ګنونپوهنه

(د اعداد تیوري)

Nummbertheory

$$k = n \pmod m$$

smakhan1946@gmail.com

لیکونکی: جورج کونتبروور

ژباړی: ډاکتر ماخان (میرې) شینواری

دلوي څېښتن په نامه

په دې هيله، چې په دې ليکنو او ژباړو به مې زمور 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 پيژندنه

د کتاب نوم: ګنونپوهنه

ليکونکی: پرفيسور جورج ګوتنبرونر

ژباړی : ډاکتر ماخان،، ميږی،، شينواری

د خپريدو لړۍ .....

خپرندوی: د افغانستان کلتوري ودې ټولنه

جرمني

چاپ کال ۲۰۱۲

د ژباړي برېښنا پته : smakhan1946@gmail.com

چاپ چارې

چاپ ته يې د هر چمتو هيوادوال مرسته په سترګو منل کيږي

.

پښتو مو ژبه او شميرپوهنه پرې ساده ده

د ژباړې مننه

نیولیک

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 سکرېپټ 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 اړيينه 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:

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

ګنونتیوري د ډېرو داسې ساده برېښیدونکو پرابلمونو، ښوونه او یا د هغوي 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 ګنونپوهنې دې خویونو یو د شمیر پوهنې تیوري ودې خورا ستر د تغذیې ورشو ومونډله، چې د خپل دسځیلین 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 ګنونتیوری 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 سختې لیدل کیږي، بیاهم ګنونپوهنه 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 لوي لومړنیو ګنونو ته اړتیا پیښیږي.

په ۶/۳ برخه کې لنډ دې پرابلم ته پام شوی دی، دګنونپوهنې د بنسټیز د استعمالوړوالي دې دلته اانتظار نه کیږي، ځکه چې بنسټیزه تیوري، نه مګر د هغې استعمال د دې سکرېپټ په ککړه کې ځای لري. علاقمند لوستونکی دې په دې هکله نورو د ګنونتیوري 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 سکرېپټ د لکچر په لیکنو ولاړ دی او د تکمیل ادعا نه کوي.

جورج ګوتنبرونر اپریل ۲۰۰۲

د $(\mathbb{Z}, +, \cdot, \leq)$ خويونه

د $\mathbb{Z}$ لپاره اکسيومسيستمونه Axiomensystemen

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

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

الف::

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

ب-

$\exists\, 0 \in \mathbb{Z}\ (,, Null") : a + 0 = 0 + a = a \; \forall a \in \mathbb{Z}$ (بې اغيزه يا ناپيلی توکی)

پ –

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

ت -

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

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

الف-

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

ب –

$\exists 1 \in \mathbb{Z}, 1 \neq 0, (, , Eins")$ د $1 \cdot a = a \cdot 1 = a \; \forall a \in \mathbb{Z}$ (بې اغیزه یا ناپیلی توکی)

پ-

$a \cdot b = b \cdot a \; \forall a, b \in \mathbb{Z}$ (کموتاتیو یا د بدلېدو قانون)

ت-

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

دریم: نسبت و نظم $\leq$ `` ته باور لري:

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

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

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

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

ت ـ $a \leq b, c \in \mathbb{Z}$ په خوښه $\Rightarrow a + c \leq b + c \; \forall a, b \in \mathbb{Z}$

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- برخېږی $\mathbb{N} = \{a \in \mathbb{Z} \mid a > 0\}$ پوره منظمه ده، دا په دې معنا چې د $\mathbb{N}$ هره ناتش برخېږی A کوچنی توکی لري. (نو:

$A \neq \emptyset \Rightarrow \exists \, a_0 \in A : a_0 \leq a, \; \forall a \in A$)

یادونه ۱.۱.۱ د جمعې یا زیاتون د څلور خویونو لپاره $(\mathbb{Z}, +)$ یو ابل ګروپ جوړوي، د ضرب د خویونو سره په ګډه د $(\mathbb{Z}, +, \cdot)$ سره په اړوند د یوه کموتاتیو رینګ څخه غږیږو، د یوې(واحد) توکي سره.

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(کړۍ) دی(بېلګه: $(\mathbb{Z},+,\cdot,\leq)$)

یادونه ۱ . ۱ . ۲ سړی کړی شي وښایي: $(R,\oplus,\odot,\preceq)$ 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.

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

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

ښوونه:

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

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

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

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

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

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

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

$(\Leftarrow)$ ښوونه:

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

$(\Rightarrow)$

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

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

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

د سره

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:

$A = \mathbb{N}$ (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:

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

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

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

(د $\mathbb{N}$ تعریف وګوری) د

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

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.

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

ښوونه: وي دي

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

وښایه: $M \neq \emptyset$

که $a \geq 0$ وي ، نو دی

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

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

$$1 \cdot (-a) \leq b \cdot (-a), \tag{1.19}$$

دا په دې معنا ، چې

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

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 ډېرې یو کوچنی توکی rلري r : ، داپه دې معنا، چې $r \in \mathbb{N}_0$ او

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

له دې سره لاس ته راځي

$$a = b \cdot x_0 + r, \quad (1.22)$$

چیرته چې $0 \leq r$.

نور غواړو وښایو: $r < b$

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 املې د 3f پسې لرو:

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

باور لري

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

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

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

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. $-42 = 32 \cdot (-2) + 22$

د پښې 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 املې د پاتې سره راکوي:

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

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

⋮ (1.29)

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

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

: $i = 1$

نيسو $q_1 < 0$ ، نو باور لري

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

- تضاد يا مخامخوالی!

$i \to i + 1$
:

نيسو $q_{i+1} < 0 \Rightarrow q_{i+1} \leq -1$ ، 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 .

د ډېرې یا ست $M := \{q_i \mid q_i > 0\}$ 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 :

$$q_n = bq_{n+1} + a_n = a_n, \tag{1.35}$$

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

$$a = bq_1 + a_0 = b(bq_2 + a_1) + a_0 = q_2b^2 + ba_1b - a_0 = \cdots$$

$$= q_nb^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0 \ (q_n = a_n > 0).$$

یواځیوالی:

نیسو، چې دوه مختلفې انځورونې شتون لري. وي دې

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

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

$$-b < -\bar{a}_0 \leq 0 \overset{0 \leq a_0 < b}{\Rightarrow} -b < a_0 - \bar{a}_0 < b. \tag{1.37}$$

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.

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 بايد $q = 0$ باور ولري، له دي سره $a_0 - \bar{a}_0 = b \cdot 0 = 0$ او $a_0 = \bar{a}_0$. له دي 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 لاري لاس ته راځي:

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

په ورته توګه لاس ته راځي: $a_1 = \bar{a}_1, a_2 = \bar{a}_2, \cdots, a_m = \bar{a}_m$ ، داسي چې په ټوليزه 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 تري راځي: کينه لور له صفر لويه ده، تضاد.

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

پېژند (تعريف)1.2.2 : پورتنی د $a \in \mathbb{N}$ ټواځنی انځورونه د $b \in \mathbb{N}, \ b \geq 2$ له لاري د a ځای انځورونه بلل کيږي نسبت بنسټ b ته، سومبوليک

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

که $b=10$ وي، نو له ديکاديکي *dekadischen* يا لسميزې انځورونې غږيږو، د $b=2$ سره له بينار يا دوه ييزې انځورونې غږيږو. که $b>0$ وي، نو سړی ليکي $A=10, B=11, \ldots$ (د دې لپاره چې له $1\ 0$ څخه يې توپير وکړای شو).

يادونه1.2.3 : د a ځای انځورونه نسبت $b\geq 2$ ته کېدی شي د 1.2.1 د بنوونې په بنسټ و تاکل شي[1.2] .

$$a=q_1b+a_0 \quad 0\leq a_0<b \Rightarrow a_0$$ تاکلی. (1.42)

$$q_1=q_2b+a_1 \quad 0\leq a_1<b \Rightarrow a_1$$ تاکلی. (1.43)

q2=q3b+a2 0≤a2<b =>a2 تاکلی : (1.44)

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

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

بېلګه 1.2.5 : وي دي $a=367, b=2$ ، غوښتنه يا ثبوت: da بينار-يا دوه ييزه انځورونه $367=183\cdot 2+1=\cdots$ سړی داسې ليکي :

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	

$$\Rightarrow 367 = (101101111)_2$$

ازماپښت:

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

په $\mathbb{Z}$ کې توټه ونه 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 ټاکنه

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 دي $a \in \mathbb{Z}$ ، سږی وایي $b \in \mathbb{Z}$ a وېشي، که د یوه $q \in \mathbb{Z}$ لپاره باور ولري $a = b \cdot q$.

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

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

یادونه 2.1.2 : هر ګڼ یا عدد $a \in \mathbb{Z}$ پروپشوني $1,-1,a,-a$ لري، داسي په نامه ساده(نا اصلي) پروپشوني. که نور پروپشوني شتون ولري، نو دا اصلي پروپشوني 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. $a \mid b, b \mid a \Rightarrow a = \pm b$ $|a| = |b|$ (also)(نو .)
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 $\forall c_1, \ldots, c_n \in \mathbb{Z}$:

$$b \left| \sum_{i=1}^{n} c_i a_i \right. . \qquad (2.1)$$

ښونه:

ad 4

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

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

ad 5

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

نو له دي $b = 0$ 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 دي سره $|a| = |b|$ دی، داپه دي 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 دپرې پروېشوني b لري، ځکه چې د(4) 2.1.3 پسې باور لري: $|b| \leq |a|$ ، نو $-|a| \leq b \leq |a|$ ، له دي امله

$$b \in \{-|a|, -|a|+1, \ldots, |a|-1, |a|\}, \tag{2.3}$$

دا فقط پای ډپر دي.

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

پسې راتلنه یا لاس ته راوړنه 2.1.5 : د $(\Rightarrow a \neq 0)\ a \in \mathbb{N}$ 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 :

$$r \geq \sqrt{a} \Rightarrow a = qr \geq q\sqrt{a} > \sqrt{a}\sqrt{a} = a \tag{2.4}$$

- تضاد! له دې سره r پوره 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 دي د $1 \leq b \leq \sqrt{80} < 9$ سره وټاکل شي:

$$1, 2, 4, 5, 8; 80, 40, 20, 16, 10. \tag{2.5}$$

له دې سره ټول پروېشوني دي:

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

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

ياودونه2.1.8 : که $a \in \mathbb{Z}, a \neq 0$ وي، نو a د 2.1.4 پسې يا له مخې فقط پای ډېر پروېشوني لري. که $b \in \mathbb{Z}$ په خوښه وي، نو a او b فقط پای ډېر پروېشوني لري. د اکسيوم 3d له مخې $\mathbb{Z}$ توتالي (ټول يا بېخي) منظم دی، يعنې د a,b ګډ پروېشونی يو خورا لوي توکی دی. نو سړی کړی شي تعريف کړي:

پېژند يا تعيف2.1.9 : (خورا غټ ګډ پروېشونی يا بزرګترين مقسوم عليه Greatest comon divisor) وي دي $a,b \in \mathbb{Z}$ ، نه دواړه صفر، نو $\mathrm{ggT}(a,b)$ (انګرېزي يې gcd(a,b)) د ټولو ګډ پروېشونو خورا لوی(يعنې 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 پروېش پردې(ګډ اصلي پروېشونی 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 پروېشونو ځنونه محدود کړي، ځکه چې 1 يو ګډ پروېشونی دی، يعنې 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 پروېښنوني له دې لاس ته راځي ګډ مثبت پروېشوني دي:

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

د اويکليد يا اقليدس له مخې د ggT ټاکنه

جمله 2.2.1 : د اويکليد الګوريتم (Euklidische Algorithmus[1, 2]) وي دي $a, b \in \mathbb{N}$ او بې له تولیزو 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 $q_i, r_i \in \mathbb{Z}$ سړی 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

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

د $a = b \cdot q_0 + r_1$ لپاره.

وي دي $b \nmid a$ ، نو $a = q_0 b + r_1, 0 \leq r_1 < b$ باور لري د $r_1 \neq 0$ سره. د جوړښت له مخي باور لري

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

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

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

وښايی : $r_n = \mathrm{ggT}(a, b)$

- $r_n \mid a, b$: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 $r_n \mid r_{n-1}, r_{n-2}$

- که په ورته توګه مخ ته لاړ شو، نو تري 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 یو د a, b مثبت پروښونی 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 همداسي پسي، 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 پروښونی دی.

یادونه 2.2.2 : که د اعدادو یو (یا دواړه) $a, b \in \mathbb{Z}$ د صفر کوچني وي، نو د اوکلید الګوریتم دې په $|a|$ همداسي په $|b|$ باندې وکارول شي، ځکه چې

مور د a, b د مثبت پروښونو پیداکېدل 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:

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

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

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

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

پېژند یا تعریف2.2.4 : (کرښیز کمپرزېشن یا – یوځای ایښوونه) : 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 پسې $\alpha c + \beta d$، $\forall \alpha, \beta \in \mathbb{Z}$.

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 : $\mathrm{ggT}(a, b) = xa + yb$ یو کرښیز کمپوزېشن دی، د ټاکلو $x, y \in \mathbb{Z}$ لپاره.

ښوونه:

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

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

دویم . 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	$\cdots \Rightarrow \underbrace{r_n}_{\text{ggT}(a,b)} = r_{n-2} - q_{n-1}r_{n-1},$

$$\Rightarrow \text{ggT}(a,b) = xa + yb$$

.1

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

$$d = \text{ggT}(a,b) = a = 1 \cdot a + 0 \cdot b$$

.2 $b = 0$:

.3 $b < 0$ $-b > 0$ دی او له ۱ . حالته باو لري : نو

$$\text{ggT}(a,b) = x \cdot a + y \cdot (-b)$$

(که غوښتوني وي a 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 ښرته جوړختیزه ده، دا یو متود راکوي د $x, y \in \mathbb{Z}$ تاکلو لپاره په $\mathrm{ggT}(a,b) = xa + yb$ کې، داسې چې د اوکلید الګوریم څخه پاتې افاده کوو یا وایو له مخ ته تیرو د کرښیز کمپوزیشن لویو څخه او په لاندې راتلونکي مساوات کې یې ځایه ځایو کوو.

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

$$111 = 2 \cdot 39 + 33 \quad 3 = 33 - 5 \cdot 6$$

$$39 = 1 \cdot 33 + 6 \quad = 33 - 5(39 - 33) = 6 \cdot 33 - 5 \cdot 39$$

$$33 = 5 \cdot 6 + 3 \quad = 6(111 - 2 \cdot 39) - 5 \cdot 39$$

$$6 = 2 \cdot 3. \quad = 6 \cdot 111 - 17 \cdot 39$$

.

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

غواړو پیدا کړو:

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

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

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

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

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

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

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

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

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

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

دا په دې معنا چې $17 \mid 2k-1$.

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

دا په دې معناچې $17 \mid 9k+4$.

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 راوړني.

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 ټاکلو $x,y \in \mathbb{Z}$ لپاره، يعني $d \cdot 1 = d(x\frac{a}{d}+y\frac{b}{d})$ ، 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 $|t| \leq 1$ ، يعني $t \leq 1$ ، له دې سره $t=1$. نو $\mathrm{ggT}(\frac{a}{d},\frac{b}{d})=1$.

ad 2:

له $\mathrm{ggT}(\frac{a}{t},\frac{b}{t})=1$ د2.2.5 سره د معلومو $\alpha,\beta \in \mathbb{Z}$ لپاره راکوي $1=\alpha\frac{a}{t}+\beta\frac{b}{t}$ ، يعني $t=\alpha a+\beta b$. د وړاندنيونو(فرضيو) وروسته $|t|$ د a,b يو ګډ پروېښونی دی. وي دې $s \geq 1, s \mid a, s \mid b$ په خوښه، نو د 2.1.3 له مخې $s \mid t$ بارورلري، داسې چې $|s| \leq |t|$ دی، دا په دې معنا چې $s \leq |t|$. يعني $\mathrm{ggT}(a,b)=|t|$ دی.

ad 3:

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

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

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

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

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

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

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

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

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 پروپشونی، نو له $d = xa + yb \ (x,y \in \mathbb{Z}$ لاس ته راځي (جمله 2.2.5دې 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 پروپشونی دی. وي دې $c \in \mathbb{Z}, c \geq 1$ په خوښه د a,b پروپشونی، نو د (2) له مخې لاس ته راځي $c \mid d$ ، دا په دې معنا چې د2.1.3 پسې $|c| \leq |d|$ دی ، له دې سره $c \leq d$. يعنې d د a,b خورا غټ ګډ پروپشونی(بزرګترین مقسوم علیه مشترک؟) دی

□

جمله2.2.12 : (بنسټیزه lemma (مرستندوی جمله چې د ښوونې یا ثبوت په جریان 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)	$1 = xa + yb$

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

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

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

دپښې 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 $\mathrm{ggT}(a_1, \ldots, a_n)$ سره په نخښه 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 $\mathrm{ggT}(a_1, \ldots, a_n) = 1$ 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) نسبیي لومړني ګڼونه یا عددونه بلل کیږي، که $\mathrm{ggT}(a_i, a_j) = 1$ وي د ټولو $\forall i \neq j$ لپاره.

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

څټ 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.

