \cdot)$

Der Restklassenring $(\mathbb{Z}_m, +, \cdot)$

په $\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}\}$ تعريفوو (توکي دي)

په $\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}\}$ (m توکي دي) يو زياتون يا جمعه $\oplus$ او يو ضرب يا ځل $\odot$ تعريفوو د لاندې سره:

$$\overline{a} \oplus \overline{b} := \overline{a+b} \quad \text{او} \quad \overline{a} \odot \overline{b} := \overline{ab}. \quad (4.37)$$

ښايو : دا تعريفونه د و وکيلانو (Repräsentanten) خپلواک دي، دا په دې معنا، چي $\overline{a} = \overline{a'}, \overline{b} = \overline{b'}$ ، نو $\overline{a+b} = \overline{a'+b'}$ هم باور لرياو همداسي $\overline{ab} = \overline{ab}$ هم .

$$\overline{a} = \overline{a'} \Rightarrow a \equiv a'(m), \overline{b} = \overline{b'} \Rightarrow b \equiv b'(m),$$

نو:

(c) ketabton.com: The Digital Library

$$\left.\begin{array}{rcl} a+b & \equiv & a'+b'(m), \\ a\cdot b & \equiv & a'\cdot b'(m) \end{array}\right\} \overset{4.1.5}{\Rightarrow} \overline{a+b}=\overline{a'+b'}, \overline{ab}=\overline{a'b'}.$$

نسبت جمعي $\oplus$ ته باور لري : $(\mathbb{Z}_m, \oplus)$ يو كموتاتيو ګروپ دی. ځكه چې :

1. $\overline{a} \oplus \overline{b} \in \mathbb{Z}_m$, ځكه چې

$\overline{a} \oplus \overline{b} = \overline{a+b} \in \mathbb{Z}_m \ \forall \overline{a}, \overline{b} \in \mathbb{Z}_m.$	(4.38)

$$\overline{a} \oplus \overline{b} = \overline{a+b} \in \mathbb{Z}_m \ \forall \overline{a}, \overline{b} \in \mathbb{Z}_m. \quad (4.38)$$

2. $\overline{a} \oplus (\overline{b} \oplus \overline{c}) = (\overline{a} \oplus \overline{b}) \oplus \overline{c} \ \forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, ځكه چې

$$a+(b+c)=(a+b)+c \Rightarrow \overline{a+(b+c)}=\overline{(a+b)+c}. \quad (4.39)$$

3. $\overline{0} \in \mathbb{Z}_m$ پوره كوي $\overline{a} \oplus \overline{0} = \overline{0} \oplus \overline{a} = \overline{a} \ \forall \overline{a} \in \mathbb{Z}_m$.

4. و $\overline{a} \in \mathbb{Z}_m$ ته $\overline{-a}$ زيلتيز يا مثبت معكوس دی، ځكه چې

$$\overline{a} \oplus \overline{-a} = \overline{-a} \oplus \overline{a} = \overline{0}. \quad (4.40)$$

5. $\overline{a} \oplus \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} \oplus \overline{a} \ \forall \overline{a}, \overline{b} \in \mathbb{Z}_m$.

نسبت ضرب $\odot$ ته باور لري : $(\mathbb{Z}_m, \odot)$ يو نيم ګروپ دی د 1 سره. ځكه چې:

(c) ketabton.com: The Digital Library

1. $\overline{a} \odot \overline{b} \in \mathbb{Z}_m$, ځکه چې

$$\overline{a} \odot \overline{b} = \overline{ab} \in \mathbb{Z}_m \; \forall \overline{a}, \overline{b} \in \mathbb{Z}_m. \quad (4.41)$$

2. $\overline{a} \odot (\overline{b} \odot \overline{c}) = (\overline{a} \odot \overline{b}) \odot \overline{c} \; \forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, ځکه چې

$$a(bc) = (ab)c \Rightarrow \overline{a(bc)} = \overline{(ab)c}. \quad (4.42)$$

3. $\overline{1} \in \mathbb{Z}_m$ پوره کوي $\overline{a} \odot \overline{1} = \overline{1} \odot \overline{a} = \overline{a} \; \forall \overline{a} \in \mathbb{Z}_m$.

4. $\overline{a} \odot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \odot \overline{a} \; \forall \overline{a}, \overline{b} \in \mathbb{Z}_m$.

5. $\overline{a} \odot (\overline{b} \oplus \overline{c}) = (\overline{a} \odot \overline{b}) \oplus (\overline{a} \odot \overline{c}) \; \forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$.

(ځکه چې: $a(b+c) = ab + ac \Rightarrow \overline{a(b+c)} = \overline{ab+ac}$.).

له دې سره $(\mathbb{Z}_m, \oplus, \odot)$ يو کموتاتيو رينګ (کړۍ) دی د 1 سره، داسې په نامه ،،پاتې ټولګي رينګ يا— - کړۍ) $\bmod m$ ،، دی. د $(\mathbb{Z}_m, \oplus, \odot)$ انځورونه د جدول په مرسته صورت نيسي يا لاس ته راځي. دا د $\mathbb{Z}_4$ لپاره په لاندې ډول ليدل کيږي:

(c) ketabton.com: The Digital Library

$arrayc\vert cccc\oplus\bar{0}$	$\overline{12}$	$\bar{3}$
$\overline{00}$	$\overline{12}$	$\bar{3}$
$\overline{11}$	$\overline{03}$	$\bar{2}$
$\overline{22}$	$\overline{30}$	$\bar{1}$
$\overline{33}$	$\overline{21}$	$\bar{0}$

$arrayc\vert cccc\odot\bar{0}$	$\overline{12}$	$\bar{3}$
$\overline{00}$	$\overline{00}$	$\bar{0}$
$\overline{10}$	$\overline{12}$	$\bar{3}$
$\overline{20}$	$\overline{23}$	$\bar{1}$
$\overline{30}$	$\overline{31}$	$\bar{2}$

په کړی یا رینګ $(\mathbb{Z},+,\cdot)$ (کموتاتیو کړې د 1 سره) کې باور لري:
$ab=0 \Rightarrow a=0 \vee b=0$ [4.1] . په تولیزه توګه دا په $(\mathbb{Z}_m,+,\cdot)$ [4.2]کې تیک نه دی، دا د $m=6$ لپاره باور لري $\bar{2}\cdot\bar{3}=\bar{6}=\bar{0}$ ، چېرته چې $\bar{2},\bar{3}\neq\bar{0}$ دی.

پېژند(تعریف)4.4.1 : $(R,+,\cdot)$ دې یو کموتاتیو کړی وي د 1 سره

لومړی : یو $a\in R, a\neq 0$ صفرپروېشونی (مقسوم علیه صفر،،؟،،) بلل کیږي، که یو $b\in R, b\neq 0$ شتون ولري د$ab=0$ سره.

دویم : یو R انتیګریتي کړې (صفرپروېشوني ازاد یا بې صفرپروېشوني) بلل کیږي، که په R کې صفرپروېشونی شتون ونه لري.

(c) ketabton.com: The Digital Library

دريم : يو $a \in R$ يوون يا واحد بلل کيږي، که يو $b \in R$ شتون ولري، د $ab = 1$ سره، b د a معکوس يا په څټ بلل کيږي (نسبت و ضرب ۰ ته)، سومبوليک: $b = a^{-1}$.

څلورم : که په R کې هر $a \neq 0$ يو يوون وي، نو $(R,+,\cdot)$ يو بدن يا تن يا جسم بلل کيږي(انګريزي).

بېلګه 4.4.2 :

لومړی : $(\mathbb{Z},+,\cdot)$ يو انتيګريتي کړۍ ده، يوونونه يا واحدونه ± 1 دي.

دويم: $(\mathbb{Z}_6,+,\cdot)$ صفرپروپشوني $\overline{2},\overline{3},\overline{4}$ او يوونونه $\overline{1},\overline{5}$ لري .

دريم: $(\mathbb{Z}_5,+,\cdot)$ يو بدن دی ، لکه په لاس ته راوړنه 4.1.6 کې چې لاس ته راځي.

پېژند(تعريف)4.4.3 : يو $\overline{a} \in \mathbb{Z}_m$ لومړنی پاتې سيستم $\bmod m$ بلل کيږي،که $\mathrm{ggT}(a,m) = 1$ وي، دا په دې معنا، چې a و m ته نسبي لومړنی دی).

ليم4.4.4ا : هر $\overline{a} \in \mathbb{Z}_m$ د لومړني پاتې ټولګي توکی و مودول m ته نسبي لومړنی دی.

ښوونه: وي دې $\overline{a} \in \mathbb{Z}_m$ لومړنی پاتې سيستم او $\mathrm{ggT}(a,m) = 1$ (پرته له دې بيا سرې بل نماينده سيستم ټاکي). وي دې $b \in \overline{a}$ په خوښه، و دې ښوول شي: $\mathrm{ggT}(b,m) = 1$.

(c) ketabton.com: The Digital Library

نیسو، چي $\mathrm{ggT}(b,m) \neq 1$ ، داپه دېمعنا، چي یو لومړنی ګڼ $p \in \mathbb{P}$ شته د $p \mid b$ او $p \mid m$ سره(که وي $c \mid b, c \mid m \Rightarrow$ له دې څخه د c په لومړنیو ضریبونو توټه کونه د $p \mid b, p \mid m$ سره لاس ته راځي). د $b \in \overline{a}$ له امله باور لري:

$$b = a + km \; k \in \mathbb{Z}. \quad (4.43)$$

دا چي $p \mid b, p \mid m$ د $b = a + km$: له امله لاس ته راځي:

$$p \mid a \Rightarrow \mathrm{ggT}(a,m) \geq p \qquad (4.44)$$

-- تضاد □

جمله : په $(\mathbb{Z}_m, +, \cdot)$ کې یوونونه یاواحدونه تیک لومړني پاتېتولګي دي.

ښوونه:

لومړی: که $\overline{a} \in \mathbb{Z}_m$ لومړنی پاتي تولګی وي له دې لاس ته راځي $\Rightarrow \mathrm{ggT}(a,m) = 1$ ، د 2.2.5 پسي لاس ته راځي $1 = \alpha a + \beta m$ د ځنو $\alpha, \beta \in \mathbb{Z}$ لپاره . له دې امله

$1 = \alpha a + \beta m \equiv \alpha a(m) \Rightarrow \overline{\alpha} = (\overline{a})^{-1},$	(4.45)

(c) ketabton.com: The Digital Library

دويم : $\overline{a}$ يوون يا واحد دی.

دريم: که $\overline{a} \in \mathbb{Z}_m$ يوون يا واحد وي، نو يو $\overline{b} \in \mathbb{Z}_m$ شتون لري د $\overline{a}\overline{b} = \overline{1}$ سره ،

دا په دې معنا، چې $\overline{ab} = \overline{1}$ ، له دې سره $ab \equiv 1(m)$ ، دا په دې معن،

چې $ab - 1 = km$. نيسو چې $\mathrm{ggT}(a, m) \neq 1$ ، نو

$$\exists p \in \mathbb{P} : p \mid a, p \mid m \Rightarrow p \mid \mathbf{1}$$

-- تضاد □

جمله ګی4.4.6 : $(\mathbb{Z}_m, +, \cdot)$ تيک هلته يو بدن دی، که m يو لومړنی ګڼ وي.

ښوونه

$(\Leftarrow)$

وي دې $\overline{a} \in \mathbb{Z}_p, \overline{a} \neq \overline{0}$. دا چې $1, 2, \ldots, p-1$ نسبت p ته نسبي لومړنی دی،

نو $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ باور لري، چې ټول پاتې ټولګي لومړني دي، نو هر يو په

خوښه $\overline{a} \in \mathbb{Z}_p$ هم.

نو ټول يوونونه يا واحدونه په $\mathbb{Z}_p$ کې دي. نو د تعريف پسې باور لري : $(\mathbb{Z}_p, +, \cdot)$ يو بدن دی.

$(\Rightarrow)$ وي دې $(\mathbb{Z}_m, +, \cdot)$ يو بدن. ودې ښوول شي: $m \in \mathbb{P}$

نيسو يا فرضوو، چېm نالومړنی دی، نو

(c) ketabton.com: The Digital Library

$$m = rs, 1 < r < m, 1 < s < m. \qquad (4.46)$$

له دې سره باور لري

$$\overline{m} = \overline{0} = \overline{rs} = \overline{r} \cdot \overline{s}. \quad (4.47)$$

باور لري، چې $\overline{r}$ او $\overline{s}$ صفر $\overline{0}$ نه دي. ځکه چې: له $\overline{r} = \overline{0}$ لاس ته راځي $r \equiv 0(m)$، دا په دې معنا، چې $m \mid r$ او $m \leq r$ --تضاد یا مخامخوالی .

په ورته توګه د $\overline{s}$ لپاره. دا چې $(\mathbb{Z}_m, +, \cdot)$ یو بدن دی،نو هر $\overline{r} \in \mathbb{Z}_m$ ته یو $\overline{r}^{-1} \in \mathbb{Z}_m$ شتون لري د $\overline{r}\overline{r}^{-1} = \overline{1}$ سره. نو له $\overline{rs} = \overline{0}$ لاس ته راځي، چې $\overline{r}^{-1}\overline{rs} = \overline{r}^{-1}\overline{0} = \overline{0}$ ، دا په دې معنا، چې $\overline{s} = \overline{0}$ -- تضاد یا

مخامخوالی!

له دې امله m لومړنی عدد دی، او له دې سره $m \in \mathbb{P}$.

بېلګه 4.4.7 : $(\mathbb{Z}_5, +, \cdot)$ یو بدن دی.

معکوس یې دي:

$$\overline{1}^{-1} = \overline{1}, \overline{2}^{-1} = \overline{3}, \overline{3}^{-1} = \overline{2}, \overline{4}^{-1} = \overline{4}$$

پښنه نوټ::

[4.1] $ab = 0 \Rightarrow a = 0 \vee b = 0$

په الجر کې همدا خوي د،،صفر پروپښنې ازاد،، بلل کیږي.

(c) ketabton.com: The Digital Library

4.2 $(\mathbb{Z}_m, +, \cdot)$

موږ په راتلونکې کې د $(\mathbb{Z}_m, \oplus, \odot)$ په ځای $(\mathbb{Z}_m, +, \cdot)$ هم لیکو ، سره له دې ، د ،، + ،، او ،، . ،، سره هغه د $\mathbb{Z}$ اصلي جمعه او ضرب په معنا پوهیږو!

الجبري کونګروانځ Algebraische Kongruenzen

د کرښیزو کونګروانځو حلوړوالی

د جملې 4.4.5 پسې یو $\overline{a}$ په $\mathbb{Z}_m$ کې تیک هلته یوون یا واحد دی، که $\mathrm{ggT}(a,m)=1$ ($\overline{a}\in\mathbb{Z}_m$ لومړنی پاتې سیستم)وي. د داسې یوه $\overline{a}$ لپاره له دې امله یو $\overline{x}\in\mathbb{Z}_m$ شتون لري د $\overline{ax}=\overline{1}$ سره ، دا په دې معنا،چې $\overline{ax}=\overline{1}$ او $ax\equiv 1(m)$ دي. غوښتنه: د $\overline{x}\in\mathbb{Z}_m$ $ax\equiv 1(m)$ سره.

په تولیزه توګه: غواړو د $x\in\mathbb{Z}$ حل پیدا کړو د

$$ax\equiv b(m), a,b\in\mathbb{Z}, m\in\mathbb{N}, \quad (5.1)$$

سره داسې کرښیز کونګروانځ یا ورته والی.

جمله5.1.1 : یو کرښیز کونګروانځ $ax\equiv b(m)$ تیک هلته حل وړ دی، که $\mathrm{ggT}(a,m)\mid b$ وي. که دا حالت وي، نو تیک ناکونګروانت حل $d=\mathrm{ggT}(a,m) \bmod m$ لرو.

(c) ketabton.com: The Digital Library

شوونه : په يوه لومړي پل يا قدم کې ښايو: حلوړ $\Leftrightarrow \mathrm{ggT}(a,m) \mid b$.

$\Rightarrow$

وي دې $ax \equiv b(m)$ حلوړ، دا په دې معنا، چې $\exists x_0 \in \mathbb{Z}$ د $ax_0 \equiv b(m)$ سره ، نو $m \mid ax_0 - b$ او $ax_0 - b = tm$ د يوه $t \in \mathbb{Z}$ لپاره ، له دې سره $b = ax_0 + (-t)m$ دی . له دې امله باور لري: $d = \mathrm{ggT}(a,m)$ بنی خوا وېشي، او له دې سره هم b .

$\Leftarrow$

برعکس : که $d = \mathrm{ggT}(a,m) \mid b$ وي، نو باور لري: $b = cd$ د يوه $c \in \mathbb{Z}$ لپاره او د:2.2.5 پسې $d = \alpha a + \beta m$ د ځنو $\alpha, \beta \in \mathbb{Z}$ لپاره. له دې څخه لاس ته راځي:

$$b = cd = (c\alpha)a + (c\beta)m \equiv (c\alpha)a(m), \quad (5.2)$$

دا په دې معنا، چې $x = c\alpha \in \mathbb{Z}$ د $ax \equiv b(m)$ يو حل دی.

اوس ځانونه د (اينکونګروانڅ) حلونو سره ځان مصروفوو:

وښايی: که $x_0 \in \mathbb{Z}$ حل وی، نو هر $x_1 \in \overline{x_0}$ هم حل دی($\overline{x_0} \in \mathbb{Z}_m$).

د $ax_0 \equiv b(m)$ او $x_1 = x_0 + km$ له امله د يوه $k \in \mathbb{Z}$ لپاره باور لري:

(c) ketabton.com: The Digital Library

$$ax_1 = a(x_0 + km) = ax_0 + akm \equiv ax_0 \equiv b(m), \quad (5.3)$$

نو $ax_1 \equiv b(m)$ هم.

له دي امله غوښتنه :

وي دې $x_0 \in \mathbb{Z}$ حل، دا په دې معنا، چې $ax_0 \equiv b(m)$، او $x \in \mathbb{Z}$ په خوښه نو حلونه دي، نو $ax \equiv b(m)$. له دې امله د کمښت یا تفریق له لارې:

$a(x - x_0) \equiv b - b = 0(m)$. نو

$d\frac{a}{d}(x - x_0) \equiv d \cdot 0(m) \quad \left(d = \text{ggT}(a, m) \Rightarrow \frac{a}{d} \in \mathbb{Z}\right).$	(5.4)

د(5) 4.1.5 پسې لاس ته راځي:: د $\text{ggT}(d, m) = d:$ له امله:

$$\frac{a}{d}(x - x_0) \equiv 0\left(\frac{m}{d}\right), \quad (5.5)$$

دا په دې معنا، چې $\frac{m}{d} \mid \frac{a}{d}(x - x_0)$. د 2.2.9 له امله باور $\text{ggT}(\frac{m}{d}, \frac{a}{d}) = 1$ لري:

، د بتستیزې لیسما 2.2.12سره لاس ته راځي $\frac{m}{d} \mid (x - x_0)$ ، دا په دې معنا، چې

$x - x_0 = t\frac{m}{d}$ د یوه $t \in \mathbb{Z}$ لپاره . له دې امله لاس ته راځي:

$$x = x_0 + t\frac{m}{d}. \quad (5.6)$$

(c) ketabton.com: The Digital Library

وښايي: $x_0, x_0 + 1\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}$ حلونه دي.

وي دې $x_0 + k\frac{m}{d}$ د $0 \le k < d$ سره ، نو باور لري:

$$a\Big(x_0 + k\underbrace{\frac{m}{d}}_{\in\mathbb{N}}\Big) = ax_0 + ak\underbrace{\frac{m}{d}}_{\in\mathbb{N}} = ax_0 + \underbrace{\frac{a}{d}}_{\in\mathbb{N}}km \equiv ax_0 \equiv b(m). \quad (5.7)$$

وښايي: هر حل $x \in \mathbb{Z}$ يو له دې گڼونو d سره کونگروانځ مودولو m دی.

پورته لورته $x = x_0 + t\frac{m}{d}$ دی د يوه $t \in \mathbb{Z}$ لپاره. د d سره د پاتې سره وېشنې له امله سړی $t = qd + r$ د $0 \le r < d$ سره لاس ته راوړي ، نو

$$x = x_0 + t\frac{m}{d} = x_0 + (qd + r)\frac{m}{d} = x_0 + qm + r\frac{m}{d} \equiv x_0 + r\frac{m}{d} \quad (5.8)$$

د $0 \le r < d$ سره.

وښايي: $x_0, x_0 + 1\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}$ کونگروانت مودولو m دي.

نيسو: $x_0 + k\frac{m}{d} \equiv x_0 + l\frac{m}{d}(m)$ د $0 \le k < l \le d-1$ لپاره، نو باور لري:

$$(l-k)\frac{m}{d} \equiv 0(m) \Rightarrow m \Big| (l-k)\frac{m}{d} \cdot \quad (5.9)$$

$\mathrm{ggT}(m, \frac{m}{d}) = \frac{m}{d}$ ، نو $l - k \equiv 0(\frac{m}{\frac{m}{d}})$ ، دا په دې معنا، چې $l - k \equiv 0(d)$ ، له دې سره

(c) ketabton.com: The Digital Library

$$d \mid l-k \leq d-1 < d, \quad (5.10)$$

نو $|d| \leq |l-k|$ ، دا په دې معنا، چې $d \mid l-k < d$ ـ تضاد ! □

یادونه5.1.2 : د $ax \equiv b(m)$ دټولو اینکونګروانت حلونو ته بسیا کوي، چې یو ځانګړی حل x_0 پیدا کړو. ټول اینکونګروانت حلونه دا لاندې ډېره لري

$$x_0, x_0+\frac{m}{d}, \ldots, x_0+(d-1)\frac{m}{d}; \quad (5.11)$$

له دې امله غوښتنه: د $ax \equiv b(m)$ یو ځانګړی حل $x_0 \in \mathbb{Z}$.

د حل عملي شمېرنه:

بېلګه 5.1.3 : د $32x \equiv 20(14)$; $\mathrm{ggT}(32,14) = 2 \mid 20$ له امله یو حل شتون لري.

را کمونه:

د $32x \equiv 4x(14)$ او $20 \equiv 6(14)$ له امله کونګروانت $4x \equiv 6(14)$ دی.

لومړی: د ښوونې سره سم: د $\mathrm{ggT}(4,14) = 2 \mid 6$ له امله دوه مودولو 14 اینکونګروانت حلونه شتون لري.

د اکلید په لار: $2 = \mathrm{ggT}(4,14) = (-3)\cdot 4 + 1\cdot 14$ ، نو

(c) ketabton.com: The Digital Library

(5.12)	$6 = 2 \cdot 3 = (-9) \cdot 4 + 3 \cdot 14,$

دويم : دا په دې معنا، چې $x_0 = -9$ يو حل دی.

دريم. $\operatorname{mod} 14$ اينکونګروانت حل د بېلګې په توګه دی

(5.13)	$x_1 = x_0 + 1 \cdot \frac{m}{d} = -9 + \frac{14}{2} = -2;$

دريم: نو هم $5, 12, 19, 26, \ldots$

له دې لاس ته راځي ($\Rightarrow$) د ټول حلونو ټولګه.

$$\overline{5} = \{5 + k \cdot 14 \mid k \in \mathbb{Z}\},$$

$$\overline{12} = \{12 + k \cdot 14 \mid k \in \mathbb{Z}\}.$$

پنځم: د بڼې بدلون له لارې:

$$4x \equiv 6(14) \Leftrightarrow$$

$$2 \cdot 2x \equiv 2 \cdot 3(14) \overset{\operatorname{ggT}(2,14)=2}{\Leftrightarrow}$$

$$2x \equiv 3(7) \Leftrightarrow$$

(c) ketabton.com: The Digital Library

$$2x \equiv 10(7) \Leftrightarrow$$

$$2 \cdot x \equiv 2 \cdot 5(7) \overset{\mathrm{ggT}(2,7)=1}{\Leftrightarrow}$$

$$x \equiv 5(7)$$

شپږم: دويم حل: $5 + 7 = 12$

بېلګه5.1.4 : غوښتنه يا ثبوت د $\overline{3} \bmod 16$ معکوس (نسبت ضرب ته) غواړو پيدا کړو. د[4.4.5](#) پسې $\overline{3}^{-1} \in \mathbb{Z}_{16}$ شتون لري، ځکه چې $\mathrm{ggT}(3,16) = 1$ ، نو $\overline{3}$ يو لومړنی پاتې ټولګی دی. غواړو يو x پيداکړو، د $3x \equiv 1(16)$ سره، له دې امله $3x \equiv -15(16)$ ، نو $x \equiv -5(16)$ او $x \equiv 11(16)$ ، داپه دې معن، چې $\overline{3}^{-1} = \overline{11}$.

سيمولتان کونګروانت Simultane Kongruenzen

غوښتنه : غواړو ټول $x \in \mathbb{Z}$ پيداکړو، چې لاندې سيستم حل کړي:

$$\left.\begin{array}{rcl} a_1 x & \equiv & b_1(m_1) \\ & \vdots & \\ a_k x & \equiv & b_k(m_k) \end{array}\right\} \quad (5.14)$$

(c) ketabton.com: The Digital Library

ځانګړی حالت: $a_i = 1 \ \forall i$ د لاندې نیونو یا فرضیو له مخې

لومړی : $m_1, \ldots, m_k$ جوړه نسبي لومړني.

دویم : $x \equiv b_i(m_i)$ د $\forall i$ لپاره حلوړ دی.

جمله5.2.1 : (چینایي پاتېجمله[5.1] (یعني د پاتو یا باقي مانده وو جمله)) : وي دې $m_1, \ldots, m_k \in \mathbb{N}$ جوړه نسبي لومړني او $a_1, \ldots, a_k \in \mathbb{Z}$ په خوښه. نودا لندې حلوړ دی

$$x \equiv a_1(m_1), \cdots, x \equiv a_k(m_k) \quad (5.15)$$

او د ا په حقیقت کې مودولو $m_1 \cdots m_k$ یوائځنی.

ښوونه : وي دی $M := m_1 \cdots m_k, M_i := \frac{M}{m_i}, i = 1, \ldots, k$.

نو $\operatorname{ggT}(M_i, m_i) = 1$ باور لري ، ځکه چې : که p یو لومړنی عدد وي د $p \mid M_i, p \mid m_i$ سره د یوه $1 \leq i \leq k$ لپاره، نو :

د : 3.1.5 $p \mid m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$ پسې $p \mid m_j$ د یوه $j \neq i$ لپاره --

تضاد، خکه چې m_i جوړه لومړني وو د نیونې 1 له مخې.

له دې امله $M_i x \equiv 1(m_i)$ د5.1.1 پسې یو حل $y_i \in \mathbb{Z}, 1 \leq i \leq k$ لري.

راوړو یا ترخېړنې نیسو:

(c) ketabton.com: The Digital Library

$$x_0 = \sum_{i=0}^{k} a_i M_i y_i. \quad (5.16)$$

نو باور لري: x_0 د ورکړ شوي سیستم حل دی(5.15).

وي دې $1 \leq j \leq k$ په خوښه، نو مودولو m_j باور لري

$$x_0 = a_1 M_1 y_1 + \cdots + a_j M_j y_j + \cdots + a_k M_k y_k \quad (5.17)$$

$$\equiv 0 + \cdots + a_j M_j y_j + \cdots + 0 \quad (5.18)$$

$$= a_j \underbrace{M_j y_j}_{\equiv 1(m_j)} \quad (5.19)$$

$$\equiv a_j (m_j). \quad (5.20)$$

دا په دې معنا، چې x_0 د سیستم د k کونګروانتو هر یو پوره کوي.

وي دې $\alpha, \beta \in \mathbb{Z}$ د سیستم حلونه، دا په دې

معنا،چې $\alpha \equiv a_i(m_i), \beta \equiv a_i(m_i)\ \forall i$ باور لري ، نو $\alpha - \beta \equiv 0(m_i)$

او $\alpha \equiv \beta(m_i)$ د $i = 1, \ldots, k$ لپاره. دا چې $m_1, \ldots, m_k$ جوړه لومړني دي،

د (6)4.1.5 پسې $\mathrm{kgV}(a_1, \ldots, a_k) = m_1 \cdots m_k$ باور لري او

(c) ketabton.com: The Digital Library

$\alpha \equiv \beta(m_1 \cdots m_k)$ ، دا په دې معنا، چې $m_1 \cdots m_k$ تیک یو حل شتون لري.

□

بېلګه 5.2.2 : لاندې سیستم ورکړ شوی:

$$\left.\begin{array}{lll} x & \equiv & 2(3) \\ x & \equiv & 3(5) \\ x & \equiv & 2(7) \end{array}\right\} (5.21)$$

دا چې $3, 5, 7$ جوړه نسبي لومړني دي، نو $\mod 3 \cdot 5 \cdot 7 = 105$ یو یواځنی حل لري

لومړی : د ښوونې سره سم: $M = 105, M_1 = 35, M_2 = 21, M_3 = 15$

$$35x \equiv 1(3) \quad \Rightarrow \quad y_1 = 2,$$

$$21x \equiv 1(5) \quad \Rightarrow \quad y_2 = 1,$$

$$15x \equiv 1(7) \quad \Rightarrow \quad y_3 = 1$$

$$\Rightarrow x_0 = \sum_{i=0}^{3} a_i M_i y_i = 2 \cdot 35 \cdot 2 + 3 \cdot 21 + 2 \cdot 15 = 233 \equiv 2\!\!:$$

دویم: د سکځیسیف پرځای کولو سره:

$$x \equiv 2(3) \Leftrightarrow x = 2 + 3t \;\; (t \in \mathbb{Z}).$$

(c) ketabton.com: The Digital Library

$$x \equiv 3(5) \Leftrightarrow 2+3t \equiv 3(5) \Leftrightarrow 3t \equiv 1(5) \Leftrightarrow 3t \equiv 6(5) \Leftrightarrow t \equiv 2(5)$$

$$\Leftrightarrow t = 2+5s \ (s \in \mathbb{Z}),$$

$$x = 2+3t = 2+3(2+5s) = 8+15s \ (s \in \mathbb{Z}).$$
نو

$$x \equiv 2(7) \Leftrightarrow 8+15s \equiv 2(7) \Leftrightarrow 15s \equiv -6(7) \Leftrightarrow 15s \equiv 15(7)$$

$$\Leftrightarrow s \equiv 1(7) \Leftrightarrow s = 1+7u \ (u \in \mathbb{Z}),$$

$$x = 8+15s = 8+15(1+7u) = 23+105u \ (u \in \mathbb{Z}).$$
نو

دريم : دا په دې معنا، چې $x = 23$ (مودولو) $\bmod 105$ د سیستم (5.18)یواځنی حل دی.

د دې ځانګړي حالت تر څنګ، اوس د کرښيزو کونګروانتو ټولیز سیستم تر څېړنې لاندې نيسو

$$\left.\begin{array}{rcl} a_1 x & \equiv & b_1(m_1) \\ & \vdots & \\ a_k x & \equiv & b_k(m_k) \end{array}\right\} \quad (5.22)$$

نيونه یا فرضيه :

1. $m_1, \dots, m_k \in \mathbb{N}$. جوړه نسبي لومړني
2. هر د k کونګروانت حلوړ دی.

(c) ketabton.com: The Digital Library

سرې کړې شي وښايي:

جمله5.2.3 : که کرښيزو کونګروانتو يو ټوليز[5.2] سيستم د پورته نيونو سره مخ ته ولرو، نو يواځنی تاکلی حل $\mod m_1 \cdots m_k$ شتون لري .

د لاندې يو په بل پسې اېښوونې له لارې عملي شمېرنې ته

بېلګه5.2.4 : لاندې د کرښيزو کونګروانتو سيستم دې ورکړ شوی وي:

$$\left.\begin{array}{lcl} 4x & \equiv & 12(8) \\ 3x & \equiv & 5(7) \end{array}\right\} \quad (5.23)$$

لکه ساده چې ليدل کيږي، دواړه نيونې پوره دي، د جملې 5.2.3 پسې د حلونو شتون تظمين دی.

$$4x \equiv 12(8) \Leftrightarrow x \equiv 3(2) \Leftrightarrow x \equiv 1(2) \Leftrightarrow x = 1 + 2t \ (t \in \mathbb{Z}).$$

$$3x \equiv 5(7) \Leftrightarrow 3x \equiv 12(7) \Leftrightarrow x \equiv 4(7),$$

نو $1 + 2t \equiv 4(7)$

$$\Leftrightarrow 2t \equiv 3(7) \Leftrightarrow 2t \equiv 10(7) \Leftrightarrow t \equiv 5(7)$$

$$\Leftrightarrow t = 5 + 7s \ (s \in \mathbb{Z}),$$

نو $1 + 2(5 + 7s) = 11 + 14s \ (s \in \mathbb{Z}).$

دا په دې معنا، چې $x = 11, 25, 39, 53$ مودولو $m_1 \cdot m_2 = 8 \cdot 7 = 56$ اينکونګروانت دي.

(c) ketabton.com: The Digital Library

ګـنـونـپـو هـنـه

$$\overline{11}, \overline{25}, \overline{39}, \overline{53} \in \mathbb{Z}_{56}.$$

د سیستم حل(5.20) . د ټول خلونو ټولګه:

پښي يادونه:

... پاتي جمله [5.1] د ز. ک. څخه درېسوه کاله د مخه

.... ټوليز [5.2]

د ،،ټوليز،، لاندې د5.19 ډول يا تيوپ سيستم پوهيږو، چېرته چې ټول $a_i = 1$ نه دي.

الجبري کونګروانت Algebraische Kongruenzen

پيژند(تعريف) 5.3.1 : وي دې

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad (5.24)$$

يو پولينوم د $a_0, \ldots, a_n \in \mathbb{Z}, a_n \neq 0$ سره، نو

$$f(x) \equiv 0(m) \quad (5.25)$$

يو الجبري کونګروانت يلل کيږي د درجې n . غوښتوني: ټول $x_0 \in \mathbb{Z}$ د لاندې سره

$$f(x_0) \equiv 0(m). \quad (5.26)$$

يادونه 5.3.2 :

$$a_n x^n + \cdots + a_1 x + a_0 \equiv 0(m) \Leftrightarrow \overline{a_n x^n + \cdots + a_0} = \overline{0}$$

(c) ketabton.com: The Digital Library

$$\Leftrightarrow \overline{a_n}\overline{x}^n + \cdots + \overline{a_0} = \overline{0}.$$

نو : حلونه د پولينومون صفرځايونه دي

$$\overline{f} = \overline{a_n}x^n + \cdots + \overline{a_1}x + \overline{a_0} \qquad \overline{a_0}, \overline{a_1}, \ldots, \overline{a_n} \in \mathbb{Z}_m, \quad (5.27)$$

په $\mathbb{Z}_m$ کې.

يادونه 5.3.3 : $x_0 \in \mathbb{Z}$ د $f(x) \equiv 0(m)$ حل دی، نو هر $x_1 \in \overline{x_0}$ هم (له $\mathbb{Z}_m$) حل دی، ځکه چې

$$x_1 \in \overline{x_0} \Rightarrow x_1 = x_0 + km$$

$$\Rightarrow x_1 = x_0 + km \equiv x_0(m)$$

د لاس ته راوړنو سره(3)4.1.6 :

$$\Rightarrow f(x_1) \equiv f(x_0)(m)$$

$$\Rightarrow x_1$$

بېلګه5.3.4 : لومړی: $x^3 - x \equiv 0(3)$: ټول حلونه دې پيدا شي.

$x_0 = 0, 1, 2$ حلونه دي، دا په دې معنا، چې د يادونو 5.3.3 پسې هر ټول عدد حل دی.

(c) ketabton.com: The Digital Library

دويم: $x^2-2\equiv 0(8)$: د دې عددونو $0,1,\ldots,7$ څخه کوم يو حل نه دی، دا په دې معنا، چې دا کونګروانت کوم حل نه لري.

د $f(x)\equiv 0(m)$ حل متودونو ته تشريح.

پېژند(تعريف) : که $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\ (a_i\in\mathbb{Z})$ وي، نو

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+2a_2x+a_1 \quad (5.28)$$

د $f(x)$ (فورمال) مشتق بلل کيږي.

يادونه5.3.6 : د ټول $\forall x,a\in\mathbb{Z}:$ لپاره باور لري :

$$f(x)-f(a)=(x-a)g(x) \quad (5.29)$$

د يوه پولينوم g لپاره د په $\mathbb{Z}$ کې ضريبونو سره، چېرت چې $g(a)=f'(a)$ باور لري..

($\lim_{x\to a}\frac{f(x)-f(a)}{x-a}=f'(a)$، ځکه چې f پولينوم دی، دا په دېمعنا، چې مشتقوړ $\lim_{x\to a}g(x)=g(a)$ ، ځکه چې g پولينوم دی له دې لاس ته راځي، چې ناپرېکېدونکی دی.)

د حلونوو عملي شمېرنه Praktische Berechnung der Lösungen

(c) ketabton.com: The Digital Library

لومړی : ليما 5.3.7 : $f(x) \equiv 0(m)$ تيک هلته حلوړ دی، که $f(x) = 0(p_i^{\alpha_i})$ حلوړ وي د ټولو $i = 1, \ldots, k$ لپاره او که $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ د m لومړنی ضريب ټوټه ونه وي.

ښوونه :

$(\Rightarrow)$

که $f(x) \equiv 0(m)$ حلوړ وي، نو $f(x_0) \equiv 0(m)$ باور لري د يوه $x_0 \in \mathbb{Z}$ لپاره، يعني $f(x) \equiv 0(p_i^{\alpha_i})\ \forall i = 1, \ldots, k$ هم حلوړ دی ځکه چي $p_i^{\alpha_i} \mid m\ (4.1.5(3))$.

$(\Leftarrow)$

که $f(x) \equiv 0(p_i^{\alpha_i})\ \forall i = 1, \ldots, k$ حلوړ وي، نو $f(a_i) \equiv 0(p_i^{\alpha_i})$ باور لري د ځنو $a_i \in \mathbb{Z}(i = 1, \ldots, k)$ لپاره. په ټوليزه توګه a_i مختلف دي!

د ا لاندې سيستم تر ځېړني نيسو

$$\left.\begin{array}{lll} x & \equiv & a_1(p_1^{\alpha_1}) \\ & \vdots & \\ x & \equiv & a_k(p_k^{\alpha_k}) \end{array}\right\} \quad (5.30)$$

د چيناي پاتي جملې 5.2.1 له مخې دا سيستم يو حل $a \in \mathbb{Z}$ لري (مودولونه جوړه لومړني دي) دا په د بمعنا، چي

(c) ketabton.com: The Digital Library

.

$$\left.\begin{array}{rcl} a & \equiv & a_1(p_1^{\alpha_1}) \\ & \vdots & \\ a & \equiv & a_k(p_k^{\alpha_k}) \end{array}\right\} \quad (5.31)$$

يعني د لاس ته راوړني(3)4.1.6 له لارې :

$$f(a) \equiv f(a_i)(p_i^{\alpha_i}), i = 1, \ldots, k, \quad (5.32)$$

دا په دې معنا، چې $f(a) \equiv 0(p_i^{\alpha_i})\ \forall i$ ، له دې سره د (5)4.1.5 پسې

$$f(a) \equiv 0(p_1^{\alpha_1} \cdots p_k^{\alpha_k}). \quad (5.33)$$

يعني: $a \in \mathbb{Z}$ د ورکړ شوي کونګروانت حل دی.

دويم : د $f(x) \equiv 0(p^n)$، p لېرمرنی عدد د حل متود يا لار ، $n \in \mathbb{N}$ په خوښه د حلونو مودولو p کې و حلونو مودولو p^2 ته ; له دوی څخه و حلونو مودولو p^3 ته، ... په ،، مخ ته تلنه،، کې پروت دی،... تر هغې چې سرې حل مودولو p^n لاس ته راوړي:

د $0, 1, \ldots, p-1$ ځا په ځای کوني يا ايښووني له لارې د $f(x) \equiv 0(p)$

ټول حلونه پيدا د د $f(x) \equiv 0(p^{n-1})$ ټول حلونه دې معلوم وي ، نو باور لري:

(c) ketabton.com: The Digital Library

لېما . وي دې $x_0 \in \mathbb{Z}$ د $f(x) \equiv 0(p^n)$ حل ، نو باور لري :

$$x_0 = a + tp^{n-1}, \qquad (5.34)$$

چېرته چې $a, t \in \mathbb{Z}$ د $f(a) \equiv 0(p^{n-1})$ سره دی.

ښوونه:

د $f(x_0) \equiv 0(p^n)$ له امله هم باور لري،

یعني x_0 له نیوني سره سم پېژندلی دی ، ($\operatorname{mod} p^{n-1}$) $x_0 \in \overline{a}$ د یوه $a \in \mathbb{Z}$ لپاره ، یعني $x_0 = a + tp^{n-1}$ د $t \in \mathbb{Z}$ لپاره□

نه د هر $t \in \mathbb{Z}$ لپاره دا $x_0 = a + tp^{n-1}$ د $f(x) \equiv 0(p^n)$ حل دی، دا کوم $t \in \mathbb{Z}$ دي؟

لېما5.3.9 : $x_0 = a + tp^{n-1}$ د $a, t \in \mathbb{Z}$ او $f(a) \equiv 0(p^{n-1})$ سره تیک هلته د $f(x) \equiv 0(p^n)$ یو حل دی، که $t \in \mathbb{Z}$ د کرښیز کونګروانځ یا ورته والي حل وي؟

$$f'(a)x + \frac{f(a)}{p^{n-1}} \equiv 0(p) \qquad (5.35)$$

(c) ketabton.com: The Digital Library

ښوونه:

$(\Rightarrow)$

وي دې $x_0 = a + tp^{n-1}$ د $f(a) \equiv 0(p^{n-1})$ سره د $f(x) \equiv 0(p^n)$ یو حل، د ښوول دی: دا t د کرښیز ګونګروانیخ حل دی

$$f(x_0) - f(a) = (x_0 - a)g(x_0) = tp^{n-1}g(x_0) \Rightarrow \quad (5.36)$$

$$\Rightarrow f(a) + tp^{n-1}g(x_0) = f(x_0) \equiv 0(p^n). \quad (5.37)$$

د $p^{n-1} \mid f(a)$ (نیونه یا فرضیه) او $\mathrm{ggT}(p^{n-1}, p^n) = p^{n-1}$ له امله لاس ته راځي:

$$\frac{f(a)}{p^{n-1}} + tg(x_0) \equiv 0(p). \quad (5.38)$$

دا چې $x_0 = a + tp^{n-1}$ دی، نو $p \mid x_0 - a$ باور لري: ، یعني $x_0 \equiv a(p)$ ،
د(3)4.1.6 پسې $g(x_0) \equiv g(a)(p)$ باور لری (ځکه چې g پولینوم دی)، دا په دې م عنا، چې

$$g(x_0) \equiv f'(a)(p) \Rightarrow \frac{f(a)}{p^{n-1}} + tf'(a) \equiv 0(p). \quad (5.39)$$

$(\Leftarrow)$

(c) ketabton.com: The Digital Library

وي دې $t \in \mathbb{Z}$ د $f'(a)x + \frac{f(a)}{p^{n-1}} \equiv 0(p)$ حل، دا په دې معنا، چې باورلري:

$$f'(a) \cdot t + \frac{f(a)}{p^{n-1}} \equiv 0(p). \quad (5.40)$$

ښايو؛ $x_0 = a + tp^{n-1}$ د $f(x) \equiv 0(p^n)$ يو حل دی.

لاس ته راځي: $p^{n-1}f'(a)t + f(a) \equiv 0(p^n)$. د $x_0 - a = tp^{n-1}$ له امله باور لري:

$$f'(a)(x_0 - a) + f(a) \equiv 0(p^n), \quad (5.41)$$

يعنې $f(x_0) - f(a) + f(a) \equiv 0(p^n)$ ، ځکه چې

$$f(x_0) - f(a) = (x_0 - a)g(x_0) \equiv tp^{n-1}f'(a)(p^n). \quad (5.42)$$

له دې سره $f(x_0) \equiv 0(p^n)$ ، دا په دې معنا، چې

$$x_0 = a + tp^{n-1} \quad (5.43)$$

د $f(x) \equiv 0(p^n)$ حل دی.

(c) ketabton.com: The Digital Library

لومړی : $a_i \in \mathbb{Z}$ د $f(x) \equiv 0(p_i^{\alpha_i})$ ټول حلونه د هر $i = 1, \ldots, k \ (m = p_1^{\alpha_1} \cdots p_k^{\alpha_k})$ لپاره معلوم دي، نو بیا سړی په خوښه یو k - توپل یا k –ګون جوړوي، چېرته چې $f(a_i) \equiv 0(p_i^{\alpha_i}) \ \forall i$ ، او دا سیستم باورلري:

$$\left.\begin{array}{rcl} x & \equiv & a_1(p_1^{\alpha_1}) \\ & \vdots & \\ x & \equiv & a_k(p_k^{\alpha_k}) \end{array}\right\} \quad (5.44)$$

[redacted]یم : نو دا سیستم بیا د ضرب $p_1^{\alpha_1} \cdots p_k^{\alpha_k} = m$ مودولو یوائنی حل $a \in \mathbb{Z}$ [redacted]ي. د پل یو پسې له دې امله هم د $a \in \mathbb{Z}$ $f(x) \equiv 0(m)$ یو حل دی.

[redacted]که 5.3.10 :

!

$$x^3 + 2x^2 - 2x - 6 \equiv 0(135).135 = 5^1 \cdot 3^3, p_1 = 5, \alpha_1 = 1, p_2 = 3, \alpha_2 = 3$$

لومړی : حل $\mod 5^1$:

$x^3 + 2x^2 - 2x - g \equiv 0(5)$ فقط حل $1(\neg 0, \neg 2, \neg 3, \neg 4)$ لري ، دا په دې

م عنا، چې $a_{11} = 1$. مخ ته تلنه یې اړیینه نه ده، ځکه چې $\alpha_1 = 1$.

دویم: حل $\mod 3^3$:

لومړی $\mod 3^1$:

(c) ketabton.com: The Digital Library

$x^3 + 2x^2 - 2x - 6 \equiv 0(3)$ حل $0, 2$ لري.

له دې څخه $\bmod 3^2$:

د $a = 0$ مخ ته تلنه :

$f(a) = f(0) = -6, f'(a) = -2$ يعنې بايد حل شي:

$$f'(0)x + \frac{f(0)}{p^1} \equiv 0(p), \quad (5.45)$$

دا په دې معنا، چې $-2x + (-2) \equiv 0(3) \Rightarrow t = -1$ او

$a_1 = a + tp^{n-1} =$

$0 + (-1)3 = -3$

له دې څخه $\bmod 3^3$:

$f(-3) = -9, f'(-3) = 13 \Rightarrow 13x - \frac{9}{3^2} \equiv 0(3)$ دا په دې معنا،چې

$13x \equiv 0(3)$ ، يعنې $x \equiv 1(3)$ ، يعنې $t = 1$.

$$a_{21} = a_1 + tp^{3-1} = -3 + 1 \cdot 9 = 6. \quad (5.46)$$

بېرته $\bmod 3^2$:

(c) ketabton.com: The Digital Library

د $a=2$ مخ ته بيونه يا مخ ته تلنه:

$a_1 = a + tp^{2-1}$

، چېرته چې t د

$$f'(a)x + \frac{f(a)}{p^{n-1}} \equiv 0(p); \quad (5.47)$$

حل دی.

$f'(2)=18, f(2)=0$ ، يعني حل کوو: $18x + \frac{6}{3} \equiv 0(3)$ ، دا په دې معنا، چې

$18x \equiv -2(3)$

د $\text{ggT}(18,3) = 3 \nmid -2$ له امله لاس ته راځي:

کومه $t \in \mathbb{Z}$ شتون نه لري، ينې هم a_1 شتون نه لري، داپه دې معنا،چې د $a=2$ و يو $\bmod 3^2$ حل ته مخ ته بيونه نه شته ، يعني هم $\bmod 3^3$ حل شتون نه لري.

$\bmod 5^1$: 1 $\qquad$ $\bmod 3^1$: 0 2

$\downarrow \quad \downarrow$

$\bmod 3^2$: -3 مخ ته بيونه ناشوني ده

$\downarrow$

(c) ketabton.com: The Digital Library

$\mod 3^3$ 6
:

لومړی: د $\mod 5^1$ او $\mod 3^3$ حلونو ټولګه : $(1,6)$ و لاندې سيستم ته:

$$\left.\begin{array}{lll} x & \equiv & 1(5) \\ x & \equiv & 6(3^3) \end{array}\right\} \quad (5.48)$$

ويم :

$$x = 1 + 5t \Rightarrow 1 + 5t \equiv 6(3^3) \Rightarrow 5t \equiv 5(27) \overset{ggT(5,27)=1}{\Rightarrow} t \equiv 1(27)$$

له دې سره: $x = 1 + 5t = 1 + 5 \cdot 1 = 6 \Rightarrow x = 6$ يواځنی $\mod 135$
ناکونګروانځ حل دی.

د الجبري کونګروانځو دحلونو ګڼون يا تعداد

بېلګه5.3.11 :

$$5x \equiv 10(30) \,:\, ggT(5,30) = 5 \mid 10 \Rightarrow \exists\ 5 \mod 30 \quad ,$$

$$x^2 \equiv 2(8) \,:\, ,$$

$$x^2 \equiv 1(8) \,:\, ,$$

(c) ketabton.com: The Digital Library

$x^3 - x \equiv 0(3)$: .

یادونه5.3.12 : په څرګنده توګه په ټولیز ډول ناشوني دی، چې د الجبري ویناو د حلونوو په تعداد څه ووایو. او همداسې لاندې جمله هم د تعجب وړ ده، هغه چې د ځانګړي حالت لپاره، چې د لومړني عدد مودولو دی، مګر سره له دی پوښتنې ته ځواب، چې څومره حلونه شتون لري، ولرو:

جمله (لاګرانژ (1736-1813) [5.3]) 5.3.13 : وي دې

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,\ a_i \in \mathbb{Z}$$

$(i = 1, \ldots, n)$ د $grad\ f = n$ سره او یو لومړنی عدد p دې ورکړ شوی وي. که p ټول $a_i, i = 1, \ldots, n$ ونه وېشي، نو $f(x) \equiv 0(p)$ خورا زیات $grad\ f = n(p)$ اینکونګروانیت حلونه لري.

ښوونه : سرې کړی شي له وړاندې ونیسي چې $p \nmid a_n$، داچې پرته له دې به باور ولري: $a_n x^n \equiv 0(p)$، او کونګروانیح ه یو کوچنۍ د رجه ولري.

$n = 1$:

$$a_1 x + a_0 \equiv 0(p) \quad \text{wobei} \quad p \nmid a_1; \quad (5.49)$$

که $\text{ggT}(a_1, p) \mid -a_0$، نو باور لري، چې $\text{ggT}(a_1, p) = 1 \bmod p$ اینکونګروانیخ حلونه شتون لري.

$n - 1 \to n$:

(c) ketabton.com: The Digital Library

$$a_nx^n + \cdots + a_1x + a_0 \equiv 0(p) \quad \text{mit} \quad \text{ggT}(a_n, p) = 1, p \nmid a_n. \quad (5.50)$$

یا حل نه شته، چې بیا کار تمامدی.

یا : $a \in \mathbb{Z}$ دې له هغو ځخه یو حل وي، د پورته پسې باور لري:

$$f(x_0) - f(a) = (x_0 - a)g(x_0) \quad (5.51)$$

د $f(x) \equiv 0(p)$ د هر د ورپسې حل $x_0 \in \mathbb{Z}$ لپاره، یعنې:

$$(x_0 - a)g(x_0) \equiv 0(p) \Rightarrow p \mid (x_0 - a)g(x_0); \quad (5.52)$$

د 3.1.5 له مخې لاس ته راځي $p \mid x_0 - a$ یا $p \mid g(x_0)$. که $p \mid x_0 - a$ وي، نو باور لري $x_0 \equiv a(p)$، دا په دې معنا، چې نور پسې اینکونګروانت حلونه نه شته.. که $g(x_0) \equiv 0(p)$ وي، له کوم سره چې د $f(x_0) - f(a) = (x_0 - a)g(x_0)$ له امله

grad g= $n-1$ باور لري. پسې د g a_n خورا جګ ضریب هم دی! د ورااندنیوني له مخې باور لری $p \nmid a_n$.

(c) ketabton.com: The Digital Library

د ایدکشن وړاندنیوني له مخې د $x_0 \in \mathbb{Z}$ لپاره زیات له زیاته $n-1$ امکانات ($\bmod p$) شتون لري. له دې سره $f(x) \equiv 0(p)$ زیات له زیاته $(n-1)+1 = n \bmod p$ اینکونګروانت حلونه لري.

لومړني پاتې ټولګي کروپونه $\bmod m$

Die prime Restklassengruppe $\bmod m$

د أبل ګروپ $(\mathbb{Z}_m^*, \cdot)$ $(\mathbb{Z}_m^*, \cdot)$ Die abelsche Gruppe

د 4.4.5 پسې یونونه یا واحدونه (دا په دې معنا، چې د معکوس کیدونکو توکو ضرب) ټیک د لومړنی پاتې ټولګي $\overline{a} \in \mathbb{Z}_m$ دي، دا په دې معنا، چې هر د $\operatorname{ggT}(a,m) = 1$ سره. وي دې $\mathbb{Z}_m^*$ په $\mathbb{Z}_m$ کې د ټولو واحدونو ډېری یا سټ. نو باور لري:

لیما 6.1.1 : $(\mathbb{Z}_m^*, \cdot)$ یو ابل ګروپ جوړوي.

ښوونه:

لومړی: که $\overline{a}, \overline{b} \in \mathbb{Z}_m^*$ وي، نو $\overline{a} \cdot \overline{b} \in \mathbb{Z}_m^*$ دی ، نو $\overline{a} \cdot \overline{b} \in \mathbb{Z}_m^*$ دی، خکه چې $\overline{a} \cdot \overline{a'} = \overline{1}, \overline{b} \cdot \overline{b'} = \overline{1}$ د ځنو $\overline{a'}, \overline{b'} \in \mathbb{Z}_m$ لپاره، یعني

$$(\overline{a} \cdot \overline{a'}) \cdot (\overline{b} \cdot \overline{b'}) = \overline{1} \cdot \overline{1} = \overline{1}, \quad (6.1)$$

دویم: دا په دې معنا،چې $(\overline{a}\overline{b})(\overline{a'b'}) = \overline{1}$ ، همداسې

(c) ketabton.com: The Digital Library

$$(\overline{a'b'})(\overline{a}\overline{b}) = (\overline{a'a})(\overline{b'b}) = \overline{1}\cdot\overline{1} = \overline{1}; \quad (6.2)$$

دويم: يعنې د تعريف له مخې باور لري $\overline{a}\cdot\overline{b} \in \mathbb{Z}_m^*$.

دريم : اسوحياتيويتي روښانه ده، ځکه چې په ($\mathbb{Z}_m, \cdot$) کې پوره ده، او باور لري: $\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$.

څلورام : کموتاتيويتي روښانه ده، ځکه چې همداسې له ($\mathbb{Z}_m, \cdot$) را پاتې ده.

پنځم: وي دې $\overline{a} \in \mathbb{Z}_m^*$ ، نو يو $\overline{b} \in \mathbb{Z}_m$ شتون لري، د $\overline{a}\overline{b} = \overline{1}$ سره، يعنې $\overline{b}\overline{a} = \overline{1}$ (د کموتاتيويتي له امله)، دا په دې معنا، چې$\overline{b}$ هم د $\mathbb{Z}_m$ يو يوون يا واحد دی، او له دې سره لاس ته راځي:

$$\overline{b} \in \mathbb{Z}_m^*. \quad (6.3)$$

پيژند (تعريف)6.1.2 : د ابل ګروپ $(\mathbb{Z}_m^*, \cdot)$ لومړنی پاتېتولګي ګروپ $\bmod m$ بلل کيږي.

بېلګه :

$$\mathbb{Z}_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}, \mathbb{Z}_{12}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$$

$\mathbb{Z}_m^*$ څومره توکي لري؟

(c) ketabton.com: The Digital Library

په ټولیزه توګه د یوه ګروپ $(G, \cdot)$ د توکو تعداد یا ګڼون د G نظم بلل کیږي. سومبولیک $|G|$.

پېژند یا تعریف6.1.4 : د $(\mathbb{Z}_m^*, \cdot)$ نظم د $\varphi(m)$ سره ښوول - یا په نخښه کیږي، تابع یا بلواک

$$\varphi : \mathbb{N} \to \mathbb{N}, \varphi(n) \mapsto |\mathbb{Z}_m^*| \quad (6.4)$$

د اویلر *Euler* φ - تابع بلل کیږي.

لیما 6.1.5 : وي دې $m \in \mathbb{N}$ په خوښه، نو د $k \in \mathbb{N}$ ګڼون یا تعداد $\varphi(m)$ دی د $1 \leq k \leq m$ او د $\operatorname{ggT}(k, m) = 1$ سره .

ښوونه : $\mathbb{Z}_m = \{\overline{1}, \overline{2}, \ldots, \overline{m} = \overline{0}\}$.

$\overline{k}$ لومړنی پاتې ټولګی mod m $\overline{k} \in \mathbb{Z}_m^* \overset{4.4.5}{\Leftrightarrow}$ دی

$$\Leftrightarrow \operatorname{ggT}(k, m) = 1,$$

دا په دې معنا، چې په $\mathbb{Z}_m^*$ کې د توکو تعداد یا ګڼون د k د تعداد سره برابر دی، $k \in \mathbb{N}, 1 \leq k \leq m$ د $\operatorname{ggT}(k, m) = 1$ سره . □

(c) ketabton.com: The Digital Library

پسې راتلنه یا نتیجه6.1.6 : وي دې $p \in \mathbb{P}$ یو په خوښه لومړنی ګڼ یا عدد، نو باور لری: $\varphi(p) = p - 1$.

د $\varphi(m)$ شمیرنې ته $\varphi(m)$ *Zur Berechnung von*

پېژند یا تعریف 6.1.7 : د ټولو اعداد یا د ټول اعدادو یوه ډېری لومړنس پاتې سیستم $\bmod m$ بلل کیږی، که دا له هر لومړنی ټولګي $\bmod m$ تیک یو توکی ولري.

لیما 6.1.8 : یو لومړنی پاتې سیستم تیک $\bmod m$ تیک $\varphi(m)$ توکي لري، ځکه چې د [6.1.5](#) پسې تیک یوونونه یا واحدونه $\varphi(m) = |\mathbb{Z}_m^*|$ ، یعنې لومړني پاتې ټولګي $\bmod m$ شتون لري.

بېلګه 6.1.9 :

لومړی : $m = 6\{0, 1, \ldots, 5\}$ یو پوره پاتې سیستم دی، $\{1, 5\}$ یو لومړنی پاتې سیستم دی، یعنې : $|\mathbb{Z}_6^*| = 2$ ، دا په دې معنا، چې $\varphi(6) = 2$.

دویم:

$$m = 5\{0, 1, \ldots, 4\}$$

یو پوره پاتې سیستم دی، $\{1, 5\}$ یو لومړنی پاتې سیستم دی، یعنې $|\mathbb{Z}_6^*| = 2$ ، دا په دې معنا، چې $\varphi(6) = 2$.

(c) ketabton.com: The Digital Library

جمله 6.1.10 : وي دي $m, n \in \mathbb{N}, \mathrm{ggT}(m,n) = 1$ ، $\{r_1, \ldots, r_{\varphi(m)}\}$ یو لومړنی پاتې سیستم $\bmod m$ دی، او $\{s_1, \ldots, s_{\varphi(n)}\}$ یو لومړنی پاتې سیستم $\bmod n$ دی، نو

$$T = \{nr_i + ms_j \mid i = 1, \ldots, \varphi(m), j = 1, \ldots, \varphi(n)\} \quad (6.5)$$

یو لومړنی پاتې سیستم $\bmod m \cdot n$ دی.

ښوونه: $\{r_1, \ldots, r_{\varphi(m)}\}$ و یوه پوره سیستم $\bmod m$ ته پوره یا تکمیل کړی:

$$\{r_1, \ldots, r_{\varphi(m)}, r_{\varphi(m)+1}, \ldots, r_m\} \quad (6.6)$$

او $\{s_1, \ldots, s_{\varphi(n)}\}$ و یوه پوره پاتې سیستم $\bmod n$ ته پوره کړی:

$$\{s_1, \ldots, s_{\varphi(n)}, s_{\varphi(n)+1}, \ldots, s_n\}. \quad (6.7)$$

د 4.3.8 پسې

$$R = \{nr_i + ms_j \mid i = 1, \ldots, m, j = 1, \ldots, n\} \quad (6.8)$$

یو پوره پاتې سیستم $\bmod m \cdot n$ دی، په ځانګړې توګه ټول ګڼونه یا عددونه له R یعني هم له T ټول عددونه ، انکونګروانخ $\bmod mn$ دي.

و ښایی:

که $a \in R$ او $\mathrm{ggT}(a, mn) = 1$ وي، نو $a \in T$ باور لري.

(c) ketabton.com: The Digital Library

د $a \in R$ له امله $a = nr_i + ms_j$ باور لري د ځنو $1 \leq i \leq m, 1 \leq j \leq n$ لپاره. باور لري: $\mathrm{ggT}(r_i, m) = 1, \mathrm{ggT}(s_j, n) = 1$ ، ځکه چې:

نیسو، چې $\mathrm{ggT}(r_i, m) \neq 1$ ، نو یو لومړنی ګڼ یا عدد p شتونلري د لاندې سره

$$\left.\begin{matrix} p \mid r_i, \\ p \mid m \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} p \mid nr_i, p \mid ms_j \Rightarrow p \mid \underbrace{nr_i + ms_j}_{a=} \\ p \mid mn \end{matrix}\right\} \Rightarrow \mathrm{ggT}(a, mn) \neq 1 \quad (6.9)$$

-- تضاد (په ورته توګه: $\mathrm{ggT}(s_j, n) = 1 \Rightarrow nr_i + ms_j \in T$ د T تعریف له مخې).