جملە2.3.3 : 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:

$d=\sum_{i=1}^{n} x_i a_i$	(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 $a_i\in M, i=1,\ldots,n$ $(c_i=1, c_j=0$ باور لري د $i\neq j)$ او $M\neq\emptyset$ 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 پيداښتي ګڼونه يا عددونه لري. د $\mathbb{N}$ د ټولنظم له مخې په M کې د ټولو طبيعي اعدادو ډېرې يا ستې يو خوا کوچنی توکی d^* لري، دا په دې معناچې

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

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

د پاتي 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، همداسې a_i ، په تعقيب کمښت يا تفريق هم. له دې سره له $0 \leq r_i < d^* : r_i = 0.$ څخه لرو. يعنې:

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

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

$$t \mid x_1 a_1 + \cdots + x_n a_n = d^*; \tag{2.25}$$

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

□

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

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

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

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

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

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

وي دي

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

نو باور لري $d \mid a_1, \ldots, a_n$ ، یعني $d \mid a_1$ ، 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 څټ باور لري: d' $a_1, d' \mid r_i \ (i = 2, \ldots, n)$ وېشي،، یعني داسي لاس ته راځي $a_i = q_i a_1 + r_i : d' \mid a_i \ (i = 2, \ldots, n)$ (د لیما یا جملګی 2.1.3 پسي)، یعني 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 ګډونه 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 : $d = \text{ggT}(721, 613, 114)$.

$a_1 = 114$ ، وېش له پاتې سره :

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

،

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

.

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

$\tilde{a}_1 = 37$ ، وېش له پاتې سره:

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

،

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

.

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

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

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

.

۳ - لومړنۍ ګڼونه(اعداد) Primzahlen

لومړنۍ ګڼونه$\mathbb{P}$

Die Menge der Primzahlen $\mathbb{P}$

Grundlagen بنسټونه

پېژندنه(تعريف) 3.1.1 : يو طبيعي ګڼ يا عدد p لومړنی بلل کيږي، که هغه فقط ساده پروېشوني ولري، دا په دې معنا، چې فقط $\pm 1, \pm p$ پروېشوني دي.

د ټول لومړنيو اعدادو ډېرې د $\mathbb{P}$ سره په نخښه کوو.

جمله : (اويکليد) ناپای ډېر لومړني ګڼونه شته.

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

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

ترڅېرنې نيسو

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

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

وي دي $t > 1$ د $t \mid q$ سره، نو د 2.1.3 پسې لاس ته راځی، چې $t \mid N \Rightarrow t \in M$. له $t \leq q$ ، د q خورا کوچنی توکی دی. يعنې $M \Rightarrow t = q$ لومړنی ګڼ دی، له نيونې څخه لاس ته راځي: $\exists j : q = p_j$. له دې سره $q \mid N \ (q \in M)$ باولري او په ساده توګه :

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

- تضاد □

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

ټو له 1 تر n پورې ټول ګڼونه وليکه، که ټول لومړني اعداد پېژندل شوي وي، نو سړی دې د ټولو دې لومړنيو ګڼونو په ډېرواره کرښه 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):

$$2, 3, 5, 7, \cancel{9}, 11, 13, \cancel{15}, 17, 19, \cancel{21}, 23, \cancel{25}, \cancel{27}, 29, 31, \cancel{33}, \cancel{35},$$

$$37, \cancel{39}, 41, 43, \cancel{45}, 47, \cancel{49}$$

ټول اعداد چې کرښه 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، وګورئ[Gut02b, Rie94])، کارونه يا استعمالیې په کريپټولوژي Kryptologie کې کيږي.

دويم: د لومړنيو ګڼونو جمله:

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

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

دريم: د لويي $x \in \mathbb{N}$ لپاره

نږدي:

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

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

له بلې خوا د دوه لومړنيو اعدادو ترمنځ په خوښه لويي تشياوي شتون لري:وي دې $n \in \mathbb{N}$ ، نو $(n+1)!+2, \ldots, \quad (n+1)! \quad +(n+1)$ ګڼونه

همدا اوس n يو 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

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

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

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

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

پنځم : د دیریښلیت[3.2] Dirichlet جمله : که $a, b \in \mathbb{N}$ وي د $ggT(a,b) = 1$

سره، نو ډېرې دا لاندې خوندي لري

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

ناپای ډېر لومړني اعداد. (د اریتمیتیکي پروګرشن لپاره د لومړنیو اعدادو جمله، تولیزه ښوونه ډېره پېچلي ده!)

د $\{4k+1 \mid k = 1, 2, \ldots\}$ لپاره ، همداسې $\{4k+3 \mid k = 1, 2, \ldots\}$ لپاره

لږ څه وروسته ښایو(جمله 9.2.8 همداسې جمله 3.1.10 وګورې).

شپږم: د $2^{2^n} + 1 (n \in \mathbb{N})$ بڼې عدد د فرمات عدد[3.3] *Fermat'sche Zahl* بلل

کیږي، د $n = 0, 1, 2, 3, 4$ لپاره په ریښتوني لومړني اعداد دي:

$$3, 5, 17, 257, 65.537$$

.

له دې پسې چا نور د فرمات اعداد پیدا نه کړل. تر اوسه معلومه نه ده، چې ایا پای او که ناپای ډېر فرمات ګڼونه شتون لري. د فرمات کوچنی عدد، چې تراوسه یط ځوک ترتیبولی نه شي F_{33} دی.

اوم : يو د $2^n - 1 \ (n \in \mathbb{N})$ بڼې 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، داسې نامیز $p = 2^{13.466.917} - 1$.

اتم: د ګولدبښ ګومان : هر جوړه عدد له څلور سره برابر يا تر لوی وي د دوه لومړنيو اعدادو د زياتون يا جمعې په څېر انځورورِ دی. (د بېلګې 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.

جملە3.1.5 : 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 ځلوونو $a_i, 1 \leq i \leq n$ څخه يو وېشي.

ښوونه: د n پسې 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: $p \nmid a_{n+1}$ نو $\mathrm{ggT}(p, a_{n+1}) = 1$ دی، داسې چې د بنسټيزې جملګی2.2.12 څخه لاس ته راځي، چې $p \mid a_1 \cdots a_n$. د ايندکشن د نيونې يا فرضيې څخه لاس ته راځي $p \mid a_i$ د $1 \leq i \leq n.$ لپاره.

□

لاس ته راوړنه3.1.6 : د $n = 2$ لپاره باور لري: p د $a_1 \cdot a_2$ یو پروېښونی 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 څټوالی یا معکوسوالی هم باور لري: که g یو طبیعي عدد 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 پروېښوني 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 نیونې 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 ضربېتوټه ونه یا په لوړنیو ضربیونو 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 $\mathbb{N}$ ضریبي جوړښتخښتي دي).

ښوونه:

شتونوالی:

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

: $n = 2$

ساده

: $n - 1 \to n$:

بنایو: 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 ګنونو یا عددونوضرب نه دی. وي دې k_0 د دوی ترمنځ خورا کوچنی عدد. نو k_0 لومړنی عدد نه دی. یعنې که باور ولرې $k_0 = a \cdot b$ ، چېرته چې $a < b < k_0$ ، له دې سره لاس ته راځی:

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

وښایې: n د لومړنیو عددونو ضرب نه دی.

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

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

یواخېوالی یا یواځنوالی:

وي دې $n > 1$ او

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

د کومو سره چې $p_i, q_j \in \mathbb{P}, r \leq s$. د $p_1 \mid p_1 \cdots p_r$ له املې 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 املې $p_1 = \pm 1$ یا $p_1 = \pm q_i$ (q_i لومړنی عدد) ، یعنې $p_1 = q_i$ ($p_1 > 1$) . د نمرې بدلون سره کېدی سړی لاس ته راوړي: $p_1 = q_1 \ (q_i \to q_1)$. 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 خو، تر $p_r = q_r, 1 = q_{r+1} \cdots q_s$ پورې.

که $s > r$ وی نو باور لرې چې q_{r+1} ښې 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 توټه کونه سره یوځای کړو

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

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

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

که دا دلته نه شتون لرونکو لومړنیو عددونه p د $p^0 := 1$ له لارې پوره کړو، نو سړی 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 لری، دا به دې معنا ، چې د $\{3, 7, 11, 15, 19, \dots\}$ عدونو په ډېرې کې ناپای ډېر لومړني عددونه شتون لری..

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

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

د نیوني یا فرضیي له مخي د ځنو $k_i \in \mathbb{N}_0 \ (i = 1, \ldots, s)$ لپاره $p_i = 4k_i + 3$ باور لري، یعني

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

$(4k + 3)(4l + 3) = 4m + 1$ د یوه $m \in \mathbb{N}$ لپاره. له دي امله د یوه k لپاره. له دي امله $N := p_1^2 \cdots p_s^2 + 2$ بڼه $(4n + 1) + 2 = 4n + 3$ لري.

وي دي $N = q_1 \cdots q_r$ د $N \in \mathbb{N} \ (N > 1)$ په لومړنیو ګڼونو توته ونه. نه تول q_i د بڼې $4k + 1$ دي(ځکه چې بیا به N هم له دي بڼې وی). له دي 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 تري دباندي 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 ($q_i = 4k + 3 \geq 3$).

□

د $\mathbf{ggT}$ او $\mathbf{kgV}$ ترمنځ اړيکي(د خ غ ک او خ ک ګ زياتځلي - -

$$a = \prod_{p\in\mathbb{P}} p^{\alpha_p} \quad b = \prod_{p\in\mathbb{P}} p^{\beta_p}$$

جمله3.2.1 : وي دي ، ، نو باور لري

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

$$x = \prod_{p\in\mathbb{P}} p^{\rho_p}, y = \prod_{p\in\mathbb{P}} p^{\sigma_p}$$

ښوونه: ښايو: وی دی ، نو باور لري:

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

$(\Rightarrow)$ يا له ذدې لاس ته راځي

$$x \mid y \Rightarrow y = x \cdot z$$

،

$$z = \prod_{p\in\mathbb{P}} p^{\tau_p}$$

د سره په لومړنيوضريبونو ټوټه کوني په حيث، يعني

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

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

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

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 د 1.1.4 پسې باور لري:

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

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

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

يعني $xz = y \Rightarrow x \mid y$.

وي دي $d := \mathrm{ggT}(a,b)$ 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 ویشي، د جملې 2.2.5 او جملګی یا کورولار 2.2.11 څخه $c \mid d$ لاس ته راځي، دا په دې معنی،

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

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

$$a = 2^2 \cdot 3^4 \cdot 5^2, b = 2^3 \cdot 3^2 \cdot 7^3$$

بېلګه 3.2.2 : وي دې ، نو د نا شتونو لومړنيو ګڼونو د پوره کېدنې له امله د 0 اکسپننت له لارې باور لري:

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

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

کورولار يا جمګې3.2.3 :

لومړی :

$$a_i \in \mathbb{N}, sei \ a_i = \prod_{p \in \mathbb{P}} p^{\alpha_{i,p}}, \ i = 1, \ldots, n$$

وي دې د لومړنيوضريبونو ټوټه کونه، نو باور لري

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

دويم : وي دي $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}, b = \prod_{p\in\mathbb{P}} p^{\beta_p}$ ، 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 دي، نو $v \in \mathbb{Z}$ د a,b ګډ ډېرځله (مضرب مشترک)بلل کيږي، که $a \mid v$ او $b \mid v$ وي(داپه دي 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 دي معنا، چې هم کميز او هم زياتيز يعني منفي او مثبت ګډ ډېرواره يا ګډ ډېرځله شتون لري.

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

پېژندنه(تعيف)3.2.6 : وي دي $a,b \in \mathbb{Z}$ ، 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 دي ګڼونو يو صفر وي، يا دواړه، نو تعريفوو $\mathrm{kgV}(a,b) := 0$.

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

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

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

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

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

املە د جملي 3.2.1 بنوونه پسې باور لري، چې

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

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

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

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

بېلګه 3.2.9 : وي دي $a=2^3 3^2 5. b=2^2 3^3 7$ ، نو
$a=2^3 3^2 5^1 7^0, b=2^2 3^3 5^0 7^1$

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

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

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

د $a_1, \ldots a_n$ لپاره په ټولیزه توګه:

تعریف 3.2.11 : وي دي $a_1, \ldots, a_n \in \mathbb{Z}$ ، نو $v \in \mathbb{Z}$ د $a_1, \ldots, a_n$ یو ګډ زیاتځله بلل کیږي، که $a_i \mid v, i = 1, \ldots, n$.

وي دي $a_i \neq 0, i = 1, \ldots, n$ ، نو دا د ټول مثبتو خورا کوچنیو ګډزیاتځله 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 یو $a_i = 0$ وي، نو سږی تعریفوي $\mathrm{kgV}(a_1, \ldots, a_n) := 0$.

یادونه3.2.12 : 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 گی)3.2.13 : وي دي $a_1, \ldots, a_n \in \mathbb{Z}, a_i = \prod_{p \in \mathbb{P}} p^{a_{i,p}}$ په لږمږنی ضریب ټوټه کونه، نو باور لري ($a_i \neq 0 \ \forall i$) :

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

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

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

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

$$a_i=\prod_{p\in\mathbb{P}} p^{\alpha_{i,p}}, i=1,\ldots,n$$

ښوونه : وي دي . 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 دي $\alpha_{i_0,p}=\max\limits_{1\le i\le n}(\alpha_{i,p})$ ، نو باور لري $\alpha_{i,p}\le\alpha_{i_0,p}, i=1,\ldots,n$ يعنې

$-\alpha_{i,p}\geq -\alpha_{i_0,p}$

او

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

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

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

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

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

جملګی3.2.15 : دا یو امکان دی ، چې د لویو ګنو 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).

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

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

$$A_1 = a_2 a_3 = 120, A_2 = a_1 a_3 = 90, A_3 = a_1 a_2 = 48 \Rightarrow$$

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

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

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 ګنونو a_1, a_2 خورا کوچنی ګډزیاتځله ټیک 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

$\mathrm{kgV}(a_1, \ldots, a_n) = a_1 \cdots a_n$ ټیک 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:

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

يعني $a-r=qm$ ، دا به دي معنا، چې $m \mid a-r$.

بيژند(تعريف)4.1.1 : که وي $a,b \in \mathbb{Z}, m \in \mathbb{N}$ په خوښه، نو a,b کونګروانځ مودولو m بلل کيږي، که $m \mid a-b$ ، سومبوليک يا ليکندود $a \equiv b(m)$.

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

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

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

ثبوونه : وي دي $a=qm+r, 0 \leq r < m$ او $b=q'm+r', 0 \leq r' < m$

$a \equiv b(m) \Leftrightarrow r=r'$

(د پاتې سره وېش). ښايو:

$(\Leftarrow)$

$r=r'$:

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

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

$(\Rightarrow)$

$a \equiv b(m)$:

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

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

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

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

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

يادونه : د,,≡`` له لارې په $\mathbb{Z}$ د $m \in \mathbb{N}$ لپاره يو ورته اړيکې ، په خوښه مګر کره ټاکلې، تعريف دي:

لومړی : (

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

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

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

ختی لا دېر باور لري ($\equiv$ د $+$ او $\cdot$ سره زعمور دی، د ،،کونګروانځ ،،کلمه دي پع الجبر کي پرتله شي)

لېما 4.1.5 : وي دي $a, b, c, d \in \mathbb{Z}, m \in \mathbb{N}$ 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 $k \in \mathbb{Z}, d = \mathrm{ggT}(k, m) \Rightarrow a \equiv b(\frac{m}{d})$,
6. $a \equiv b(m), a \equiv b(n), n \in \mathbb{N} \Rightarrow a \equiv b(\mathrm{kgV}(m, n))$.

ښوونه:

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

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

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

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

,

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

.

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

.

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

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

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:

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

نو د بنسټيزي 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)

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

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

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

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 ټرنو یاکارونو یا عملیو سره زغورې دی(د ورته اړیکو یا کونګروانځ اړیکو په هکله دتر مخه تېر ې 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 :

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

$a \equiv b(m), f(x) = c_0 + c_1 x + \cdots + c_k x^k$ د $c_i \in \mathbb{Z}$ سره، نو باور لرې

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

څلورم :

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

(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 :

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

اوم :

$a \equiv b(m), m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ په لومړنیو ضریبونو تجزیه کوئ

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

(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

$$\Rightarrow a \equiv b(p_1^{a_1} \cdots p_k^{a_k}) : a \equiv b(m)$$

د پروېشنورواليTeilbarkeitsregeln قوانين

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

جمله4.2.1 : $n = (a_k a_{k-1} \ldots a_1 a_0)$ 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. $n \equiv (a_0 + 10a_1 + 10^2 a_2) - (a_3 + 10a_4 + 10^2 a_5) + - \cdots (7)$, (13) resp. ,
6. $n \equiv a_0 + 10a_1 + 10^2 a_2(8)$,
7. $n \equiv a_0 + a_1 + \cdots + a_k(9)$,
8. $n \equiv a_0 - a_1 + a_2 - + \cdots + (-1)^k a_k(11)$.

بنوونه:

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

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

دويم :

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

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

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

دريم :

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

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

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

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

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

پنځم :

1. د۱ - له امله

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

$$+10^6(a_6 + 10a_7 + 10^2a_8) + \cdots \tag{4.17}$$

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

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

، داسي چې

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

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

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

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

$$n = a_0 + 10a_1 + \cdots + 10^k a_k \equiv \tag{4.20}$$

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

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

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

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

$$n = a_0 + 10a_1 + \cdots + 10^k a_k \equiv \tag{4.23}$$

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

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

جمله ګي 4.2.2 : (پروپشنور قوانين) که $n = (a_k \dots a_0)_{10} \in \mathbb{N}$ 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. $8 \mid n \Leftrightarrow 8 \mid (a_2 a_1 a_0)_{10}$,

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 بېلګې په توګه د دې لومړنیو درې راوړل شوي قوانین ښایو، نو ټول کېدی شي په ورته توګه وښوول شي.