وښایی:

که $a \in T$ وي، نو باور لري: $\mathrm{ggT}(a, mn) = 1$.

د $a \in T \subseteq R$ له امله باور لري:

$$a = nr_i + ms_j \; (1 \leq i \leq \varphi(m), 1 \leq j \leq \varphi(n)); \quad (6.10)$$

نیسو، چې $\mathrm{ggT}(a, mn) \neq 1$ ، نویو لومړنی ګڼ یا عدد p شتون لري د لاندې سره:

$$p \mid a = nr_i + ms_j \wedge p \mid mn. \quad (6.11)$$

له دې سره لاس ته راځي $p \mid m$ یا $p \mid n$ ،

(c) ketabton.com: The Digital Library

بې له ټولیزو بندیزونو یا محدودیتونو دې $p \mid m$ وي (ورته $p \mid n$). نو $p \mid ms_j$ او $p \mid a$ باور لري، یعني $p \mid nr_i$ ، له دې سره د 3.1.5له مخې $p \mid n \vee p \mid r_i$ ، باور لري $p \nmid n$ ، ځکه چې پرته له دې $\mathrm{ggT}(m,n) \neq 1$. له دې امله $p \mid r_i$ لاس ته راځي، د $p \mid m$ سره لاس ته راځي $\mathrm{ggT}(r_i,m) \neq 1$ - تضاد، ځکه چې r_i د لومړني پاتي سیستم $\bmod m$ توکی دی.

یعني: T یو لومړنی پاتي سیستم $\bmod mn$ دی. □

کورولار 6.1.11 : وي دې $m,n \in \mathbb{N}$ د $\mathrm{ggT}(m,n) = 1$ سره، نو باور لري:

$$\varphi(mn) = \varphi(m)\varphi(n). \quad (6.12)$$

ښوونه: د 6.1.10 له مخې

$$T = \{nr_i + ms_j \mid i = 1,\ldots,\varphi(m), j = 1,\ldots,\varphi(n)\} \quad (6.13)$$

یو لومړنی پاتي سیستم $\bmod mn$ دی، نو T $\varphi(m)\cdot\varphi(n)$ توکي لري. دا چې هر پاتي سیستم $\varphi(mn)$ همدا اوس $\varphi(mn)$ توکي لري، نو لاس ته راځي: $\varphi(m)\cdot\varphi(n) = \varphi(m\cdot n)$. □

یادونه6.1.12 : یو تابع $f:\mathbb{N}\to\mathbb{N}$ د لاندې خویونو سره

(c) ketabton.com: The Digital Library

$$f(mn) = f(m)f(n)\ \forall m,n : \mathrm{ggT}(m,n) = 1 \quad (6.14)$$

ضريبي يا ځليزه تابع ببليږي.

له دې سره د اويلر φ -تابع د يوه ضريبي تابع بېلګه ده(کاپيتل يا برخه11 وګورئ).

پسې راتلنه يا ترې لاس ته راوړنه 6.1.13 : وي دې $m \in \mathbb{N}$ او $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ د لومړنيضريب ټوټه ونه، نو باور لري $\mathrm{ggT}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ ، يعنې

$$\varphi(p_i^{\alpha_i} \cdot p_j^{\alpha_j}) = \varphi(p_i^{\alpha_i}) \cdot \varphi(p_j^{\alpha_j}). \quad (6.15)$$

له دې سره د اندکشن له لارې :

$$\varphi(m) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}), \quad (6.16)$$

دا په دې معنا، چې د $\varphi(m)$ شمېرنه د $\varphi(p^n)$ په شمېرنه ور اړول کيږي، د لومړني عدد p او $n \in \mathbb{N}$ لپاره.

جمله 6.1.14 : وي دې p يو لومړنی ګڼ يا عدد، $k \in \mathbb{N}$ ، نو باور لري::

$$\varphi(p^k) = p^k - p^{k-1} \qquad (p^0 := 1). \quad (6.17)$$

(c) ketabton.com: The Digital Library

ښوونه : $R = \{1, 2, \ldots, p^k\}$ دې یو پوره پاتې سیستم $\bmod p^k$ وي. لومړی هغه $a \in R$ پیدا کړی، چې و p^k ته نسبي لومړني نه وي:

$\mathrm{ggT}(a, p^k) \neq 1$

$\Rightarrow$

$$\exists\, q \in \mathbb{P} : q \mid a, q \mid p^k \overset{3.1.5}{\Rightarrow} q \mid p \Rightarrow q = p \Rightarrow p \mid a,$$ (6.18)

$p \mid a$

$\Rightarrow$

$$\mathrm{ggT}(a, p^k) \geq p > 1 \Rightarrow \mathrm{ggT}(a, p^k) \neq 1.$$ (6.19)

$\mathrm{ggT}(a, p^k) \neq 1 \Rightarrow$ $\exists\, q \in \mathbb{P} : q \mid a, q \mid p^k \overset{3.1.5}{\Rightarrow} q \mid p \Rightarrow q = p \Rightarrow p \mid a,$	(6.18)
$p \mid a \Rightarrow \mathrm{ggT}(a, p^k) \geq p > 1 \Rightarrow \mathrm{ggT}(a, p^k) \neq 1.$	(6.19)

دا په دې معنا، چې $a \in R$، کوم چې p^k ته نسبي لومړني نه دي، ټیک هغه دي د $p \mid a$ سره. یعنې غوښتوني: ټول $a \in R$، $p \mid a$، دا په دې معنا، چې $a = p \cdot t \ (t = 1, 2, \ldots)$.

(c) ketabton.com: The Digital Library

د $1 \leq a \leq p^k \ (a \in R)$ له امله باور لري $1 \leq pt \leq p^k$ ، يعني

بايد $1 \leq t \leq p^{k-1}$ باور ولري.

برعکس هر $t \in \mathbb{N}$ د $1 \leq t \leq p^{k-1}$ سره هم $p \mid pt = a$ پوره کوي. يعني

ټيک p^{k-1} ګڼونه $a \in R$ شتون لري د $p \mid a$ سره، يعني

$$\mathrm{ggT}(a, p^k) \neq 1$$

$$\Rightarrow \exists p^k - p^{k-1} a \in R : \mathrm{ggT}(a, p^k) = 1$$

. له دې سره د پيژند له مخې هم باور لري: $\varphi(p^k) = p^k - p^{k-1}$. □

کورولار يا وړه جمل6.1.15: وي دې $m \in \mathbb{N}, m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ په لومړنيو ضريبونو ټوټه کونه ، نو باور لري:

$$\varphi(m) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \cdot \ (6.20)$$

(دا په دې معنا، چې په په پاتېتولګې کړی(رين، حله) $\bmod m$ کې د يونونو يا واحدونو ګڼون يا تعداد شتون لري).

بېلګه :

لومړی :

$$m = 25m = 5^2 \Rightarrow \varphi(25) = 25 - 5 = 20$$

يعني $|\mathbb{Z}_{25}^*| = 20$ ، دا په دې معنا، چې په $\mathbb{Z}_{25}$ کې ټيک 20 يونونه يا واحدونه شتون لري.

(c) ketabton.com: The Digital Library

دویم:

$$m = 72m = 2^3 3^2 \Rightarrow \varphi(72) = (2^3 - 2^2)(3^2 - 3) = 4 \cdot 6 = 24$$

یعنې $|\mathbb{Z}^*_{72}| = 24$ دا په دې معنا، چې په $\mathbb{Z}_{72}$ کې ټیک 24 یونونه یا واحدونه شتون لري.

د اویلر جمله

Der Satz von Euler

لیما6.1.17 : وي دې $G = \{g_1, \ldots, g_n\}$ یو پای ، ابل ګروپ، نو باور لري:

لومړی: د هر $a \in G$ لپاره باور لري $ag_i \neq ag_j \ \forall i \neq j$ ،

دویم : د هر $a \in G : a^n = e$ لپاره باور لري، د کوم سره چې e د $(G, \cdot)$ یوون یا واحد دی، او $n = |G|$ دی.

ښوونه:

یو ته :

وړاندنیونه $ag_i = ag_j$ د یوه $a \in G, i \neq j$ لپاره، نو د $a^{-1} \in G :$ سره د ضربولو له لارې لاس ته راځي:

$$a^{-1}ag_i = a^{-1}ag_j, \text{ (6.21)}$$

دا په دې معنا، چې $g_i = g_j$ د $i \neq j$ سره. ــتضاد!

(c) ketabton.com: The Digital Library

دويم ته:

$e(g_1 \cdots g_n) = g_1 \cdots g_n$ د لومړي ټکی له مخې $ag_i \neq ag_j$ باور لري ، يعنې د $i = 1, \ldots, n$ لپاره ببرته n مختلف توکي لاس ته راځي. له دې سره باور لري

$$g_1 \cdots g_n = (ag_1)(ag_2) \cdots (ag_n) = a^n (g_1 \cdots g_n), \quad (6.22)$$

همداسې

$$e(g_1 \cdots g_n)(g_1 \cdots g_n)^{-1} = a^n (g_1 \cdots g_n)(g_1 \cdots g_n)^{-1}. \quad (6.23)$$

له دې سره ترلې $e = a^n, n = |G|$ راکوي . □

جمله 6.1.18 : (اويلر[6.1]) وي دې $a, m \in \mathbb{N}, \mathrm{ggT}(a, m) = 1$ ، نو باور لري:

$$a^{\varphi(m)} \equiv 1(m). \quad (6.24)$$

ښوونه: د $\mathrm{ggT}(a, m) = 1$ له امله باور لري: $\overline{a} \in \mathbb{Z}_m$ لومړنی پاتې توګلی $\bmod m$ دی، يعنې $\overline{a} \in \mathbb{Z}_m^*$ باور لري . د $|Z_m^*| = \varphi(m)$ له امله د تعريف له مخې، د6.1.17 له مخې لاس ته راځي:

$$\overline{a}^{\varphi(m)} = \overline{1}, \quad \text{d.h.} \quad \overline{a^{\varphi(m)}} = \overline{1}, \quad (6.25)$$

(c) ketabton.com: The Digital Library

داسې چې $a^{\varphi(m)} \equiv 1\,(m)$ باور لري. □

يو ځانګړی غوره حالت او د6.1.18 مشهور غوره حالت غواړو په لاندې کې ځانله تر څېړني لاندې ونيسو:

کورولار6.1.19 :(کوچنی فرمات) د ټولو $a \in \mathbb{Z}, p \in \mathbb{P}$ لپاره باور لري:

$$a^p \equiv a(p).\ (6.26)$$

ښوونه: دی $\operatorname{ggT}(a,p) = 1$ ، نو د 6.1.18 له مخې باور لري: $a^{\varphi(m)} \equiv 1(p)$ او د $\varphi(p) = p - 1$ له امله لاس ته راځي:

$$a^{p-1} \equiv 1(p),\ (6.27)$$

نو په ځانګړې توګه $a^p \equiv a(p)$.

که وي $\operatorname{ggT}(a,p) \neq 1$ ، نو باور لري $a = pt, p \mid a \Rightarrow a^p \equiv 0 \equiv a(p)$

..جمله 6.20.1 : (ويلسن [6.2] 1741-1793) : د يوه پيداپښتي ګڼ يا طبيعي عدد p لپاره باور لري:

p لومړنی عدد دی (6.28)

$$\Leftrightarrow (p-1)! \equiv -1(p).$$

ښوونه:

(c) ketabton.com: The Digital Library

$(\Rightarrow)$

وي دې $p \in \mathbb{N}$ لومړنی عدد. که وي $p = 2$، نو باور لري:

$(2-1)! = 1 \equiv -1(2),$ (6.29)

نو غوښتنه تیک ده.

وي دې $p > 2$، نو د ټولو $a \in \mathbb{N}$ لپاره باور لري د $1 \leq a \leq p-1 : \mathrm{ggT}(a,p) = 1$ سره. د 6.1.19 له مخې د دې a لپاره لاس ته راځي: $a^{p-1} \equiv 1(p)$.

له دې سره ټول عددونه $1 \leq a \leq p-1$ د الجبري کونګوروانځ $x^{p-1} \equiv 1(p)$ حلونه دي. د 5.3.13 له مخې کونګروانځ $x^{p-1} \equiv 1(p)$ خورازیات $p-1$)= د پولینوم درجه ده ($\bmod p$ بنکونګروانت حلونه، له دې سره لاس ته راځي : $1, 2, \ldots, p-1$ همدا اوس ټول انکونګروانت $\bmod p$ حلونه دي.

پسې الجبري کونګروانځ

$$(x-1)(x-2)\cdots(x-(p-1)) \equiv 0(p)$$

$\bmod p$ انکونګروانت حلونه $1, 2, \ldots, p-1$ لري. د $\mathrm{grad} = p-1$ له ا مله $1, 2, \ldots, p-1$ تیک $\bmod p$ انکونګروانت حلونه دي) د 5.3.13 سره د

(c) ketabton.com: The Digital Library

ضريب دی، نو x^{p-1} يو دی، نو د p له لارې پروېشوني نه ده(. د ضربولو وروسته سړی يو د $p-1$ درجې پولينوم د مطلق لړي

$$c_0 = (-1)(-2)\cdots(-(p-1)) = (-1)^{p-1}(p-1)! = (p \quad (6.30)$$

سره لاس ته راوړي، ځکه چې $p > 2$، نو ناجوړه يا طاق دی.

له $x^{p-1} \equiv 1(p)$ څخه د دې کونګروانتونو کمون له لارې سړی يو الجبري کونګروانت لاس ته راوړي

$$f(x) \equiv 0(p), \qquad \operatorname{grad} f \leq p-2 \quad (6.31)$$

او مطلق غړی $-1 - c_0 = -1 - (p-1)!$. دا کونګروانت زيات له زياته $\operatorname{grad}\ f \leq p - 2 \bmod p$ انکونګروانت حلونه لري، که p نه د f ټول ضريبونه وويشي (5.3.13) مګر: $1, 2, \ldots, p-1$ p-1 انکونګروانت $\bmod p$ حلونه دي. له دې سره لاس ته راځي: د p f ټول کونګروانتونه وېشي، په ځانګړې توګه $-1 - c_0$، دا په دې معنا، چې

$$p \mid -1 - c_0 \Rightarrow -1 - c_0 \equiv 0(p) \Rightarrow c_0 \equiv -1(p), \quad (6.32)$$

دا په دې معنا، چې $(p-1)! \equiv -1(p)$.

$(\Leftarrow)$

(c) ketabton.com: The Digital Library

وي دې $n \in \mathbb{N}$ د $(n-1)! \equiv -1(n)$ سره . نیسو، چې $n \notin \mathbb{P}$. له دې سره یو لومړنی ګڼ p د $p \mid n$ سره او $2 \le p \le n-1$ سره شتون لري، له دې سره

$$p \mid (n-1)! \Rightarrow (n-1)! \equiv 0(p). \quad (6.33)$$

د $(n-1)! \equiv -1(n)$ له امله د $p \mid n$ سره لاس ته راځي،چې $(n-1)! \equiv -1(p)$. له دې سره لاس ته راځي

$$0 \equiv (n-1)! \equiv -1(p) \Rightarrow p \mid 0-(-1) = 1 \quad (6.34)$$

--- تضاد ($p > 1, p \in \mathbb{P}$) □

یادونه 6.1.21 : د ویلسن 6.1.20) 1741-1793 (جملې له امله دا تروسه یوائنۍ ځرګنده یا معلوم د لومړنیو ګڼو قضیه انځوروي!

د $(\mathbb{Z}_m^*, \cdot)$ جوړښت Struktur von $(\mathbb{Z}_m^*, \cdot)$

د $(\mathbb{Z}_m^*, \cdot)$ نظم د اویلر φ -تابع په ځخه معلوم دی: $|\mathbb{Z}_m^*| = \varphi(m)$.

د ګروپ تیوري له مخې خورا ځانګړي ګروپونه داسې په نامه ،، ځیوکلیکي،، ګروپونه دي:

پیژند(تعریف) 6.2.1 : یو پای ګروپ $(G, \cdot)$ ځیوکلیکي دی، که

(c) ketabton.com: The Digital Library

$$G = \{a, a^2, \ldots, a^{|G|} = e\} \quad (6.35)$$

د لږ تر لږه یوه $a \in G$ لپاره باور ولري. یو توکی $a \in G$ د دې خوي سره د $(G, \cdot)$ تولیدېدونکی توکی بلل کیږي.

یادونه 6.2.2:

لومړی: د یوه څیوکلیکي ګروپ $(G, \cdot)$ هر توکی g کیدی شي د یوه کره یا همغه کلک توکي $a \in G$ د توان په تو ګه ولیکل شي: $g = a^n$ د یوه $n \in \mathbb{N}$ لپاره د $1 \leq n \leq |G|$ سره.

دویم : هر څیوکلیکي ګرړپ $(G, \cdot)$ د ابل ګروپ دی.

($g, h \in G \Rightarrow g = a^m, h = a^n$ د یوه تولیدي توکي لپاره $a \in G \Rightarrow g \cdot h = a^m \cdot a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m = h \cdot g$)

بیلګه 6.2.3:

لومړی: $(\mathbb{Z}_5^*, \cdot)$ څیوکلیکي دی:

$$\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} \ (\varphi(5) = 4) \overline{2}^1 = \overline{2}, \overline{2}^2 = \overline{4}, \overline{2}^3 = \overline{3}, \overline{2}^4 = \overline{1} \Rightarrow a = \overline{2}$$

د $(\mathbb{Z}_5^*, \cdot)$ یو تولیدي سیستم دی.

(c) ketabton.com: The Digital Library

همداسې: $\bar{3}^1 = \bar{3}, \bar{3}^2 = \bar{4}, \bar{3}^3 = \bar{2}, \bar{3}^4 = \bar{1}$ ، نو $a = \bar{3}$ هم د $(\mathbb{Z}_5^*, \cdot)$ یو توليدي سيستم دی.

دويم : $(\mathbb{Z}_8^*, \cdot)$ خيوکليکي نه دی:

$\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ $(\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4)\bar{3}^2 = \bar{1}$ دا په دې

$\bar{5}^2 = \bar{1}, \bar{7}^2 = \bar{1}$

معنا،چې $\bar{3}$ توليدي نه دی، همداسې باور لري:

دريم: $(\mathbb{Z}_2^*, \cdot)$ او $(\mathbb{Z}_4^*, \cdot)$ خيوکليکي نه دي

$\mathbb{Z}_2^* = \{\bar{1}\} - trivial; \mathbb{Z}_4^* = \{\bar{1}, \bar{3}\}, \bar{3}$ -ساده دی،

)

$\mathbb{Z}_2^* = \{\bar{1}\} - trivial; \mathbb{Z}_4^* = \{\bar{1}, \bar{3}\}, \bar{3}$ توليدي توکی دی)

اوس نو کوم $(\mathbb{Z}_m^*, \cdot)$ خيوکليکي دی؟

پيژند(تعريف) 6.2.4: يو تول ګڼ يا –عدد $g \in \mathbb{Z}$ ساده رېښه $\bmod m$ بلل کيږي، که $\bar{g} \in \mathbb{Z}_m^*$ لومړنی پاتې تولګيګروپ $(\mathbb{Z}_m^*, \cdot)$ توليد کړي.

بېلګه 6.2.5:

لومړی: 2 يو ساده رېښه $\bmod 5$ دی(پورته بېلګه وګورئ: $\bar{2}$ $(\mathbb{Z}_5^*, \cdot)$ توليدوي)،

همداسې: $g = 3$ ساده رېښه $\bmod 5$ دی.

(c) ketabton.com: The Digital Library

دويم: كومه ساده ريښه $\bmod 8$ شتون نه لري (همداسې: $(\mathbb{Z}_8^*, \cdot)$ څيوكليكي نه دی).

دريم: 1 سادهريښه $\bmod 2$ ، 3ساده ريښه $\bmod 4$ دی.

يادونه 6.2.6: $g \in \mathbb{Z}$ ساده ريښه $\bmod m$ دی، نو بيا هم هر $g' \in \overline{g}$.

د هغه مودول $m \in \mathbb{N}$ ټاکنه، د كوم لپاره چې $(\mathbb{Z}_m^*, \cdot)$ څيوكليكي دی(دا په دې معنا، چې د هغه لپاره چې ساده ريښې $\bmod m$ شتون لري) [6.3]:

ليما 6.2.7: وي دې $(G, \cdot)$ يو پای ابل ګروپ او $a \in G$ نو باور لري:

$$a^k = e \quad k \in \mathbb{N} \Leftrightarrow \operatorname{ord} a \mid k. \qquad (6.36)$$

له دې سره نظم $\operatorname{ord} a$ خورا كوچنی طبيعي عدد $n \in \mathbb{N}$ دی، چې د هغې لپاره $a^n = e$ بارور لري.

جمله 6.2.8 : وي دې p يو لومړنی عدد، نو $(\mathbb{Z}_p^*, \cdot)$ څيكليكي يا تل بېرته راګرځېدونی دی.

(داپه دې معنا، چې زات وخت ساده ريښې $\bmod p$ شتون لري، خو شمېرنو ته يې توليز متود شتون نه الري؟

ليما 6.2.9: وې دې $p > 2$ يو لومړنی عدد ، او $g \in \mathbb{Z}$ يوه ساده ريښه $\bmod p$. كه $g^{p-1} \not\equiv 1 (p^2)$ وي، نو g هم يوه ساده ريښه $\bmod p^\alpha \; \forall \alpha \in \mathbb{N}$ ده.

(c) ketabton.com: The Digital Library

جمله 6.2.10: وي دې $p > 2$ لومړنی عدد، نو $(\mathbb{Z}^*_{p^\alpha}, \cdot)\ \forall\alpha \in \mathbb{N}$ څیکلیکي دی(دا په دې معنا، چېیوه ساده رېښه $\bmod p^\alpha\ \forall\alpha \in \mathbb{N})$ شتون لري).

ښوونه: له ښوونې : که g ساده رېښه $\bmod p$ وي، نو باور لري:

$$g^{p-1} \not\equiv 1(p^2) \vee (g+p)^{p-1} \not\equiv 1(p^2). \tag{6.37}$$

پام؛ $g + p$ ساده رېښه $\bmod p$ دی.($\exists \Rightarrow$)له دې لاس ته راځي تل یو g شتون لري لکه په 6.2.9 کې غوښتل شوي). □

بیلګه 6.2.11 : وي دې $p = 5$ ، د 6.2.3 له مخې $g = 2$ یوه ساده رېښه $\bmod 5$ دی، د

$$g^{p-1} = 2^4 = 16 \not\equiv 1(25) \tag{6.38}$$

له امله $g = 2$ یوه ساده رېښه $\bmod 5^\alpha\ \forall\alpha \in \mathbb{N}$ ده، دا په دې معنا، چې

$$\bmod 25, 125, 625, \ldots$$

په همدې توګه : $g = 3$ یوه ساده رېښه $\bmod 5$ ده، د

$$g^{p-1} = 3^{p-1} = 3^4 = 81 \not\equiv 1(25) \tag{6.39}$$

له ا مله 3 هم یوه ساده رېښه $\bmod 5^\alpha\ \forall\alpha \in \mathbb{N}$ دی.

(c) ketabton.com: The Digital Library

جمله 6.2.12: $p > 2$ دي یو لومړنی عدد وي، نو $(\mathbb{Z}_{2p^\alpha}, \cdot)$ ځیوکلیکي دی $\forall \alpha \in \mathbb{N}$. (دا په دې معنا، چې یوه ساده ریښنه $\bmod 2p^\alpha \; \forall \alpha \in \mathbb{N}$ شتون لري).

ښوونه: له ښوونې څخه: g دې ناجوړه وي، $g \in \mathbb{Z}$، او یوه ساده ریښه $\bmod p^\alpha$، نو g هم یوه ساده ریښنه $\bmod 2p^\alpha$ ده ($\forall \alpha \in \mathbb{N}$)، که g جوړه وي، نو $g + p^\alpha$ ناجوړه دی او ساده ریښنه $\bmod p^\alpha$. □

بیلګه 6.2.13: وي دې $p = 5$، د 6.2.11 له مخې $g = 3$ یوه ساده ریښنه $\bmod 5^\alpha \; \forall \alpha \in \mathbb{N}$ ده او ناجوړه، نو لاس ته راځي: 3 یوه ساده ریښنه $\bmod 2 \cdot 5^\alpha \; \forall \alpha \in \mathbb{N}$ ده، دا په دې معنا، چې $\bmod 10, 50, 250, \ldots$

د 6.2.11 له مخې $g = 2$ هم ساده ریښنه $\bmod 5^\alpha \; \forall \alpha \in \mathbb{N}$ ده، مګر جوړه، بیا هم $g' = g + p^\alpha = 2 + 5^\alpha$ ناجوړه او ساده ریښنه $\bmod 5^\alpha$ ده، نو $g' = 2 + 5\alpha$ هم ساده ریښنه $\bmod 25^\alpha$ ده.

لیما 6.2.14: د $\alpha \geq 3$ لپاره $(\mathbb{Z}^*_{2^\alpha}, \cdot)$ ځیکلیکي نه دی. (دا په دې معنا، چې ساده ریښنه $\bmod 2^\alpha$ شتون نه لري د $\alpha \geq 3$ لپاره).

جمله : (ګاوس 1777-1855 ,). $(\mathbb{Z}^*_m, \cdot)$ تیک هلته ځیکلیکي دی، که د $m \in \{2, 4, p^\alpha, 2p^\alpha\}$ سره $p > 2, p \in \mathbb{P}$ او $\alpha \in \mathbb{N}$ په خوښه وي

(6.40)

(c) ketabton.com: The Digital Library

نسبت $m = 2^\alpha, \alpha \in \mathbb{N}$ ته نو هم باور لري: $(\mathbb{Z}^*_{2^\alpha}, \cdot)$ ،، نږدي،، ``fast,, ځیکلیکي دی:

جمله 6.2.16 : هر $\overline{a} \in \mathbb{Z}^*_{2^\alpha}$ ته یو یواځنی ټاکلی $j \in \{0,1\}$ او $n \in \{1, 2, \ldots, 2^{\alpha-2}\}$ شته دی د لاندې سر ه.

(6.41)	$\overline{a} = \overline{(-1)^j 5^n}.$

کارونه: کریپتولوژي Anwendung: Kryptologie

د خبررسونې لپاره تل اړیین همداسې غوښتنوړ دی، چې معلومات فقط نیوونکي B او نه بل چا ته ورسیږي. کریپتولوژي د متودونو پوهنه ده، چې د خورا کم یا مینیمال ورزیات معلومات له مخې (د له B لارې ورکړشوی) ځوک د B → A څخه خبر پرانستلی نه شي، چې دا معلومات ونه لري.

بیلګه 6.3.1: (``Caesar,,)) الفبې: A,B, . . . ,Z، $n \in \mathbb{N}$ په خوښه ټاکل شوی، تعریفوو:

A = n-ter Buchstabe, n- م توری

B = (n+1)-ter Buchstabe,) توری م-(n+1)

⋮

Y = (n-2)-ter Buchstabe توری م-,)n-2(

Z = (n-1)-ter Buchstabe. توری م – ( )

(c) ketabton.com: The Digital Library

له دې سره د ``n=6,, لپاره بریدتکی قلفیږي و FSLWNKK ته وازېدنه ښووني ده، که $n = 6$ معلوم وي.

دا تروسه جوت د خبرونو شفرکونه یا قلفونه متمآن متود داسي په نامه تلنلار انځوروي.

فکر یا ا ند

په ټولیزه توګه یو ډېر په راتلونکي وخت کې، ډېرستر، طبیعي یا پیداېښتي ګڼ(عدد) $n \in \mathbb{N}$ په لومړنی ګڼونو نه شي ټوټه کیدی، حتی هلته هم نه، که سړی وپوهیږي، چې فقط دوه لومړني ضریبونه یا څله ووني رامنځ ته کیږي:

(6.42)	$n = p \cdot q \quad (p, q \in \mathbb{P}).$

تلنلار

که A وB به ته یو خبر استول غواړي، نو دوه ډېر ستر ګڼونه p, q ټاکي او یو عدد $e > 1, e \in \mathbb{N}$ ، ، چې($n = p \cdot q$) $\varphi(n)$ ته نسبي لومړني عدد دی، او په (څرګند ډول) n او e معلوم ورکوي. دلته غوره ټکی: که سړی n, e هم وپیژني، د n دواړه لومړني صریبونه (په ټولیزه توګه) p, q نه ټاکل کیږي. دا عددونه p, q باید سړی وپیژني د دې لپاره، چې

(6.43)	$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$

وټاکي (باید د خبرونو د وازولو لپاره وشمیرل شي: د یوه کرښیز کونګروانیځ $\bmod \varphi(n)$ حل یا اوبیونه).

د یوه خبر د قلفولو یا شفر کولو لپاره $\bmod \varphi(n)$ دا د یوه عدد بڼه (لکه په بینار بڼه) اړوي او پیداېښتي یت طبیعي عدد $w \in \mathbb{N}$ لاس ته راوړي. سړی کړی شي

(c) ketabton.com: The Digital Library

لاس ته راوړي، داسې چې خبر په بلوکونو برخو یا سترو ټوټو د $w < n = p \cdot q$ اوږدوالي سره ټوټه کړي، او دا ځانله یو پېهه ګوني دول ولېږي. دا قلف شوی $l < n$ لغات w د یوه کوچني باقيي c په توګه تعریف دی، کوم چې د $w^e \in \mathbb{N}$ سره د وېشني سره د $n = pq$ له لارې منځ ته راځي، داپه دې معنا، چې $w^e \equiv c(n)$. A اوس $c \in \mathbb{N}$ ورلېږي. د دې لپاره چې w وټاکي، له دې امله الجبري کونګروانېڅ

$x^e \equiv c(n)$	(6.44)

باید حل شي(w یو حل یا اوبی دی) .

دا چې $n \in \mathbb{N}$ ډېر لوي دی، امکان شتون لري، چې دا فقط په لومړنیو ضریبونو ټوټه شي، او $x^e \equiv c$ د یوګونو اعادو مودولو پسې حل شي(پېسې د چیني پاتې جمله 5.2.1 وکتل شي) . له دې سره باید د n دواړه لومړنیضریبونه p, q وټاکل شي.(نتشفر کیدی.

دا د p, q لپاره ډېر لوي دی،، ناشونی،،) نو له $n, e, c \in \mathbb{N}$ څخه خبر په تولیزه توګه نه شي وازیدی یا اشفري کیدی.نت

د $c \in \mathbb{N}$ وازول (د $w \in \mathbb{N}$ ټاکلولپاره) کیدی شي په لاندې توګه لاس ته راشي:

د $d \in \mathbb{N}$ $\bmod \varphi(n)$ یواځنی لاندې کرښیز کونګروانېڅ زیاتیز- یا مثبت حل دی

$ex \equiv 1(\varphi(n)),$	(6.45)

(c) ketabton.com: The Digital Library

نو باور لري، چې $w^{ed} \equiv w(n) : w \in \mathbb{N}$ خورا کوچنی ځلورئ یا مربع با قي دی،

کوم چې د n له لارې د $w^{ed} \in \mathbb{N}$ په وېش منځ ته راځي.(دا چې $c \equiv w^e$ یعني

$w^{ed} \equiv c^d$ نو له دې سره د $w \in \mathbb{N}$ شمیرنه ده د B لپاره ممکن د لویو

$n = pq, e, c, d \in \mathbb{N}$ شخه).

بشوونه: د $\text{ggT}(e, \varphi(n)) = 1$ له امله کرښیز کونګروانېنخ $ex \equiv 1(\varphi(n))$ د

5.1.1 له مخې ټیک یو $\operatorname{mod} \varphi(n)$ ناګونګروانېنخ حل لري: d .

وښایی:

(6.46)	$w^{ed} \equiv w(n).$

د $\text{ggT}(p, q) = 1$ او $n = pq$ له امله دې فقط وښوول شي، چې

(6.47)	$w^{ed} \equiv w(p) \wedge w^{ed} \equiv w(q)$

باور لري(د (6)4.1.5 له مخې لاس ته راځي، چې $w^{ed} \equiv w(pq)$ ځکه چې $\text{kgV}(p, q) = pq$ (

$p \mid w$ دی، نو هم $p \mid w^{ed}$ ،، یعني $p \mid w^{ed} - w$ ، داسي چې $w^{ed} \equiv w(p)$

باور لري. $p \nmid w$ دی : دا چې $ed \equiv 1(\varphi(n))$ (d حل دی) بار لري

(c) ketabton.com: The Digital Library

$ed = 1 + k \cdot \varphi(n)$	(6.48)

د یوه $k \in \mathbb{N}$ لپاره($e, d, 1, \varphi(n)$ زیاتیز یا مثبت دي). دا چې $\mathrm{ggT}(w, p) = 1$ ،
د ،، کوچني فرمات،، 6.1.19له مخې باور لري.

$w^{\varphi(n)}\ 1(p),$ $w^{p-1} \equiv 1(p).$ دا په دې معنا چې	(6.49)

له دې سره لرو:

$w^{ed} = w^{1+k\varphi(n)} = w^{1+k(p-1)(q-1)} =$ $= w(w^{p-1})^{k(q-1)} \equiv w \cdot 1^{k(q-1)} = w(p).$	(6.50)

ورته: $w^{ed} \equiv w(q) \Rightarrow$ غوښتنه. □

یادونه: 6.3.2 : B کړی شي د لاس ته راوړي خبر ښخه د c $d \in \mathbb{N}$ او $n = pq$
له لارې پټه خبر w وشمیري

بیلګه 6.3.3 (ګڼونه په رښتیا ډېر واړه دي!)

B $p = 3, q = 23$ غوره ټاکي، یعني $n = 23 \cdot 3 = 69, \varphi(n) = 2 \cdot 22 = 44$
او ټاکي $e > 1 \in \mathbb{N}, e = 3$ (و 44 ته نسبي لومړنی).

B معلومات ورکوي : $n = 69, e = 3$ او له A ښخه شفري خبر یا کود یا پټ خبر
$c = 12$ تر لاسه کوي.

(c) ketabton.com: The Digital Library

حلونه یا اوبیونه يي: $ex \equiv 1(\varphi(n))$ ، دا په دې معنا، چې $3x \equiv 1(44)$ ،

$\bmod 44$ یواځنی ټاکلی حل: $d = 15$. له دې سره $c^d \equiv w(n)$ ، دا په دې معنا،

چې $12^{15}(69)$.

$$12^{15} : 12^2 \equiv 6(69), 12^4 \equiv 6^2 = 36(69), 12^5 \equiv 36 \cdot 12 \equiv 18(69),$$

$$, 12^{10} \equiv 18^2 = 324 \equiv 48(69), 12^{15} = 12^{10} \cdot 12^5 \equiv 48 \cdot 18 \equiv 36(69)$$

.

نو $w \equiv 12^{15} \equiv 36(n)$ ، دا پټ لغات 36 وو.

۷ ـ د حقیقي اعدادو g –ادیکي ودیزیینه

g-adische Entwicklung reeller Zahlen

ټولزه ودیزیینه Allgemeine Entwicklungen

په برخه 1 کې د هر $a \in \mathbb{N}$ لپاره (له دې سره د هر $a \in \mathbb{Z}, a \neq 0$ لپاره) وښوول شو:

که $g \in \mathbb{N}, g \geq 2$ وي ، نو $a_n > 0, 0 \leq a_i \leq g \ (i = 0, \ldots, n-1)$ شتون لري د

$$a = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0 \qquad (7.1)$$

سره

(c) ketabton.com: The Digital Library

(د $a \in \mathbb{N}$ g -اديکي وده).

د صفر سره نابرابرو حقيقي عددونو ته تړليزونه:

د $\pi = 3,1415\ldots$ لپاره باور لري:

$$\pi = 3 \cdot 10^0 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + \cdots = \sum_{i=0}^{\infty} a_i 10^{-i}. \tag{7.2}$$

جمله 7.1.1 : $\alpha > 0$ دې يو حقيقي عددوي او $g \in \mathbb{N}, g \geq 2$. نو $a_i \in \mathbb{N}_0 \ (i = 0, 1, 2, \ldots)$ شتون لري د $0 \leq a_i \leq g \ (i = 1, 2, \ldots)$ سره، داسې چې دي

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i}. \tag{7.3}$$

که α ريښتونی يا راشنل نه وي، نو دا انځورونه يواځنۍ ده (داسې په نامه g -اديکي انځورونه).

ښوونه : د يوه داسې انځورونې يواځنوالی:

که $\alpha \in \mathbb{R}^+$ ناراشنل وي، نو $\lceil \alpha \rceil$ د α پسې خوراکوچنی عدد په ګوته کوي.

د تړليزې ښوونې روښانهونه يا تشريح:

$\pi = 3,1415\ldots$ ، تعريف کړئ$a_0 = \lceil \pi \rceil = 3$ ، $\alpha_1 = \pi - \lceil \pi \rceil$ جوړ کړئ او $a_1 = \lceil 10 a_1 \rceil = \lceil 1,415\ldots \rceil = 1$ تعريف کړئ،

(c) ketabton.com: The Digital Library

$\alpha_2 = 10\alpha_1 - [10\alpha_1] = 0,415\ldots$ جوړ کوئ او تعریف کړئ ... ،

$a_2 = [10\alpha_2] = 4$

ټولیز : دې $\alpha \in \mathbb{R}^+, g \in \mathbb{N}, g \geq 2$ په خوښه وي. اندوکتیو جوړکړئ:

$$\alpha_1 = \alpha - [\alpha], \ldots, \alpha_{i+1} = g\alpha_i - [g\alpha_i], \tag{7.4}$$

او له دې سره تعریف کړئ

$$a_0 = [\alpha], \ldots, a_i = [g\alpha_i]. \tag{7.5}$$

باور لري: $0 \leq a_i \leq g \ \forall i > 0$ ، ځکه چې

$$0 \leq \alpha_i = g\alpha_{i-1} - [g\alpha_{i-1}] < 1 \overset{g>0}{\Rightarrow} 0 \leq g\alpha_i \leq g \Rightarrow \tag{7.6}$$

$$\Rightarrow \ 0 \leq [g\alpha_i] = a_i < g. \tag{7.7}$$

باور لري

$$\alpha_1 = \alpha - [\alpha] = \alpha - a_0 \quad \Rightarrow \quad \alpha = a_0 + \alpha_1$$
$$\alpha_2 = g\alpha_1 - [g\alpha_1] \quad \Rightarrow \quad \alpha_2 = g\alpha_1 - a_1 \Rightarrow \alpha_1 = \alpha_2 g^{-1} + ($$

$$\Rightarrow \alpha = a_0 + a_1 g^{-1} + \alpha_2 g^{-1}. \quad (7.8$$

و ښایی:

(c) ketabton.com: The Digital Library

$$\alpha = a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + \alpha_{n+1} g^{-n} \ \forall n \in \mathbb{N}$$

.

$n = 1 :$

$$\alpha = a_0 + a_1 g^{-1} + \alpha_2 g^{-1}$$

پورته لور ته واز دی

$n \to n + 1 :$

$$\alpha_{n+2} = g\alpha_{n+1} - [g\alpha_{n+1}] = g\alpha_{n+1} - a_{n+1} \Rightarrow \alpha_{n+1} = a_{n+1} g^{-1} + \alpha_{n+2} g^{-1}$$

$$\Rightarrow \alpha = a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + \alpha_{n+1} g^{-n} = \tag{7.9}$$

$$= a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + (a_{n+1} g^{-1} + \alpha_{n+2} g^{-1}) g^{-n} = \tag{7.10}$$

$$= a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + a_{n+1} g^{-(n+1)} + \alpha_{n+2} g^{-(n+1)} \tag{7.11}$$

$\Rightarrow$

چې د $n + 1$ لپاره هم تیک دی.

ناپای لړۍ تخیرنې لاندې نیسو: $\sum_{i=0}^{\infty} a_i g^{-i}$ د همدا اوس تعریف تعریف شوو a_i سره.

وښایی: دا لړۍ د α : په لور ځي یا : α ته کونورکنت کیږي.

(c) ketabton.com: The Digital Library

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i}. \qquad (7.12)$$

n - مه ټوټه – یا پارشل جمعه(زیاتون)

$$s_n = \sum_{i=0}^{n} a_i g^{-i} = a_0 + a_1 g^{-\mathbf{1}} + \cdots + a_n g^{-n} \qquad (7.13)$$

$s_n = \alpha - \alpha_{n+1} g^{-n} \ \forall n \in \mathbb{N}$
پوره کوي

د $0 \leq \alpha_{n+1} < 1$ او د $g^{-n} > 0 \ (g > 0)$ له امله باور لري

$$0 \leq a_{n+1} g^{-n} < g^{-n} \ \forall n \in \mathbb{N}; \qquad (7.14)$$

له دې سره لرو: $\lim_{n\to\infty} (\alpha_{n+1} g^{-n}) = 0$ دا په دې معنا، چې

$\lim_{n\to\infty} (\alpha - s_n) = 0 \Rightarrow \lim_{n\to\infty} s_n = \alpha$ ، دا په دې معنا، چې $\sum_{i=0}^{\infty} a_i g^{-i}$ مطلق د
α په لور هڅیږي.
یواځنوالی(یواځیوالی):

شتون لري د $\alpha \notin \mathbb{Q}$ نیسوچې،

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = \sum_{i=0}^{\infty} b_i g^{-i}, \qquad (7.15)$$

(c) ketabton.com: The Digital Library

سره، چیرته چې $a_i \neq b_i$ د یوه i لپاره ، وي دې i_0 خورا کوچنی عدد د $a_{i_0} \neq b_{i_0}$ سره. بې له تولیزمحدودیت دې $a_{i_0} > b_{i_0}$ وی.

یعنې

$$a_0 = b_0, a_1 = b_1, \ldots, a_{i_0-1} = b_{i_0-1}, \qquad (7.16)$$

او لاس ته راځي $\sum_{i=i_0}^{\infty} a_i g^{-i} = \sum_{i=i_0}^{\infty} b_i g^{-i}$ ، له دې سره (د تولیز پولې ته تلنې له امله کیدی شي سره راتول شي)

$$0 = \sum_{i=i_0}^{\infty}(a_i - b_i)g^{-i} = \qquad (7.17)$$

$$= \underbrace{(a_{i_0} - b_{i_0})}_{\geq 1} g^{-i_0} + \sum_{i=i_0+1}^{\infty} \underbrace{(a_i - b_i)}_{\leq^1 -g+1} g^{-i} \geq g^{-i_0} + \sum_{i=i_0+1}^{\infty} (-g + \qquad (7.18)$$

$$= g^{-i_0} + (-g+1) \sum_{i=i_0+1}^{\infty} g^{-i} = g^{-i_0} + (-g+1) g^{-i_0+1} \underbrace{\sum_{i=0}^{\infty} g^{-}}_{=^2 \frac{g}{-1+g}} \qquad (7.19)$$

$$= g^{-i_0} - (g-1) g^{-i_0-1} \frac{g}{g-1} = g^{-i_0} - g^{-i_0} = 0. \qquad 7.20)$$

له دې سره باید په دې تخمین کې هرچیرته برابروالی باور ولري، نو له دې لاس ته راځي:

(c) ketabton.com: The Digital Library

$$a_{i_0} - b_{i_0} = 1 \wedge a_i - b_i = -(g-1) \ \forall i > i_0, \quad (7.21)$$

دا په دې معنا، چې

$$b_{i_0} = a_{i_0} - 1 \wedge b_i - a_i = g - 1 \ \forall i > i_0. \quad (7.22)$$

$a_i = 0$ او $b_i = g - 1 \ \forall i > i_0$ باور لري:

نیسو چې $0 < a_i$ ، نو د $b_i \leq g - 1$ سره لاس ته راځي، چې $b_i - a_i < g - 1$ -تضاد!

له دې سره ټول زیتوني یا د جمعي اجزاوې د α په انځورونه کې د $i > i_0$ سره صفر دي، دا په دې معنا،چې

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = a_0 + a_1 g^{-1} + \cdots + a_{i_0} g^{-i_0} = a_0 + \frac{a_1}{g} + \cdots \quad (7.23)$$

تضاد دی! نو: α فقط یوه g -ادیکي وده لري.□

یادونه 7.1.2 : دی $g = 10$ (لسمیز سیستم)، نو سړی د $\alpha = \sum_{i=0}^{\infty} a_i g^{-i}$ لپاره لیکي هم

$$a_0, a_1 a_2 \ldots \quad 0 \leq a_i < 10 \ \forall i \geq 1. \quad (7.24)$$

کورولار 7.1.3 : $\alpha > 0$ یو راشنل عدد دی، نو α خورا زیات دوه g -ادیکي انځورونې ، داسې په نامه

(c) ketabton.com: The Digital Library

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = \sum_{i=0}^{\infty} b_i g^{-i}, \tag{7.25}$$

د کوم سره چې

1. $a_i = 0 \ \forall i > i_0$,
2. $b_{i_0} = a_{i_0} - 1$ او $b_i = g - 1 \ \forall i > i_0$.

کله $\alpha \in \mathbb{Q}^+$ دوه **g** –اديکي انځورونه لري؟

پيژند(تعريف) 7.1.4: سړی وايي، $\alpha \in \mathbb{Q}, \alpha = \frac{a}{b}$ يو پای انځورونه لري، که وي

$$\alpha = \frac{a}{b} = \sum_{i=0}^{\infty} a_i g^{-i}, \tag{7.26}$$

د کړم سره چې $a_i = 0 \ \forall i > i_0 \ \left(\frac{a}{b} = a_0 + a_1 g^{-1} + \cdots + a_{i_0} g^{-i_0}\right)$

.کورولار 7.1.5: $\frac{a}{b} \in \mathbb{Q}^+$ تيک دوه مختلف g - اديکي ودې لري، که $\frac{a}{b}$ يو يواځنۍ انځورونه ولري.

ښوونه :

$(\Rightarrow)$

$\alpha = \frac{a}{b}$ دوه انځورونې لري، نو له دوي څخه يو د 7.1.3 له مخې پاي دی.

(c) ketabton.com: The Digital Library

$(\Leftarrow)$

وي دې $\alpha = \sum_{i=0}^{i_0} a_i g^{-i}$ يوه پای انځورونه، نو باور لري

$$\frac{a}{b} = \sum_{i=0}^{i_0-1} a_i g^{-i} + a_{i_0} g^{-i_0} = \sum_{i=0}^{i_0-1} a_i g^{-i} + (a_{i_0} - 1) g^{-i_0} + g^{-i_0} = \quad (7.27)$$

$$= \sum_{i=0}^{i_0-1} a_i g^{-i} + (a_{i_0} - 1) g^{-i_0} + \sum_{i=i_0+1}^{\infty} (g-1) g^{-i}, \quad (7.28)$$

دا چې

$$-g^{-i_0} + \sum_{i=i_0+1}^{\infty} (g-1) g^{-i} = -g^{-i_0} + (g-1) g^{-(i_0+1)} \underbrace{\sum_{i=0}^{\infty} g^{-i}}_{\to \frac{g}{g-1}} = \quad (7.29)$$

$$= -g^{-i_0} + (g-1) g^{-(i_0+1)} \frac{g}{g-1} = \quad (7.30)$$

$$= -g^{-i_0} + g^{-i_0} = 0. \quad (7.31)$$

نو له دې سره يوه 2 -مه g -اديکي انځورونه لري.□

(c) ketabton.com: The Digital Library

کوم $\alpha \in \mathbb{Q}^+$ یوه پای g –اديکي انځورونه لري؟

جمله 7.1.6: که $\alpha \in \mathbb{Q}^+, \alpha = \frac{a}{b}$ وي د $a, b \in \mathbb{N}$ او $\mathrm{ggT}(a,b) = 1$ سره، نو α تيک هلته يوو پای(او له دې سره 2مختلف) g -اديکي وده لري، که هر د مخرج لومړنۍ پروېشوني بنست وېشي.

ښوونه:

$(\Rightarrow)$

وي دې

$$\frac{a}{b} = \sum_{i=0}^{n} a_i g^{-i} = a_0 + a_1 g^{-1} + \cdots + a_n g^{-n}, \tag{7.32}$$

نو باور لري

$$\frac{ag^n}{b} = a_0 g^n + a_1 g^{n-1} + \cdots + a_n \in \mathbb{Z}, \tag{7.33}$$

له دې سره $b \mid ag^n$. وي دې p په خوښه د b لومړنی پروېشونی، نو $p \mid ag^n$ لاس ته راځي ، د 3.1.5 له مخې لاس ته راځي $p \mid a \vee p \mid g^n$ ، باور لري $p \nmid a$ ، ځکه چې پرته له دې به $\mathrm{ggT}(a,b) \geq p > 1$ -تضاد وي.

له دې سره لاس ته راځي $p \mid g^n$ ، دا چې $p \in \mathbb{P}$ د 3.1.5 سره لاس ته راځي $p \mid g$

$(\Leftarrow)$

(c) ketabton.com: The Digital Library

وي دې

$$b = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \qquad (7.34)$$

د ماتلاندې يا مخرج په لومړني ضريبونو تېته کونه، نو $p_i \mid b$ باور لري ، نو د وړاند نيونې له مخې $p_i \mid g \; \forall i = 1, \ldots, k$ له دې سره $p_i^{\alpha_i} \mid g^{\alpha_i} \; (i = 1, \ldots, k)$.

وي دې $m := \max\{\alpha_1, \ldots, \alpha_n\}$. نو باور لري

$$p^{\alpha_i} \mid g^m \; (i = 1, \ldots, k), \qquad (7.35)$$

دا چې $m \geq \alpha_i$.

د $\mathrm{ggT}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1 \; \forall i \neq j$ له امله باور لري

$$\mathrm{kgV}(p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = b; \qquad (7.36)$$

د تمريني بيلګې *24* له مخې باور لري: $b \mid g^m$. له دې سره دی $\frac{a}{b} g^m \in \mathbb{N}$ او وي دې

$$\frac{a}{b} g^m = a_0 + a_1 g + \cdots + a_n g^n \qquad (7.37)$$

g -اديکي وده، د کوم سره چې $0 \leq a_i < g \; \forall i \geq 1$.

له دې لاس ته راځي:

(c) ketabton.com: The Digital Library

$$\frac{a}{b}=\frac{a_0}{g^m}+\frac{a_1}{g^{m-1}}+\cdots+\frac{a_n}{g^{m-n}}=a_0g^{-m}+a_1g^{-m+1}+\cdots+a_ng^{n-m}, \quad (7.38)$$

دا په دې معنا، چې $\frac{a}{b}$ يوه پای g –اديکي وده لري. □

لاس ته راوړنه 7.1.7 : وي دې

$$g=10,\alpha=\frac{a}{b}\in\mathbb{Q},\mathrm{ggT}(a,b)=1,b>0$$

دا چې لومړنۍ پروېشونې همداسې لري، بايد مخرج د لپاره وي، له دې سره شرايط پوره دي. له دې سره په ل

دا چې $g=10$ فقط لومړنی پروطشونی $p=2$ همداسې $p=5$ لر ي، بايد د لپاره مخرج(ماتلاندې) $b=2^\alpha 5^\beta$ $\alpha,\beta\in\mathbb{N}_0$ وي، د دې لپاره چې شرايط پوره شي.
له دې سره په لسميز کې باور لري:

$$\alpha=\frac{a}{b},\mathrm{ggT}(a,b)=1$$

که يو پای(او له دې سره دوه مختلف) انځورونه ولری $\Leftrightarrow$

$$\Leftrightarrow b=2^\alpha 5^\beta,\alpha,\beta\in\mathbb{N}_0$$

.

له دې سره هم : $\exists p:p\mid b$ او $p\nmid 10\Rightarrow$ (له دې لاس ته راځي) چې فقط يوه لسميزه انځورونه شتون لري.

بيلگه :

لومړی: $\alpha=\frac{287}{100}\in\mathbb{Q}^+$، د $b=2^2 5^2$ له امله α يوه پای او له دې سره دوه لسميز انځورونه لري:

$$\alpha=2.870000\ldots=2.869999\ldots$$

(c) ketabton.com: The Digital Library

دويم: $\alpha = \frac{5}{3} \in \mathbb{Q}^+$ ، دا چې $b = 3^1$ د $2^\alpha 5^\beta$ په بڼه نه دی، نو α فقط یوه لسمیزه انځورونه لري. یا د وېشنې له لارې، یا د 7.1.1د ښوونې سره سم (α_i, a_i) :

$$\alpha = 1.6666\ldots$$

دریم: $\alpha = 1 \in \mathbb{Q}^+$ د $\alpha = \frac{1}{1}$ او $\operatorname{ggT}(1,1) = 1$ له امله لاس ته راځي چې $\alpha = 1$ یو پای او له دې سره دوه مختلف لسمیز انځورونه لري ($(\alpha = \frac{3}{3}$ اجازه نه لري، ځکه چې $\operatorname{ggT}(a,b) \neq 1\ldots)$):

$$\alpha = 1.0000\cdots = 0.9999\ldots$$

$$0.999\ldots = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \cdots = 9\left[\underbrace{\sum_{i=0}^{\infty}\left(\frac{1}{10}\right)^i}_{\to\frac{1}{1-\frac{1}{10}}=\frac{10}{9}} - 1\right] = \quad (7.39)$$

$$= 9\left[\frac{10}{9} - 1\right] = 10 - 9 = 1. \quad (7.40)$$

پریودیکي وده

د یوه حقیقی عدد په لسمیزه وده کې کله کله ځنې عددونه منظم منځ ته راځي، لکه $\alpha = 1.70714285714285\ldots$ ،

پوښتنه: کوم حقیقی اعداد دا خویونه لري:؟

(c) ketabton.com: The Digital Library

پيژند(تعريف) 7.2.1: د يوه حقيقی عدد $\alpha > 0$ يوه g -اديکي يا g –ايزه وده

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = a_0 + a_1 \frac{1}{g} + a_2 \frac{1}{g^2} + \cdots \qquad (7.41)$$

تل بيرته راګرځيدونې يا پريوديکي بلل کيږي، که $n, e \in \mathbb{N}$ شتون ولري د لا ندې سره

$$a_{n+i} = a_{n+e+i} \; \forall i = 0, 1, 2, \ldots . \qquad (7.42)$$

که n مينيمال يا خورا کوچنی ټاکلی وي، نو $a_1 a_2 \ldots a_{n-1}$ ترمخ پريود يا - راګرځيدنه بلل کيږي او $n-1$ د هغه اوږدوالی، که $n = 1$ وي(داپه دې معنا، چې ∄ترمخ پريود)، نو وده سوچه پريوديک بلل کيږي.

که e خورا کوچنی ټاکلی وي، نو $a_n a_{n+1} \ldots a_{n+e-1}$ تلبيرته راګرځيدونې بلل کيږي او e د هغه اوږدوالی.

د $g = 10:$ لپاره سومبول يا نخښ:

$$\alpha = a_0 . \underbrace{a_1 a_2 \ldots a_{n-1}}_{Vorperiode} \underbrace{a_n a_{n+1} \ldots a_{n+e-1}}_{Periode} \underbrace{a_{n+e}}_{=a_n} \ldots \underbrace{a_{n+2e-1}}_{=a_{n+e-1}} \cdots \qquad (7.43)$$

بيلګه 7.2.2 :

د الماني پښتو: اوږدوال =Länge ;

تل بيرته راګرځيدنه ، له مخه ت ل بيرته را ګرځيدنه = periode ; Vor peride

(c) ketabton.com: The Digital Library

$$\alpha = 1.\underbrace{70}_{Vorperiode}\overbrace{\underbrace{714285}_{Periode}}^{Länge\ 6714285\dots}$$

Länge 2

1.

.2 $\alpha = 2.87000\dots = 2.86999\dots$.

له مخ پريود87 نسبت 86 ته، اوږدوالى2 ، پريود 0 ، نسبت 9 ته،، اوږدوالى 1

جمله 7.2.3: يو مثبت(زياتيز) عدد α د يوه $g \geq 2$ لپاره(او له دې سره د $g \geq 2$ لپاره) تيک هلته يو پريوديکي g -ايزه وده لري، که α راشنل وي.

ښوونه:

($\Leftarrow$)

وي وې $\alpha = \frac{a}{b}, \mathrm{ggT}(a,b) = 1, b > 0$ او $g \geq 2$. لکه د 7.1.1 په ښوونه کې وي دې

$$\alpha_1 = \alpha - [\alpha],$$

$$a_0 = [\alpha],$$

$$\vdots$$

$$\alpha_{i+1} = g\alpha_1 - [g\alpha_i],$$

(c) ketabton.com: The Digital Library

$$a_i = [g\alpha_i].$$

و بنایئ $b\alpha_i \in \mathbb{Z}$:

$i = 1$:

$$b\alpha_1 = b(\alpha - [\alpha]) = b\alpha - b[\alpha] = b \cdot \tfrac{a}{b} - \underbrace{\left[\frac{a}{b}\right]}_{\in\mathbb{Z}} \cdot b \in \mathbb{Z}$$

.

$i \to i+1$:

$$b\alpha_{i+1} = b(g\alpha_i - [g\alpha_i]) = \underbrace{(b\alpha_i)}_{Ind.VS:\in\mathbb{Z}} g - b\underbrace{[g\alpha_i]}_{\in\mathbb{Z}} \in \mathbb{Z}$$

.

پیژند (تعریف) $b_i := b\alpha_i \ \forall i \in \mathbb{N}$ ، وبنایئ: $b_i \equiv g^{i-1} b_1 (b) \ \forall i \in \mathbb{N}$

$i = 1$:

$$g^{1-1} b_1 = b_1 \equiv b_1(b)$$

.

$i \to i+1$:

$b_{i+1} =$ $b\alpha_{i+1} = b(g\alpha_i - \underbrace{[g\alpha_i]}_{=a_i}) = \underbrace{(b\alpha_i)}_{=b_i} g - \underbrace{ba_i}_{\equiv 0(b)} \equiv g^{i-1} b_1 g$	(7.44)

(c) ketabton.com: The Digital Library

$= g^i b_1.$	(7.45)

د $0 \le \alpha_i < 1$ له امله باور لري

$$0 \le b\alpha_i = b_i < b \ (b > 0) \ \forall i \in \mathbb{N}; \quad (7.46)$$

نو فقط پای ډېر $b_i, i \in \mathbb{N}$ شته دی، له دې سره باید د دوي ترمنځ برابرې منځ ته راشي، دا په دې معنا،چې د $\exists n, e \in \mathbb{N}$ $b_n = b_{n+e}$ سره. پورته لور ته $(i = n)$ باور لري:

$$g^{n-1} b_1 \equiv b_n = b_{n+e} \equiv b_1 g^{n+e-1}(b), \quad (7.47)$$

د g^i سره د ضرب له لارې ($i \in \mathbb{N}$ په خوښه) لاس ته راځي:

$$g^{n-1+i} b_1 \equiv g^{n-1+e+i} b_1 (b), \quad (7.48)$$

دا په دې معنا، چې دپورته لور ته : $b_{n+i} \equiv b_{n+e+i}$ ، یعنې $b \mid b_{n+e+i} - b_{n+i}$.

د $0 \le b_{n+i} < b$ او $0 \le b_{n+e+i} < b$ له امله کمښت $< b$ دی، له دې سره لاس ته راځي

(c) ketabton.com: The Digital Library

$$b_{n+e+i} = b_{n+i}\ \forall i \in \mathbb{N};$$ (7.49)

د $b_n = b_{n+e}$ له امله (پورته) باور لري $b_{n+e+i} = b_{n+i}\ \forall i \in \mathbb{N}_0$.

له دې شره:

$$b\alpha_{n+e+i} = b\alpha_{n+i}\ (b \neq 0)$$ (7.50)

او

$$g\alpha_{n+e+i} = g\alpha_{n+i}\ \forall i \in \mathbb{N}_0, \qquad [g\alpha_{n+e+i}] = [g\alpha_{n+i}]\ \forall i \in \mathbb{N}_0,$$ (7.51)

نو $a_{n+e+i} = a_{n+i}\ \forall i \in \mathbb{N}_0$.

له دې سره د $\alpha = \frac{a}{b}$ g -ایزه وده تل بیرته راګرځیدونې ده.

$(\Rightarrow)$

وي دې $\alpha > 0$ حقیقي د پریودیکي ودې سره، داپه دې معنا، چې $n, e \in \mathbb{N}$ شتون لري د

$$a_{n+e+k} = a_{n+k}\ \forall k \in \mathbb{N}_0$$

سره؟

$a_{n+e+k} = a_{n+k}\ \forall k \in \mathbb{N}_0$;

ښوول کیږي: $\alpha \in \mathbb{Q}$:

(c) ketabton.com: The Digital Library

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + a_{n+1} g^{-(n+1)} + \cdots + \quad (7.52)$$

$$+a_{n+e-1} g^{-(n+e-1)} + \underbrace{a_{n+e}}_{=a_n} g^{-(n+e)} + \underbrace{a_{n+e+1}}_{=a_{n+1}} g^{-(n+e+1)} + \cdots + \quad (7.53)$$

$$+\underbrace{a_{n+2e-1}}_{=a_{n+e-1}} g^{-(n+2e-1)} + \cdots = \quad (7.54)$$

$$= \sum_{i=0}^{\infty} a_i g^{-i} + a_n g^{-n} \underbrace{(1 + g^{-e} + g^{-2e} + \cdots)}_{\sum_{k=0}^{\infty} (g^{-e})^k \to \frac{1}{1-\frac{1}{g^e}} = \frac{g^e}{g^e - 1}} + \cdots + \quad (7.55)$$

$$a_{n+e-1} g^{-(n+e-1)} \underbrace{(1 + g^{-e} + g^{-2e} + \cdots)}_{\sum_{k=0}^{\infty} (g^{-e})^k \to \frac{1}{1-\frac{1}{g^e}} = \frac{g^e}{g^e - 1}} = \quad (7.56)$$

$$= \sum_{i=0}^{\infty} a_i g^{-i} + \frac{g^e}{g^e - 1} (a_n g^{-n} + \cdots + a_{n+e-1} g^{-(n+e-1)}) \in \mathbb{Q}. \quad (7.57)$$

بیلګه 7.2.4: $g = 10, \alpha = 0.134\overline{2158}$ ، داچي دا یوه پریودیکي لسمیزه وده ده، لاس ته راځي: α یو راشنل عدد دی، کوم؟

$n = 4, e = 4$ ، د ترمخپریود اوږدوالی: $n - 1 = 3 \Rightarrow$ د 7.2.3 د بنووني له مخې:

(c) ketabton.com: The Digital Library

$$\alpha = \frac{134}{1000} + \frac{10^4}{10^4-1}(2\cdot\frac{1}{10^4} + \frac{1}{10^5} + 5\cdot\frac{1}{10^6} + 8\cdot\frac{1}{10^7}) = \cdots = \quad (7.5$$

ځانګړی حالت: سوچه پریودیکي وده

پوښتنه: کله د $\alpha \in \mathbb{R}^+$ g –ایزه وده سوچه –پریودیکي ده؟

د 7.2.3 له مخې باید α راشنل وي، د $g = 10$ لپاره هر $\alpha \in \mathbb{Q}^+$ د

$$\alpha = a_0.\overline{a_1 a_2 \dots a_e} \qquad (7.59)$$

سره غواړو پیداکړو.