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

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

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

یادونه 4.2.3 : سړی کړی شي د معلومو پروېشقوانینو پسې 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 $n = 97234382 \mid n$ $2 \mid 8$ $3 \mid n$ $3 \mid 36$ $4 \nmid n$, da ; , da ; ,
da $4 \nmid 38$ $5 \nmid n$ $5 \nmid 8$ $6 \mid n$ $2 \mid n, 3 \mid n \wedge \mathrm{ggT}(2,3) = 1$; , da ; , da ;
$7 \nmid n$ $7 \nmid (438 - 723 + 009) = -276$ $8 \nmid n$ $8 \nmid 438$ $9 \mid n$, da , da ; , da

$9 \mid 36$; $11 \nmid n$, 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 وېشنې 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 داسې په نامه،، پاتې ټولګي،، لاس ته راوړي، فورمال د 4.1.4 پسې ،، $\equiv$ ،، 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 بنه $a + km$ لري(د $k \in \mathbb{Z}$ لپاره)، ځکه چې:

$$x \in \overline{a} \Leftrightarrow x \equiv a(m) \Leftrightarrow x - a = km \qquad k \in \mathbb{Z} \Leftrightarrow x = a + km$$

د یوه

لپاره . له دې سره

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

په خوښه

$$\forall a \in \mathbb{Z} : \overline{a} = \overline{r} \qquad r \in \mathbb{Z}$$

دویم : د کوم سره چې په m باندې د a د

وېشنې پاتې دی ($0 \leq r < m$)، ځکه چې:

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

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

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

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

دا په دې معن، چې $0 \leq r \leq m-1$ ، دا په دې معنا، چې زیات له زیاته m مختلف پاتې ټولګي شتون لري.

که $\overline{r} = \overline{r'}, 0 \leq r \leq m-1, 0 \leq r' \leq m-1$ باور ولري، نو $r \equiv r'(m)$ باور لري ، په m باندې د r, r' د وېشنې څخه r همداسې r' پاتې(که غواړی: باقي) پاتې کیږي، دا باید د 4.1.3 پسې باور ولري: $r = r'$. برعکس: $r = r' \Rightarrow \overline{r} = \overline{r'}$. نو ټیک 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 (تعریف) 4.3.4: د $\mathbb{Z}$ یوه برخه ډېرې کومه چې له هر پاتې ټولګي ټیک یو توکی خوندي لري، نو پوره مودولو m پاتې سیستم بلل کیږي.

بېلګه4.3.5 : $m = 4, \mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}; \{0, 1, 2, 3\}$ یو پوره پاتې سیستم $\mathrm{mod}\, 4$ دی، همداسې $\{4, -3, -2, 4\}$ یا $\{100, 99, 98, 97\}$.

لیما 4.3.6 : یوه برخډېرې $\{r_1, \ldots, r_m\} \subseteq \mathbb{Z}$ ټیک هلته یو پوره پاتې سیستم مودولو m دی، که $r_i \not\equiv r_j(m)\ \forall i, j = 1, \ldots, m : i \neq j$ وي.

ښوونه:

$(\Rightarrow)$

که $\{r_1,\ldots,r_m\}$ یو پوره پاتې سیستم وي، نو $r_i,$ ، $i=1,\ldots,m$ 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 دی، او ټول مختلف دي، نو $\{r_1,\ldots,r_m\}$ یو پوره پاتې سیستم دی.

کورولار یا جمله ګی 4.3.7 : وې دي $\{r_1,\ldots,r_m\}\subseteq\mathbb{Z}$ یو پوره پاتېسیستم مودولو m او $a,b\in\mathbb{Z}$ دي د $\mathrm{ggT}(a,m)=1$ سره وي، نو $\{ar_1+b,\ldots,ar_m+b\}$ 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

$$ar_i \equiv ar_j(m), \tag{4.30}$$

او له دې سره د(4)4.1.6 له امله :

$$r_i \equiv r_j(m), \tag{4.31}$$

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

نو له دي 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 ګي4.3.8 : وي دي $\{r_1, \ldots, r_m\} \subseteq \mathbb{Z}$ يو پوره پاتي سيستم مودولو m ، $\{s_1, \ldots, s_n\} \subseteq \mathbb{Z}$ يو پوره پاتي سيستم مودولو n او $\gcd(m,n) = 1$ ، نو

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

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

يو پوره پاتي 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 $i \neq k$ همداسي $j \neq l$ 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 دي سره $nr_i \equiv nr_k (m)$.

له دي امله د لاس ته راوړني پسي(4) 4.1.6 لاس ته راځي: $r_i \equiv r_k (m)$ ځکه چې

$$\gcd(m,n) = 1 \Rightarrow i = k$$

د4.3.6 له مخي . له دي 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 پاتي ټولګي کړی يا -- رينګ $(\mathbb{Z}_m, +, \cdot)$

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 لاندي سره:

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

بنايو : دا تعريفونه د و وکيلانو (Repräsentanten) خپلواک دي، دا په دي معنا، چې $\overline{a} = \overline{a'}, \overline{b} = \overline{b'}$ ، 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:

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

نسبت جمعي $\oplus$ ته باور لري : $(\mathbb{Z}_m, \oplus)$ يو کموتاتيو گروپ دی. ځکه چې :

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

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

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

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

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

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

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

$$\overline{a} \oplus \overline{-a} = \overline{-a} \oplus \overline{a} = \overline{0}.$$ (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 گروپ دی د 1 سره. ځکه چې:

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

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

$a(b+c) = ab + ac \Rightarrow \overline{a(b+c)} = \overline{ab + ac}$

(ځکه چې: .).

له دې سره $(\mathbb{Z}_m, \oplus, \odot)$ یو کموتاتیو رینګ (کړی) دی د 1 سره، داسې په نامه ،،پاتې ټولګي رینګ یا— - کړی) $\mathrm{mod}\, m$،، دی. د $(\mathbb{Z}_m, \oplus, \odot)$ انځورونه د جدول په مرسته صورت نیسي یا لاس ته راځي. دا د $\mathbb{Z}_4$ لپاره په لاندې ډول لیدل کیږي:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{00}$	$\overline{11}$	$\overline{22}$	$\overline{33}$
$\overline{1}$	$\overline{12}$	$\overline{23}$	$\overline{30}$	$\overline{01}$
$\overline{2}$	$\overline{23}$	$\overline{30}$	$\overline{01}$	$\overline{12}$
$\overline{3}$	$\overline{30}$	$\overline{01}$	$\overline{12}$	$\overline{23}$

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

په کړی یا رینګ $(\mathbb{Z}, +, \cdot)$ (کموتاتیو کړي 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 ټیک نه دی، دا د $m = 6$ لپاره باور لري $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$ ، چېرته چې $\overline{2}, \overline{3} \neq \overline{0}$ دی.

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

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

دویم : یو R انټیګریټي کړي (صفرپروېښوني ازاد یا بې صفرپروېښوني) بلل کیږي، که په R کې صفرپروېښونی شتون ونه لري.

دریم : یو $a \in R$ یوون یا واحد بلل کیږي، که یو $b \in R$ شتون ولري، د $ab = 1$ سره، a د b معکوس یا په څټ بلل کیږي (نسبت و ضرب ۰ ته)، سومبولیک: $b = a^{-1}$.

څلورم : که په R کې هر $a \neq 0$ یو یوون وي، نو $(R, +, \cdot)$ یو بدن یا تن یا جسم بلل کیږي(انګریزي).

بېلګه 4.4.2 :

لومړی : $(\mathbb{Z}, +, \cdot)$ یو انټیګریټي کړی ده، یوونونه یا واحدونه ± 1 دي.

دویم: $(\mathbb{Z}_6, +, \cdot)$ صفرپروېښوني $\overline{2}, \overline{3}, \overline{4}$ او یوونونه $\overline{1}, \overline{5}$ لري .

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

پېژندنه(تعریف)4.4.3 : یو $\overline{a} \in \mathbb{Z}_m$ لومړنی پاتې سیستم $\mathrm{mod}\, m$ بلل کیږي،که $\mathrm{ggT}(a, m) = 1$ وي، دا په دې معنا، چې a و m ته نسبي لومړنی دی).

لېم4.4.4ا : 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 سیستم او $\mathrm{ggT}(a, m) = 1$ (پرته له دې بیا سړی بل نماینده سیستم ټاکي). وي دې $b \in \overline{a}$ په خوښه، و دې ښوول شي:

$$\mathrm{ggT}(b, m) = 1$$

.

نیسو، چې $\gcd(b,m)\neq 1$ ، داپه دېمعنا، چې 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 ضربیونو 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 چې $p\mid b, p\mid m$ د $b=a+km$: له امله لاس ته راځي:

$$p\mid a\Rightarrow \gcd(a,m)\geq p \quad (4.44)$$

-- تضاد □

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

ښوونه:

لومړی: که $\overline{a}\in\mathbb{Z}_m$ لومړنی پاتې ټولګی وي له دې لاس ته راځي $\Rightarrow \gcd(a,m)=1$ ، د 2.2.5 پسې 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)

دویم : $\overline{a}$ یوون یا واحد دی.

دریم: که $\overline{a} \in \mathbb{Z}_m$ یوون یا واحد وي، نو یو $\overline{b} \in \mathbb{Z}_m$ 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 $ab - 1 = km$. نیسو چې $\gcd(a, m) \neq 1$ ، نو
$$\exists p \in \mathbb{P} : p \mid a, p \mid m \Rightarrow p \mid 1$$

-- تضاد □

جمله گی4.4.6 : $(\mathbb{Z}_m, +, \cdot)$ تیک هلته یو بدن دی، که m یو لومړنی ګڼ وي.

ښوونه

$(\Leftarrow)$

وي دي $\overline{a} \in \mathbb{Z}_p, \overline{a} \neq \overline{0}$. 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 یو په
خوښه $\overline{a} \in \mathbb{Z}_p$ هم.

نو ټول یوونونه یا واحدونه په $\mathbb{Z}_p$ کې دي. نو د تعریف پسې باور لري : $(\mathbb{Z}_p, +, \cdot)$
یو بدن دی.

$(\Rightarrow)$ وي دي $(\mathbb{Z}_m, +, \cdot)$ یو بدن. ودي ښوول شي: $m \in \mathbb{P}$

نیسو یا فرضوو، چېm نالومړنی دی، نو

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

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 شتون لري د $\overline{r}^{-1} \in \mathbb{Z}_m$ سره. نو له $\overline{rr}^{-1} = \overline{1}$ 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:

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

پښه نوټ::

$$ab = 0 \Rightarrow a = 0 \vee b = 0 \quad 4.1$$

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

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

مورِ په راتلونکي 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 ټیک 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 املې 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 ټولیزه 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.

جملە5.1.1 : یو کرښیز کونګروانځ $ax \equiv b(m)$ ټیک هلته حل وړ دی، که $\mathrm{ggT}(a,m) \mid b$ وي. که دا حالت وي، نو ټیک ناګونګروانت حل $d = \mathrm{ggT}(a,m) \bmod m$ لرو.

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

$\Rightarrow$

وي دي $ax \equiv b(m)$ حلور، 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: $d = \mathrm{ggT}(a,m)$ ښی خوا وېشي، او له دې سره هم b .

$\Leftarrow$

برعکس : که $d = \mathrm{ggT}(a,m) \mid b$ وي، نو باور لري: $c \in \mathbb{Z}$ د يوه $b = cd$ 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 (اينکونګروانځ) 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:

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

نو $ax_1 \equiv b(m)$ هم.

له دي امله غوښتنه :

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

$$a(x - x_0) \equiv b - b = 0(m)$$

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 پسي 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 دي 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 بتسټيزي ليسما 2.2.12سره لاس ته راځي $\frac{m}{d} \mid (x - x_0)$ ، دا په دي معنا، چې $x - x_0 = t\frac{m}{d}$ د يوه $t \in \mathbb{Z}$ لپاره . له دي امله لاس ته راځي:

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

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

وي دي $x_0+k\frac{m}{d}$ 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 کنونو d سره کونګروانځ 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 املە 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: $x_0, x_0+1\frac{m}{d}, \ldots, x_0+(d-1)\frac{m}{d}$ کونګروانت مودولو m دي.

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

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

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

یادونه5.1.2 : د $ax \equiv b(m)$ دتولو اینکونګروانت حلونو ته بسیا کوي، چې یو ځانګړی حل x_0 پیدا کړو. تول اینکونګروانت حلونه دا لاندې څېره 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 $32x \equiv 20(14); \quad \mathrm{ggT}(32,14) = 2 \mid 20$ 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 بنووني 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

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

دویم : دا په دې معنا، چې $x_0 = -9$ یو حل دی.

دریم. $\mod 14$ اینکونګروانت حل د بېلګې په توګه دی

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

دریم: 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 بنې بدلون له لارې:

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

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

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

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

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

$$x \equiv 5(7)$$

شپږم: دویم حل: $5+7=12$

بېلګه5.1.4 : غوښتنه یا ثبوت د $\overline{3} \bmod 16$ معکوس (نسبت ضرب ته) غواړو پیدا کړو. د4.4.5 پسې $\overline{3}^{-1} \in \mathbb{Z}_{16}$ شتون لري، ځکه چې $\mathrm{ggT}(3,16)=1$ ، نو $\overline{3}$ یو لومړنی پاتې تولګی دی. غواړو یو x پیداکړو، 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 $\overline{3}^{-1} = \overline{11}$.

سیمولتان کونګروانت Simultane Kongruenzen

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

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

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 $m_1 \cdots m_k$ یواځنی.

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

نو $\mathrm{ggT}(M_i, m_i) = 1$ 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 :

$p \mid m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$ د :3.1.5 پسې $p \mid m_j$ د یوه $j \neq i$ لپاره -- تضاد، خکه چې m_i جوړه لومړني وو د نیوني 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 ترځېړنې نیسو:

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

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

وي دي $1 \leq j \leq k$ 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 دي معنا، چې x_0 د سيستم د k کونګروانتو هر يو پوره کوي.

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

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 پسي $\mathbf{kgV}(a_1, \ldots, a_k) = m_1 \cdots m_k$ باور لري او

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

□

بېلګه 5.2.2 : لاندې سیستم ورکړ شوی:

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

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:

$$M = 105, M_1 = 35, M_2 = 21, M_3 = 15$$

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

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

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

$$\Rightarrow x_0 = \sum_{i=0}^{3} a_i M_i y_i = 2 \cdot 35 \cdot 2 + 3 \cdot 21 + 2 \cdot 15 = 233 \equiv 23$$

دویم: د سکځیسیف پرځای کولو سره:

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

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

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

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

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

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

د دې ځانګړي حالت تر څنګ، اوس د کرښیزو کونګروانتو تولیز سیستم تر څېړنې لاندې نیسو

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

نیونه یا فرضیه :

$$m_1, \ldots, m_k \in \mathbb{N}$$

1. جوړه نسبي لومړني .
2. هر دk کونګروانت حلوړ دی.

سړی کړی شي وښايي:

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

د لاندي يو په بل پسي ايښوونې له لارې عملي شمېرنې ته

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

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

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

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

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

$$1 + 2t \equiv 4(7) \Leftrightarrow 2t \equiv 3(7) \Leftrightarrow 2t \equiv 10(7) \Leftrightarrow t \equiv 5(7)$$

نو

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

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

نو

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

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

د سیستم حل5.20) . د ټول خلونو ټولګه:

پښې یادونه:

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

.... ټولیز [5.2]

د ،،ټولیز،، لاندې د5.19 ډول یا تیوپ سیستم پوهیرو، چېرته چې ټول $a_i = 1$ نه دي.

الجبري کونګروانت Algebraische Kongruenzen

پېژند(تعریف) 5.3.1 : وي دي

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

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

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

یو الجبري کونګروانت یلل کیږي د درجېn . غوښتوني: ټول $x_0 \in \mathbb{Z}$ د لاندې سره

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

یادونه 5.3.2 :

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

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

نو : حلونه د پولینومون صفرځایونه 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 $\mathbb{Z}_m$ کي.

یادونه 5.3.3 : د $x_0 \in \mathbb{Z}$ $f(x) \equiv 0(m)$ 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 دي پیدا شي.

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

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

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

پېژند(تعریف) : که

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \ (a_i \in \mathbb{Z})$$

وي، نو

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1 \quad (5.28)$$

د $f(x)$ (فورمال) مشتق بلل کیږي.

یادونه5.3.6 : د ټول $\forall x, a \in \mathbb{Z}$: لپاره باور لري :

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

د یوه پولینوم g لپاره د په $\mathbb{Z}$ کې ضریبونو 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 پولینوم دی، دا په دېمعنا، چې مشتقور $\lim_{x \to a} g(x) = g(a)$ ، ځکه چې g پولینوم دی له دې لاس ته راځي، چې ناپرېکېدونکی دی.)

د حلونوو عملي شمېرنه Praktische Berechnung der Lösungen

لومړی : لیما 5.3.7 : $f(x) \equiv 0(m)$ تیک هلته حلور دی، که $f(x) = 0(p_i^{\alpha_i})$

حلور وي د ټولو $i = 1, \ldots, k$ لپاره او که $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ د m لومړنی ضریب ټوټه ونه وي.

ښوونه :

$(\Rightarrow)$

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

$(\Leftarrow)$

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

د ا لاندې سیستم تر څېړنې نیسو

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

د چینایي پاتې جملې 5.2.1 له مخې دا سیستم یو حل $a \in \mathbb{Z}$ لري (مودولونه جوړه لومړني دي) دا په د ېمعنا، چې

.