جمله 7.2.5: که $\frac{a}{b} \in \mathbb{Q}^+$ وي د $\mathrm{ggT}(a,b) = 1, b > 0$ سره، نو د g – ایزه وده ټیک هلته سوچه پریودیکي ده، که $\mathrm{ggT}(b,g) = 1$ وي. که دا حالت وي، نو د e پریودیکي اوږدوالی د $\bar{g} \in \mathbb{Z}_b^*$ د نظم سره برابر دی(دا په دې معنا، چې د خورا کوچني طبیعي ګڼ k سره برابر دی، د $\bar{g}^k = \bar{1} \in \mathbb{Z}_b^*$ سره).

ښوونه:

$(\Rightarrow)$

وي دې $\frac{a}{b} \in \mathbb{Q}^+, \mathrm{ggT}(a,b) = 1, b > 0$ د سوچه-پریودیکي g –ایزه وې سره، دا په دې معنا،چې په $a_{n+i} = a_{n+e+i}\ \forall i \geq 0$ کې $n = 1$ دی، که e خورا کوچنی یا مینیمال وي.

(c) ketabton.com: The Digital Library

د 7.2.3 ښووني له مخې باور لري

$$g^{n+e-1}b_1 \equiv g^{n-1}b_1(b), \tag{7.60}$$

نو د $n=1$ له امله $g^e b_1 \equiv b_1(b)$ دی.

وښایئ: $\text{ggT}(b, b_1) = 1$

نیسو چې $\exists p \in \mathbb{P}$ د لاندې سره

$$p \mid b, p \mid b_1 \overset{7.1.1}{\Rightarrow} b\alpha_1 = b\left(\frac{a}{b} - \left[\frac{a}{b}\right]\right) = a - b\underbrace{\left[\frac{a}{b}\right]}_{\in\mathbb{N}},$$

له دې سرهه لاس ته راځي $p \mid a$ – تضاد و $\text{ggT}(a,p) = 1$ ته.

له دې سره د $g^e b_1 \equiv b_1(b)$ څخه د (5)4.1.5 له مخې لاس ته راځي

$$g^e \equiv 1(b). \tag{7.61}$$

وښایئ: $\text{ggT}(b, g) = 1$. نیسو چې $\exists p \in \mathbb{P}$ د $p \mid b, p \mid g$ سره، نو باور لري

$$p \mid b, p \mid g^e = 1 + tb \ (t \in \mathbb{N}), \tag{7.62}$$

نو هم $p \mid 1$ -تضاد.

(c) ketabton.com: The Digital Library

وي دې $\frac{a}{b}$ سوچه پريوديکي، نو وښايئ $e = \operatorname{ord} \bar{g}$ په $(\mathbb{Z}_b^*, \cdot)$ کې.

پورته لور ته باور لري:

$$g^e \equiv 1(b) \wedge \operatorname{ggT}(b, g) = 1; \qquad (7.63)$$

دا په دې معنا، چې $\bar{g} \in \mathbb{Z}_b^*$ او $\bar{g}^e = \bar{1}$ په $(\mathbb{Z}_b^*, \cdot)$ کې دي. يعني $\operatorname{ord} \bar{g} \leq e$ (د پيژند له مخې $\operatorname{ord} \bar{g}$ خورا کوچنی طبيعي عدد k دی د $\bar{g}^k = \bar{1}$ سره).

وي دې $\operatorname{ord} \bar{g} = k$، نو په $(\mathbb{Z}_b^*, \cdot)$ کې باور لري $\bar{g}^k = \bar{1}$، دا په دې معنا، چې $g^k \equiv 1(b)$ او $g^{k+i} \equiv g^i(b)\ \forall i \geq 0$، له دې سره هم $g^{k+i} b_1 \equiv g^i b_1(b)$ باور لري د b_1 سره د 7.2.3 ښوونې له مخې $\forall i \geq 0$.

له دې ښوونې لاس ته راځي:

$$b_{k+i+1} \equiv b_{k+i}(b), \qquad (7.64)$$

نو $b_{k+i+1} = b_{k+i}$، او

$$a_{1+k+i} = a_{1+i}\ \forall i \geq 0. \qquad (7.65)$$

دا چې د e د $a_{1+e+i} = a_{1+i}\ \forall i \geq 0\ (n = 1)$ سره خورا کوچنئ ده، لاس ته راځي $e \leq k = \operatorname{ord} \bar{g}$. له دې امله په $(\mathbb{Z}_b^*, \cdot)$ کې باور لري $e = k = \operatorname{ord} \bar{g}$

(c) ketabton.com: The Digital Library

$(\Leftarrow)$

وي دي $ggT(b, g) = 1$ ، د ښوولو دی: د $\frac{a}{b}$ g -ایزه وده سوچه پریودیک ده.

دا چې $\frac{a}{b} \in \mathbb{Q}^+$ د 7.2.3له مخې یو پریودیکي اونځورونه شتون لري، یعني د لاندې سره:

$$g^{n-1}b_1 \equiv g^{n+e-1}(b). \tag{7.66}$$

داچې $ggT(b, g) = 1$ ، نو $ggT(b, g^{n-1}) = 1$ هم شتون لري، یعني دپورته کونګروانځ څخه لاس ته راځي $b_1 \equiv g^e b_1(b)$. یعني د ټولو $i \geq 0 : g^i b_1 \equiv g^{e+i} b_1(b)$ لپاره، نو د جملې7.2.3 د ښوونې له مخې لرو: $b_{i+1} \equiv b_{e+i+1}(b)$ ، له دې سره $b_{i+1} = b_{e+i+1} \; \forall i \geq 0$ او $a_{1+i} = a_{1+e+i} \; \forall i \geq 0$. دا په دې معنا،چې د $\frac{a}{b}$ g –ایز یا g –ایډیکي انځورونه پریودیکي ده د $n = 1$ سره، یعني سوچه تل بیرته راګرځیدونی یا پریودیکي. □

یادونه 7.2.6: ایا د $\frac{a}{b} \in \mathbb{Q}^+$ g -ایزه وده د $ggT(a, b) = 1, b > 0$ سره، سوچه پریودیکي ده، او هم د پریود اوږدوالی د ماتلاندې یا مخرج b په واک کې دی!

بیلګه 7.2.7:

1. $g = 10, a = \frac{3}{7} \in \mathbb{Q}^+$.

دا چې $ggT(3, 7) = 1$ د 7.2.5له مخې باور لري: $\frac{a}{b} = \frac{3}{7}$ سوچه پریودیکي لسمیزه

(c) ketabton.com: The Digital Library

وده لري($\mathrm{ggT}(7,10)=1$)، د کوم سره چي د بريود اوږدوالی $e=\mathrm{ord}\,\overline{10}$ په $(\mathbb{Z}_7^*,\cdot)$ کي دی:

$$10^1\not\equiv 1(7), 10^2\not\equiv 1(7),\ldots,10^6\equiv 1(7)$$

(د لومړي ځل لپاره)....

. $e=6$also نو, $\Rightarrow \mathrm{ord}\,\overline{10}=6$

$$\left(\frac{3}{7}=0.\overline{428571}\right)$$

.2 $g=\mathbf{10},\alpha=\frac{15}{7}\in\mathbb{Q}^+$.

$\mathrm{ggT}(15,7)=\mathbf{1}$

سوچه پريوديکي د $e=\mathrm{ord}\,\overline{10}=6$ سره.

$$\left(\frac{15}{7}=2.\overline{142857}\right)$$

ټوليز حالت: نه سوچه – پريوديکي وده

جمله 7.2.8 : وي دې $\frac{a}{b}\in\mathbb{Q}^+,\mathrm{ggT}(a,b)=1,b>0$. دی

$$g=p_1^{\alpha_1}\cdots p_k^{\alpha_k} \quad (7.67)$$

د بنسټ $g\geq 2$ په لومړنيو ضريبونو ټوټه کونه او

$b=p_1^{\beta_1}\cdots p_k^{\beta_k}\cdot t$	(7.68)

(c) ketabton.com: The Digital Library

(د همغه p_i سره!) د $\mathrm{ggT}(g,t)=1$ سره، نو د ترمخ پريود اوږدوالی($n-1$

) په g -ايز دوه کې خورا کوچنی طبيعي عدد γ دی، د کوم لپاره چې $\frac{b}{t} \mid g^{\gamma}$ دی، او

د $\bar{g}$ پريود اوږدوالی د پريود د نظم سره پرابر دی په $(\mathbb{Z}_t^*,\cdot)$ کې.

بېلګه 7.2.9: $g=\mathbf{10}, \frac{a}{b}=\frac{239}{140}\in\mathbb{Q}^+$ ، لسميزه وده سوچه پريوديک نه ده، ځکه

چې $\mathrm{ggT}(b,g)=\mathrm{ggT}(140,10)\neq 1$.

د پريود ا وږدوالی:

$$\left.\begin{array}{rcl} g=10 & = & 2\cdot 5 \\ b=140 & = & 2^2\cdot 5\cdot 7 \end{array}\right\} \Rightarrow t=7, \frac{b}{t}=\frac{140}{7}=20$$

$$20\nmid 10^1, 20\mid 10^2=100 \Rightarrow \gamma=2.$$

د پريود اوږدوالی:

په $e=\mathrm{ord}\,\bar{g}$ $(\mathbb{Z}_t^*,\cdot)$ کې: $e=\mathrm{ord}\,\overline{10}$ په $(Z_7^*,\cdot)$ کې ، پورته لور ته لاس

ته راځي $e=6$.

$$\Rightarrow \frac{a}{b}=a_0.\underbrace{a_1a_2}_{Vorperiode}\underbrace{\overline{a_3a_4a_5a_6a_7a_8}}_{Periode}; \qquad \frac{239}{140}=1.70\overline{714285}$$

n-te Potenzreste م-n توان

په ځانګړي حالت بيرته اړول

(c) ketabton.com: The Digital Library

دلته $x^n \equiv a(m)$ په

(8.2)	$x^n \equiv a(p^\alpha)$

بیره اړول کیږي د $\mathrm{ggT}(a,p)=1$ سره (یعني په $(\mathbb{Z}^*_{p^\alpha},\cdot)$ کې شمیرنه).

لیما 8.1.2: د $x^2 \equiv a(m)$ د $m = p_1^{\alpha_1}\cdots p_l^{\alpha_k}$ سره ټیک هلته حولوړ ده، که

(8.3) $$x^2 \equiv a(p_i^{\alpha_i}) \quad i = 1, 2, \ldots, k$$

حلوړ وي(برخه 5 وګورئ)

لیما 8.1.3: د $x^n \equiv a(p^\alpha), p \in \mathbb{P}, \alpha \in \mathbb{N}$ د $a = p^k a'$ لپاره د $\mathrm{ggT}(p,a')=1$ سره ټیک هلته حلوړ ده، که $n \mid k$ او $x^n \equiv a'(p^{\alpha-k})$ حلوړ وي $(0 \leq a < p^\alpha)$.

ښوونه:

$(\Rightarrow)$

دې د $x_0 \in \mathbb{Z}$ د $x^n \equiv a(p^\alpha)$ حل وي، نو باور لري:

(8.4) $$x_0^n \equiv a(p^\alpha),$$

(c) ketabton.com: The Digital Library

دا په دې معنا، چې $x_0^n = a + rp\alpha$ دی د یوه $r \in \mathbb{Z}$ لپاره.

وي دې $x_0 = p^\beta s$ د $\mathrm{ggT}(p, s) = 1 \ (\beta \in \mathbb{N}_0)$ سره، نو باور لري:

$$x_0^n = (p^\beta s)^n = p^{n\beta} s^n = a + rp^\alpha = p^k a' + rp^\alpha. \qquad (8.5)$$

د $a = p^k a' < p^\alpha$ له امله باور لري: $k < \alpha \ (a' > 0)$، یعني $p^k \mid p^\alpha$، له دې سره دېورته لور ته:

$$p^{n\beta - k} s^n = a' + rp^{\alpha - k}; \qquad (8.6)$$

له دې سره باور لري: $p^k \mid p^{n\beta} s^n$، د $\mathrm{ggT}(p, s) = 1$ له امله هم $\mathrm{ggT}(p^k, s^n) = 1$ دي، یعني د 2.2.11 سره لاس ته راځي: $p^k \mid p^{n\beta}$، یعني $k \leq n\beta$.

که $k < n\beta$ وی، نو $n\beta - l > 0$ به وی او د

$$p^{n\beta - k} s^n = a' + rp^{\alpha - k} \qquad (8.7)$$

له مخې به مو لرودی: $p \mid a'$ او $\mathrm{ggT}(p, a') \neq 1$ چې تضاد دی.

له دې سره: $k = n\beta$ او $n \mid k$، پسې لاس ته راځي:

$$s^n = a' + rp^{\alpha - k}, \qquad (8.8)$$

دا په دې معنا، چې $s^n \equiv a'(p^{\alpha - k})$ او $s \in \mathbb{Z}$ د $x^n \equiv a'(p^{\alpha - k})$ یو حل دی.

(c) ketabton.com: The Digital Library

$(\Leftarrow)$

وي دې $x_0 \in \mathbb{Z}$ د $x^n \equiv a'(p^{\alpha-k})$ حل د $n \mid k$ او د $\mathrm{ggT}(a', p) = 1$ سره، نو باور لري $x_0^n \equiv a'(p^{\alpha-k})$، يعنې $x_0^n p^k \equiv a' p^k (p^\alpha)$ هم. د $n \mid k$ له امله باور لري $k = nt$

د يوه $t \in \mathbb{N}$ لپاره.

$$x_0^n p^{nt} \equiv a(p^\alpha) \Rightarrow (x_0 p^t)^n \equiv a(p^\alpha), \quad (8.9)$$

له دې سره $s = x_0 p^t \in \mathbb{Z}$ د کونګروانت $x^n \equiv a(p^\alpha)$ يو حل دی.□

يادونه 8.1.4: له دې سره د $x^n \equiv a'(p^{\alpha-k})$ له حل x_0 څخه د $\mathrm{ggT}(a', p) = 1$ سره د $x^n \equiv a(p^\alpha)$ هر حل x_1 شمېرل کيدی شي:

$$x_1 = x_0 p^t, \quad (8.10)$$

د کوم سره چې $k = nt$ باور لري.

لاس ته راوړنه 8.1.5: د مسآلې $x^n \equiv a(p^\alpha)$ سره سړی کړی شي ځان په حالت $\mathrm{ggT}(a, p) = 1$ محدود کړي $(\Rightarrow \mathrm{ggT}(a, p^\alpha) = 1)$، دا په دې معنا، چې سړی کړی شي په $(\mathbb{Z}^*_{p^\alpha}, \cdot)$ کې شميرنه وکړي $(\overline{a} \in \mathbb{Z}^*_{p^\alpha})$.

ليما 8.1.6: x_0 د $x^n \equiv a(p^\alpha)$ حل دی د $\mathrm{ggT}(a, p) = 1$ سره، نو $\mathrm{ggT}(x_0, p) = 1$ هم باور لري (دا په دې معنا، چې $\overline{x_0}^n = \overline{a} \in \mathbb{Z}^*_m \Rightarrow \overline{x_0} \in \mathbb{Z}^*_m$).

(c) ketabton.com: The Digital Library

ښوونه: د $x_0^n \equiv a(p^\alpha)$ له امله باور لري $p^\alpha \mid x_0^n - a$، دا په دې معنا، چې

$x_0^n - a = tp^\alpha \ (t \in \mathbb{N}) \Rightarrow a = x_0 - tp^\alpha.$	(8.11)

نیسو چې $\exists q \in \mathbb{P}$ د $q \mid x_0, q \mid p$ سره، نو $q = p$ او $q = p \mid a$ لرو له دې لرو: تضاد دی.

له دې سره موږ سرچینه پیز ه مسآله په $(\mathbb{Z}_{p^\alpha}^*, \cdot)$ کې شمیرنه باندې بیرته واړوله.

پیژند(تعریف) 8.1.7 : و ي دې $m \in \mathbb{N}, a \in \mathbb{Z}$ د $\mathrm{ggT}(a,m) = 1$ سره، نو $a \in \mathbb{Z}$ یو *n* –م توان مودولو m بلل کیږي، که $x^n \equiv a(m)$ حلوړ وي.(دا په دې معنا،، چې $\overline{a} \in \mathbb{Z}_m^*$ د یوه توکي $\overline{x_0} \in \mathbb{Z}_m^*$ n -م توان دی).

بیلګه 8.1.8: $m = 6, a = 0, 1, 3, 4$ دویمتوانپاتې $\bmod 6$ دی، د $a = 2, 5$ دویم توانپاتې $\bmod 6$ نه دی(پورته وګورئ).

پسې: هر $a \in \mathbb{Z}$ دریم توانپاتې $\bmod 6$ دی(پورته وګور ئ)

د $x^n \equiv a(p^\alpha), \mathrm{ggT}(a,p) = 1$ د حل لپاره تګلار

لومړی: تولیز د الجبري کونګروانت لپاره له برخې5 څخه(مفصل)

دویم: که د داسې په نامه اندکسجدول لهمخې یوه ساده رېښه $\bmod p^\alpha$ شتون ولري.)

پام دې وي: د ګاوس 6.2.15 له مخې ، د هر لومړني عدد $p \neq 2$ او هر $\alpha \in \mathbb{N}$ لپاره یوه ساده ریښه $\bmod p^\alpha$ شتون لري، ورپسې د 2 او $4 = 2^2$ ته، مګر نه د 2^α لپاره د $\alpha \geq 3$ سره، د دې لپاره: ځانله پام په کار ی)

(c) ketabton.com: The Digital Library

پيژند 8.1.9 : $m \in \mathbb{N}$ دې داسې وي، چې $(\mathbb{Z}_m^*, \cdot)$ څيوکليکي يا تل بيرته راګرځيدونی دی، دا په دې معنا،چې ساده ريښه $g \bmod m$ شتون($\exists$) لري، دا په دې معنا،چې $\overline{g}$ توليدوي $(\mathbb{Z}_m^*, \cdot)$ او دی

$$\mathbb{Z}_m^* = \{\overline{g}, \overline{g}^2, \ldots, \overline{g}^{\varphi(m)}\}. \tag{8.12}$$

که $\overline{a} \in \mathbb{Z}_m^*$ په خوښه وي، نو خورا کوچنی طبيعي عدد k يا 0 بلل کيږي، چې د هغې لپاره $\overline{a} = \overline{g}^k$ د a اينډکس دی نسبت g ته، سومبوليک: $I_g(a)$.

يادونه 8.1.10: $I_g(a)$ يواځنی ټاکلی دی، ځکه چې

$$\mathbb{Z}_m^* = \{\overline{g}, \overline{g}^2, \ldots, \overline{g}^{\varphi(m)}\} \tag{8.13}$$

او د دوي څخه ټول توکي مختلف دي: $\overline{a} = \overline{g}^{I_g(a)}$ ټيک يو ځل رامنځ ته کيږي. د اينډکی جدول د هر $\overline{a} \in \mathbb{Z}_m^*$ لپاره (څيکليکي وړاندنيونه) $I_g(a) \in \mathbb{N}_0$ راکوي.

بيلګه 8.1.11: $m = 14 = 2 \cdot 7$ ، د ګاوس 6.2.15 له مخې $(\mathbb{Z}_{14}^*, \cdot)$ له دې امله څيوکليکي دی، يعني يوه ساده ريښه $\bmod 14$ ستون لري.

$g = 3$ يوه ساده ريښه $\bmod 7$ده، خکه چې

$$\mathbb{Z}_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\} \tag{8.14}$$

او $\overline{3} = \overline{3}, \overline{3}^2 = \overline{2}, \overline{3}^3 = \overline{6}, \overline{3}^4 = \overline{4}, \overline{3}^5 = \overline{5}, \overline{3}^6 = \overline{1}$ ، داپه دې معنا، چې$\overline{3}$ $\mathbb{Z}_7^*$ توليدوي،

(c) ketabton.com: The Digital Library

دا چي g ناجوړه یا طاق دی، د 6.2.12 د ښووني له مخې ترې لاس ته راځي:

$g = 3$ هم سادهرېښه $\bmod 14$ دی.

$$\mathbb{Z}_{14}^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\} \tag{8.15}$$

$$(\varphi(14) = \varphi(2 \cdot 7) = \varphi(2)\varphi(7) = 1 \cdot 6 = 6)$$

د $\overline{3} \in \mathbb{Z}_{14}^* : \overline{3} = \overline{3}, \overline{3}^2 = \overline{9}, \overline{3}^3 = \overline{13}, \overline{3}^4 = \overline{11}, \overline{3}^5 = \overline{5}, \overline{3}^6 = \overline{1}$ توان.

له دې سره لاندې اینډکس جدول راکوي:

(8.16)

$\overline{a}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{9}$	$\overline{11}$	$\overline{13}$
$I_g(a)$	0	1	5	2	4	3

لیما 8.1.12: وي دې g ساده رېښه $\bmod m$ ، نو باور لري:

لومړی: $g^i \equiv g^j (m) \Leftrightarrow i \equiv j(\varphi(m))$

دویم : $a, b \in \mathbb{Z}, \mathrm{ggT}(a, m) = \mathrm{ggT}(b, m) = 1$ دي ، نو باور لري

$$I_g(ab) \equiv I_g(a) + I_g(b)(\varphi(m)). \tag{8.17}$$

ښوونه:

لومړی: $(\Rightarrow)$ (لاس ته راځي)

(c) ketabton.com: The Digital Library

وي دې $g^i \equiv g^j(m)$ د $i > j$ لپاره، نو په $(\mathbb{Z}_m^*, \cdot)$ کې $\overline{g}^i = \overline{g}^j$ باور لري،
يعني د $\overline{g}^{-j} \in \mathbb{Z}_m^*$ سره د ضرب له مخې لرو:

$$\overline{g}^{i-j} = \overline{1}. \tag{8.18}$$

دا چې د $\overline{g}$ $(\mathbb{Z}_m^*, \cdot)$ ګروپ توليدوي، $\operatorname{ord} \overline{g} = \varphi(m)$ دی. د [6.2.7](#) له مخې لاس ته راځي

$$\varphi(m) \mid i - j, \tag{8.19}$$

داپه دې معنا، چې $i \equiv j(\varphi(m))$.

$(\Leftarrow)$

برعکس دې $i \equiv j(\varphi(m))$ وي، نو باور لري

$$\varphi(m) \mid i - j \Rightarrow i - j = t\varphi(m)\ t \in \mathbb{Z}; \tag{8.20}$$

يعني $i = j + t\varphi(m)$ او:

$$\overline{g}^i = \overline{g}^{j+t\varphi(m)} = \overline{g}^j \left(\overline{g}^{\varphi(m)}\right)^t = \overline{g}^j, \tag{8.21}$$

دا په دې معنا، چې $\overline{g^i} = \overline{g^j}$ او له دې سره $g^i \equiv g^j(m)$.

(c) ketabton.com: The Digital Library

لومړی: د $\mathrm{ggT}(a,m) = \mathrm{ggT}(b,m) = 1$ له امله باور لري: $\overline{a},\overline{b} \in \mathbb{Z}_m^*$ یعنې $\overline{a}\overline{b} \in \mathbb{Z}_m^*$، یعنې $I_g(ab)$ او باور لري

$$\overline{g}^{I_g(ab)} = \overline{ab} = \overline{a}\overline{b} = \overline{g}^{I_g(a)+I_g(b)}, \qquad (8.22)$$

دویم یعنې $\overline{g^{I_g(ab)}} = \overline{g^{I_g(a)+I_g(b)}}$، له دې سره

$$g^{I_g(ab)} \equiv g^{I_g(a)+I_g(b)}(m) \overset{1.}{\Rightarrow} I_g(ab) \equiv I_g(a) + I_g(b)(\varphi(m)). \qquad (8.23)$$

ترې لاس ته راوړنه 8.1.13: وي دې $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ د $\mathrm{ggT}(a_i, m) = 1\ (i = 1, \ldots, k)$ سره او g دې یوه ساده ریښه $\bmod m$ وي، نو د ایندکشن سره لاس ته راځي:

$$I_g(a_1 \cdots a_k) \equiv I_g(a_1) + \cdots + I_g(a_k)(\varphi(m)). \qquad (8.24)$$

په ځانګړې توګه دې وي $a_i = a(i = 1, \ldots, k)$، نو لاس ته راځي

$$I_g(a^k) \equiv kI_g(a)(\varphi(m)). \qquad (8.25)$$

دا خویونه د هغه ورسره بلد لوګاریتم سره ورته دی، چې په انالیز کې څېړل شوي.

له دې امله I_g د اعدادو تیوریکي لوګاریتم بلل کیږي.

(c) ketabton.com: The Digital Library

د حل ساده متودونه Einfache Lösungsmethode

ځانګړی حالت

له دې سره د ځنو الجبري کونګروانتونو د حل ساده امکانات شته، که یوه ساده ریښه شتون ولري:

$\alpha)$ ورکړل شوي: $ax \equiv b(m)$ د $\mathrm{ggT}(a,m) = \mathrm{ggT}(b,m) = 1$ سره او g ساده ریښه $\bmod n$ ده. په $\mathbb{Z}_m^*$ کې حل کوو $\overline{ax} = \overline{b}$ ، یعنې:

$$\overline{g}^{I_g(ax)} = \overline{g}^{I_g(b)} \iff g^{I_g(ax)} \equiv g^{I_g(b)}(m) \tag{8.26}$$

$$\overset{8.1.12}{\iff} I_g(ax) \equiv I_g(b)(\varphi(m)) \tag{8.27}$$

$$\iff I_g(a) + I_g(x) \equiv I_g(b)(\varphi(m)) \tag{8.28}$$

$$\iff I_g(x) \equiv I_g(b) - I_g(a)(\varphi(m)). \tag{8.29}$$

دې له ایندکس جدول څخه وټاکل شي. x د دې کرښیز مساوات حل وي، نو $I_g(x)$ که

لیما 8.2.1: $3x \equiv 5(14); \mathrm{ggT}(3,14) = \mathrm{ggT}(5,14) = 1, g = 3$ ساده ریښه $\bmod 14$ ده، حل کوو:

(8.30)	$I_3(x) \equiv I_3(5) - I_3(3)(6).$

$I_3(x) \equiv 5 - 1 = 4(6) \Rightarrow I_3(x) = 4$ (

(c) ketabton.com: The Digital Library

(0 ≥ کوچنی حل)

$\Rightarrow x = \overline{11}$

$\beta)$

$ax^n \equiv b(m)$ ورکړل شوي د $\mathrm{ggT}(a,m) = \mathrm{ggT}(b,m) = 1$ سره او g ساده ریښه $\bmod m$ ده. د حل دی: $\overline{ax}^n = \overline{b}$ په $(\mathbb{Z}_m^*, \cdot)$ کې، یعنې

$$\overline{g}^{I_g(ax^n)} = \overline{g}^{I_g(b)} \Leftrightarrow g^{I_g(ax^n)} \equiv g^{I_g(b)}(m) \quad (8.31)$$

$$\Leftrightarrow I_g(ax^n) \equiv I_g(b)(\varphi(m)) \quad (8.32)$$

$$\Leftrightarrow I_g(a) + I_g(x^n) \equiv I_g(b)(\varphi(m)) \quad (8.33)$$

$$\Leftrightarrow nI_g(x) \equiv I_g(b) - I_g(a)(\varphi(m)) \quad (8.34)$$

له دې لاس ته راځي: په نامعلومه $I_g(x)$ کې د دې کرښیز کونګروانت په حل بیرته اړوو، که دا حلوړ وي، نو $I_g(x)$ د اندکس جدول کې پیدا کړئ او اړونده $\overline{x} \in \mathbb{Z}_m^*$ وټاکئ.

بیلګه 8.2.2:

$$5x^2 \equiv 9(14), \mathrm{ggT}(5,14) = \mathrm{ggT}(9,14) = 1, g = 3$$

ساده ریښه $\bmod 14$ دی، له دې سره حل کوو:

(c) ketabton.com: The Digital Library

$$2I_3(x) \equiv I_3(9) - I_3(5)(6) \Rightarrow 2I_3(x) \equiv 2 - 5 = -3(6). \quad (8.35)$$

د $\mathrm{ggT}(2,6) = 2 \nmid -3$ له امله حل نه شته، او لهدې سره د پيل يا سرچينييز کونگروانت $5x^2 \equiv 9(14)$ حل هم نه شته.

$$5x^3 \equiv 9(14), \mathrm{ggT}(5,14) = \mathrm{ggT}(9,14) = 1, g = 3$$

ساده رېښه $\bmod 14$ ده، د حل دی:

$$3I_3(x) \equiv I_3(9) - I_3(5) = 2 - 5 = -3(6). \quad (8.36)$$

د $\mathrm{ggT}(3,6) = 3 \mid -3$ له امله يو حل شتون لري (حتا 3 انکوگروانت حلونه):

$$I_3(x) = \begin{cases} 1 & \overline{3} \\ 3 \;\Rightarrow & \overline{5} \\ 5 & \overline{13} \end{cases} \quad (8.37)$$

د $\overline{x}$. په حيث

$\gamma)$

د $a \cdot b^x \equiv c(m)$ ورکړ شوي د $\mathrm{ggT}(a,m) = \mathrm{ggT}(b,m) = \mathrm{ggT}(c,m) = 1$

سره او g ساده رېښه $\bmod m$ ده. د حل ده: $\overline{a} \cdot \overline{b}^x = \overline{c}$ په $(\mathbb{Z}_m^*, \cdot)$ کې.

يعنې:

(c) ketabton.com: The Digital Library

$$\overline{g}^{I_g(ab^x)} = \overline{g}^{I_g(c)} \Leftrightarrow g^{I_g(ab^x)}(m) \equiv g^{I_g(c)}(m) \quad (8.38)$$

$$\overset{8.1.12}{\Leftrightarrow} I_g(a) + xI_g(b) \equiv I_g(c)(\varphi(m)), \quad (8.39)$$

دا په دې معن، چې باتې دی په x کې یو کرښیز کونګروانت حل کړو.