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

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

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

دا په دي معنا، چې $f(a) \equiv 0(p_i^{\alpha_i})\ \forall i$ ، له دي 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 لړمړنی عدد د حل متود يا لار ، په خوښه $n \in \mathbb{N}$ 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 سړی حل مودولو p^n لاس ته راوړي:

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

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

لپما . وي دي $x_0 \in \mathbb{Z}$ 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،

يعني x_0 له نيوني سره سم پېژندلی دی ، ($\bmod p^{n-1}$) $x_0 \in \overline{a}$ د يوه $a \in \mathbb{Z}$
لپاره ، يعني $x_0 = a + tp^{n-1}$ 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؟

لپما5.3.9 : $x_0 = a + tp^{n-1}$ د $a, t \in \mathbb{Z}$ او $f(a) \equiv 0(p^{n-1})$ سره ټيک
هلته د $f(x) \equiv 0(p^n)$ يو حل دی، که $t \in \mathbb{Z}$ د کرښيز کونګروانځ يا ورته والي
حل وي؟

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

ښوونه:

$(\Rightarrow)$

وي دي $x_0 = a + tp^{n-1}$ د $f(a) \equiv 0(p^{n-1})$ سره د $f(x) \equiv 0(p^n)$ يو حل، د ښوول دی: دا t د کرښيز ګونګروانځ 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 $p^{n-1} \mid f(a)$ (نيونه يا فرضيه) او $\gcd(p^{n-1}, p^n) = p^{n-1}$ 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: ، يعني $x_0 \equiv a(p)$ ، د(3)4.1.6 پسې $g(x_0) \equiv g(a)(p)$ باور لری (ځکه چې g پولينوم دی)، دا په دي م عنا، چې

$$g(x_0) \equiv f'(a)(p) \Rightarrow \frac{f(a)}{p^{n-1}} + tf'(a) \equiv 0(p). \quad (5.39)$$

$(\Leftarrow)$

وي دي $t \in \mathbb{Z}$ د $f'(a)x + \frac{f(a)}{p^{n-1}} \equiv 0(p)$ حل، دا په دي معنا، چې باورلري:

$$f'(a) \cdot t + \frac{f(a)}{p^{n-1}} \equiv 0(p). \quad (5.40)$$

بنايو؛ $x_0 = a + tp^{n-1}$ 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:

$$f'(a)(x_0 - a) + f(a) \equiv 0(p^n), \quad (5.41)$$

يعني $f(x_0) - f(a) + f(a) \equiv 0(p^n)$ ، 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 دي سره $f(x_0) \equiv 0(p^n)$ ، دا په دي معنا، چې

$$x_0 = a + tp^{n-1} \quad (5.43)$$

د $f(x) \equiv 0(p^n)$ حل دی.

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:

$$\left.\begin{array}{rcl} x & \equiv & a_1(p_1^{\alpha_1}) \\ & \vdots & \\ x & \equiv & a_k(p_k^{\alpha_k}) \end{array}\right\} \quad (5.44)$$

یم : نو دا سیستم بیا د ضرب $p_1^{\alpha_1} \cdots p_k^{\alpha_k} = m$ مودولو یواځنی حل $a \in \mathbb{Z}$

ي. د پل یو پسې له دي املې $f(x) \equiv 0(m)$ هم د $a \in \mathbb{Z}$ یو حل دی.

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 $\mathbf{mod}\, 5^1$:

$x^3 + 2x^2 - 2x - g \equiv 0(5)$ فقط حل $1(\neg 0, \neg 2, \neg 3, \neg 4)$ لري ، دا په دي

م عنا، چې $a_{11} = 1$. مخ ته تلنه یې اړیښنه نه ده، ځکه چې $\alpha_1 = 1$.

دویم: حل $\mathbf{mod}\, 3^3$:

لومړی $\mathbf{mod}\, 3^1$:

$x^3+2x^2-2x-6\equiv 0(3)$ حل $0,2$ لري.

له دې څخه $\bmod 3^2$:

د $a=0$ مخ ته تلنه :

$f(a)=f(0)=-6, f'(a)=-2$ يعني بايد حل شي:

$$f'(0)x+\frac{f(0)}{p^1}\equiv 0(p), \quad (5.45)$$

$-2x+(-2)\equiv 0(3)\Rightarrow t=-1$ او دا په دې معنا، چې

$a_1=a+tp^{n-1}=$

$0+(-1)3=-3$

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

$13x\equiv 0(3)$ ، يعني $x\equiv 1(3)$ ، يعني $t=1$.

$$a_{21}=a_1+tp^{3-1}=-3+1\cdot 9=6. \quad (5.46)$$

بېرته $\bmod 3^2$:

د $a = 2$ مخ ته بیونه یا 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.

$f'(2) = 18, f(2) = 0$ ، یعني 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، ینې هم a_1 شتون نه لري، داپه دې معنا،چې د $a = 2$ و یو $\mathbf{mod}\, 3^2$ حل ته مخ ته بیونه نه شته ، یعني هم $\mathbf{mod}\, 3^3$ حل شتون نه لري.

$$\begin{array}{cc} \mathbf{mod}\, 5^1 & \mathbf{mod}\, 3^1 \\ \vdots & \vdots \\ 1 & 0 \quad 2 \\ & \downarrow \quad \downarrow \\ & \mathbf{mod}\, 3^2 \\ & \text{مخ ته بیونه ناشوني ده} \quad -3 \\ & \vdots \\ & \downarrow \end{array}$$

$$\begin{matrix} \mod 3^3 \\ : \end{matrix} \quad 6$$

لومړی: د $\mod 5^1$ او $\mod 3^3$ حلونو ټولګه : $(1,6)$ و لاندې سیستم ته:

$$\left.\begin{matrix} x & \equiv & 1(5) \\ x & \equiv & 6(3^3) \end{matrix}\right\} \quad (5.48)$$

ویم :

$$x = 1 + 5t \Rightarrow 1 + 5t \equiv 6(3^3) \Rightarrow 5t \equiv 5(27) \overset{ggT(5,27)=1}{\Rightarrow} t \equiv 1(27)$$

$x = 1 + 5t = 1 + 5 \cdot 1 = 6 \Rightarrow x = 6$ یواځنی $\mod 135$ له دې سره:
ناکونګروانځ حل دی.

د الجبري کونګروانځو دحلونو ګڼون یا تعداد

بېلګه5.3.11 :

$$5x \equiv 10(30) : ggT(5,30) = 5 \mid 10 \Rightarrow \exists\, 5 \mod 30 \quad ,$$

$$x^2 \equiv 2(8) : ,$$

$$x^2 \equiv 1(8) : ,$$

$$x^3 - x \equiv 0(3) \ : .$$

یادونه5.3.12 : په څرګنده توګه په تولیز 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 دی

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, a_i \in \mathbb{Z}$$

$(i = 1, \ldots, n)$ 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 : سړی 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 کوچنی د رجه ولري.

$n = 1$:

$$a_1 x + a_0 \equiv 0(p) \quad \text{wobei} \quad p \nmid a_1; \tag{5.49}$$

که $\mathrm{ggT}(a_1, p) \mid -a_0$ ، نو باور لري، چې $\mathrm{ggT}(a_1, p) = 1 \bmod p$ اینکونګروانیخ حلونه شتون لري.

$n - 1 \to n$:

$$a_n x^n + \cdots + a_1 x + a_0 \equiv 0(p) \quad \text{mit} \quad (5.50)$$
$$ggT(a_n, p) = 1, p \nmid a_n.$$

یا حل نه شته، چې بیا کار تامدی.

یا : $a \in \mathbb{Z}$ دې له هغو څخه 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 g د a_n خورا جګ ضریب هم دی! د $p \nmid a_n$ وړاندنیوني له مخې باور لرې .

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 ټولکي 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 $\mathrm{ggT}(a,m) = 1$ سره. وي دې $\mathbb{Z}_m^*$ په $\mathbb{Z}_m$ کې د ټولو واحدونو ډېرې یا ستې. نو باور لري:

لېما 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 $(\overline{ab})(\overline{a'b'}) = \overline{1}$ ، همداسې

$$(\overline{a'b'})(\overline{ab}) = (\overline{a'a})(\overline{b'b}) = \overline{1} \cdot \overline{1} = \overline{1}; \quad (6.2)$$

دويم: يعني 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 $\overline{ab} = \overline{1}$ سره، يعني $\overline{b}\overline{a} = \overline{1}$ (د کموتاتيويتي له املې)، دا په دې معنا، چې $\overline{b}$ هم د $\mathbb{Z}_m$ يو يوون يا واحد دی، او له دې سره لاس ته راځي:

$$\overline{b} \in \mathbb{Z}_m^*. \quad (6.3)$$

پېژند (تعريف)6.1.2 : د ابل گروپ $(\mathbb{Z}_m^*, \cdot)$ لومړنی پاتېټولګي گروپ $\bmod m$ 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؟

په ټولیزه توګه د یوه ګروپ $(G,\cdot)$ د توکو تعداد یا ګنون 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 دي $m \in \mathbb{N}$ په خوښه، نو د $k \in \mathbb{N}$ ګنون یا تعداد $\varphi(m)$ دی د $1 \leq k \leq m$ او د $\mathrm{ggT}(k,m) = 1$ سره .

ښوونه : $\mathbb{Z}_m = \{\overline{1}, \overline{2}, \ldots, \overline{m} = \overline{0}\}$.

$\overline{k}$ لومړنی پاتې ټولګی mod m

دی

$$\overline{k} \in \mathbb{Z}_m^* \overset{4.4.5}{\Leftrightarrow} \Leftrightarrow \mathrm{ggT}(k,m) = 1,$$

دا په دې معنا، چې په $\mathbb{Z}_m^*$ کې د توکو تعداد یا ګنون د k د تعداد سره برابر دی، د $k \in \mathbb{N}, 1 \leq k \leq m$ $\mathrm{ggT}(k,m) = 1$ سره . □

پسې راتلنه یا نتیجه6.1.6 : وي دې $p \in \mathbb{P}$ یو په خوښه لومړنی ګڼ یا عدد، نو باور لرې: $\varphi(p) = p - 1$.

د $\varphi(m)$ شمیرنې ته *Zur Berechnung von* $\varphi(m)$

پېژند یا تعریف 6.1.7 : د ټولو اعداد یا د ټول اعدادو یوه ډېرې لومړنس پاتې سیستم $\bmod m$ بلل کیږی، که دا له هر لومړنی ټولګي $\bmod m$ ټیک یو توکی ولري.

لیما 6.1.8 : یو لومړنی پاتې سیستم ټیک $\bmod m$ ټیک $\varphi(m)$ توکي لري، ځکه چې د 6.1.5 پسې ټیک 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 $\varphi(6) = 2$.

جمله 6.1.10 : وي دي $m, n \in \mathbb{N}, \mathrm{ggT}(m,n) = 1$ ، $\{r_1, \ldots, r_{\varphi(m)}\}$ يو لومړنی پاتي سيستم $\mathrm{mod}\, m$ دی، او $\{s_1, \ldots, s_{\varphi(n)}\}$ يو لومړنی پاتي سيستم $\mathrm{mod}\, n$ دی، نو

$$T = \{nr_i + ms_j \mid i = 1, \ldots, \varphi(m), j = 1, \ldots, \varphi(n)\} \quad (6.5)$$

يو لومړنی پاتي سيستم $\mathrm{mod}\, m \cdot n$ دی.

ښوونه: $\{r_1, \ldots, r_{\varphi(m)}\}$ و يوه پوره سيستم $\mathrm{mod}\, m$ ته پوره يا تکميل کړئ:

$$\{r_1, \ldots, r_{\varphi(m)}, r_{\varphi(m)+1}, \ldots, r_m\} \quad (6.6)$$

او $\{s_1, \ldots, s_{\varphi(n)}\}$ و يوه پوره پاتي سيستم $\mathrm{mod}\, n$ ته پوره کړئ:

$$\{s_1, \ldots, s_{\varphi(n)}, s_{\varphi(n)+1}, \ldots, s_n\}. \quad (6.7)$$

د 4.3.8 پسي

$$R = \{nr_i + ms_j \mid i = 1, \ldots, m, j = 1, \ldots, n\} \quad (6.8)$$

يو پوره پاتي سيستم $\mathrm{mod}\, m \cdot n$ دی، په ځانګړي توګه ټول ګڼونه يا عددونه له R يعني هم له T ټول عددونه ، انکونګروانځ $\mathrm{mod}\, mn$ دي.

و ښايي:

که $a \in R$ او $\mathrm{ggT}(a, mn) = 1$ وي، نو $a \in T$ باور لري.

د $a \in R$ له امله $a = nr_i + ms_j$ باور لري د ځنو $1 \le i \le m, 1 \le j \le n$ لپاره. باور لري: $\text{ggT}(r_i, m) = 1, \text{ggT}(s_j, n) = 1$ ، ځکه چې:

نیسو، چې $\text{ggT}(r_i, m) \neq 1$ ، نو یو لومړنی ګڼ یا عدد p شتونلري د لاندې سره

$$\left.\begin{array}{l} p \mid r_i, \\ p \mid m \end{array}\right\} \Rightarrow \left\{\begin{array}{l} p \mid nr_i, p \mid ms_j \Rightarrow p \mid \underbrace{nr_i + ms_j}_{a=} \\ \\ p \mid mn \end{array}\right\} \Rightarrow \text{ggT}(a, mn) \neq 1 \quad (6.9)$$

-- تضاد (په ورته توګه: $\text{ggT}(s_j, n) = 1 \Rightarrow nr_i + ms_j \in T$ د T تعریف له مخې).

وښایی:

$\text{ggT}(a, mn) = 1$. که $a \in T$ وي، نو باور لري:

د $a \in T \subseteq R$ له امله باور لري:

$$a = nr_i + ms_j \ (1 \le i \le \varphi(m), 1 \le j \le \varphi(n)); \quad (6.10)$$

نیسو، چې $\text{ggT}(a, mn) \neq 1$ ، 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 $p \mid n$ ،

بې له تولیزو بندیزونو یا محدودیتونو دي $p \mid m$ 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 3.1.5 له 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 پاتې سیستم $\bmod m$ توکی دی.

یعنې: T یو لومړنی پاتې سیستم $\bmod mn$ دی. □

کورولار 6.1.11 : وي دي $m,n \in \mathbb{N}$ 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 پاتې سیستم $\bmod mn$ دی، نو T $\varphi(m)\cdot\varphi(n)$ توکي لري. دا چې هر پاتې 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

$$f(mn) = f(m)f(n) \ \forall m,n : \mathrm{ggT}(m,n) = 1 \quad (6.14)$$

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 تري 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::

$$\varphi(p^k) = p^k - p^{k-1} \qquad (p^0 := 1). \quad (6.17)$$

بنوونه : $R = \{1, 2, \ldots, p^k\}$ دي يو پوره پاتي سيستم $\bmod p^k$ وي. لومړی هغه $a \in R$ پيدا کړی، چې و p^k ته نسبي لومړني نه وي:

$$\text{ggT}(a, p^k) \neq 1$$

$$\Rightarrow$$

$$\exists\, q \in \mathbb{P} : q \mid a, q \mid p^k \overset{3.1.5}{\Rightarrow} q \mid p \Rightarrow q = p \Rightarrow p \mid a, \tag{6.18}$$

$$p \mid a$$

$$\Rightarrow$$

$$\text{ggT}(a, p^k) \geq p > 1 \Rightarrow \text{ggT}(a, p^k) \neq 1. \tag{6.19}$$

$\text{ggT}(a, p^k) \neq 1 \Rightarrow$	
$\exists\, q \in \mathbb{P} : q \mid a, q \mid p^k \overset{3.1.5}{\Rightarrow} q \mid p \Rightarrow q = p \Rightarrow p \mid a,$	(6.18)
$p \mid a \Rightarrow \text{ggT}(a, p^k) \geq p > 1 \Rightarrow \text{ggT}(a, p^k) \neq 1.$	(6.19)

دا په دې معنا، چې $a \in R$ ، کوم چې p^k ته نسبي لومړني نه دي، ټيک هغه دي د $p \mid a$ سره. يعني غوښتوني: ټول $a \in R$ ، $p \mid a$ ، دا په دې معنا، چې $a = p \cdot t \ (t = 1, 2, \ldots)$

.

د $1 \leq a \leq p^k \ (a \in R)$ له امله باور لري $1 \leq pt \leq p^k$ ، يعني $1 \leq t \leq p^{k-1}$ باپد 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 تيک 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 دي سره د پيژند له مخي هم باور لري: $\varphi(p^k) = p^k - p^{k-1}$. □

کورولار يا وړه جمل6.1.15: وي دي $m \in \mathbb{N}, m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ په لومړنيو ضريبونو ټوټه کونه ، نو باور لري:

$$\varphi(m) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \cdot \quad (6.20)$$

(دا په دي معنا، چې په په پاتېټولګي کړی(رين، حله) $\bmod m$ کي 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 دي معنا، چې په $\mathbb{Z}_{25}$ کي ټيک 20 يونونه يا واحدونه شتون لري.

دویم:

$$m = 72m = 2^3 3^2 \Rightarrow \varphi(72) = (2^3 - 2^2)(3^2 - 3) = 4 \cdot 6 = 24$$

یعني $|\mathbb{Z}_{72}^*| = 24$ 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.

ثبوونه:

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:

$$a^{-1}ag_i = a^{-1}ag_j, \quad (6.21)$$

دا په دې معنا، چې $g_i = g_j$ د $i \neq j$ سره. ــتضاد!