بیلګه 8.2.3:

$$3 \cdot 5^x \equiv 11(14) \ \mathrm{ggT}(3,14) = \mathrm{ggT}(5,14) = \mathrm{ggT}(11,14) = \mathbf{1}, g = 3$$

ساده ریښه دی، له دې سره حل کوو:

$$\underbrace{I_3(3)}_{=1} + x\underbrace{I_3(5)}_{=5} \equiv \underbrace{I_3(11)}_{=4} \underbrace{(6)}_{=\varphi(14)}, \quad (8.40)$$

دا په ې معنا، چې $5x \equiv 3(6)$، یعني حل کوو $5x \equiv 15(6)$، له دېسره $x \equiv 3(6)$، دا په دې معنا، چې $x_0 = 3$.

ترې لاس ته راتلنه 8.2.4 : د $x^n \equiv a(m)$ $\mathrm{ggT}(a,m) = 1$ سره او g ساده ریښه $\bmod m$ حلوړ ده....

$$\ldots \Leftrightarrow \overline{g}^{I_g(x^n)} = \overline{g}^{I_g(a)} \text{ په } (Z_m^*, \cdot) \text{ کې } \ldots \quad (8.41)$$

$$\overset{8.1.12}{\Leftrightarrow} I_g(x^n) \equiv I_g(a)(\varphi(m)) \quad (8.42)$$

(c) ketabton.com: The Digital Library

$$\Leftrightarrow \quad nI_g(x) \equiv I_g(a)(\varphi(m)) \tag{8.43}$$

$$\overset{5.1.1}{\Leftrightarrow} \quad \mathrm{ggT}(n, \varphi(m)) \mid I_g(a). \tag{8.44}$$

داچې سړی پورته لور ته په $m = p^\alpha, p \in \mathbb{P}, \alpha \in \mathbb{N}$ او په $\mathrm{ggT}(a, m) = 1$ ځان محدودولی شي، نو ټول حالتون پرته له $m = 2^k$ څخه د $k \geq 3$ سره رانیول شوي یا رانغاړل شوي دي(پرتله 6.1.10: د $p^\alpha, p \neq 2, \alpha \in \mathbb{N}$ لپاره په خوبنه $(\mathbb{Z}^*_{p^\alpha}, \cdot)$ ځیکلیکي دی، دا په دې معنا، چې یوه ساده ریښه $\bmod p^\alpha$ شتون ري). دا په جمله 8.2.7 کې په ځانله ډول ځیرل کیږي. د n - م توان لپاره یوه بله قضیه لاندې نتیجه انځوروي:

جمله : $m \in \mathbb{N}$ دې د $\mathbb{Z}^*_m$ سره ځیکلیکي وي. د $a \in \mathbb{Z}$ $\mathrm{ggT}(a, m) = 1$ سره ټیک هلته n –م توان $\bmod m$ دی، که د $d := \mathrm{ggT}(n, \varphi(m))$ سره باور ولري:

$$a^{\frac{\varphi(m)}{d}} \equiv 1(m). \tag{8.45}$$

نو د $x^n \equiv a(m)$ د $\bmod m$ انکونګروانت حلونو ګنون یا تعداد d دی.

ښوونه:

$(\Rightarrow)$

(c) ketabton.com: The Digital Library

$$a^{\frac{\varphi(m)}{d}} \equiv (x_0^n)^{\frac{\varphi(m)}{d}} = \left(x_0^{\varphi(m)}\right)^{\frac{n}{d}} = 1^{\frac{n}{d}} = 1(m). \quad (8.46)$$

$(\Leftarrow)$

وي دې $a^{\frac{\varphi(m)}{d}} \equiv 1(m)$ ، دا چې $\mathbb{Z}_m^*$ ځیوکلیکي دی یوه ساده ریښه $g \bmod m$ شتون لري . یعنې

(8.47)	$\overline{a} = \overline{g}^{I_g(a)},$

دا په دې معنا، چې $a \equiv g^{I_g(a)}(m)$ او

(8.48)	$1 \equiv a^{\frac{\varphi(m)}{d}} \equiv \left(g^{I_g(a)}\right)^{\frac{\varphi(m)}{d}} = g^{\frac{\varphi(m)I_g(a)}{d}}(m),$

دا په دې معنا، چې $\overline{1} = \overline{g}^{\frac{\varphi(m)I_g(a)}{d}}$. د 6.2.7 له مخې لاس ته راځي

$$\underbrace{\operatorname{ord}(\overline{g})}_{=\varphi(m)} \left| \frac{\varphi(m)I_g(a)}{d} \right., \quad (8.49)$$

دا په دې معنا، چې $d\varphi(m) \mid \varphi(m)I_g(a) \Rightarrow d \mid I_g(a)$

له دې سره د5.1.1 له مخې کربنیز کونګروانت

$$ny \equiv I_g(a)(\varphi(m)) \quad (8.50)$$

حلوړ دی، یعنې $a \in \mathbb{Z}$ n -مه ریښه ده.

(c) ketabton.com: The Digital Library

پسي د 5.1.1 له مخې باور لري: دا کربنيز کونګروانت $d \bmod \varphi(m)$ انکونګروانت حلونه لري. د $y_0 \in \mathbb{Z}$ لپاره د

$$ny_0 \equiv I_g(a)(\varphi(m)) \qquad (8.51)$$

سره ټيک يو $x_0 \in \mathbb{Z}$ شتون لري د $x_0^n \equiv a(m)$ سره، ځکه چې:

له $y_0 = I_g(x_0) = I_g(x_1)$ لاس ته راځي

$$\overline{x_1} = \overline{g}^{I_g(x_1)} = \overline{g}^{I_g(x_0)} = \overline{x_0}, \qquad (8.52)$$

يعني ټيک يو $\overline{x_0} \in \mathbb{Z}_m^*$ شتون لري.

له دې سره $x^m \equiv a(m)$ هم ټيک $d = \mathrm{ggT}(n, \varphi(m)) \bmod m$ انکونګروانت حلونه لري. □

بيلګه 8.2.6: وي دې $x^5 \equiv 7(25)$ حلوړ، دا په دې معنا، چې:

ايا $a = 7$ پنځة توان $\bmod 25$ دی؟ی.

د ګاوس له مخې: $a = 7, n = 5, m = 25 = 5^2$ ځيوکليکي د $\mathbb{Z}_{5^2}^*$

$$\varphi(m) = \varphi(25) = 20$$

(c) ketabton.com: The Digital Library

$$\Rightarrow d := \mathrm{ggT}(n, \varphi(m)) = \mathrm{ggT}(5, 20) = 5 \quad (8.53)$$

$$\Rightarrow a^{\frac{\varphi(m)}{d}} = 7^{\frac{20}{5}} = 7^4 \equiv (-1)^2(25) = 1(25), \quad (8.54)$$

دا په دې معنا، چې7 پنځم توان $\bmod 25$ دی.

ټول حلونه د د ساده ريښې $g = 2$ او اندکس جدول له مخې لاس ته راځي

$\Rightarrow 5 \bmod 25$

انکونګوانت حلونه $2, 7, 12, 17, 22$.

د $x^n \equiv a(2^k), k \geq 3$ لپاره د حل متودونه

په پای کې لکه نور چې ويلي مو وو د

$m = 2^k, k \geq 3,$

حالت $\mathbb{Z}^*_{2^k}$ د نه ځيکليکي، سره ځانونه په کار اچوو:

جمله 8.2.7: وي دې $k \geq 3, a \in \mathbb{Z}$ ، د $\mathrm{ggT}(a, 2^k) = 1$ سره ټيک هلته n ــم توان $\bmod 2^k$ دی، که د $d = \mathrm{ggT}(n, 2^{k-2})$ لپاره باور ولري:

1. $a^{\frac{2k-2}{d}} \equiv 1(2^k)$,
2. $a \equiv 1(4)$ يا n ناجوړه يا طاق دی.
3.

د $x^n \equiv a(m)$ د $\bmod 2^k$ انکوګروانتو حلونو ګڼ،ڼ(تعداد) نو بيا 1 دی د n ناجوړه يا طاق لپاره، او $2d$ د جوړه n لپاره.

(c) ketabton.com: The Digital Library

د $x^n \equiv a(2^k)$ د حل(نو) پیداکول له ښووني 8.2.7 څخه:

$\overline{a} \in \mathbb{Z}_{2^k}$ په لاندې بڼه

$$\overline{a} = \overline{(-1)^j 5^l}, \qquad j \in \{0,1\}, l \in \{1,\ldots,2^{k-2}\} \tag{8.55}$$

په يواځني ډول د 6.2.16له مخې انځور کړئ، راوړو

$$nx \equiv l(2^{k-2}); \text{ همداسې } nx \equiv j(2) \tag{8.56}$$

کرښيز کونګروانت دي، که د α د $nx \equiv j(2)$ راکمشوی حل وي او د β $nx \equiv l(2^{k-2})$ راکړ شوی حل، نو دی

(8.57)	$\overline{x_0} = \overline{(-1)^\alpha 5^\beta}$

د $x^n \equiv a(2^k)$ حل دی. له دې سره سرې ټول حلونه لاس ته راوړي.

بيلګه 8.2.8 :

.1 $x^3 \equiv 9(32) : N = 3, a = 9, m = 2^5(k = 5)$.

و ښايئ: $a = 9$.توانپاتي $\text{mod } 32$ دی (راوړو: $\mathbb{Z}_{32}^*$ د ګاوس له مخې ځيوکليکي نه دی ، ځکه چې $k \geq 3, p = 2$) د 8.2.7سره سم:

$$d = \text{ggT}(n, 2^{k-2}) = \text{ggT}(3,8) = 1 \Rightarrow \tag{8.58}$$

$$a^{\frac{2^{k-2}}{d}} = 9^{2^{5-2}} = \left(9^4\right)^2 = \left(81^2\right)^2 \equiv 1(32), \tag{8.59}$$

(c) ketabton.com: The Digital Library

۳ . 9نو دريٍ توانپاتي دی

حل: د $n = 3$ ناجوړه يا طاق له امله فقط يو انکونګروانت $\bmod 32$ حلونه لري:، د 8.2.7 ښوونې سره سم:

$$\overline{a} = \overline{9} = \overline{(-1)^j 5^l}, \qquad j \in \{0, 1\}, l \in \{1, \ldots, 2^{k-2}\} \tag{8.60}$$

: $\bmod 32$4.

$$5^0 \equiv 1, 5^1 \equiv 5, 5^2 \equiv -7, 5^3 \equiv -3, 5^4 \equiv -15, 5^5 \equiv -11, 5^6 \equiv 9(32),$$

4. يعني $j = 0, l = 6 \leq 2^{k-2} = 8$، له دې سره $\overline{9} = \overline{(-1)^0 5^6}$ ، د حل دي:
$nx \equiv j(2)$ ، دا په دې معنا، چې $3x \equiv 0(2)$ ، دا په دې معنا،چې $\alpha = 0$ (راکم شوي)، $nx \equiv l(2^{k-2})$ دا په ي معن، چې $3x \equiv 6(8)$ ، دا په دې معنا، چې $\beta = 2 \Rightarrow$ له دې لاس ته راځي يوګونی حل $\bmod 32$ دی.

$$\overline{x_0} = \overline{(-1)^\alpha 5^\beta} = \overline{25}. \tag{8.61}$$

$x^4 \equiv 177(224) : n = 4, a = 177, m = 224 = 7 \cdot 2^5,$.

$ggT(177, 224) = 1$,

له دې جلا تر راوړو: $x^4 \equiv 177(7)$ او $x^4 \equiv 177(2^5)$

$x^4 \equiv 177(7)$

(c) ketabton.com: The Digital Library

$\Rightarrow x^4 \equiv 2(7) : n = 4, a = 2, p = 7$; د ګاوس له مخې ځیوکلیکي دی، د8.2.5 سره سم:

$$\varphi(7) = 6, d = \text{ggT}(n, \varphi(7)) = 2; a^{\frac{\varphi(7)}{2}} = 8 \equiv 1(7) \Rightarrow \quad (8.62)$$

د 8.2.5 له مخې باور لري 2 د 4–م توان د سره اینکونګروانت حلونه دی

$x^4 \equiv 177(2^5)$ $\Rightarrow x_1 = 2, x_2 = 5$.

$\Rightarrow x^4 \equiv 17(2^5) : n = 4$

جوړه مګر $a = 17 \equiv 1(4)$ ، $17^{\frac{2^3}{4}} = 17^2 \equiv 1(32)$

او همداسې د 8.2.7 له مخې : 17 د 4-م توان $\bmod 32$ دی د $8 \bmod 32$ سره اینکونګروانت حلونه $y_1, y_2, \ldots, y_8$ دي.

(د $\overline{a} = \overline{(-1)^j 5^l}$ سره سم او $nx \equiv j(2)$ کربنیزکوګروانت همداسې $nx \equiv l(2^{k-2}) \Rightarrow$ څخه لاس ته راځي تول α ، تول $\beta \Rightarrow$ څخه لاس ته راځي تول $\overline{y} = \overline{(-1)^{\alpha} 5^{\beta}}$.)

د حینایيي پاتې جملې سره سم:

$$\left. \begin{array}{rcl} x & \equiv & x_i(7), \\ x & \equiv & y_s(32) \end{array} \right\} \qquad i = 1, 2, s = 1, \ldots, 8, \qquad (8.63)$$

یعني 16 سیستمي له دې لاس ته راځي 16 حلونه.

(c) ketabton.com: The Digital Library

څلوريز پاتې(که غواړئ: مربع باقيمانده)Quadratische Reste

ځانګړی حالت

موږ اوس يوځانګړی حالت رااخلو، او د هده حلوړوالی تيک تر څيرني لاندې نيسو:

$n = 2$ دا په دې معنا،چې

$$x^2 \equiv a(m) \qquad (9.1)$$

د څيرني دی. د دې د حلوړولي لپاره ساده قضيي تر څيرني لاندې نيول زموږموخه ده.

پيژند 9.1.1 : $m \in \mathbb{N}, a \in \mathbb{Z}, \mathrm{ggT}(a,m) = 1$ مربعيز توانپاتې $\bmod m$ بلل کيږي، او هم لنډ مربعيز پاتې، که $x^2 \equiv a(m)$ حلوړ وي.

دا لاندې د $m = 2$ لپاره باور لري:

ليما يا جملګئ 9.1.2: وي دې $a \in \mathbb{Z}$ د $\mathrm{ggT}(a,m) = 1 \Rightarrow a$ سره ناجوړه(طاق)، دا په دې معنا،چې $2n+1$. نو باور لري:

هر ناجوړه عدد

$$x_0 = 2k + 1 \ (k \in \mathbb{Z}) \qquad (9.2)$$

حلوړ $\bmod 2$ دی.

ښوونه: $x_0^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 1(2) \ (\equiv 2n + 1 \equiv a(2))$.

د عمومي قضيي 8.2.5 (هلته $n \in \mathbb{N}$ په خوښه)، څيکليکي يا تل بيرته راګرځيدونکی حالت له مخې:

(c) ketabton.com: The Digital Library

جمله 9.1.3 : وي دې $m \in \mathbb{N}, m \geq 3; a \in \mathbb{Z}$ د $\mathrm{ggT}(a,m)=1$ سره تیک هلته مربع پاتې $\bmod m$ دی، که

$$a^{\frac{\varphi(m)}{2}} \equiv 1(m); \qquad (9.3)$$

د $x^2 \equiv a(m)$ د حلونو تعداد یا ګنون 2 وي.

ښوونه: ځکه چې $d = \mathrm{ggT}(2, \varphi(m))$ او دا چې $\varphi(m)$ د $m \geq 3$ لپاره دی تل جوړه دی، نو د 8.2.5 له مخې باور لري،:

لومړی: که د m د په لومړني ضربیتجزیه کې یو ناجوړه(طاق) p_i رامنځ ته شي، نو $p_i - 1$ جوړه یا جفت دی او له دې امله $\varphi(m) \equiv 0(2)$ دی.

دویم: که نه ، نو بیا ۲-م توان دی، یعني $\varphi(m) = \frac{m}{2}$ جوړه دی.

($m = 2^\alpha$ د $\alpha \geq 2$ سره ، ځکه چې $m \geq 3$)

جملګی ۴ . ۱ . ۹ : (اویلر)

د $x^n \equiv a(2^k), k \geq 3$ لپاره د حل متودونه

په پای کې لکه نور چې ویلي مو وو د
$m = 2^k, k \geq 3,$

حالت $\mathbb{Z}^*_{2^k}$ د نه خیکلیکي، سره ځانونه په کار اچوو:

جمله 8.2.7: وي دې $k \geq 3, a \in \mathbb{Z}$ ، د $\mathrm{ggT}(a, 2^k) = 1$ سره تیک هلته n –م توان $\bmod 2^k$ دی، که د $d = \mathrm{ggT}(n, 2^{k-2})$ لپاره باور ولري:

4. $a^{\frac{2k-2}{d}} \equiv 1(2^k)$,

(c) ketabton.com: The Digital Library

.5 $a \equiv 1(4)$ يا n ناجوړه يا طاق دی.

.6

د $x^n \equiv a(m)$ د $\bmod 2^k$ انکوګروانتو حلونو ګڼېږ(تعداد) نو بيا 1 دی د n ناجوړه يا طاق لپاره، او $2d$ د جوړه n لپاره.

د $x^n \equiv a(2^k)$ د حل(نو) پيداکول له ښووني 8.2.7 څخه:

$\overline{a} \in \mathbb{Z}_{2^k}$ په لاندې بڼه

$$\overline{a} = \overline{(-1)^j 5^l}, \qquad j \in \{0,1\}, l \in \{1,\ldots,2^{k-2}\} \qquad (8.55)$$

په يواځني ډول د 6.2.16له مخې انځور کړئ، راوړو

(8.56)	$nx \equiv j(2)$ همداسې $nx \equiv l(2^{k-2})$;

کرښيز کونګروانت دي، که د α د $nx \equiv j(2)$ راکشوی حل وي او د β $nx \equiv l(2^{k-2})$ راکم شوی حل، نو دی

$$\overline{x_0} = \overline{(-1)^{\alpha} 5^{\beta}} \qquad (8.57)$$

د $x^n \equiv a(2^k)$ حل دی. له دې سره سرې ټول حلونه لاس ته راوړي.

بېلګه : 8.2.8

$$x^3 \equiv 9(32) : N = 3, a = 9, m = 2^5 (k = 5)$$

.2 .

و ښايئ: $a = 9$.توانياتي $\bmod 32$ دی (راوړو: $\mathbb{Z}_{32}^*$ د ګاوس له مخې څيوکليکي نه دی ، ځکه چې $k \geq 3, p = 2$) د 8.2.7سره سم:

$$d = \mathrm{ggT}(n, 2^{k-2}) = \mathrm{ggT}(3,8) = 1 \Rightarrow \qquad (8.58)$$

(c) ketabton.com: The Digital Library

$$a^{\frac{2^{k-2}}{d}} = 9^{2^{5-2}} = \left(9^4\right)^2 = \left(81^2\right)^2 \equiv 1(32), \qquad (8.59)$$

۳ . 9 نو دريې توانپاتې دى

حل: د $n = 3$ ناجوړه يا طاق له امله فقط يو انکونګروانت mod 32 حلونه لري:، د 8.2.7 ښووني سره سم:

$$\overline{a} = \overline{9} = \overline{(-1)^j 5^l}, \qquad j \in \{0, 1\}, l \in \{1, \ldots, 2^{k-2}\} \qquad (8.60)$$

: mod 324.

$$5^0 \equiv 1, 5^1 \equiv 5, 5^2 \equiv -7, 5^3 \equiv -3, 5^4 \equiv -15, 5^5 \equiv -11, 5^6 \equiv 9(32),$$

4. يعني $j = 0, l = 6 \leq 2^{k-2} = 8$، له دې سره $\overline{9} = \overline{(-1)^0 5^6}$ ، د حل دي: $nx \equiv j(2)$ ، دا په دې معنا، چې $3x \equiv 0(2)$، دا په دې معنا،چې $\alpha = 0$ (راکم شوي)، $nx \equiv l(2^{k-2})$ دا په ې معن، چې $3x \equiv 6(8)$ ، دا په دې معنا، چې $\beta = 2 \Rightarrow$ له دې لاس ته راځي يوګونی حل mod 32 دى.

$$\overline{x_0} = \overline{(-1)^{\alpha} 5^{\beta}} = \overline{25}. \qquad (8.61)$$

$x^4 \equiv 177(224) : n = 4, a = 177, m = 224 = 7 \cdot 2^5,$

$\mathrm{ggT}(177, 224) = 1$,

له دې جلا تر راوړو: $x^4 \equiv 177(7)$ او $x^4 \equiv 177(2^5)$

$x^4 \equiv 177(7)$

$\Rightarrow x^4 \equiv 2(7) : n = 4, a = 2, p = 7$; د ګاوس له مخې ځيوکليکي دى، د8.2.5 سره سم:

$$\varphi(7) = 6, d = \mathrm{ggT}(n, \varphi(7)) = 2; a^{\frac{\varphi(7)}{2}} = 8 \equiv 1(7) \Rightarrow \qquad (8.62)$$

د 8.2.5 له مخې باور لري 2 د 4–م توان د سره اينکونګروانت حلونه دى

(c) ketabton.com: The Digital Library

$$\Rightarrow x_1 = 2, x_2 = 5$$

.

$$x^4 \equiv 177(2^5)$$

$$\Rightarrow x^4 \equiv 17(2^5) : n = 4$$

جوړه مګر $a = 17 \equiv 1(4)$ ، $17^{\frac{2^3}{4}} = 17^2 \equiv 1(32)$

او همداسې د 8.2.7 له مخې : 17 د 4-م توان $\mod 32$ دی د $8 \mod 32$ سره اینکونګروانت حلونه $y_1, y_2, \ldots, y_8$ دي.

(د $\overline{a} = \overline{(-1)^j 5^l}$ سره سم او $nx \equiv j(2)$ کرښیزکوګروانت همداسې $nx \equiv l(2^{k-2}) \Rightarrow$ څخه لاس ته راځي ټول α ، ټول $\beta \Rightarrow$ څخه لاس ته راځي ټول $\overline{y} = \overline{(-1)^{\alpha} 5^{\beta}}$.)

د حينايیي پاتې جملې سره سم:

$$\left.\begin{array}{lll} x & \equiv & x_i(7), \\ x & \equiv & y_s(32) \end{array}\right\} \qquad i = 1, 2, s = 1, \ldots, 8, \tag{8:63}$$

يعني 16 سيستمي له دې لاس ته راځي 16 حلونه.

څلوريز پاتې(كه غواړئ: مربع باقيمانده) ځانګړی حالت

موږ اوس يوځانګړی حالت رااخلو، او د هده حلوړوالی ټيک تر څيړنې لاندې نيسو:

(c) ketabton.com: The Digital Library

$n=2$ *دا په دې معنا،چې*

$$x^2 \equiv a(m) \qquad (9.1)$$

د ښيرنې دی. د دې د حلوړولي لپاره ساده قضيي تر ښيرنې لاندې نيول زمورړموخه ده.

پيژند 9.1.1 : $m \in \mathbb{N}, a \in \mathbb{Z}, \mathrm{ggT}(a,m)=1$ مربعيز توانپاتي $\bmod m$ بلل کيږي، او هم لنډ مربعيز پاتې، که $x^2 \equiv a(m)$ حلوړ وي.

دا لاندې د $m=2$ لپاره باور لري:

ليما يا جملګۍ 9.1.2: وي دې $a \in \mathbb{Z}$ د $\mathrm{ggT}(a,m)=1 \Rightarrow a$ سره ناجوړه(طاق)، دا په دې معنا،چې $2n+1$. نو باور لري:

هر ناجوړه عدد

$$x_0 = 2k+1 \ (k \in \mathbb{Z}) \quad (9.2)$$

حلوړ $\bmod 2$ دی.

ښوونه: $x_0^2 = (2k+1)^2 = 4k^2+4k+1 \equiv 1(2) \ (\equiv 2n+1 \equiv a(2))$.

د عمومي قضيي [8.2.5](#) (هلته $n \in \mathbb{N}$ په خوښه)، ښيکليکي يا تل بيرته راګرځيدونکی حالت له مخې:

جمله 9.1.3 : وي دې $m \in \mathbb{N}, m \geq 3; a \in \mathbb{Z}$ د $\mathrm{ggT}(a,m)=1$ سره تيک هلته مربع پاتې $\bmod m$ دی، که

$$a^{\frac{\varphi(m)}{2}} \equiv 1(m); \quad (9.3)$$

د $x^2 \equiv a(m)$ د حلونو تعداد يا ګڼون 2 وي.

ښوونه: ځکه چې $d = \mathrm{ggT}(2, \varphi(m))$ او دا چې $\varphi(m)$ د $m \geq 3$ لپاره دی تل جوړه دی، نو د [8.2.5](#) له مخې باور لري،:

(c) ketabton.com: The Digital Library

لومړی: که د m په لومنیو ضربیتجزیه کې یو ناجوړه p_i منځ ته راشي، نو $p_i - 1$ جوړه دی او له دې امله $\varphi(m) \equiv 0(2)$،

دویم: که نه، نو یو ۲-م ـتوان دی، یعنې $\varphi(m) = \frac{m}{2}$، جوړه.
($m = 2^\alpha$ د $\alpha \geq 2$ سره ځکه چې $m \geq 3$)

کورولار ۹ . ۱ . ۴ (اویلر $(\mathbf{Euler})$) : وي دې $p > 2$ لومړنی عدد، د $a \in \mathbb{Z}$ $\mathrm{ggT}(a, p) = 1$ (خورا غټ پروېشوی یا بزرګترین قاسم مشترک) سره تېک هلته مربعیز باقي یا پاتې $\bmod p$ دی، که

$$a^{\frac{p-1}{2}} \equiv 1(p).\ (9{:}4)$$

ښوونه: د ګاوس 6.2.15 له مخ او د $p \neq 2$ له امله $(\mathbb{Z}_p^*, \cdot)$ تل بیرته راګرځیدنی یا ځیکلیکي دی.

جملګی ۹ . ۱ . ۵ - وي دې $p > 2$ یو لومړنی عدد، $a \in \mathbb{Z}$ له $\mathrm{ggT}(a, p) = 1$ سره تېک هلته مربع باقي یا پاتې $\bmod p^\alpha\ \forall \alpha \in \mathbb{N}$ دی، که a مربع باقي $\bmod p$ وي

ښوونه:

$(\Rightarrow)$

ساده دی.

$(\Leftarrow)$

(c) ketabton.com: The Digital Library

که a مربع باقي $\bmod p$ وي، نو د جملګي9.1.4 له مخې باور لري: $a^{\frac{p-1}{2}} \equiv 1(p)$

، يعني $a^{\frac{p-1}{2}} = 1 + tp$ د يوه $t \in \mathbb{Z}$ لپاره. له دې امله د هر $\alpha \in \mathbb{N}$ لپاره باور ري:

$a^{\frac{\varphi(p^\alpha)}{2}} = a^{\frac{1}{2}p^{\alpha-1}(p-1)} = \left(a^{\frac{p-1}{2}}\right)^{p^{\alpha-1}} = (1+tp)^{p^{\alpha-1}} \equiv 1(p^\alpha),$	(9.5)

ځکه: (ایندکشن په α پسې).

$\alpha = 1$	
$(1+tp)^{p^{\alpha-1}} = 1 + tp \equiv 1(p).$	(9.6)
$\alpha \to \alpha + 1$	
$(1+tp)^{p^\alpha} = \left[(1+tp)^{p^{\alpha-1}}\right]^p = (1+rp^\alpha)^p =$	(9.7)
$= \underbrace{1 + \underbrace{\binom{p}{1}}_{=p} rp^\alpha + \cdots + r^p p^{\alpha p}}_{=1+sp^{\alpha+1}} \equiv 1(p^{\alpha+1}).$	(9.8)

د جملې 9.1.3 پسې لرو($m = p^\alpha$ لپاره): $a \in \mathbb{Z}$ مربع پاتې $\bmod p^\alpha$ دی. □

د ناځيکليکي حالت لپاره، يعنې $m = 2^k, k \geq 3$ بايد $a \in \mathbb{Z}$ ناجوړه(طاق) وي، لکه لاندې جمله چې ښايي:

(c) ketabton.com: The Digital Library

جمله ۹ . ۱ ۶ : وي دي $a \in \mathbb{Z}$ ناجوړه، نو کونګروانځ یا ورته والی $x^2 \equiv a(2^k)$ دی

لومړی- د $k = 1$ لپاره تل حلوړ دی او تیک یو حل لري.

دویم - د $k \geq 3$ لپاره حلوړ دی، د 4 حلونو سره، که $a \equiv 1(8)$ وي، پرته له ې نه.

ښوونه: لومړی- پورته وګوری: $m = 2 = 2^1$ ، دا چي تول ناجوړه ګنونه یا اعداد $\bmod 2$ دي، نو تیک یو حل شتون لري.

دویم: د ګاوس [6.2.15](#) له مخي ، $(\mathbb{Z}_4, \cdot)$ تلبیرته راګرځیدونی یا ځیکلیکي دی، یعني د [9.1.3](#) له مخي: $a \in \mathbb{Z}$ ناجوړه مربع پاتي $\ldots \bmod 4$ دی.

$\ldots \Leftrightarrow a^{\frac{\varphi(4)}{2}} \equiv 1(4) \Leftrightarrow a^{\frac{2}{2}} \equiv 1(4) \Leftrightarrow a \equiv 1(4).$	(9.9)

دریم: په همدي ترتیب د [9.1.3](#) پسي: د $x^2 \equiv a(4)$ د حلونو ګنون یا تعداد 2 دی.

. وي دي $m = 2^k, k \geq 3$ حلوړ، نو دی

$x_0^2 \equiv a(2^k)$	(9.10)

څلورم- د یوه $x_0 \in \mathbb{Z}$ لپاره، له دي سره $x_0^2 \equiv a(8)$ ، ځکه چي $8 \mid 2^k \ (k \geq 3)$ ، پسي د [8.1.6](#) له مخي باور لري: خورا غټ ګډ پرویشونی(بزرګترین مقسوم علیه) $\mathrm{ggT}(x_0, 2^k) = 1$ ، نوله دي سره $\mathrm{ggT}(x_0, 8) = 1 \ (8 \mid 2^k, k \geq 3)$. دا په دي معنا، چي $x_0 \in \mathbb{Z}$ نسبت و 8 ته نسي لومړنی عدد دی، یعني : $x_0 = 1, 3, 5, 7(8)$ ، له دي سره $x_0^2 \equiv 1(8)$.

(c) ketabton.com: The Digital Library

په ټولیزه توګه:

(9.11)	$a \equiv x_0^2 \equiv 1(8).$

پنځم- وي دي په ځټ يا برعکس $a \equiv 1(8)$، يعني هم $a \equiv 1(4)$، پسې باور لري

(9.12)	$a^{2^{k-3}} \equiv 1(2^k)\ (k \geq 3).$

شپږم- ايندکشن: د نيوني يا قرضيي له مخي.