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 ټرلې $e = a^n, n = |G|$ راکوي . □

جمله 6.1.18 : (اويلر[6.1]) وي دې $a, m \in \mathbb{N}, \mathrm{ggT}(a, m) = 1$ ، نو باور لري:

$$a^{\varphi(m)} \equiv 1(m). \quad (6.24)$$

ثبوونه: د $\mathrm{ggT}(a, m) = 1$ له امله باور لري: $\overline{a} \in \mathbb{Z}_m$ لومړنی پاتې تولګی $\mathrm{mod}\, m$ دی، يعنې $\overline{a} \in \mathbb{Z}_m^*$ باور لري . د $|Z_m^*| = \varphi(m)$ له امله د تعريف له مخې، د 6.1.17 له مخې لاس ته راځي:

$$\overline{a}^{\varphi(m)} = \overline{1}, \quad \text{d.h.} \quad \overline{a^{\varphi(m)}} = \overline{1}, \quad (6.25)$$

$a^{\varphi(m)} \equiv 1(m)$ داسي چي باور لري. □

یو ځانګړی غوره حالت او د6.1.18 مشهور غوره حالت غواړو په لاندي کي ځانله تر څېړنې لاندي ونیسو:

کوروار6.1.19 :(کوچنی فرمات) د تولو $a \in \mathbb{Z}, p \in \mathbb{P}$ لپاره باور لري:

$$a^p \equiv a(p). \quad (6.26)$$

ښوونه: دی $\mathrm{ggT}(a,p) = 1$ ، نو د 6.1.18 له مخي باور لري: $a^{\varphi(m)} \equiv 1(p)$ او د $\varphi(p) = p - 1$ له امله لاس ته راځي:

$$a^{p-1} \equiv 1(p), \quad (6.27)$$

نو په ځانګړي توګه $a^p \equiv a(p)$.

که وي $\mathrm{ggT}(a,p) \neq 1$ ، نو باور لري $a = pt, p \mid a \Rightarrow a^p \equiv 0 \equiv a(p)$

..جمله 6.1.20 :) وېلسن [6.2] 1741-1793 (: د یوه پیداېښتي ګڼ یا طبیعي عدد p لپاره باور لري:

p لومړنی عدد دی

$$\Leftrightarrow (p-1)! \equiv -1(p). \quad (6.28)$$

ښوونه:

$(\Rightarrow)$

وي دي $p \in \mathbb{N}$ لومړنی عدد. که وي $p = 2$، نو باور لري:

$$(2-1)! = 1 \equiv -1(2), \quad (6.29)$$

نو غوښتنه ټیک ده.

وي دي $p > 2$، 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 مخي د دي a لپاره لاس ته راځي: $a^{p-1} \equiv 1(p)$.

له دي سره ټول عددونه $1 \leq a \leq p-1$ د الجبري کونګورواټ $x^{p-1} \equiv 1(p)$ حلونه دي. د 5.3.13له مخي کونګرواټ $x^{p-1} \equiv 1(p)$ خورازیات $p-1$)= د پولینوم درجه ده (بنکونګروانت حلونه، له دي سره لاس ته راځي : $\bmod p$ $1, 2, \ldots, p-1$ همدا اوس ټول انکونګروانت $\bmod p$ حلونه دي.

پسې الجبري کونګرواټ

$$(x-1)(x-2)\cdots(x-(p-1)) \equiv 0(p)$$

$\bmod p$ انکونګروانت حلونه $1, 2, \ldots, p-1$ لري. د $\mathrm{grad} = p-1$ له ا مله $1, 2, \ldots, p-1$ $\bmod p$ ټیک انکونګروانت حلونه دي) د 5.3.13 سره د

ضریب دی، نو x^{p-1} یو دی، نو د p له لاري پروېشوني نه ده(. د ضربولو وروسته سړی یو د $p-1$ درجې پولینوم 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 یا طاق دی.

له $x^{p-1} \equiv 1(p)$ څخه د دې کونګروانتونو کمون له لاري سړی یو 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 زیات له زیاته $\operatorname{grad} f \leq p-2 \bmod p$ انکونګروانت حلونه لري، که p نه د f ټول ضریبونه ووېشي (5.3.13) مګر: $1, 2, \ldots, p-1$ p-1 انکونګروانت $\bmod p$ حلونه دي . له دې سره لاس ته راځي: p د f ټول کونګروانتونه وېشي، په ځانګړي توګه $-1-c_0$، دا په دې معنا، چې

$$p \mid -1-c_0 \Rightarrow -1-c_0 \equiv 0(p) \Rightarrow c_0 \equiv -1(p), \quad (6.32)$$

$(p-1)! \equiv -1(p)$ دا په دې معنا، چې.

$(\Leftarrow)$

وي دي $n \in \mathbb{N}$ د $(n-1)! \equiv -1(n)$ سره . نيسو، چې $n \notin \mathbb{P}$. له دې سره يو لومړنی ګڼ p د $p \mid n$ سره او $2 \leq p \leq n-1$ 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 یواځنۍ څرګنده 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 څخه معلوم دی: $|\mathbb{Z}_m^*| = \varphi(m)$.

د ګروپ تیوري له مخې خورا ځانګړي ګروپونه داسې په نامه ،، څیوکلیکي،، ګروپونه دي:

پیژندنه(تعریف) 6.2.1 : یو پای ګروپ $(G, \cdot)$ څیوکلیکي دی، که

$$G = \{a, a^2, \ldots, a^{|G|} = e\} \tag{6.35}$$

د لږ تر لږه يوه $a \in G$ لپاره باور ولري. يو توکی $a \in G$ د دې خوي سره د $(G, \cdot)$ توليدېدونکی توکی بلل کيږي.

يادونه 6.2.2:

لومړی: د يوه څيوکليکي ګروپ $(G, \cdot)$ هر توکی g کيدی شي د يوه کره يا همغه کلک توکي $a \in G$ د توان په تو ګه وليکل شي: $g = a^n$ د يوه $n \in \mathbb{N}$ لپاره د $1 \leq n \leq |G|$ سره.

دويم : هر څيوکليکي ګروپ $(G, \cdot)$ د ابل ګروپ دی.

($g, h \in G \Rightarrow g = a^m, h = a^n$ د يوه توليدي توکي لپاره

$a \in G \Rightarrow g \cdot h = a^m \cdot a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m = h \cdot g$)

بيلګه 6.2.3:

لومړی: $(\mathbb{Z}_5^*, \cdot)$ څيوکليکي 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 $(\mathbb{Z}_5^*, \cdot)$ يو توليدي سيستم دی.

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

يو $(\mathbb{Z}_5^*, \cdot)$ هم د $a = \overline{3}$ ، نو

توليدي سيستم دی.

دويم : $(\mathbb{Z}_8^*, \cdot)$ څيوکليکي نه دی:

$\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ $(\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4)\overline{3}^2 = \overline{1}$

دا په دي

$\overline{5}^2 = \overline{1}, \overline{7}^2 = \overline{1}$

معنا،چې $\overline{3}$ توليدي نه دی، همداسي باور لري:

دريم: $(\mathbb{Z}_2^*, \cdot)$ او $(\mathbb{Z}_4^*, \cdot)$ څيوکليکي نه دي

$\mathbb{Z}_2^* = \{\overline{1}\} - trivial; \mathbb{Z}_4^* = \{\overline{1}, \overline{3}\}, \overline{3}$ (

-ساده دی،

$\mathbb{Z}_2^* = \{\overline{1}\} - trivial; \mathbb{Z}_4^* = \{\overline{1}, \overline{3}\}, \overline{3}$

توليدي توکی دی)

اوس نو کوم $(\mathbb{Z}_m^*, \cdot)$ څيوکليکي دی؟

پيژندنه(تعريف) 6.2.4: يو ټول ګڼ يا –عدد $g \in \mathbb{Z}$ ساده ريښه $\bmod m$ بلل کيږي، که $\overline{g} \in \mathbb{Z}_m^*$ لومړنی پاتې ټولګيګروپ $(\mathbb{Z}_m^*, \cdot)$ توليد کړي.

بيلګه 6.2.5:

لومړی: 2 يو ساده ريښه $\bmod 5$ دی(پورته بيلګه وکورئ: $\overline{2}$ توليدوي)، $(\mathbb{Z}_5^*, \cdot)$

همداسي: $g = 3$ ساده ريښه $\bmod 5$ دی.

دویم: کومه ساده ریښه $\mod 8$ شتون نه لري (همداسې: $(\mathbb{Z}_8^*, \cdot)$ خیوکلیکي نه دی).

دریم: 1 سادهریښه $\mod 2$ ، 3ساده ریښه $\mod 4$ دی.

یادونه 6.2.6: $g \in \mathbb{Z}$ ساده ریښه $\mod m$ دی، نو بیا هم هر $g' \in \overline{g}$.

د هغه مودول $m \in \mathbb{N}$ تاکنه، د کوم لپاره چې $(\mathbb{Z}_m^*, \cdot)$ خیوکلیکي دی(دا په دې معنا، چې د هغه لپاره چې ساده ریښې $\mod m$ شتون لري) [6.3]:

لیما 6.2.7: وي دي $(G, \cdot)$ یو پای ابل ګروپ او $a \in G$ نو باور لري:

$$a^k = e \quad k \in \mathbb{N} \Leftrightarrow \operatorname{ord} a \mid k. \tag{6.36}$$

له دې سره نظم $\operatorname{ord} a$ خورا کوچنی طبیعي عدد $n \in \mathbb{N}$ دی، چې د هغې لپاره $a^n = e$ بارور لري.

جمله 6.2.8 : وي دي p یو لومړنی عدد، نو $(\mathbb{Z}_p^*, \cdot)$ خیکلیکي یا تل ښېرته راګرځېدونی دی.

(داپه دې معنا، چې زات وخت ساده ریښې $\mod p$ شتون لري، خو شمېرنو ته یې تولیز متود شتون نه الري؟

لیما 6.2.9: وي دي $p > 2$ یو لومړنی عدد ، او $g \in \mathbb{Z}$ یوه ساده ریښه $\mod p$. که $g^{p-1} \not\equiv 1 (p^2)$ وي، نو g هم یوه ساده ریښه $\mod p^\alpha \ \forall \alpha \in \mathbb{N}$ ده.

جمله 6.2.10: وي دي $p > 2$ لومړنی عدد، نو $(\mathbb{Z}_{p^\alpha}^*, \cdot)\ \forall \alpha \in \mathbb{N}$ څیکلیکي دی($\mathrm{mod}\, p^\alpha\ \forall \alpha \in \mathbb{N}$) دا په دي معنا، چپیوه ساده ریښه شتون لري).

ښوونه: له ښووني : که g ساده ریښه $\mathrm{mod}\, p$ 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 ریښه $\mathrm{mod}\, p$ دی.($\Rightarrow \exists$)له دي لاس ته راځي تل یو g شتون لري لکه په 6.2.9 کي غوښتل شوي). □

بیلګه 6.2.11 : وي دي $p = 5$، د 6.2.3 له مخي $g = 2$ یوه ساده ریښه $\mathrm{mod}\, 5$ دی، د

$$g^{p-1} = 2^4 = 16 \not\equiv 1(25) \tag{6.38}$$

له امله $g = 2$ یوه ساده ریښه $\mathrm{mod}\, 5^\alpha\ \forall \alpha \in \mathbb{N}$ ده، دا په دي معنا، چې

$$\mathrm{mod}\, 25, 125, 625, \ldots$$

په همدي توګه : $g = 3$ یوه ساده ریښه $\mathrm{mod}\, 5$ 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 ریښه $\mathrm{mod}\, 5^\alpha\ \forall \alpha \in \mathbb{N}$ دی.

جمله 6.2.12: $p > 2$ دي يو لومړنی عدد وي، نو $(\mathbb{Z}_{2p^\alpha}, \cdot)$ څيوکليکي دی $\forall \alpha \in \mathbb{N}$. (دا په دي معنا، چي يوه ساده ريښه $\mathrm{mod}\, 2p^\alpha\ \forall \alpha \in \mathbb{N}$ شتون لري).

ښوونه: له ښووني څخه: g دي ناجوړه وي، $g \in \mathbb{Z}$ ، او يوه ساده ريښه $\mathrm{mod}\, p^\alpha$ ، نو g هم يوه ساده ريښه $\mathrm{mod}\, 2p^\alpha$ ده ($\forall \alpha \in \mathbb{N}$) ، که g جوړه وي، نو $g + p^\alpha$ ناجوړه دی او ساده ريښه $\mathrm{mod}\, p^\alpha$. □

بيلګه 6.2.13: وي دي $p = 5$ ، د 6.2.11 له مخي $g = 3$ يوه ساده ريښه $\mathrm{mod}\, 5^\alpha\ \forall \alpha \in \mathbb{N}$ ده او ناجوړه، نو لاس ته راځي: 3 يوه ساده ريښه $\mathrm{mod}\, 2 \cdot 5^\alpha\ \forall \alpha \in \mathbb{N}$ ده، دا په دي معنا، چي $\mathrm{mod}\, 10, 50, 250, \ldots$

د 6.2.11 له مخي $g = 2$ هم ساده ريښه $\mathrm{mod}\, 5^\alpha\ \forall \alpha \in \mathbb{N}$ ده، مګر جوړه، بيا هم $g' = g + p^\alpha = 2 + 5^\alpha$ ناجوړه او ساده ريښه $\mathrm{mod}\, 5^\alpha$ ده، نو $g' = 2 + 5\alpha$ هم ساده ريښه $\mathrm{mod}\, 25^\alpha$ ده.

ليما 6.2.14 : د $\alpha \geq 3$ لپاره $(\mathbb{Z}^*_{2^\alpha}, \cdot)$ څيکليکي نه دی. (دا په دي معنا، چي ساده ريښه $\mathrm{mod}\, 2^\alpha$ شتون نه لري د $\alpha \geq 3$ لپاره).

جمله : (ګاوس 1777-1855 ,). $(\mathbb{Z}^*_m, \cdot)$ تيک هلته څيکليکي دی، که $m \in \{2, 4, p^\alpha, 2p^\alpha\}$ د $p > 2, p \in \mathbb{P}$ سره او $\alpha \in \mathbb{N}$ په خوښه وي

(6.40)

نسبت $m = 2^\alpha, \alpha \in \mathbb{N}$ ته نو هم باور لري: $(\mathbb{Z}_{2^\alpha}^*, \cdot)$ ،، نږدي،، ,,fast`` خيکليکي دی:

جمله 6.2.16 : هر $\overline{a} \in \mathbb{Z}_{2^\alpha}^*$ ته يو يواځنی 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: کريپتولوژيAnwendung: Kryptologie

د خبررسوني لپاره تل اړيين همداسي غوښتنوړ دی، چې معلومات فقط نيوونکي B او نه بل چا ته ورسيږي. کريپتولوژي د متودونو پوهنه ده، چې د خورا کم يا مينيمال ورزيات معلومات له مخې (د له B لاري ورکړشوی) څوک د $A \to B$ څخه خبر پرانستلی نه شي، چې دا معلومات ونه لري.

بيلګه 6.3.1: (,,Caesar``) الفبې: A,B, ... ,Z, ، $n \in \mathbb{N}$ په خوښه ټاکل شوی، تعريفوو:

A = n-ter Buchstabe, م توری -n

B = (n+1)-ter Buchstabe,) توری م-(n+1)

⋮

Y = (n-2)-ter Buchstabe م توری-,)n-2(

Z = (n-1)-ter Buchstabe. توری م – ( )

له دې سره د ``n=6,, لپاره بریدټکی قلفیږي و FSLWNKK ته وازېدنه ښوونې ده، که $n=6$ معلوم وي.

دا تروسه جوت د خبرونو شفرکونه یا قلفونه متمآنِ متود داسې په نامه تلنلار انځوروي.

فکر یا ا ند

په ټولیزه توګه یو ډېر په راتلونکي وخت کې، ډېرستر، طبیعي یا پیدابښتي ګڼ(عدد) $n \in \mathbb{N}$ په لومړنۍ ګڼونو نه شي ټوټه کیدی، حتی هلته هم نه، که سړی وپوهیږي، چې فقط دوه لومړني ضریبونه یا ځله وونې رامنځ ته کیږي:

$n = p \cdot q \quad (p, q \in \mathbb{P}).$	(6.42)

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

$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$	(6.43)

وټاکي (باید د خبرونو د وازولو لپاره وشمیرل شي: د یوه کربنیز کونګروانخ $\bmod \varphi(n)$ 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 پیدابښتي یت طبیعي عدد $w \in \mathbb{N}$ لاس ته راوړي. سړی کړی شي

$w < n = p \cdot q$ لاس ته راوړي، داسي چې خبر په بلوکونو برخو يا سترو توټو د $l < n$ اوږدوالي سره توټه کړي، او دا ځانله يو پهه ګوني دول وليږي. دا قلف شوی لغات w د يوه کوچني بافي c په توګه تعريف 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 $c \in \mathbb{N}$ ورليږي. د دې لپاره چې w وټاکي، له دې امله الجبري کونګروانخ

(6.44)	$x^e \equiv c(n)$

بايد حل شي(w يو حل يا اوبی دی) .

دا چې $n \in \mathbb{N}$ ډېر لوي دی، امکان شتون لري، چې دا فقط په لومړنيو ضريبونو توټه شي، او $x^e \equiv c$ د يوګونو اعادو مودولو پسې حل شي(پېسې د چيني پاتې جمله 5.2.1 وکتل شي) . له دې سره بايد د n دواړه لومړنيضريبونه p, q وټاکل شي.(نتشفر کيدی. دا د p, q لپاره ډېر لوي دی،، ناشونی،،) نو له $n, e, c \in \mathbb{N}$ څخه خبر په ټوليزه توګه نه شي وازيدی يا اشفري کيدی.نت

د $c \in \mathbb{N}$ وازول (د $w \in \mathbb{N}$ تاکلولپاره) کيدی شي په لاندې توګه لاس ته راشي:
د $d \in \mathbb{N}$ $\mathrm{mod}\, \varphi(n)$ يواځنی لاندې کرښيز کونګروانخ زياتيز- يا مثبت حل دی

(6.45)	$ex \equiv 1(\varphi(n)),$

نو باور لري، چې $w^{ed} \equiv w(n) : w \in \mathbb{N}$ خورا کوچنی څلوری 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 $w \in \mathbb{N}$ شمیرنه ده د B لپاره ممکن د لویو $w^{ed} \equiv c^d$ نو له دې سره د $n = pq, e, c, d \in \mathbb{N}$ څخه).

بنوونه: د $\mathrm{ggT}(e, \varphi(n)) = 1$ له امله کرښیز کونګروانیځ $ex \equiv 1(\varphi(n))$ د $\mathrm{mod}\, \varphi(n)$ ناګونګروانیځ حل لري: d .

5.1.1 له مخې نیک یو

وښایی:

(6.46)	$w^{ed} \equiv w(n).$

د $\mathrm{ggT}(p, q) = 1$ 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 $\mathrm{kgV}(p, q) = pq$)

$p \mid w$ دی، نو هم $p \mid w^{ed}$ ،، یعني $p \mid w^{ed} - w$ ، داسې چې $w^{ed} \equiv w(p)$

باور لري. $p \nmid w$ دی : دا چې $ed \equiv 1(\varphi(n))$ (d حل دی) بار لري

$ed = 1 + k \cdot \varphi(n)$	(6.48)

د يوه $k \in \mathbb{N}$ لپاره($e, d, 1, \varphi(n)$ زياتيز يا مثبت دي). دا چې $\mathrm{ggT}(w, p) = 1$ ،
د ،، کوچني فرمات،، 6.1.19له مخې باور لري.

$w^{p-1} \equiv 1(p).$ $w^{\varphi(n)}\ 1(p),$ 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. □

يادونه: 6.3.2 : B کړی شي د لاس ته راوړي خبر څخه c د او $d \in \mathbb{N}$ $n = pq$
له لارې پټه خبر w وشميري

بيلګه 6.3.3 (ګڼونه په ربښتيا ډېر واړه دي!)

B غوره ټاکي، يعني $p = 3, q = 23$ $n = 23 \cdot 3 = 69, \varphi(n) = 2 \cdot 22 = 44$
او ټاکي $e > 1 \in \mathbb{N}, e = 3$ (و 44 ته نسبي لومړنی).

B معلومات ورکوي : $n = 69, e = 3$ او له A څخه شفري خبر يا کود يا پټ خبر
$c = 12$ تر لاسه کوي.

حلونه یا اوبیونه یې: $ex \equiv 1(\varphi(n))$ ، دا په دې معنا، چې $3x \equiv 1(44)$ ،

$\mod 44$ 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 ــادیکي ودیزیینه

g-adische Entwicklung reeller Zahlen

تولزه 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

(د $a \in \mathbb{N}$ g -ادیکي وده).

د صفر سره نابرابرو حقیقي عددونو ته ټولیزونه:

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 : $\alpha > 0$ دي یو حقیقي 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، داسي چې دي

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i}. \tag{7.3}$$

که α ریښتونی یا راشنل نه وي، نو دا انځورونه یواځنئ ده (داسي په نامه g -ادیکي انځورونه).

ښوونه : د یوه داسي انځوروني یواځنوالی:

که $\alpha \in \mathbb{R}^+$ ناراشنل وي، نو $\lceil \alpha \rceil$ د α پسي خوراکوچنی عدد په ګوته کوي.

د ټولیزې ښووني روښانهونه یا تشریح:

$\pi = 3,1415\ldots$ ، تعریف کړئ $a_0 = \lceil \pi \rceil = 3$ ، $\alpha_1 = \pi - \lceil \pi \rceil$ جوړ کړئ او $a_1 = \lceil 10a_1 \rceil = \lceil 1,415\ldots \rceil = 1$ تعریف کړئ،

$\alpha_2 = 10\alpha_1 - [10\alpha_1] = 0,415\ldots$ جوړ کوئ او تعریف کړئ ... ،

$a_2 = [10\alpha_2] = 4$

تولیز : دي $\alpha \in \mathbb{R}^+, g \in \mathbb{N}, g \geq 2$ په خوښه وي. اندوکتیو جوړکړئ:

$$a_1 = \alpha - [\alpha], \ldots, \alpha_{i+1} = g\alpha_i - [g\alpha_i], \tag{7.4}$$

او له دي 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

$$\begin{aligned} \alpha_1 = \alpha - [\alpha] = \alpha - a_0 &\Rightarrow \alpha = a_0 + \alpha_1 \\ \alpha_2 = g\alpha_1 - [g\alpha_1] &\Rightarrow \alpha_2 = g\alpha_1 - a_1 \Rightarrow \alpha_1 = \alpha_2 g^{-1} + \end{aligned}$$

$$\Rightarrow \alpha = a_0 + a_1 g^{-1} + \alpha_2 g^{-1}. \tag{7.8}$$

و بنایی:

$$\alpha = a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + \alpha_{n+1} g^{-n} \ \forall n \in \mathbb{N}$$

.

$$n = 1 :$$

$$\alpha = a_0 + a_1 g^{-1} + \alpha_2 g^{-1}$$

پورته لور ته واز دی

$$n \to n + 1 :$$

$$\alpha_{n+2} = g\alpha_{n+1} - [g\alpha_{n+1}] = g\alpha_{n+1} - a_{n+1} \Rightarrow \alpha_{n+1} = a_{n+1} g^{-1} + \alpha_{n+2} g^{-1}$$

$$\Rightarrow \alpha = a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + \alpha_{n+1} g^{-n} = \quad (7.9)$$

$$= a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + \left(a_{n+1} g^{-1} + \alpha_{n+2} g^{-1}\right) g^{-n} = \quad (7.10)$$

$$= a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + a_{n+1} g^{-(n+1)} + \alpha_{n+2} g^{-(n+1)} \quad (7.11)$$

$$\Rightarrow$$

چې د $n+1$ لپاره هم ټیک دی.

ناپای لړئ تخیرني لاندې نیسو: $\sum_{i=0}^{\infty} a_i g^{-i}$ د همدا اوس تعریف تعریف شوو a_i سره.

وښایی: دا لړئ د : α په لور ځي یا : α ته کونورکنت کیږي.

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i}. \tag{7.12}$$

n - مه توټه – يا پارشل جمعه(زياتون)

$$s_n = \sum_{i=0}^{n} a_i g^{-i} = a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} \tag{7.13}$$

$$s_n = \alpha - \alpha_{n+1} g^{-n} \ \forall n \in \mathbb{N}$$

پوره کوي

د $0 \leq \alpha_{n+1} < 1$ او د $g^{-n} > 0 \ (g > 0)$ له امله باور لري

$$0 \leq a_{n+1} g^{-n} < g^{-n} \ \forall n \in \mathbb{N}; \tag{7.14}$$

له دي سره لرو: $\lim_{n\to\infty} (\alpha_{n+1} g^{-n}) = 0$ دا په دي معنا، چې

$\lim_{n\to\infty} (\alpha - s_n) = 0 \Rightarrow \lim_{n\to\infty} s_n = \alpha$ ، دا په دي معنا، چې $\sum_{i=0}^{\infty} a_i g^{-i}$ مطلق د

α په لور هڅيږي.

يواځنوالی(يواځيوالی):

شتون لري د $\alpha \notin \mathbb{Q}$ نيسوچې،

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = \sum_{i=0}^{\infty} b_i g^{-i}, \tag{7.15}$$

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.

یعني

(7.16)

$$a_0 = b_0, a_1 = b_1, \ldots, a_{i_0-1} = b_{i_0-1},$$

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 املې کیدی شي سره راتول شي)

$$0 = \sum_{i=i_0}^{\infty} (a_i - b_i) g^{-i} = \quad (7.17)$$

$$= \underbrace{(a_{i_0} - b_{i_0})}_{\geq 1} g^{-i_0} + \sum_{i=i_0+1}^{\infty} \underbrace{(a_i - b_i)}_{\leq 1} g^{-i} \geq g^{-i_0} + \sum_{i=i_0+1}^{\infty} (-g + \quad (7.18)$$

$$= g^{-i_0} + (-g+1) \sum_{i=i_0+1}^{\infty} g^{-i} = g^{-i_0} + (-g+1) g^{-i_0+1} \underbrace{\sum_{i=0}^{\infty} g^{-}}_{= \frac{g}{-1+g}} \quad (7.19)$$

$$= g^{-i_0} - (g-1) g^{-i_0-1} \frac{g}{g-1} = g^{-i_0} - g^{-i_0} = 0. \quad 7.20)$$

له دې سره باید په دې تخمین کې هرچیرته برابروالی باور ولري، نو له دې لاس ته راځي:

$$a_{i_0} - b_{i_0} = 1 \wedge a_i - b_i = -(g-1)\ \forall i > i_0, \tag{7.21}$$

دا په دي معنا، چې

$$b_{i_0} = a_{i_0} - 1 \wedge b_i - a_i = g - 1\ \forall i > i_0. \tag{7.22}$$

$a_i = 0$ او $b_i = g - 1\ \forall i > i_0$ باور لري:

نيسو چې $0 < a_i$ ، نو د $b_i \leq g - 1$ سره لاس ته راځي، چې $b_i - a_i < g - 1$ -تضاد!

له دي سره ټول زيتوني يا د جمعي اجزاوي د α په انځورونه کي د $i > i_0$ سره صفر دي، دا په دي معنا،چې

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = a_0 + a_1 g^{-1} + \cdots + a_{i_0} g^{-i_0} = a_0 + \frac{a_1}{g} + \cdots + \tag{7.23}$$

تضاد دی! نو: α فقط يوه g -اديکي وده لري.□

يادونه 7.1.2 : دی $g = 10$ (لسميز سيستم)، نو سړی د $\alpha = \sum_{i=0}^{\infty} a_i g^{-i}$ لپاره ليکي هم

$$a_0, a_1 a_2 \ldots \quad 0 \leq a_i < 10\ \forall i \geq 1. \tag{7.24}$$

کورولار 7.1.3 : $\alpha > 0$ يو راشنل عدد دی، نو α خورا زيات دوه g -اديکي انځورونې ، داسې په نامه

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = \sum_{i=0}^{\infty} b_i g^{-i}, \tag{7.25}$$

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 $\mathbf{g}$ –اديکي انځورونه لري؟

پيژند(تعريف) 7.1.4: سړی وايي، $\alpha \in \mathbb{Q}, \alpha = \frac{a}{b}$ يو پای انځورونه لري، که وي

$$\alpha = \frac{a}{b} = \sum_{i=0}^{\infty} a_i g^{-i}, \tag{7.26}$$

$a_i = 0 \ \forall i > i_0 \ \left(\frac{a}{b} = a_0 + a_1 g^{-1} + \cdots + a_{i_0} g^{-i_0}\right)$ د کږم سره چې

کورولار 7.1.5: $\frac{a}{b} \in \mathbb{Q}^+$ ټيک دوه مختلف g - اديکي ودې لري، که $\frac{a}{b}$ يو يواځنئ انځورونه ولري.

ښوونه :

$(\Rightarrow)$

$\alpha = \frac{a}{b}$ دوه انځورونې لري، نو له دوي څخه يو د 7.1.3 له مخې پاي دی.

$(\Leftarrow)$

$$\alpha = \sum_{i=0}^{i_0} a_i g^{-i}$$

وي دي 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 دي سره يوه 2 -مه g -اديکي انځورونه لري.□

کوم $\alpha \in \mathbb{Q}^+$ یوه پای g –ادیکي 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 ټیک هلته یوو پای(او له دې سره 2مختلف) g -ادیکي وده لري، که هر د مخرج لومړنئ پروېشوني بنسټ وېشي.

ښوونه:

$(\Rightarrow)$

وي دي

$$\frac{a}{b} = \sum_{i=0}^{n} a_i g^{-i} = a_0 + a_1 g^{-1} + \cdots + a_n g^{-n}, \qquad (7.32)$$

نو باور لري

$$\frac{a g^n}{b} = a_0 g^n + a_1 g^{n-1} + \cdots + a_n \in \mathbb{Z}, \qquad (7.33)$$

له دې سره $b \mid a g^n$. وي دي p په خوښه د b لومړنی پروېشونی، نو $p \mid a g^n$ 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 $p \mid g$

$(\Leftarrow)$

وي دي

$$b = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \tag{7.34}$$

د ماتلاندي يا مخرج په لومړني ضريبونو ټوټه 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 دي $m := \max\{\alpha_1, \ldots, \alpha_n\}$. نو باور لري

$$p^{\alpha_i} \mid g^m \ (i = 1, \ldots, k), \tag{7.35}$$

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

$$\mathrm{kgV}(p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = b; \tag{7.36}$$

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 دي

$$\frac{a}{b} g^m = a_0 + a_1 g + \cdots + a_n g^n \tag{7.37}$$

g -ادیکي وده، د کوم سره چې $0 \leq a_i < g \ \forall i \geq 1$.

له دې لاس ته راځي:

$$\frac{a}{b} = \frac{a_0}{g^m} + \frac{a_1}{g^{m-1}} + \cdots + \frac{a_n}{g^{m-n}} = a_0 g^{-m} + a_1 g^{-m+1} + \cdots + a_n g^{n-m}, \quad (7.38)$$

دا په دې معنا، چې $\frac{a}{b}$ يوه پای g –اديکي وده لري. □

لاس ته راوړنه 7.1.7 : وي دې

$$g = 10, \alpha = \tfrac{a}{b} \in \mathbb{Q}, \mathrm{ggT}(a,b) = 1, b > 0$$

دا چې لومړنئ 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 $\alpha, \beta \in \mathbb{N}_0$ لپاره مخرج(ماتلاندې) $b = 2^\alpha 5^\beta$ وي، د دې لپاره چې شرايط پوره شي.
له دې سره په لسميز کې باور لري:

$$\alpha = \tfrac{a}{b}, \mathrm{ggT}(a,b) = 1$$

که يو پای(او له دې سره دوه مختلف) انځورونه ولری ⇔

$$\Leftrightarrow b = 2^\alpha 5^\beta, \alpha, \beta \in \mathbb{N}_0$$

.

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.

بيلکه :

لومړی: $\alpha = \frac{287}{100} \in \mathbb{Q}^+$ ، د $b = 2^2 5^2$ له املـه α يوه پای او له دې سره دوه لسميز انځورونه لري:

$$\alpha = 2.870000\ldots = 2.869999\ldots$$

دویم: $\alpha = \frac{5}{3} \in \mathbb{Q}^+$ ، 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 بنوونې سره سم (α_i, a_i) :

$$\alpha = 1.6666\ldots$$

دریم: $\alpha = 1 \in \mathbb{Q}^+$ د $\alpha = \frac{1}{1}$ او $\mathrm{ggT}(1,1) = 1$ 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 $\mathrm{ggT}(a,b) \neq 1\ldots$):

$$\alpha = 1.0000\cdots = 0.9999\ldots$$

$$0.999\ldots = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \cdots = 9\left[\underbrace{\sum_{i=0}^{\infty}\left(\frac{1}{10}\right)^i}_{\to \frac{1}{1-\frac{1}{10}} = \frac{10}{9}} - 1\right] = \tag{7.39}$$

$$= 9\left[\frac{10}{9} - 1\right] = 10 - 9 = 1. \tag{7.40}$$

پریودیکي وده

د یوه حقیقی عدد په لسمیزه وده کې کله کله ځنې عددونه منظم منځ ته راځي، لکه $\alpha = 1.707142857142857\ldots$ ،

پوښتنه: کوم حقیقی اعداد دا خویونه لري:؟

پیژند(تعریف) 7.2.1: د یوه حقیقی عدد $\alpha > 0$ یوه g -ادیکي یا g –ایزه 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 بیرته راګرځیدونې یا پریودیکي بلل کیږي، 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 مینیمال یا خورا کوچنی ټاکلی وي، نو $a_1 a_2 \ldots a_{n-1}$ ترمخ پریود یا - راګرځیدنه بلل کیږي او $n-1$ د هغه اوږدوالی، که $n = 1$ وي(داپه دې معنا، چې ترمخ پریود)، نو وده سوچه پریودیک بلل کیږي.

که e خورا کوچنی ټاکلی وي، نو $a_n a_{n+1} \ldots a_{n+e-1}$ تلبیرته راګرځیدونې بلل کیږي او e د هغه اوږدوالی.

د $g = 10$: لپاره سومبول یا نخښ:

$$\alpha = a_0 . \underbrace{a_1 a_2 \ldots a_{n-1}}_{Vorperiode} \underbrace{a_n a_{n+1} \ldots a_{n+e-1}}_{Periode} \underbrace{a_{n+e}}_{=a_n} \cdots \underbrace{a_{n+2e-1}}_{=a_{n+e-1}} \cdots \qquad (7.43)$$

بیلګه 7.2.2 :

د المانې پښتو: اوږدوال =Länge ;

تل بیرته راګرځیدنه ، له مخه ت ل بیرته را ګرځیدنه = periode ; Vor peride

$$\alpha = 1.\underbrace{70}_{Vorperiode}\underbrace{\underbrace{714285}_{Periode}}_{Länge\ 2}\ \underbrace{\quad}_{Länge\ 6714285\ldots}$$

1.