نيسو چې د لپاره سم دی، د لپاره باور لري:

(9.13) (9.14)	$a^{2^{(k+1)-3}} = \left(a^{2^{k-3}}\right)^2 = (1+t2^k)^2 = 1+2t2^k+t^2 2^{2k} = 1+s2^{k+1} \equiv \equiv 1(2^{k+1}).$

اوم- له دې سره لرو $a \equiv 1(4)$ او $(d = \mathrm{ggT}(2, 2^{k-2}) = 2)$

(9.15)	$a^{\frac{2^{k-2}}{d}} = a^{2^{k-3}} \equiv 1(2^k);$

اتم- نو د 8.2.7 له مخې لرو، چې $a \in \mathbb{Z}$ مربع پاتې يا باقي $\bmod 2^k$ دی. له دې سره $2d = 4$ حلونه باور لري. □

بيلګه ۹ . ۱ . ۷ : ايا $x^2 \equiv 110(211)$ حلوړ دی؟ ($\Leftrightarrow$ 110مربع پاتې $\bmod 211$ دی؟)

(c) ketabton.com: The Digital Library

دا چې 211 يو لومړنی ګڼ یا عدد دی، او $ggT(110,211)=1$ د اويلر 9.1.4 پسې
بار لري، ټیک هلته حلوړ دی، که وي:

(9.16)		$a^{\frac{p-1}{2}} = 110^{105} \equiv 1(211)$

- ډير کار غواړي!

Legendre-Symbol (1752-1833) لژندر-سومبول:

د $x^2 \equiv a(m), ggT(a,m)=1$ د حلوړوالي لپاره نوې لار.

پيژند یا تعریف ۹ . ۲ . ۱ : (لژندر سيمبول [9.1]): وي دې $p>2$ يو لومړنی ګڼ یا عدد،
$a \in \mathbb{Z}$ د لژندر سومبول له مخي مربع پاتي د دې لاندې له لارې تعریع دی:

(9.17)	a مربع باقي mod p دی. P|a نه مربع باقي mod p دی.	$\left(\frac{a}{p}\right) = \begin{cases} 1 \\ 0 \\ -1 \end{cases}$

ساده خويونه:

جملګی ۹ . ۲ . ۲ : که $a \equiv a'(p)$ وي، باور لري

(c) ketabton.com: The Digital Library

(9.18)	$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$.

بـﻮونه:

(9.19)	$\left(\frac{a}{p}\right) = 1$ مربع باقي $\bmod p$
(9.20)	$\Leftrightarrow \quad x^2 \equiv a(p)$
(9.21)	$\Leftrightarrow \quad x^2 \equiv a'(p)$
(9.22)	$\Leftrightarrow \quad \left(\frac{a'}{p}\right) = 1.$

جملکی ۹ . ۳ – وېش له باقي يا پاتي سره:

(9.23)	$a = p \cdot s + r$

د $0 \leq r < p$ سره، له دې امله دی $a = ps + r \equiv r(p)$ ، نو د 9.2.2 پسې:

(9.24)	$\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right) \ldots$ لندونه

جمله ۹ . ۲ . ۴ : وي دې $p > 2$ يو لومړنی عدد او $a \in \mathbb{Z}$ د(خورا غټ ګډ پروېشونی) $\operatorname{ggT}(a, p) = 1$ سره ، نو باور لري

(c) ketabton.com: The Digital Library

(9.25)	$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(p).$

ښوونه:

- که $\left(\frac{a}{p}\right) = 1$ وي، نو a مربع پاتې $\bmod p$ دی او د 9.1.4 پسي یا له $a^{\frac{p-1}{2}} \equiv 1(p)$ مخې:، له دې سره دی

(9.26)	$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(p).$

- که $\left(\frac{a}{p}\right) = -1$ وي، نو a مربع باقي نه $\bmod p$ دی او د 9.1.4 له مخې یا $a^{\frac{p-1}{2}} \not\equiv 1(p)$ $a^{\frac{p-1}{2}} - 1 \not\equiv 0(p)$ پسي:، دا په دې معنا، چې . د 6.1.18 له مخې باور لري

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

نو $a^{p-1} - 1 \equiv 0(p)$، د اسې چې په بدن (انګریزي یې فیلډ) $(\mathbb{Z}_p, +, \cdot)$ کې (p لومړنی کڼ یا عدد) باور لري:

(9.28)	$\bar{0} = \overline{a^{p-1} - 1} = \overline{(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)} = \underbrace{\overline{a^{\frac{p-1}{2}} - 1}}_{\neq \bar{0}}\,\overline{a^{\frac{p-1}{2}} + 1};$

دا چې بدن صفر نه لري، لرو

(9.29)	$\overline{a^{\frac{p-1}{2}} + 1} = \bar{0}.$

له دې سره $a^{\frac{p-1}{2}} + 1 \equiv 0(p)$ او $a_1, \ldots, a_n \in \mathbb{Z}$، دا په دې معنا، چې

(c) ketabton.com: The Digital Library

(9.30)	$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (p).$

کورولار ۹ . ۲ . ۵: $p>2$ دې لومړني عدد وي او $a_1,\dots,a_n \in \mathbb{Z}$ د خ غ ګ یعني $\mathrm{ggT}(a_i,p)=1$ $(i=1,\dots,n)$ سره، نو باور لري

(9.31)	$\left(\frac{a_1\cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\cdots\left(\frac{a_n}{p}\right).$

ښوونه: $\mathrm{ggT}(a_1\cdots a_n,p)=1$، ځکه چې پرته له دې به $p \mid a_1\cdots a_n$، داسي چي د یوه $1\le i\le n$ لپاره د 3.1.5 له مخې $p \mid a_i$ لرو. – تضاد یا مخمخوالی! له دي سره $\left(\frac{a_1\cdots a_n}{p}\right)$ تعریف دی.

(9.32)	$\left(\frac{a_1\cdots a_n}{p}\right) \equiv (a_1\cdots a_n)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}}\cdots a_n^{\frac{p-1}{2}} \equiv \left(\frac{a_1}{p}\right)\cdots\left(\frac{a_n}{p}\right) (p).$

له دې امله p کمښت وېشي، یعني $p \mid (\pm1)-(\pm1)$. دا کمښت صفر دی، که دواړه عددونه برابر وي، او پرته له دې ±2.

له $p>2$ امله باورلري: $p \nmid \pm2 \Rightarrow$ یعني لاس ته راغلی کمښت $=0 \Rightarrow$ لاس ته راځي (9.26). □

لاس ته راوړنه ۹ . ۲ . ۶ :

لومړی- $a=\pm p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ دې د $a\in\mathbb{Z}$ $(a\neq0)$ په لومړنیو ضریبونو ټوټه کونه یا تجزیه وي. نو د 9.2.5 له مخې باور لري:

(c) ketabton.com: The Digital Library

(9.33)	$$\left(\frac{a}{p}\right)=\left(\frac{\pm1}{p}\right)\left(\frac{p_1^{\alpha_1}}{p}\right)\cdots\left(\frac{p_k^{\alpha_k}}{p}\right),$$

دويم: نو شميرو: $\left(\frac{-1}{p}\right)$ او $\left(\frac{q^{\alpha}}{p}\right)$ د خ غ پ(قاسم بزرګ مشبرک) $\mathrm{ggT}(p,q^{\alpha})=1$ سره، دا په دې معنا، چې $p\neq q$.

دريم: $\left(\frac{q^2}{p}\right)=1$ ، ځکه چې $x^2\equiv q^2(p)$ د حل په حيث $x_0=q$ لري، دا په دې معنا، چې q^2 تل مربع باقي $\bmod p$ دی.

څلورم: ځانګړی حالت: $\left(\frac{1}{p}\right)=1\ (1=1^2\overset{2.}{\Rightarrow}$ مو غوښتنه يا ثبوت دی.

پنځم: له ې امله فقط د شميرلو لپاره: $\left(\frac{-1}{p}\right)$ او $\left(\frac{q}{p}\right)$ د $p\neq q$ سر لومړنی عدد 2 < دی، ځکه چې

(9.34)	$$\left(\frac{q^{2k}}{p}\right)=\left(\frac{(q^k)^2}{p}\right)=1.$$

کورولار يا جملګی ۹ . ۲ . ۷ : وي دې $p>2$ لومړنی عدد، نو باور لري:

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

لومړی- -1 تيک هلته مربع باقي $\bmod p$ دی، که $p\equiv1(4)$ وي.

ښوونه:

لومړی- د له مخې باور لري:

(c) ketabton.com: The Digital Library

(9.35)	$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} (p);$

دويم: نو p کمښت يا تفريق وېشي، دا 0 يا ± 2 دی. د $p > 2$ له امله دی

$p \nmid \pm 2 \Rightarrow$ (له دې لاس ته راځي)

$\Rightarrow 0 =$ کمښت

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

دويم: مربع پاتې دی

(9.37)	$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \overset{1.}{\Leftrightarrow} \ldots$
(9.38)	$\Leftrightarrow \frac{p-1}{2}$ جوړه
(9.39)	$\Leftrightarrow \frac{p-1}{2} = 2k \ (k \in \mathbb{N})$
(9.40)	$\Leftrightarrow p - 1 = 4k$
(9.41)	$\Leftrightarrow p = 4k + 1$
(9.42)	$\Leftrightarrow p \equiv 1(4).$

لاندې جمله د ديريښلت د جملې څوکه انځوروي، چې نوره غواړو وښايو:

(c) ketabton.com: The Digital Library

جمله ۹ . ۲ . ۸ : د $4k+1$ $(k\in\mathbb{N})$ بڼې ناپای ډېر لومړني ګڼونه شتون لري.

ښوونه: ناسیده، نیسو چې د دې بڼې پای ډېر ګڼونه شتون لري:

$p_1,\dots,p_n$. وي دې

(9.43)	$N:=(2p_1\cdots p_n)^2+1,$

نو باور ري: $N=2m+1$ ، یعني ناجوړه، ا په دې معنا، چې $2\nmid N$.

د $N>1$ له امله یو لومړنی عدد p د $p\mid N$ شتون لري، داپه دې معنا، چې $N\equiv 0(p)$. نو:

(9.44)	$(2p_1\cdots p_n)^2\equiv -1(p).$

دا په دې معنا چې -1 مربع پاتې یا باقي $\bmod p$ دی. د [9.2.7](#) له مخې لرو یا لاس ته راځي:

(9.45)	$p\equiv 1(4),$

دا په دې معنا چې $p=4k+1$. د نیونې یا فرضیې له مخو لاس ته راځي: $p=p_i$ د یوه $1\le i\le n$ لپاره. له دې امله باور لري

(9.46)	$p\mid(2p_1\cdots p_n)^2;$

د $p\mid N$ له امله لاس ته راځي:

(9.47)	$p\mid N-(2p_1\cdots p_n)^2=1,$

نو $p\le 1$ - تضاد یا ردونه. □

(c) ketabton.com: The Digital Library

د ګاوس ليما يا جملګۍ

جمله ۹ ، ۲ . ۹ : (د ګاوس جمله ګۍ) وي دي $p > 2$ لومړنی عدد، $a \in \mathbb{Z}$ د خورا غټ ګډ پروېشوني (بزرګترين مقسوم عليه مشترک) $\mathrm{ggT}(a,p) = 1$ سره.

جوړووو: $1 \cdot a, 2 \cdot a, \ldots, \frac{p-1}{2} \cdot a$ او د p له لارې باقي سره د وېش له لارې د اړونده پاتې سره، نو باور لري

(9.48)	$\left(\frac{a}{p}\right) = (-1)^{n(a)},$

چيرته چي $n(a)$ سره د باتي يا باقي ګڼون يا تعداد په نخښه کيږي، چي له $\frac{p}{2}$ لوی دي.

ښوونه: د $i = 1, 2, \ldots, \frac{p-1}{2}$ لپاره دې وي:

(9.49)	$ia = pq_i + t_i \quad 0 \leq t_i < p$

(د پاتي سره پش). نو $t_i \neq 0 \; \forall i$ باور لري، پرته له دې $ia = pq_i$ ، يعني $p \mid ia$ ، داسي چي(د 3.1.5 له مخي): $p \mid i$ يا $p \mid a$ ، داچي $\mathrm{ggT}(a,p) = 1$ (خ غ ګ) ، بايد باور ولري ($\Rightarrow p \leq i$)، د $1 \leq i \leq \frac{p-1}{2} < p$ له مخي يو مخامخوالی يا تضاد لاس ته راځي!

په ځانګړي ډول باور لري:

(9.50)	$t_i \equiv ia(p) \; \forall i = 1, 2, \ldots, \frac{p-1}{2}.$

(c) ketabton.com: The Digital Library

وي دي $r_1,\ldots,r_{n(a)}$ پورتنۍ پاتي له $\frac{p}{2}<t_i<p, s_1,\ldots,s_k$ سره پاتي له $1\le t_i\le\frac{p}{2}$ سره دا په دې معنا، چې $1\le t_i\le\frac{p-1}{2}$ (p ناجوړه!)

$$\Rightarrow n(a)+k=\frac{p-1}{2}. \tag{9.51}$$

وښايئ: $r_1,\ldots,r_{n(a)},s_1,\ldots,s_k$ ټول سره توپير لري.

نيسو $t_i=t_j$ د $i>j$ لپاره، نو

$$ia-ja=pq_i-pq_j=p(q_i-q_j); \tag{9.52}$$

$q_i-q_j=0$ دی، نو $ia-ja=0$ ، دا په دې معنا چې $(i-j)a=0$ ، يعني $i=j\ (a\neq 0)$ -تضاد يا مخامخوالی!

دی $q_i-q_j\neq 0$ ، نو $p\mid(i-j)a$ ، د [3.1.5](#) له مخې لاس ته راځي $p\mid i-j$ يا $p\mid a$ ، د $\text{ggT}(p,a)=1$ (خ غ ګ) له امله لرو $p\mid i-j$ - تضاد يا مخامخوالی! ($0\le i-j<\frac{p-1}{2}<p$ ، له کوم به چې $i-j=0$ لاس ته راغلی وی.)

جوړ کړی

$$\alpha_i=p-r_i\ (i=1,\ldots,n(a)), \tag{9.53}$$

نو ټول $\alpha_1,\ldots,\alpha_{n(a)}$ مختلف يا نابرابردي(ټول $r_1,\ldots,r_{n(a)}$ مختلف دي).

پسې لرو $\alpha_i\neq s_j\ \forall i,j$ ځکه چې :

$$\alpha_i=p-r_i=s_j\ \Rightarrow\ r_i+s_j=p\equiv 0(p) \tag{9.54}$$

(c) ketabton.com: The Digital Library

(9.55)	i, j $\Rightarrow \quad ia + ja \equiv 0(p) \;\; (t_i \equiv ia(p) \;\forall i)$
(9.56)	$\Rightarrow \; p \mid (i+j)a \overset{3.1.5}{\Leftrightarrow} p \mid i+j \;\; (\mathrm{ggT}(a,p) = 1);$

د $1 \leq i, j \leq \frac{p-1}{2}$ له امله باور لري: $1 \leq i + j \leq p - 1 < p$ -تضاد!

(9.57)	$\alpha_1, \ldots, \alpha_{n(a)}, s_1, \ldots, s_k$

تول مختلف دي یا توپیر لري.

باور لري: $0 < \alpha_i \leq \frac{p-1}{2}$ ، ځکه چې

(9.58)	$\frac{p}{2} < r_i < p \Rightarrow -p < -r_i < \frac{p}{2} \Rightarrow 0 < p - r_i = \alpha_i < \frac{p}{2};$
(9.59)	$0 < s_j < \frac{p-1}{2}$

د پیژند له مخې باور لري.
له دې سره هم

(9.60)	$1 \leq s_j \leq \frac{p-1}{2}; \quad 1 \leq \alpha_i \leq \frac{p-1}{2}$ او

دا چې

(9.61)	$n(a) + k = \frac{p-1}{2}$

(c) ketabton.com: The Digital Library

(ټول باقي يا پاتې توپير لري) $\alpha_1, \dots, \alpha_{n(a)}, s_1, \dots, s_k$ $\frac{p-1}{2}$ تيک طبيعي اعداد دي د 1 او $\frac{p-1}{2}$ ترمنځ. له دې سره: تيک اعداد $\alpha_1, \dots, \alpha_{n(a)}, s_1, \dots, s_k$ دي.

له دې لاس ته راځي:

(9.62)	$\alpha_1 \cdots \alpha_{n(a)} s_1 \cdots s_k = 1 \cdot 2 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)!$
(9.63)	$\Rightarrow (p-r_1)\cdots(p-r_{n(a)}) s_1 \cdots s_k = \left(\frac{p-1}{2}\right)!$
(9.64)	$\Rightarrow (-1)^{n(a)} r_1 \cdots r_{n(a)} s_1 \cdots s_k \equiv \left(\frac{p-1}{2}\right)!(p)$
(9.65)	$\Rightarrow (-1)^{n(a)} t_1 \cdots t_{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)!(p)$
(9.66)	(د r_i, s_j له تعريف څخه)
(9.67)	$\Rightarrow (-1)^{n(a)} 1 \cdot a \cdots \left(\frac{p-1}{2}\right) \cdot a \equiv \left(\frac{p-1}{2}\right)!(p)$
(9.68)	(د تعريع له مخې: $ia = pq_i + t_i \equiv t_i(p)$)
(9.69)	$\Rightarrow (-1)^{n(a)} a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(p).$

(c) ketabton.com: The Digital Library

باور لري $\mathrm{ggT}((\frac{p-1}{2})!, p) = 1$ ، ځکه چي پرته له دې به وی

$$p \Big| \left(\frac{p-1}{2}\right)! = 1 \cdot 2 \cdots \frac{p-1}{2}, \qquad (9.70)$$

يعني د 3.1.5 له مخې:

$$\exists k : 1 \leq k \leq \frac{p-1}{2} < p \quad : \quad p \mid k \qquad (9.71)$$

- اتضاد!

$$\Rightarrow \quad (-1)^{n(a)} a^{\frac{p-1}{2}} \equiv 1(p) \qquad (9.72)$$

$$\Rightarrow \quad a^{\frac{p-1}{2}} \equiv (-1)^{n(a)}(p) \qquad (9.73)$$

$$\overset{9.2.4}{\Leftrightarrow} \quad \left(\frac{a}{p}\right) \equiv (-1)^{n(a)}(p) \qquad (9.74)$$

$$\Rightarrow \quad p \qquad (9.75)$$

کمبنت وېشي $\in \{0, \pm 2\}$ د

$$\Rightarrow \qquad (9.76)$$

کښت بايد صفر
وي $(p > 2, p \nmid 2!)$

$$\Rightarrow \quad \left(\frac{a}{p}\right) = (-1)^{n(a)}. \qquad (9.77)$$

بيلګه 9.2.10 . ايا 7 څلورى پاتې يا مربع باقي $\bmod 13$ دى؟

$p = 13, a = 7, \mathrm{ggT}(a, p) = 1$ (ggT خورا غټ ګډ پروېشونى) ;جوړ کړی :
$1 \cdot 7, \ldots, 6 \cdot 7$

(c) ketabton.com: The Digital Library

د 13 له لارې په وېش کې پاتې :

$t_1 = 7, t_2 = 1, t_3 = 8, t_4 = 2, t_5 = 9, t_6 = 3;$	(9.78)

د دې پاتو ګڼون يا تعداد $n(7)$ له $\frac{13}{2}$ لوي دي ، دا په دې معنا، چې $7 \geq$ برابر 3 دی. له دې امله

$\left(\frac{7}{13}\right) = (-1)^3 = -1,$	(9.79)

دا په دې معنا، چې $a = 7$ مربع ـــيا څلوریپاتې $\bmod 13$ نه دی.

د $\left(\frac{q}{p}\right)$ شميرنه:

د $\left(\frac{q}{p}\right)$ شميرنې ته، د له ۲ لوي p, q مختلفو لومړنيو ګڼونو سره.

جمله 11 : 2 : 9 : p, q مختلف لومړني ګڼونه دي، $p > 2$ ، نو باور لري:

1. $q = 2$:

$$\left(\frac{2}{q}\right) = (-1)^{\frac{p^2-1}{8}}, \qquad (9.80)$$

2. $q > 2$:

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]}. \qquad (9.81)$$

(c) ketabton.com: The Digital Library

دريم: ($[x]$ د x پسي کوچنی عدد یا ګڼ په نخښنه کوي)

ښوونه: د 9.2.9 ښوونې ته ورته (ټاکو $a = q$) باور لري:

$$iq = pq_i + t_i\ (i = 1, \dots, \frac{p-1}{2}),\ 0 < t_i < p, q_i = \left[\frac{iq}{p}\right]. \qquad (9.82)$$

جوړ کړی:

$$\sum_{i=1}^{\frac{p-1}{2}} iq = \sum_{i=1}^{\frac{p-1}{2}} (pq_i + t_i) = p\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right] + \sum_{i=1}^{\frac{p-1}{2}} t_i, \qquad (9.83)$$

له دې سره:

$$q \cdot \underbrace{\sum_{i=1}^{\frac{p-1}{2}} i}_{=\frac{1}{2}(\frac{p-1}{2})(\frac{p-1}{2})} = q\frac{p^2-1}{8} = p\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right] + \sum_{i=1}^{n(q)} r_i + \sum_{i=1}^{k} s_i \qquad (9.84)$$

($r_i \dots$ پاتي (باقي) $> \frac{p}{2}$ ، $s_i \dots$ پاتي $\leq \frac{p}{2}$). د 9.2.9 ښووني له مخي باور لري:

$$\left\{1, 2, \dots, \frac{p-1}{2}\right\} = \{p - r_1, \dots, p - r_{n(q)}, s_1, \dots, s_k\}; \qquad (9.85)$$

نو باور لري:

(c) ketabton.com: The Digital Library

$$\frac{p^2-1}{8}=\sum_{i=1}^{\frac{p-1}{2}} i=\sum_{i=1}^{n(q)}(p-r_i)+\sum_{i=1}^{k} s_i=p\cdot n(q)-\sum_{i=1}^{n(q)} r_i+\sum_{i:} \quad (9.86)$$

د (9.64) او (9.66) کمون(تفریق) له لارې:

$$(q-1)\frac{p^2-1}{8}=p\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]-p\cdot n(q)+2\sum_{i=1}^{n(q)} r_i. \qquad (9.87)$$

له دې سره $\bmod 2$:

$$(q-1)\frac{p^2-1}{8}\equiv\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]-n(q)(2). \qquad (9.88)$$

- که $q>2$ وي، نو q ناجوړه(طاق) دی، یعني $q-1$ جوړه(جفت)، نو $q-1\equiv 0(2)$. له دې سره:

$$0\equiv\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]-n(q)(2)\Rightarrow n(q)\equiv\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right](2). \qquad (9.89)$$

- د 9.2.9 له مخې لرو یا لاس ته راځي:

$$\left(\frac{q}{p}\right)=(-1)^{n(q)}=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]}. \qquad (9.90)$$

(c) ketabton.com: The Digital Library

- که $q=2$ وي، نو $q-1=1$ ، او د $1\le i\le \frac{p-1}{2}$ لپاره باور لري:

$$0<\frac{2}{p}\le\frac{2i}{p}\le\frac{p-1}{p}<1, \qquad (9.91)$$

- نو $\left[\frac{2i}{p}\right]=0$ د $1\le i\le \frac{p-1}{2}$ لپاره ، له دې سره پاتېږي

$$\frac{p^2-1}{8}\equiv -n(q)(2)\Rightarrow n(q)\equiv\frac{p^2-1}{8}(2). \qquad (9.92)$$

د 9.2.9 له مخې لاس ته راځي:

$$\left(\frac{2}{p}\right)=(-1)^{n(q)}=(-1)^{\frac{p^2-1}{8}}. \qquad (9.93)$$

جمله ګوتې 9.2.12 : وي دې $p>2$ يو لومړني ګڼ، نو باور لري: 2 تيک څلورۍ پاتې يا مربع باقي ده، که $p=8k\pm1(k\in\mathbb{Z})$ وي .

ښوونه: 2 څلورۍ پاتې

$$\bmod p \;\Leftrightarrow\; \left(\frac{2}{p}\right)=1 \qquad (9.94)$$

$$\overset{9.2.11}{\Leftrightarrow}(-1)^{\frac{p^2-1}{8}}=1 \qquad (9.95)$$

(c) ketabton.com: The Digital Library

$$\Leftrightarrow \quad \frac{p^2-1}{8} \qquad (9.96)$$

جوړه دی

$$\Leftrightarrow \quad \frac{p^2-1}{8} = 2n \quad n \in \mathbb{N} \qquad (9.97)$$

$$\Leftrightarrow \quad p^2 - 1 = 16n. \qquad (9.98)$$

د $p > 2$ لومړنی ګڼ $\bmod 8$ لاندې بڼه لري

$$8k \pm 1, 8k \pm 2, 8k \pm 3, 8k \pm 4 \qquad (9.99)$$

$p > 2$ لومړنی کڼ $\Rightarrow p$ ناجوړه ګڼ $\Rightarrow 8k \pm 1, 8k \pm 3$

که وی $p = 8k \pm 3 \Rightarrow$

$$p^2 - 1 = 64k^2 \pm 48k + 9 - 1 \equiv 8(16) \not\equiv 0(16), \qquad (9.100)$$

دا په دې معنا، چې $p^2 - 1 \neq 16n$ تضاد یا په ځنوالي

په ځښ یا برعکس:

(c) ketabton.com: The Digital Library

$$p = 8k \pm 1 \Rightarrow p^2 - 1 = 64k^2 \pm 16k + 1 - 1 \equiv 0(16), \quad (9.101)$$

دا په دې معنا، چې $p^2 - 1 = 16n$. له دې سره

$$p^2 - 1 = 16n \Leftrightarrow p = 8k \pm 1. \quad (9.102)$$

د Legendre-Symbo لپاره د څلورۍ – یا مربع ریځیپروسیټي قانون reciprocity law

جمله 9.2.13 : (مربع ریځیپروځیتي): وي دې p, q لومړني ګڼونه، ≥ 2 دواړه ، نو

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$	(9.103)

ښوونه: وي دې

$$M := \left\{(i,j) \in \mathbb{N} \times \mathbb{N} \middle| 1 \leq i \leq \frac{p-1}{2}, 1 \leq j \leq \frac{p-1}{2}\right\}, \quad (9.104)$$

نو M تیک $\frac{p-1}{2}\frac{p-1}{2}$ توکي لري. راوړو

$$M_1 = \{(i,j) \in M \mid qi > pj\}, \quad (9.105)$$

$$M_2 = \{(i,j) \in M \mid qi < pj\}. \quad (9.106)$$

(c) ketabton.com: The Digital Library

- باور لري $qi = pj$ ، لاس ته راځي $p \mid qi$ ، يعني $p \mid i \; (\mathrm{ggT}(p,q) = 1)$ -
تضاد يا مخمخوالی و $1 < i \leq \frac{p-1}{2} < p$ ته. له دې سره:

$$M = M_1 \cup M_2, M_1 \cap M_2 = \emptyset. \tag{9.107}$$

وښايۍ:

$$M_1 = \left\{ (i,j) \in \mathbb{N} \times \mathbb{N} \middle| 1 \leq i \leq \frac{p-1}{2}, 1 \leq j < \frac{qi}{p} \right\}, \tag{9.108}$$

$$M_2 = \left\{ (i,j) \in \mathbb{N} \times \mathbb{N} \middle| 1 \leq i < \frac{pj}{q}, 1 \leq j \leq \frac{q-1}{2} \right\}. \tag{9.109}$$

- د M_1 لپاره: د هر څه د مخه يا لومړی باور لري $M_1 \subseteq \{\dots\}$ ، ځکه چې

$$(i,j) \in M_1 \Rightarrow qi > pj \Rightarrow 1 \leq j < \frac{qi}{p}. \tag{9.110}$$

- په څټ يا برعکس: $\{\dots\} \subseteq M_1$ ، ځکه چې

$$1 \leq i \leq \frac{p-1}{2}, 1 \leq j < \frac{qi}{p} \Rightarrow \frac{qi}{p} \leq \frac{q}{p}\frac{p-1}{2} - \frac{q}{2}\frac{p-1}{p} < \frac{q}{2} \tag{9.111}$$

$$\Rightarrow \left[\frac{qi}{p}\right] \leq \left[\frac{q}{2}\right] \leq \frac{q-1}{2}, \tag{9.112}$$

(c) ketabton.com: The Digital Library

$$1 \leq j < \frac{qi}{p} \Rightarrow 1 \leq j \leq \left[\frac{qi}{p}\right] \leq \frac{q-1}{2}, \qquad (9.113)$$

- دا په دې معنا، چې $(i,j) \in M$. بالاخره: $(i,j) \in M_1$ ، ځکه چې

$$1 \leq j < \frac{qi}{p} \Rightarrow pj < qi. \qquad (9.114)$$

- ورته د M_2 لپاره.
ګڼل يې: د هر لپاره توکي شتون لري، له دې سره باور لري

M_1 ټيک $\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right]$ توکي لري ((9.115)

ورته

M_2 ټيک $\sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right]$ توکي لري (9.116)

نو $M = M_1 \cup M_2, M_1 \cap M_2 = \emptyset$ ټيک

$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}$	(9.117)

(c) ketabton.com: The Digital Library

توکي لري. د 9.2.11 له مخې باور لري:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}[\frac{qi}{p}]}(-1)^{\sum_{j=1}^{\frac{q-1}{2}}[\frac{pj}{q}]}=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}[\frac{qi}{p}]+\sum_{j=1}^{\frac{q-1}{2}}[\frac{pj}{q}]}= \quad (9.11$$

$$=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \quad (9.11$$

جمله ګی 9.2.14 : p, q مختلف > 2 لومړني ګڼونه یا اعداد دي، نو باور لري

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right) \quad (9.120)$$

ټیک هلته، که $p \equiv 1(4)$ یا $q \equiv 1(4)$ یا دواړه وي.

ښوونه: د 9.2.13 له مخې یا پسې:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \quad (9.121)$$

د $\left(\frac{q}{p}\right)=\pm1$ سره د ضرب له لارې لاس ته راوړو:

$$\left.\begin{array}{lcl}\left(\frac{q}{p}\right)= \ \ 1\Rightarrow & \left(\frac{p}{q}\right) & =(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)\\ \left(\frac{q}{p}\right)= -1\Rightarrow & \left(\frac{p}{q}\right)(-1)^2 & =(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)\end{array}\right\}\Rightarrow\left(\frac{p}{q}\right) \quad (9.122)$$

(c) ketabton.com: The Digital Library

له دې سره:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p} \Leftrightarrow (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2}\frac{q-1}{2}$$ جوړه (9.123)

$$\Leftrightarrow \frac{p-1}{2} \vee \frac{q-1}{2}$$ یا دواړه جوړه دي (9.124)

$$\Leftrightarrow \frac{p-1}{2} = 2n \vee \frac{q-1}{2} = 2m \Leftrightarrow p-1 = 4n, q-$$ (9.125)

$$\Leftrightarrow p \equiv 1(4) \vee q \equiv 1(4) \vee$$ دواړه. (9.126)

بیلګه 9.2.15 : ایا $a = -21$ څلوری پاتې یا مربع باقي $\bmod 61$ دي؟

(دا په دې معنا چې $x^2 \equiv -21(61)$ اوبیوړ یا حلوړ دی؟)

$p = 61 \in \mathbb{P}, \mathrm{ggT}(-21, 61) = 1$ له دې سره میژندر:

$$\left(\frac{-21}{61}\right) = \left(\frac{(-1)\cdot 3 \cdot 7}{61}\right) \overset{9.2.5}{=} \left(\frac{-1}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right) \overset{9.2.7}{=} 1 \left(\frac{3}{61}\right.$$ (9.127)

$$\overset{9.2.1}{=} \left(\frac{61}{3}\right)\left(\frac{7}{61}\right) \overset{Red.}{=} \left(\frac{1}{3}\right)\left(\frac{7}{61}\right) = 1\left(\frac{7}{61}\right) = \left(\frac{7}{61}\right)$$ (9.128)

(c) ketabton.com: The Digital Library

$$\overset{Red.}{=} \left(\frac{5}{7}\right) \overset{9.2.14}{=} \left(\frac{7}{5}\right) \overset{Red.}{=} \left(\frac{2}{5}\right) \overset{9.2.12}{=} -1 \qquad (9.129)$$

$\Rightarrow -21$ $\bmod 61$ څلوری پاتې نه دي.