2. $\alpha = 2.87000\cdots = 2.86999\ldots$.

له مخ پريود87 نسبت 86 ته، اوږدوالی2 ، پريود 0 ، نسبت 9 ته،، اوږدوالی 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) ټيک هلته يو پريوديکي g -ايزه وده لري، که α راشنل وي.

ښوونه:

$(\Leftarrow)$

وي وي $\alpha = \frac{a}{b}, \mathrm{ggT}(a,b) = 1, b > 0$ او $g \geq 2$. لکه د 7.1.1 په ښوونه کې وي دې

$$\alpha_1 = \alpha - [\alpha],$$

$$a_0 = [\alpha],$$

$$\vdots$$

$$\alpha_{i+1} = g\alpha_1 - [g\alpha_i],$$

$$a_i = [g\alpha_i].$$

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)

$= g^i b_1.$	(7.45)

د $0 \leq \alpha_i < 1$ له امله باور لري

$$0 \leq b\alpha_i = b_i < b \ (b > 0) \ \forall i \in \mathbb{N}; \tag{7.46}$$

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 $\exists n, e \in \mathbb{N}$ د $b_n = b_{n+e}$ سره. پورته لور ته $(i = n)$ باور لري:

$$g^{n-1}b_1 \equiv b_n = b_{n+e} \equiv b_1 g^{n+e-1}(b), \tag{7.47}$$

د g^i سره د ضرب له لارې ($i \in \mathbb{N}$ په خوښه) لاس ته راځي:

$$g^{n-1+i}b_1 \equiv g^{n-1+e+i}b_1(b), \tag{7.48}$$

دا په دې معنا، چې دپورته لور ته : $b_{n+i} \equiv b_{n+e+i}$ ، يعنې $b \mid b_{n+e+i} - b_{n+i}$.

د $0 \leq b_{n+i} < b$ او $0 \leq b_{n+e+i} < b$ له امله کمښت $< b$ دی، له دې سره لاس ته راځي

$$b_{n+e+i} = b_{n+i} \ \forall i \in \mathbb{N}; \tag{7.49}$$

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 دي شره:

$$b\alpha_{n+e+i} = b\alpha_{n+i} \ (b \neq 0) \tag{7.50}$$

او

$$g\alpha_{n+e+i} = g\alpha_{n+i} \ \forall i \in \mathbb{N}_0, \qquad [g\alpha_{n+e+i}] = [g\alpha_{n+i}] \ \forall i \in \mathbb{N}_0, \tag{7.51}$$

نو $a_{n+e+i} = a_{n+i} \ \forall i \in \mathbb{N}_0$.

له دي سره د $\alpha = \frac{a}{b}$ g -ايزه وده تل بيرته راګرځيدوني ده.

$(\Rightarrow)$

وي دي $\alpha > 0$ حقيقي د پريوديکي ودي سره، داپه دي معنا، چې $n, e \in \mathbb{N}$ شتون لري د

$$a_{n+e+k} = a_{n+k} \ \forall k \in \mathbb{N}_0$$

سره؟

$$a_{n+e+k} = a_{n+k} \ \forall k \in \mathbb{N}_0$$

;

بنسول کيږي: $\alpha \in \mathbb{Q}$:

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = a_0 + a_1 g^{-1} + \cdots + a_n g^{-n} + a_{n+1} g^{-(n+1)} + \cdots + \quad (7.52)$$

$$+ a_{n+e-1} g^{-(n+e-1)} + \underbrace{a_{n+e}}_{=a_n} g^{-(n+e)} + \underbrace{a_{n+e+1}}_{=a_{n+1}} g^{-(n+e+1)} + \cdots + \quad (7.53)$$

$$+ \underbrace{a_{n+2e-1}}_{=a_{n+e-1}} g^{-(n+2e-1)} + \cdots = \quad (7.54)$$

$$= \sum_{i=0}^{\infty} a_i g^{-i} + a_n g^{-n} \underbrace{\left(1 + g^{-e} + g^{-2e} + \cdots\right)}_{\sum_{k=0}^{\infty} (g^{-e})^k \to \frac{1}{1-\frac{1}{g^e}} = \frac{g^e}{g^e-1}} + \cdots + \quad (7.55)$$

$$a_{n+e-1} g^{-(n+e-1)} \underbrace{\left(1 + g^{-e} + g^{-2e} + \cdots\right)}_{\sum_{k=0}^{\infty} (g^{-e})^k \to \frac{1}{1-\frac{1}{g^e}} = \frac{g^e}{g^e-1}} = \quad (7.56)$$

$$= \sum_{i=0}^{\infty} a_i g^{-i} + \frac{g^e}{g^e - 1} \left(a_n g^{-n} + \cdots + a_{n+e-1} g^{-(n+e-1)}\right) \in \mathbb{Q}. \quad (7.57)$$

بيلګه 7.2.4: $g = 10, \alpha = 0.1342\overline{158}$ ، داچې دا يوه پريوديکي لسميزه وده ده، لاس ته راځي: α يو راشنل عدد دی، کوم؟

$n = 4, e = 4$ ، د ترمخپريود اوږدوالی: $\Rightarrow n - 1 = 3$ د 7.2.3 د ښوونې له مخې:

$$\alpha = \frac{134}{1000} + \frac{10^4}{10^4-1}(2\cdot\frac{1}{10^4} + \frac{1}{10^5} + 5\cdot\frac{1}{10^6} + 8\cdot\frac{1}{10^7}) = \cdots = \quad (7.5$$

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 د $\alpha \in \mathbb{Q}^+$

$$\alpha = a_0.\overline{a_1 a_2 \dots a_e} \qquad (7.59)$$

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).

ثبوونه:

$(\Rightarrow)$

وي دې $\frac{a}{b} \in \mathbb{Q}^+, \mathrm{ggT}(a,b) = 1, b > 0$ د سوچه-پریودیکي g –ایزه وي 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.

د 7.2.3 بنوونې 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.

$\mathrm{ggT}(b,b_1)=1$

وښایئ:

نیسو چې $\exists p \in \mathbb{P}$ د لاندې سره

$$p \mid b, p \mid b_1 \overset{7.1.1}{\equiv} b\alpha_1 = b\left(\frac{a}{b} - \left[\frac{a}{b}\right]\right) = a - b\underbrace{\left[\frac{a}{b}\right]}_{\in\mathbb{N}},$$

له دې سره $p \mid a$ لاس ته راځي – تضاد او $\mathrm{ggT}(a,p)=1$ 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: $\mathrm{ggT}(b,g)=1$. 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.

وي دي $\frac{a}{b}$ سوچه پريوديکي، نو وښايئ $e = \operatorname{ord} \bar{g}$ په $(\mathbb{Z}_b^*, \cdot)$ کي.

پورته لور ته باور لري:

$$g^e \equiv 1(b) \wedge \mathrm{ggT}(b, g) = 1; \tag{7.63}$$

دا په دي معنا، چې $\bar{g} \in \mathbb{Z}_b^*$ او $\bar{g}^e = \bar{1}$ په $(\mathbb{Z}_b^*, \cdot)$ کي دي. يعني ($\operatorname{ord} \bar{g} \leq e$ د پيژند له مخي $\operatorname{ord} \bar{g}$ خورا کوچنی طبيعي عدد k دی د $\bar{g}^k = \bar{1}$ سره).

وي دي $\operatorname{ord} \bar{g} = k$ ، نو په $(\mathbb{Z}_b^*, \cdot)$ کي باور لري $\bar{g}^k = \bar{1}$ ، دا په دي معنا، چې $g^k \equiv 1(b)$ او $g^{k+i} \equiv g^i(b)\ \forall i \geq 0$ ، له دي 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 مخي $\forall i \geq 0$.

له دي ښوونې لاس ته راځي:

$$b_{k+i+1} \equiv b_{k+i}(b), \tag{7.64}$$

نو $b_{k+i+1} = b_{k+i}$ ، او

$$a_{1+k+i} = a_{1+i}\ \forall i \geq 0. \tag{7.65}$$

دا چې 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 دي امله په $(\mathbb{Z}_b^*, \cdot)$ کي باور لري $e = k = \operatorname{ord} \bar{g}$

$(\Leftarrow)$

وي دي $\gcd(b, g) = 1$ ، 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 مخي یو پریودیکي اونځورونه شتون لري، یعني د لاندي سره:

$$g^{n-1} b_1 \equiv g^{n+e-1}(b). \tag{7.66}$$

داچې $\gcd(b, g) = 1$ ، نو $\gcd(b, g^{n-1}) = 1$ هم شتون لري، یعني دپورته کونګروانځ ځخه 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 جملي7.2.3 د ښوونې له مخي لرو:

$b_{i+1} \equiv b_{e+i+1}(b)$ ، له دي 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 دي معنا،چې د $\frac{a}{b}$ g –ایز یا g –ایدیکي انخورونه 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 $\gcd(a, b) = 1, b > 0$ سره، سوچه پریودیکي ده، او هم د پریود اوږدوالی د ماتلاندي یا مخرج b په واک کي دی!

بیلګه 7.2.7:

1. $g = 10, \alpha = \frac{3}{7} \in \mathbb{Q}^+$.

دا چې $\gcd(3, 7) = 1$ د 7.2.5له مخي باور لري: $\frac{a}{b} = \frac{3}{7}$ سوچه پریودیکي لسمیزه

وده لري($\mathrm{ggT}(7,10)=1$)، د کوم سره چې د بریود اوږدوالی $e=\mathrm{ord}\,\overline{10}$ په $(\mathbb{Z}_7^*,\cdot)$ کې دی:

$$10^1 \not\equiv 1(7), 10^2 \not\equiv 1(7), \ldots, 10^6 \equiv 1(7)$$

(د لومړي ځل لپاره)....

$\Rightarrow \mathrm{ord}\,\overline{10}=6$, نو also $e=6$.

$\left(\frac{3}{7}=0.\overline{428571}\right)$

2. $g=10, \alpha=\frac{15}{7}\in\mathbb{Q}^+$.

$\mathrm{ggT}(15,7)=1$

سوچه پریودیکي د $e=\mathrm{ord}\,\overline{10}=6$ سره.

$\left(\frac{15}{7}=2.\overline{142857}\right)$

تولیز حالت: نه سوچه – پریودیکي وده

جمله 7.2.8 : وي دي $\frac{a}{b}\in\mathbb{Q}^+, \mathrm{ggT}(a,b)=1, b>0$. دی

$$g=p_1^{\alpha_1}\cdots p_k^{\alpha_k} \tag{7.67}$$

د بنسټ $g\geq 2$ په لومړنیو ضریبونو توټه کونه او

(7.68)	$b=p_1^{\beta_1}\cdots p_k^{\beta_k}\cdot t$

(د همغه p_i سره!) د $\mathrm{ggT}(g,t)=1$ سره، نو د ترمخ پریود اوږدوالی($n-1$
) په g -ایز دوه کې خورا کوچنی طبیعي عدد γ دی، د کوم لپاره چې $\frac{b}{t} \mid g^{\gamma}$ دی، او
د $\bar{g}$ پریود اوږدوالی د پریود د نظم سره پرابر دی په $(\mathbb{Z}_t^*,\cdot)$ کې.

بیلګه 7.2.9: $g=10, \frac{a}{b}=\frac{239}{140} \in \mathbb{Q}^+$ ، لسمیزه وده سوچه پریودیک نه ده، ځکه
چې $\mathrm{ggT}(b,g)=\mathrm{ggT}(140,10) \neq 1$.

د پریود اوږدوالی:

$$\left.\begin{array}{rcl} g=10 & = & 2\cdot 5 \\ b=140 & = & 2^2\cdot 5\cdot 7 \end{array}\right\} \Rightarrow t=7, \frac{b}{t}=\frac{140}{7}=20$$

$$20 \nmid 10^1, 20 \mid 10^2=100 \Rightarrow \gamma=2.$$

د پریود اوږدوالی:

$e=\mathrm{ord}\,\bar{g}$ په $(\mathbb{Z}_t^*,\cdot)$ 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-م توان n-te Potenzreste

په ځانګړي حالت بیرته اړول

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 $x^2 \equiv a(m)$ سره تیک هلته حلوړ ده، که $m = p_1^{\alpha_1}\cdots p_l^{\alpha_k}$

$$x^2 \equiv a(p_i^{\alpha_i}) \quad i = 1,2,\ldots,k \tag{8.3}$$

حلوړ وي(برخه 5 وګورئ)

لیما 8.1.3: د $x^n \equiv a(p^\alpha), p \in \mathbb{P}, \alpha \in \mathbb{N}$ لپاره د $a = p^k a'$ $\mathrm{ggT}(p,a')=1$ سره تیک هلته حلوړ ده، که $n \mid k$ او $x^n \equiv a'(p^{\alpha-k})$ حلوړ وي $(0 \le a < p^\alpha)$.

ثبوونه:

$(\Rightarrow)$

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

$$x_0^n \equiv a(p^\alpha), \tag{8.4}$$

دا په دي معنا، چې $x_0^n = a + rp\alpha$ دی د يوه $r \in \mathbb{Z}$ لپاره.

وي دي $x_0 = p^\beta s$ د $\mathrm{ggT}(p,s) = 1 \ (\beta \in \mathbb{N}_0)$ سره، نو باور لري:

$$x_0^n = (p^\beta s)^n = p^{n\beta} s^n = a + rp^\alpha = p^k a' + rp^\alpha. \tag{8.5}$$

د $a = p^k a' < p^\alpha$ له امله باور لري: $k < \alpha \ (a' > 0)$ ، يعني $p^k \mid p^\alpha$ ، له دي سره دپورته لور ته:

$$p^{n\beta-k} s^n = a' + rp^{\alpha-k}; \tag{8.6}$$

له دي 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، يعني د 2.2.11 سره لاس ته راځي: $p^k \mid p^{n\beta}$ ، يعني $k \leq n\beta$.

که $k < n\beta$ وی، نو $n\beta - l > 0$ به وی او د

$$p^{n\beta-k} s^n = a' + rp^{\alpha-k} \tag{8.7}$$

له مخي به مو لرودی: $p \mid a'$ او $\mathrm{ggT}(p,a') \neq 1$ چې تضاد دی.

له دي سره: $k = n\beta$ او $n \mid k$ ، پسي لاس ته راځي:

$$s^n = a' + rp^{\alpha-k}, \tag{8.8}$$

دا په دي معنا، چې $s^n \equiv a'(p^{\alpha-k})$ او $s \in \mathbb{Z}$ د $x^n \equiv a'(p^{\alpha-k})$ يو حل دی.

$(\Leftarrow)$

وي دي $x_0 \in \mathbb{Z}$ د $x^n \equiv a'(p^{\alpha-k})$ حل د $n \mid k$ او د $\gcd(a', p) = 1$ سره، نو باور لري $x_0^n \equiv a'(p^{\alpha-k})$ ، يعني $x_0^n p^k \equiv a' p^k (p^\alpha)$ هم. د $n \mid k$ له املە باور لري $k = nt$

د يوه $t \in \mathbb{N}$ لپاره.

$$x_0^n p^{nt} \equiv a(p^\alpha) \Rightarrow (x_0 p^t)^n \equiv a(p^\alpha), \tag{8.9}$$

له دي 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 دي سره د $x^n \equiv a'(p^{\alpha-k})$ له حل x_0 څخه د $\gcd(a', p) = 1$ سره د $x^n \equiv a(p^\alpha)$ هر حل x_1 شميرل کيدی شي:

$$x_1 = x_0 p^t, \tag{8.10}$$

د کوم سره چې $k = nt$ باور لري.

لاس ته راوړنه 8.1.5: د مسآلي $x^n \equiv a(p^\alpha)$ سره سړی کړی شي ځان په حالت $\gcd(a, p) = 1$ محدود کړي $(\Rightarrow \gcd(a, p^\alpha) = 1)$ ، دا په دي 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 $\gcd(a, p) = 1$ سره، نو $\gcd(x_0, p) = 1$ هم باور لري (دا په دي معنا، چې $\overline{x_0}^n = \overline{a} \in \mathbb{Z}^*_m \Rightarrow \overline{x_0} \in \mathbb{Z}^*_m$).

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 مور سرچینه ییز 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 $x^n \equiv a(m)$ حلور 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: $m = 6, a = 0, 1, 3, 4$ دویمتوانپاتي $\mathrm{mod}\, 6$ دی، $a = 2, 5$ د دویم توانپاتي $\mathrm{mod}\, 6$ نه دی(پورته وګورئ).

پسې: هر $a \in \mathbb{Z}$ دریم توانپاتي $\mathrm{mod}\, 6$ 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 ریښه $\mathrm{mod}\, p^\alpha$ 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 $\mathrm{mod}\, p^\alpha$ 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)

پيژند 8.1.9 : $m \in \mathbb{N}$ دي داسي وي، چې $(\mathbb{Z}_m^*, \cdot)$ څيوکليکي يا تل بيرته راګرځيدونی دی، دا په دي معنا،چې ساده ريښه $g \bmod m$ شتون($\exists$) لري، دا په دي 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 ايندکس 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 ايندکس 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 دي املې څيوکليکي دی، يعني يوه ساده ريښه $\bmod 14$ ستون لري.