پام یا یادونه 9.2.16: $x^2 \equiv a(m)$ ، چیرته چې m لومړنی ګڼ نه دی، نو لیژندر سومبول تعریف ده دی یا پیءند نه لري، مګر: وي دې $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ د m په لومړنیو ضریبونو یا څله وونو ټوټه کیدنه.نو باور لري:

a مربع بقي $\bmod m \ldots$ دی.

$$\ldots \Leftrightarrow x^2 \equiv a(m) \qquad (9.130)$$

$$\Leftrightarrow x^2 \equiv a(p_i^{\alpha_i}) \quad i = 1, \ldots, k \qquad (9.131)$$

$$\overset{9.1.5}{\Leftrightarrow} x^2 \equiv a(p_i) \quad i = 1, \ldots, k \qquad (9.132)$$

$\Leftrightarrow a$ څلوری پاتې $\bmod p_i \quad i = 1, \ldots, k$ (9.133)

$$\Leftrightarrow \left(\frac{a}{p_i}\right) = 1 \quad i = \mathbf{1}, \ldots, k. \qquad (9.134)$$

جاکوبي سومبول Jacobi-Symbol

(c) ketabton.com: The Digital Library

په لاندي کې د $x^2 \equiv a(m)$ د اوبی یا حل د پرېکړې لپاره یو بل امکان څېړو، مګر د لږ واړه بندیز سره:

پېژند 9.3.1: (جاکوب[9.2] سومبول): m دې یو ناجوړه طبیعي ګڼ وي، چېرته چې $m = p_1 \cdots p_k$ نه اړین مختلف طبیعي لومړني ګڼونه دي. $a \in \mathbb{Z}$ دی د $\mathrm{ggT}(a,m) = 1$ سره، نو څلورۍ ـیامربع باقي د جاکوب له مخې په لاندې توګه تعریف دی

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)_L$$	(9.135)

او $\left(\frac{a}{1}\right) = 1$ [9.3]

یادونه 9.3.2: زیات وخت دا سومبول د کمیزو یا منفي ګڼونو $m < 0$ لپاره هم تعریفیږي:

$$\left(\frac{a}{m}\right) := \left(\frac{a}{\vert m\vert}\right).$$	(9.136)

دا موږ نه پرېږدو، د دې لاړې لاندې ترې لاس ته راتلنه په روښانه توګه ساده لاس ته راوړل کيږي.

یادونه 9.3.3

(c) ketabton.com: The Digital Library

لومړی . $m \in \mathbb{N}$ جوړه دی، نو نو د $x^2 \equiv a(m)$ اوبيوړوالي – يا د حلوړوالی پرابلم په يوه ناجوړه مودل بيرته اړوو، ځکه چې: $m = 2^\alpha n$ د ناجوړه n سره(تل شونی دی)، نو باور لري :

(9.137)	$x^2 \equiv a(m) \Leftrightarrow x^2 \equiv a(2^\alpha)$ او $x^2 \equiv a(n)$

دويم. دلته $x^2 \equiv a(2^\alpha)$ له 9.1.6 سره پای شو او n ناجوړه دې

دريم: د پيژند يا تعريف له مخې دی

(9.138)	$\left(\frac{a}{m}\right)_J = \pm 1,$ ځکه چې $\left(\frac{a}{p_i}\right)_L = \pm 1.$

څلورم: $\left(\frac{a}{m}\right)_J = -1$ دی، نو a څلوری پاتې يا مربع باقي $\mod m$ نه ده، ځکه چې د تعريف له مخې:

(9.139)	$-\mathbf{1} = \left(\frac{a}{m}\right)_J = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)_L,$

پنځم: يني لږ تر لږه $\left(\frac{a}{p_i}\right)_L = -1$ يو دی، دا په دې معنا، چې د دې i لپاره a څلوری پاتې $\mod p_i$ نه دی. له دې سره a هم مربع باقي $\mod m$ نه دی.

(c) ketabton.com: The Digital Library

$$\left(x_0^2 \equiv a(m) \overset{p_i|m}{\Rightarrow} x_0^2 \equiv a(p_i)\right)$$

شپېرم: $\left(\frac{a}{p_i}\right)_L = -1$ دی، نو a نه اړيين يو مربع باقي $\bmod p_i$ دی(کيدی شي وي، مګر بايد نه دی، چې وي).

بيلګه : $\left(\frac{2}{15}\right)$ جاکوبي- سومبل دی($15 \in \mathbb{N}$ ناجوړه(طاق) $(2,15)=1$) ، د تعريف له مخې:

(9.140)	$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right),$

له دې سره د 9.2.12 له مخې باور لري: $\left(\frac{2}{3}\right) = -1$ ځکه چې $3 \neq 8k \pm 1, \left(\frac{2}{5}\right) = -1$ ځکه چې $5 \neq 8k \pm 1$.

يعني:

(9.141)	$\left(\frac{2}{15}\right) = (-1)(-1) = 1,$

مګر 2 مربع باقي $\bmod 15$ نه دی. له دې امله په لومړنيو ضريبونو تجزيه.....

لومړی: $a \equiv a'(m)$ دی، نو باور لري

(c) ketabton.com: The Digital Library

(9.142)	$\left(\frac{a}{m}\right)_J = \left(\frac{a'}{m}\right)_J .$

دويم: جمله ګۍ 9.2.5 ته ورته د ليجندر-سومبول لپاره او هم د جاکوبي سومبول لپاره باور لري

(9.143)	$\left(\frac{ab}{m}\right)_J = \left(\frac{a}{m}\right)_J \left(\frac{b}{m}\right)_J .$

ځلورم: پسي باور لري:

(9.144)	$\left(\frac{a}{m_1 m_2}\right)_J = \left(\frac{a}{m_1}\right)_J \left(\frac{a}{m_2}\right)_J .$

يادونه: که په راتلونکي کي د سومبوأل ډول غوره وي، نو د $\left(\frac{a}{p}\right)_L$ سره د لجيندر-سومبول او له $\left(\frac{a}{p}\right)_J$ سره د جاکوبي سومبول سره توپيروو. دا پورته تعريف له دي امله وايي، چي جا کوبي سومبول د ليجندر – سومبول ضرب دى.

ځانګړي حالتونه: $a = -1, a = 2$

ليجندر ته ورته: د $a = -1$ همداسې د $a = 2$ لپاره جاکوبي-سومبول را اخلو:

(c) ketabton.com: The Digital Library

لیما یا وړه جمله : $m = m_1 \cdots m_k \in \mathbb{N}$ ناجوړه دی، نو باور لري:

لومړی:

(9.145)	$$\frac{m-1}{2} \equiv \sum_{i=1}^{k} \frac{m_i-1}{2}(2),$$

دویم:

(9.146)	$$\frac{m^2-1}{8} \equiv \sum_{i=1}^{k} \frac{m_i^2-1}{8}(2).$$

ښوونه : دا چې m ناجوړه دی، باید هر m_i هم ناجوړه وي($\Rightarrow \frac{m_i-1}{2} \in \mathbb{N}$)

لومړی $\frac{m-1}{2} \in \mathbb{N}, \frac{m_i-1}{2} \in \mathbb{N}$ ، ایندکشن:

$k = 1$:

دلته نه ښوول کیږي.

$k \to k+1$:

وي دې $m = m_1 \cdots m_k n_{k+1} \in \mathbb{N}$ ناجوړه، نو هر m_i ناجوړه دی،، او هم $2 \mid m_{k+1} - 1$ ناجوړه دی او همداسي $2 \mid m_{k+1} - 1$ هم، نو په ټولیزه توګه دا ضرب په 4 وېشوړ دی

(9.147)	$$(m_1 \cdots m_k - 1)(m_{k+1} - 1) =$$

(c) ketabton.com: The Digital Library

$= \underbrace{m_1 \cdots m_k m_{k+1}}_{=m} - m_1 \cdots m_k - m_{k+1} + 1;$	

له دي امله: $m - 1 \equiv m_1 \cdots m_k - 1 + m_{k+1} - 1 (4)$ ، کين او ښي لور ته جوړه ګڼ ځای دی، د $ggT(4,2) = 2$ له امله د (5)4.1.5 له مخې لاس ته راځي:

(9.148)	$\frac{m-1}{2} \equiv \frac{m_1 \cdots m_k - 1}{2} + \frac{m_{k+1} - 1}{2}(2).$

د اينډکشن پسي لرو:

(9.149)	$\frac{m-1}{2} \equiv \sum_{i=1}^{k} \frac{m_i - 1}{2} + \frac{m_{k+1} - 1}{2} = \sum_{i=1}^{k+1} \frac{m_i - 1}{2}(2).$

وښايی: که $a \in \mathbb{N}$ ناجوړه وي، نو $8 \mid a^2 - 1$ باور لري:

	$a = 2t + 1 \Rightarrow$
(9.150)	$a^2 = 4t^2 + 4t + 1 = 4t(t+1) + 1$
(9.151)	$\Rightarrow a^2 - 1 = 4t(t+1),$

جيرته جي يا t يا $t+1$ جوړه دی، دا په دي معنا، چي ضريب يا ځله وونی 2 لري. له دي سره باور لري

(9.152)	$8 \mid a^2 - 1 \left(\Rightarrow \frac{m_i^2 - 1}{8} \in \mathbb{N} \right).$

(c) ketabton.com: The Digital Library

۱ - ايندکشن:

۲ - $k = 1$:

۳ – دلته هم نه ښوول کيږي

$k \to k+1$
:

۴ – وي دې $m = m_1 \cdots m_k m_{k+1} \in \mathbb{N}$ ، ناجوړه، نو ټول m_i ناجوړه دي او $m_1 \cdots m_k$ هم، نو

$8 \mid m_1^2 \cdots m_k^2 - 1$ او $8 \mid m_{k+1}^2 - 1.$	(9.153)

۵ – له دې سره $m_1^2 \cdots m_k^2 - 1 \equiv 0(8), m_{k+1}^2 - 1 \equiv 0(8)$ ، يعني د 4.1.5 له مخې

$(m_1^2 \cdots m_k^2 - 1)(m_{k+1}^2 - 1) \equiv 0(64).$	(9.154)

۶ - دا په دې معنا، چې $64 \mid m_1^2 \cdots m_k^2 m_{k+1}^2 - m_1^2 \cdots m_k^2 + 1 - m_{k+1}^2$ ، نو

$m_1^2 \cdots m_k^2 m_{k+1}^2 - 1 \equiv m_1^2 \cdots m_k^2 - 1 + m_{k+1}^2 - 1(64),$	(9.155)

۷ – نو:

$\frac{m^2-1}{8} \equiv \frac{m_1^2 \cdots m_k^2 - 1}{8} + \frac{m_{k+1}^2 - 1}{8}(8),$	(9.156)

(c) ketabton.com: The Digital Library

۸ – دا په دې معنا، چې د ابندکشن له مخې:

(9.157)	$$\frac{m^2-1}{8} \equiv \sum_{i=1}^{k} \frac{m_i^2-1}{8} + \frac{m_{k+1}^2-1}{8} = \sum_{i=1}^{k+1} \frac{m_i^2-1}{8} (8).$$

د دې پرېکړې لپاره چې ایا -1 یا 2 خلوری پاتې (مربعباقي) دی که نه:

جمله : وي دې $m \in \mathbb{N}$ ناجوړه، نو باور لري:

۱ – (9.158) ۲ – (9.158)	$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}},$$ $$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

ښوونه: وي دې $m = p_1 \cdots p_k$ ناجوړه، $p_i \in \mathbb{P}$ ، تول p_i ناجوړه، یعني > 2

- ۱

(9.160)	$$\left(\frac{-1}{m}\right) \overset{Def.}{=} \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right)_L \overset{9.2.7}{=} \prod_{i=1}^{k} (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^{k} \frac{p_i-1}{2}}.$$

۲ – دا چې د(1)9.3.5 له مخې باور لري:

(c) ketabton.com: The Digital Library

$$\sum_{i=1}^{k}\frac{p_i-1}{2}\equiv\frac{m-1}{2}(2)\Rightarrow\sum_{i=1}^{k}\frac{p_i-1}{2}=\frac{m-1}{2}+2t\ (t\in\mathbb{N}),$$	(9.161)

۳ ــ او $(-1)^{2t}=1$ ، لاس ته راځي:

$$(-1)^{\sum_{i=1}^{k}\frac{p_i-1}{2}}=(-1)^{\frac{m-1}{2}}.$$	(9.162)

۴ ــ

$$\left(\frac{2}{m}\right)\overset{Def.}{=}$$ $$\prod_{i=1}^{k}\left(\frac{2}{p_i}\right)_L\overset{9.2.11}{=}\prod_{i=1}^{k}(-1)^{\frac{p_i^2-1}{2}}=(-1)^{\sum_{i=1}^{k}\frac{p_i^2-1}{8}}\overset{9.3.5(2)}{=}$$	(9.163)
$$\overset{9.3.5(2)}{=}\quad(-1)^{\sum_{i=1}^{k}\frac{m^2-1}{8}}.$$	(9.164)

د جاکوبي-سومبول لپاره څلورې – یا مربع رڅیپروسیتي قانون

لیجندر- سومبول ته ورته د جاکوبې-سومبول لپاره هم مربع ریڅیپروښیتي قانون) باور لري:

جمله : (مربع رڅیپروښیتي قانون) وې دي $m,n\in\mathbb{N}$ د ناجوړه(طاق) $\operatorname{ggT}(m,n)=1, m,n$ (خورا غټ ګډ پروېشونی) سره، نو با ور لري:

(c) ketabton.com: The Digital Library

$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$	(9.165)

ښوونه: وي دې $m = p_1 \cdots p_k,\ p_i \in \mathbb{P}$ ، p_i نه په اړينه توګه مختلف،
$n = q_1 \cdots q_s,\ q_j \in \mathbb{P}$ ، q_j نه په اړينه توګه مختلف. د $\mathrm{ggT}(m,n) = 1$ له
امله باور لري: $\mathrm{ggT}(p_i, q_j) = 1, p_i, q_j > 2\ \forall i,j$. پسې

$\left(\frac{n}{m}\right) \overset{Def.}{=} \prod_{j=1}^{s}\left(\frac{m}{q_j}\right)_L = \prod_{i=1}^{s}\left(\frac{p_1\cdots p_k}{q_j}\right) \overset{9.2.5}{=} \prod_{j=1}^{s}\left(\prod_{i=1}^{k}\left(\frac{p_i}{q_j}\right)\right);$	(9.166)
$\left(\frac{n}{m}\right) \overset{Def.}{=} \prod_{i=1}^{k}\left(\frac{n}{p_i}\right)_L = \prod_{i=1}^{k}\left(\frac{q_1\cdots q_s}{p_i}\right) \overset{9.2.5}{=} \prod_{i=1}^{k}\left(\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\right);$	(9.167)

نو:

$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) \quad =$	

(c) ketabton.com: The Digital Library

$$\prod_{j=1}^{s}\prod_{i=1}^{k}\left[\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right] \overset{9.2.13}{=} \prod_{j=1}^{s}\prod_{i=1}^{k}\left[(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}\right] =$$	(9.168)
$$= (-1)^{\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right)}.$$	(9.169)

دا چې باور لري:

$$\sum_{i=1}^{k}\frac{p_i-1}{2} \equiv \frac{m-1}{2}(2),$$ او $$\sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{n-1}{2}(2)$$	(9.170)

پسې لاس ته راځي

$$\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right) \overset{9.3.5(1)}{=}$$	
$$\left(\frac{m-1}{2}+2t\right)\left(\frac{n-1}{2}+2n\right) =$$	(9.168)
$$= \frac{m-1}{2}\frac{n-1}{2}+2v.$$	(9.169)

(c) ketabton.com: The Digital Library

له دې سره په ټولیزه توګه باور لري:

$$(-1)^{\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right)}=(-1)^{\frac{m-1}{2}\frac{n-1}{2}+2v}=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$	(9.173)

پایله 9.3.8 : $a<0$ دی، نو

$$\left(\frac{a}{m}\right)=\left(\frac{-\lvert a\rvert}{m}\right)=\left(\frac{-1}{m}\right)\left(\frac{a}{m}\right),$$	(9.174)

د هغه سره چې $\left(\frac{-1}{m}\right)$ د 9.3.6 له مخې ټاکلی، او $\lvert a\rvert>0$.

پایله 9.3.9 : (ورته و 9.2.14 ته)

$$\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\frac{n-1}{2}},$$	(9.175)

نو ترې لاس ته راځي:

$\Leftrightarrow \left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)$	
$\frac{m-1}{2}\frac{n-1}{2}\Leftrightarrow (-1)^{\frac{m-1}{2}\frac{n-1}{2}}=1$	(9.176) جوړه(جفت)
$\Leftrightarrow \frac{m-1}{2}\vee\frac{n-1}{2}$	(9.177) جوړه

جاکوبي-سومبول دا کره کوي، چې ایا a مربع باقي $\bmod m$ دی(که جاکوبي-سومبول 1 وي، نو پرېکړه نه شته).

بیلګه 9.3.10 :

(c) ketabton.com: The Digital Library

۱ - $x^2 \equiv -8(15)$ ابیوړ یا حل وړ دی؟

(دا په دې معنا، چې $a = -8$ مربعپاتې $\bmod 15$ دی؟)

$m = -8 < 0, n = 15 \notin \mathbb{P}, \text{ggT}(-8, 15) = 1, 15$

ناجوړه له دې لاس ته راځي جاکوبي

$\left(\frac{-8}{15}\right)_J =$	
$\left(\frac{-1}{15}\right)\left(\frac{8}{15}\right) \overset{9.3.6}{=} (-1)\left(\frac{8}{15}\right) = (-1)\underbrace{\left(\frac{4}{15}\right)}_{=1}\left(\frac{2}{15}\right) \overset{9.3.6}{=}$	(9.178)
$\overset{9.3.6}{=} \quad (-1)\cdot 1\cdot 1 = -1$	(9.179)

۲ – (لرو چې) $\Rightarrow -8$ مربع باقي $\bmod 15$ نه دی.

۳ – $x^2 \equiv 59(125)$ اوبیوړ یا حلوړ دی؟

$\text{ggT}(59, 125) = \mathbf{1}, a \in \mathbb{Z}, m \in \mathbb{N}$

، دواړه ناجوړه، جاکوبي:

$\left(\frac{59}{125}\right)_J \overset{9.3.7}{=}$	

(c) ketabton.com: The Digital Library

(9.180)	$\left(\frac{125}{59}\right) \overset{Red.}{=} \left(\frac{7}{59}\right) \overset{9.3.7}{=} -\left(\frac{59}{7}\right) \overset{Red.}{=} -\left(\frac{3}{7}\right) \overset{9.3.7}{=} \left(\frac{7}{3}\right) =$
(9.180)	$= \left(\frac{1}{3}\right) = 1 \ldots$ وینا نه شته

۴ – مګر(تل کيږي:) 5^3 $m = 125 =$ ، يعني $p_1 = 5$ ، وشميره:

(9.182)	$\left(\frac{59}{5}\right)_L = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$

۵ - 59 $\overset{9.1.5}{\Rightarrow}$ مربع باقي $\bmod 125$ دي.

۶ – ايا $x^2 \equiv 15(67)$ اوبيوړ يا حلوړ دی؟ (دا په دې معنا، چې $a = 15$ څلوری – يا مربع پاتې $\bmod 67$ دی؟)

$$\left(\frac{15}{67}\right) \overset{9.3.7}{=} \left(\frac{67}{15}\right)(-1) \overset{Red.}{=} (-1)\left(\frac{7}{15}\right) \overset{9.3.7}{=} (-1)\left(\frac{15}{7}\right)(-1) \overset{Red.}{=} \left(\frac{1}{7}\right) = 1.$$

مګر دا چې $\left(\frac{15}{67}\right)$ يو ليجندر – سومبول دی، لاس ته رځي: 15 مربع باقي $\bmod 67$ دی.

۷ – ايا $x^2 \equiv 67(77)$ اوبيوړ دی؟

نسبي لومړنی، ناجوړه، $77 \notin \mathbb{P} \Rightarrow$ لاس ته راځي جاکوبي $77 \notin \mathbb{P} \Rightarrow$

(c) ketabton.com: The Digital Library

$$\left(\frac{67}{77}\right) \overset{9.3.7}{=} \left(\frac{77}{67}\right)(-1)^{gerade} = \left(\frac{77}{67}\right) \overset{Red.}{=} \left(\frac{10}{67}\right). \qquad (9.184)$$

$\notin \mathbb{P} \Rightarrow$

۸ - جوړه دی،

نه [9.2.13](9.2.13)او نه [9.3.7](9.3.7) استعماوړ د کاروني وړ دی! له دې لاس ته راځي:

په لومړنيو ګڼونو ټوټه کونه:

$$\left(\frac{10}{67}\right)_L = \left(\frac{2}{67}\right)\left(\frac{5}{67}\right) = (-1)(-1) = 1\ldots \qquad (9.185)$$

وينا نه ده!

$$\left(\frac{2}{67}\right)_L \overset{9.2.12}{=} -1, \qquad (9.186)$$

ځکه چې $67 \not\equiv \pm 1(8);$

$$\left(\frac{5}{67}\right)_L \overset{9.2.13}{=} \left(\frac{67}{5}\right) \overset{Red.}{=} \left(\frac{2}{5}\right) \overset{9.2.12}{=} -1,$$

ځکه چې

$$5 \not\equiv \pm 1(8). \qquad (9.187)$$

۹ - مګر د پيژند له مخې:

$$\left(\frac{67}{77}\right) = \left(\frac{67}{7}\right)\left(\frac{67}{11}\right) = \left(\frac{4}{7}\right)\left(\frac{1}{11}\right) = 1 \cdot 1. \qquad (9.188)$$

۱۰ – دا چې دواړه (!) ليجندر – سومبولونه برابر 1 دي، لاس ته راځي، چې 67 مربع باقي $77 \mod$ دی.

(c) ketabton.com: The Digital Library

د ډاکتر ماخان شينواري چاپ شوې ليکنې:

1988 Vienna (Austria):

لومړی:

H.K. Kaiser , M. Shinwari : Aproximation compact pological algebra : general algebra 6 ; Page 117 – 122 contributions to

1987 Vienna (Austria):

دويم:

Diss . Interpolation und Aproximation durch Polynime in Universalen Algebren . Uni. Wien

Dissertation Interpolation and Aproximation by Polynome in universal Algebras, at the University of Vienna/Austria

لاندې د شميرپوهنې پښتوټول کتابونه په المان کې د ،، افغانستان کلتوري ودې ټولنه،،له خوا چاپ شوي دي

2000 Bonn (Germany):

دريم: د شميرپوهنې ستر کتاب : د شميرپوهنې برسيره د انجنري، فزيک او اقتصاد لپاره ، همداسې د ښوونکو او زده کوونکو لپاره (دا کتاب په ۹۰۰ مخونو کې چاپ او دا نوې ليکنه به يې ځنو ځايونو غزيدلې او ځنې ځايونه ترې لرې شوي دي)

2003 Bonn (Germany):

څلورم: څمککچپوهنه(هندسه) ، په سلو، زرو کې شميرنه، د ګټې – او ګټې د کټې شميرنه ، د اختمالوالي شمېرنه کتاب د ښوونځي ټولې اړتياوې پوره کوي

2003 Bonn (Germany):

پنځم: الجبرونه (د الجبر بنستونه دي)

2003 Bonn (Germany):

(c) ketabton.com: The Digital Library

شپږم: د شمیرپوهنې انګرېزي – پښتو ډکشنري.

<u>*2003 Bonn (Germany):*</u>

اووم: د شمیرپوهنې الماني ـ پښتو ـ او پښتو الماني ډکشنري

Mathematical dictionary German/ Pashto and Pashto/German

<u>*2003 Bonn (Germany):*</u>

اتم: دفرنځیال برابرون (دا کتاب په دې ځانګه کې یو پیل دی، ساده لیکل شوی)

Differential equation Translation; An Introduction

<u>*Bonn (Germany): 2003*</u>

نهم: د شمیر پوهنې فرمولونو ټولګه

Mathematical Formulas

<u>*2003 Bonn (Germany):*</u>

لسم: شمیرپوهنه له عربي په پښتو

<u>1997 Bonn (Germany):</u>

یوولسم: د افغانستان په هکله سپیني خبرې: په المان کې

،،د افغانستان روغې او بیا ابادولو ټولنه،، له خوا

یادونه: له ۲۰۰۰ کال دمخه ډاکتر ماخان شینواري د ،،د افغانستان روغې او بیا ابادولو ټولنه،، له خوا درې ساسي مجلې هم را وستلې.

د ډاکتر ماخان ،،میرې،، شینواري لیکنې او ژباړې چې په چاپیدو یې پیل کیږي

2012 Bonn; Germany; Kabul Afghanistan

(c) ketabton.com: The Digital Library

ژباړې:

: *Prof. Brinkmann. (From Brinkmann.du.de)*

لاندې د برينکمن ليکنې چې له پرينکمن ن ج څخه ژباړل شوي دي.

١ - شميرپوهنه د ښوونځي لپاره لومړی ټوک

٢ – شميرپوهنه د ښوونځي لپاره دويم ټوک

٣ – شميرپوهنه د ښوونځي لپاره دريم ټوک

۴ - د احتمالوالي شميرنه د ښوونځي لپاره

۵ – احصايه يا ستاتيستيک دښوونځي لپاره

لاندې کتابونه د شتوتګارت د پوهنتون د استادانو د لکچرونو څخه چې د شتوتګارت پوهنتون ن ج څخه خپاره شوي را ژباړل شوي.

۶ – اناليزی ١

٧ – اناليزې ٢

٨ – کرښيز الجبر

٩ - د شميرپوهنې بنسټونه

١٠ - د فرمولونو ټولګه

١١ – فنکشنل اناليز

١٢ – وکتور شميرنه

نورې ژباړې

١٣ – له www./grundstudium.info/linearealgebra څخه:کرښيز الجبر

(c) ketabton.com: The Digital Library

۱۴ – Georg Gutenbrunner ګڼونپوهنه یا د اعدادو تیوري

زما لیکنې

Bonn (Germany):

۱۵ - د شمیرپوهنې ستر کتاب دویم چاپ د پوره تغیراتو سره : دا کتاب د شمیرپوهنې برخې برسیره د

انجنري، فزیک او اقتصاد لپاره ، همداسې د ښوونکو او زدهکوونکو لپاره پوره ګټور دی. په کتاب کې د اړتیا سره زیاتونه او کونه راغلې

۱۶ - ځمککچپوهنه (هندسه) دویم چاپ د پوره تغیراتو سره

۱۷ – الجبر بنسټونه دویم چاپ له تغیراتو سره

۱۸ - ډېرۍ پوهنه یا سټ تیوري

۱۹ – د شمیرپوهنې سم اند (منطق ریاضي)

۲۰ - د یو څو شمیرپوهانو ژوندلیک

۲۱ – د شمیر پوهنې ګډې وډې لیکنې

۲۲- داهم ژباړه ده، خو لیکونکی یې متآسفانه راڅخه نابلد شوی: د مشتق او انتیګرال شمیرنو ته تمرینونه او اوبیونې یا حلونه یې

۲۳ – د شمیرپوهنې انګریزي پښتو او عربي + دري ډکشنري

۲۴ – د شمیرپوهنې پښتو انګرېزي ډکشنري

۲۵ – د شمیرپوهنې پښتو ډکشنري د شمیرپوهنیزو وییونو په پښتو روښانه ونه

۲۶ - د زړه له کومې(دا هغه لیکنې دي، چې ځنې یې په نړیول جالونو کې خپرې شوي دي.)

۲۷ – د افغانستان په هکله سپینې خبرې، چې وبه غزیږي.

(c) ketabton.com: The Digital Library

نوري ليکنې، چې په ژباړه يې پيل شوی، خو لا پوره نه دي

– د شتوتکارت پوهنتون لکچرنوټونو څخه ، چې د شتوتګارت پوهنتون ن ج څخه خپريږي:

د ګروپونو تيوري

- د ښوونځي لپاره فزيک د برينکمن ليکنه

له پنځم ټولګي څخه تر اووم ټولګې پورې ژباړل شوی (دا چې زما دويم مسلک فزيک دی، دا ليکنې ژباړم. دا هم د دې ليکوال يوه ډېره ښه ليکنه ده، چې -د شميرپوهنې په څير- دلته هم زيات تمرينونه د حل يا اوبيونې سره په کې راغلي او ماته زيات ګټور برېښي)

(c) ketabton.com: The Digital Library

د ليکوال ژوند ته لنډه کتنه

ماخان په اولني نوم میړي شینواری د اروابنادي پستو او اروابناد نوررحمان زوي په ۱۳۲۰ ؟ ه لمریز کې د شینوارو هسکه مینه کې دې نړۍ ته سترگې راغړولي. د هسکي مینې د لومړني ښوونځي (د لومړنيو زده کوونکو څخه) څخه وروسته د رمحمان بابا لیسه له ۱۹۵۴ تر ۱۹۶۵ پورې(ښوونځي له لومړي ټولگې پیل او د دویم ټولگې څخه گام او پای).	

د ۱۹۶۶ تر سپتبر د کابل طب پوهنځی. له ۱۹۶۶ سپتمبر څخه د اتریش برس، چې هلته یې د شمیرپوهنې ډاکتري په پوره ستونځو تر لاسه کړه.

د۱۹۹۸۷ ش ک تر ۱۹۸۸ د فبروري تر پای د دباندنیو چارو وزارت کې مامور.

د ۱۹۸۸ مارچ څخه تر ۱۹۹۲ جون پورې په بن کې د افغانستان جمهوریت سفارت شارژد افیر(صفر نه وو).

له هغې وروسته په جرمني کې سیاسي پناه. له ۲۰۰۸ مارچ څخه د ۲۰۰۹ دسمبر پورې د د ریاضي ځانگه کې د پوهنې وزارت درسي نساب کې دنده.

ماخان میړي په ۱۹۷۲ کې له لرې د میرمن ښاپیرۍ سره واده شوی، چې د واده خبر ورته اتریش ته راغی.

ده د میرمن ښاپیرۍ سره په ۱۹۶۳ ز ک کې کوزده کړې وه.

دوي ته لوي څښتن په اتریش ویانا کې د مای په شلم ۱۹۷۹ ز ک دوه بچیان وبخښل، چې ځانگه او اباسین نومیږي. ځانگه په المان کې د پوهنتون علمي همکاره وه او د حقوقو ډاکتره ده او اباسین ملي اقتصاد او ټولنیزه سایکولوژي لوستلې.

Get more e-books from www.ketabton.com
Ketabton.com: The Digital Library