$g = 3$ يوه ساده ريښه $\bmod 7$ ده، ځکه 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 دي معنا، چې$\overline{3}$ توليدوي، $\mathbb{Z}_7^*$

دا چې g ناجوړه یا طاق دی، د 6.2.12 د ښوونې له مخې تر لاس ته راځي: $g=3$ هم سادهریښه $\bmod 14$ 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 ایندکس جدول راکوي:

$\overline{a}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{9}$	$\overline{11}$	$\overline{13}$
$I_g(a)$	0	1	5	2	4	3

(8.16)

لیما 8.1.12: وي دې g ساده ریښه $\bmod m$ ، نو باور لري:

$$g^{i}\equiv g^{j}(m)\Leftrightarrow i\equiv j(\varphi(m))$$

لومړی:

دویم : $a,b\in\mathbb{Z},\text{ggT}(a,m)=\text{ggT}(b,m)=1$ 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)

وي دي $g^i \equiv g^j(m)$ د $i > j$ لپاره، نو په $(\mathbb{Z}_m^*, \cdot)$ کي $\overline{g}^i = \overline{g}^j$ باور لري، يعني د $\overline{g}^{-j} \in \mathbb{Z}_m^*$ سره د ضرب له مخي لرو:

$$\overline{g}^{i-j} = \overline{1}. \tag{8.18}$$

دا چي $\overline{g}$ د $(\mathbb{Z}_m^*, \cdot)$ ګروپ توليدوي، $\operatorname{ord} \overline{g} = \varphi(m)$ دی. د 6.2.7 له مخي لاس ته راځي

$$\varphi(m) \mid i - j, \tag{8.19}$$

داپه دي معنا، چي $i \equiv j(\varphi(m))$.

$(\Leftarrow)$

برعکس دي $i \equiv j(\varphi(m))$ 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 دي معنا، چي $\overline{g^i} = \overline{g^j}$ او له دي سره $g^i \equiv g^j(m)$.

لومړی: د $\gcd(a,m)=\gcd(b,m)=1$ له امله باور لري: $\overline{a},\overline{b}\in\mathbb{Z}_m^*$ يعني $\overline{ab}\in\mathbb{Z}_m^*$ ، يعني $I_g(ab)$ او باور لري

$$\overline{g}^{I_g(ab)}=\overline{ab}=\overline{a}\,\overline{b}=\overline{g}^{I_g(a)+I_g(b)}, \tag{8.22}$$

$\overline{g^{I_g(ab)}}=\overline{g^{I_g(a)+I_g(b)}}$ دويم يعني ، له دې سره

$$g^{I_g(ab)}\equiv g^{I_g(a)+I_g(b)}(m)\overset{1.}{\Rightarrow} I_g(ab)\equiv I_g(a)+I_g(b)(\varphi(m)). \tag{8.23}$$

تري لاس ته راوړنه 8.1.13: وي دي $a_1,a_2,\ldots,a_k\in\mathbb{Z}$ د $\gcd(a_i,m)=1\ (i=1,\ldots,k)$ سره او g دې يوه ساده ريښه $\bmod m$ وي، نو د ايندکشن سره لاس ته راځي:

$$I_g(a_1\cdots a_k)\equiv I_g(a_1)+\cdots+I_g(a_k)(\varphi(m)). \tag{8.24}$$

په ځانګړې توګه دې وي $a_i=a(i=1,\ldots,k)$ ، نو لاس ته راځي

$$I_g(a^k)\equiv kI_g(a)(\varphi(m)). \tag{8.25}$$

دا خويونه د هغه ورسره بلد لوګاريتم سره ورته دی، چې په انالیز کې څېړل شوي.

له دې امله I_g د اعدادو تيوريکي لوګاريتم بلل کيږي.

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:

$\alpha)$ وركړل شوي: $ax \equiv b(m)$ د $\mathrm{ggT}(a,m) = \mathrm{ggT}(b,m) = 1$ سره او g

ساده ریښه $\mathbb{Z}_m^*$ ده. په $\mathrm{mod}\, n$ کې حل کوو $\overline{ax} = \overline{b}$ ، یعني:

$$\overline{g}^{I_g(ax)} = \overline{g}^{I_g(b)} \Leftrightarrow g^{I_g(ax)} \equiv g^{I_g(b)}(m) \tag{8.26}$$

$$\overset{8.1.12}{\Leftrightarrow} I_g(ax) \equiv I_g(b)(\varphi(m)) \tag{8.27}$$

$$\Leftrightarrow I_g(a) + I_g(x) \equiv I_g(b)(\varphi(m)) \tag{8.28}$$

$$\Leftrightarrow I_g(x) \equiv I_g(b) - I_g(a)(\varphi(m)). \tag{8.29}$$

دې له ایندکس جدول څخه وټاکل شي. x د دې کړښیز 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 $\mathrm{mod}\, 14$ ده، حل کوو:

(8.30)	$I_3(x) \equiv I_3(5) - I_3(3)(6).$

$I_3(x) \equiv 5 - 1 = 4(6) \Rightarrow I_3(x) = 4$ (

(0 ≤ کوچنی حل)

$$\Rightarrow x = \overline{11}$$

$\beta)$

$ax^n \equiv b(m)$ ورکړل شوي د $\mathrm{ggT}(a,m) = \mathrm{ggT}(b,m) = \mathbf{1}$ سره او g ساده ریښه $\bmod m$ ده. د حل دی: $\overline{ax}^n = \overline{b}$ په $(\mathbb{Z}_m^*, \cdot)$ کې، یعنې

$$\overline{g}^{I_g(ax^n)} = \overline{g}^{I_g(b)} \Leftrightarrow g^{I_g(ax^n)} \equiv g^{I_g(b)}(m) \tag{8.31}$$

$$\Leftrightarrow I_g(ax^n) \equiv I_g(b)(\varphi(m)) \tag{8.32}$$

$$\Leftrightarrow I_g(a) + I_g(x^n) \equiv I_g(b)(\varphi(m)) \tag{8.33}$$

$$\Leftrightarrow nI_g(x) \equiv I_g(b) - I_g(a)(\varphi(m)) \tag{8.34}$$

له دې لاس ته راځي: په نامعلومه $I_g(x)$ کې د دې کړښیز کونګروانت په حل بیرته اړوو، که دا حلور 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:

$$2I_3(x) \equiv I_3(9) - I_3(5)(6) \Rightarrow 2I_3(x) \equiv 2 - 5 = -3(6). \quad (8.35)$$

د $\text{ggT}(2,6) = 2 \nmid -3$ له امله حل نه شته، او لهدي سره د پيل يا سرچينيز کونگروانت $5x^2 \equiv 9(14)$ حل هم نه شته.

$$5x^3 \equiv 9(14), \text{ggT}(5,14) = \text{ggT}(9,14) = 1, g = 3$$

ساده ريښه $\mod 14$ ده، د حل دی:

$$3I_3(x) \equiv I_3(9) - I_3(5) = 2 - 5 = -3(6). \quad (8.36)$$

د $\text{ggT}(3,6) = 3 \mid -3$ له امله يو حل شتون لري (حتا 3 انکوګروانت حلونه):

$$I_3(x) = \begin{cases} 1 \\ 3 \\ 5 \end{cases} \Rightarrow \begin{matrix} \overline{3} \\ \overline{5} \\ \overline{13} \end{matrix} \quad (8.37)$$

د $\overline{x}.$ په حيث

$\gamma)$

$a \cdot b^x \equiv c(m)$ ورکړ شوي د $\text{ggT}(a,m) = \text{ggT}(b,m) = \text{ggT}(c,m) = 1$

سره او g ساده ريښه $\mod m$ ده. د حل ده: $\overline{a} \cdot \overline{b}^x = \overline{c}$ په $(\mathbb{Z}_m^*, \cdot)$ کي.

يعني:

$$\overline{g}^{I_g(ab^x)} = \overline{g}^{I_g(c)} \Leftrightarrow g^{I_g(ab^x)}(m) \equiv g^{I_g(c)}(m) \tag{8.38}$$

$$\overset{8.1.12}{\Leftrightarrow} I_g(a) + xI_g(b) \equiv I_g(c)(\varphi(m)), \tag{8.39}$$

دا په دې معن، چې باتي دی په x کې یو کربنیز کونګروانت حل کړو.

بیلګه 8.2.3:

$$3 \cdot 5^x \equiv 11(14)\, \mathrm{ggT}(3,14) = \mathrm{ggT}(5,14) = \mathrm{ggT}(11,14) = 1, g = 3$$

ساده ریبنه دی، له دې سره حل کوو:

$$\underbrace{I_3(3)}_{=1} + x\,\underbrace{I_3(5)}_{=5} \equiv \underbrace{I_3(11)}_{=4}\ \underbrace{(6)}_{=\varphi(14)}, \tag{8.40}$$

دا په ې معنا، چې $5x \equiv 3(6)$ ، یعنې 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 : $x^n \equiv a(m)$ د $\mathrm{ggT}(a,m) = 1$ سره او g ساده ریبنه $\mathbf{mod}\, m$ حلوړ ده....

$$\ldots \Leftrightarrow \overline{g}^{I_g(x^n)} = \overline{g}^{I_g(a)} \tag{8.41}$$

په $(Z_m^*, \cdot)$ کې

$$\overset{8.1.12}{\Leftrightarrow} I_g(x^n) \equiv I_g(a)(\varphi(m)) \tag{8.42}$$

$$\Leftrightarrow \quad nI_g(x) \equiv I_g(a)(\varphi(m)) \tag{8.43}$$

$$\overset{5.1.1}{\Leftrightarrow} \quad \mathrm{ggT}(n, \varphi(m)) \mid I_g(a). \tag{8.44}$$

$m = p^\alpha, p \in \mathbb{P}, \alpha \in \mathbb{N}$ داچې سړی پورته لور ته په $\mathrm{ggT}(a, m) = 1$ او په $k \geq 3$ ځان محدودولی شي، نو ټول حالتون پرته له $m = 2^k$ څخه د سره رانیول شوي یا رانغاړل شوي دي(پرتله 6.1.10: د $p^\alpha, p \neq 2, \alpha \in \mathbb{N}$ لپاره په خوښه $(\mathbb{Z}^*_{p^\alpha}, \cdot)$ څیکلیکي دی، دا په دې معنا، چې یوه ساده ریښه $\bmod p^\alpha$ شتون ري). دا په جمله 8.2.7 کې په ځانله ډول څیړل کیږي. د n - م توان لپاره یوه بله قضیه لاندې نتیجه انځوروي:

جمله : $m \in \mathbb{N}$ دې د $\mathbb{Z}^*_m$ سره څیکلیکي وي. د $a \in \mathbb{Z}$ سره تیک هلته $\mathrm{ggT}(a, m) = 1$ دی، که د n –م توان $\bmod m$ سره باور ولري:

$$d := \mathrm{ggT}(n, \varphi(m))$$

$$a^{\frac{\varphi(m)}{d}} \equiv 1(m). \tag{8.45}$$

نو د $x^n \equiv a(m)$ د $\bmod m$ انکونګروانت حلونو ګڼون یا تعداد d دی.

ښوونه:

$(\Rightarrow)$

$$a^{\frac{\varphi(m)}{d}} \equiv (x_0^n)^{\frac{\varphi(m)}{d}} = \left(x_0^{\varphi(m)}\right)^{\frac{n}{d}} = 1^{\frac{n}{d}} = 1(m). \qquad (8.46)$$

$(\Leftarrow)$

وي دي $a^{\frac{\varphi(m)}{d}} \equiv 1(m)$ ، دا چې $\mathbb{Z}_m^*$ څيوکليکي دی يوه ساده ريښه $g \bmod m$ شتون لري . يعني

$\overline{a} = \overline{g}^{I_g(a)},$	(8.47)

دا په دي معنا، چې $a \equiv g^{I_g(a)}(m)$ او

$1 \equiv a^{\frac{\varphi(m)}{d}} \equiv \left(g^{I_g(a)}\right)^{\frac{\varphi(m)}{d}} = g^{\frac{\varphi(m)I_g(a)}{d}}(m),$	(8.48)

$$\overline{1} = \overline{g}^{\frac{\varphi(m)I_g(a)}{d}}$$

دا په دي معنا، چې . د 6.2.7 له مخي لاس ته راځي

$$\underbrace{\operatorname{ord}(\overline{g})}_{=\varphi(m)} \Big| \frac{\varphi(m)I_g(a)}{d}, \qquad (8.49)$$

$$d\varphi(m) \mid \varphi(m)I_g(a) \Rightarrow d \mid I_g(a)$$

دا په دي معنا، چې

له دي سره د5.1.1 له مخي کربنيز کونګروانت

$$ny \equiv I_g(a)(\varphi(m)) \qquad (8.50)$$

حلور دی، يعني $a \in \mathbb{Z}$ n -مه ريښه ده.

پسې د 5.1.1 له مخې باور لري: دا کرښيز کونګروانت $d \bmod \varphi(m)$ انکونګروانت حلونه لري. د $y_0 \in \mathbb{Z}$ لپاره د

$$ny_0 \equiv I_g(a)(\varphi(m)) \tag{8.51}$$

سره تيک 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

$$\overline{x_1} = \overline{g}^{I_g(x_1)} = \overline{g}^{I_g(x_0)} = \overline{x_0}, \tag{8.52}$$

يعني تيک يو $\overline{x_0} \in \mathbb{Z}_m^*$ شتونن لري.

له دې سره $x^m \equiv a(m)$ هم تيک $d = \mathrm{ggT}(n, \varphi(m)) \bmod m$ انکونګروانت حلونه لري. □

بيلګه 8.2.6: وي دې $x^5 \equiv 7(25)$ حلوړ، دا په دې معنا، چې:

ايا $a = 7$ پنخة توان $\bmod 25$ دی؟ی.

$a = 7, n = 5, m = 25 = 5^2$ د ګاوس له مخې: $\mathbb{Z}_{5^2}^*$ څيوکليکي د

$$\varphi(m) = \varphi(25) = 20$$

$$\Rightarrow d := \text{ggT}(n, \varphi(m)) = \text{ggT}(5, 20) = 5 \tag{8.53}$$

$$\Rightarrow a^{\frac{\varphi(m)}{d}} = 7^{\frac{20}{5}} = 7^4 \equiv (-1)^2(25) = 1(25), \tag{8.54}$$

دا په دي معنا، چې 7 پنځم توان $\mod 25$ دی.

ټول حلونه د د ساده ریښي $g = 2$ او اندکس جدول له مخي 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 کي لکه نور چې ویلي مو وو د

$$m = 2^k, k \geq 3,$$

حالت $\mathbb{Z}_{2^k}^*$ د نه څیکلیکي، سره ځانونه په کار اچوو:

جمله 8.2.7: وي دي $k \geq 3, a \in \mathbb{Z}$ ، د $\text{ggT}(a, 2^k) = 1$ سره ټیک هلته n ــم توان $\mod 2^k$ دی، که د $d = \text{ggT}(n, 2^{k-2})$ لپاره باور ولري:

1. $a^{\frac{2k-2}{d}} \equiv 1(2^k)$,
2. $a \equiv 1(4)$ یا n ناجوړه یا طاق دی.
3.

د $x^n \equiv a(m)$ د $\mod 2^k$ انکوګروانتو حلونو ګڼ،ڼ(تعداد) نو بیا 1 دی د n ناجوړه یا طاق لپاره، او $2d$ د جوړه n لپاره.

د $x^n \equiv a(2^k)$ د حل(نو) پیداکول له بنوونې 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 یواځنې ډول د 6.2.16له مخې انځور کړئ، راوړو

$$nx \equiv j(2) \text{ همداسې } nx \equiv l(2^{k-2}); \tag{8.56}$$

کرښیز کونګروانت دي، که α د $nx \equiv j(2)$ راکمشوی حل وي او β د $nx \equiv l(2^{k-2})$ راکم 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 سړی ټول حلونه لاس ته راوړي.

بیلګه 8.2.8 :

1. $x^3 \equiv 9(32) : N = 3, a = 9, m = 2^5 (k = 5)$

.

و بنایئ: $a = 9$.توانپاتي $\mathbb{Z}_{32}^*$ دی (راوړو: $\mathrm{mod}\, 32$ دی د ګاوس له مخې څیوکلیکي نه دی ، ځکه چې $k \geq 3, p = 2$) د 8.2.7سره سم:

$$d = \mathrm{ggT}(n, 2^{k-2}) = \mathrm{ggT}(3,8) = 1 \Rightarrow \tag{8.58}$$

$$a^{\frac{2^{k-2}}{d}} = 9^{2^{5-2}} = \left(9^4\right)^2 = \left(81^2\right)^2 \equiv 1(32), \tag{8.59}$$

۳ . 9 نو دري 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:

$$\overline{a} = \overline{9} = \overline{(-1)^j 5^l}, \qquad j \in \{0,1\}, l \in \{1,\ldots,2^{k-2}\} \tag{8.60}$$

: $\bmod 324$.

$$5^0 \equiv 1, 5^1 \equiv 5, 5^2 \equiv -7, 5^3 \equiv -3, 5^4 \equiv -15, 5^5 \equiv -11, 5^6 \equiv 9(32),$$

4. يعنې $j = 0, l = 6 \leq 2^{k-2} = 8$ ، 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 $\bmod 32$ دی.

$$\overline{x_0} = \overline{(-1)^\alpha 5^\beta} = \overline{25}. \tag{8.61}$$

$$x^4 \equiv 177(224) : n = 4, a = 177, m = 224 = 7 \cdot 2^5,$$

.

$$\text{ggT}(177, 224) = 1$$

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 څیوکلیکي دی، د8.2.5 سره سم:

$$\varphi(7) = 6, d = \text{ggT}(n, \varphi(7)) = 2; a^{\frac{\varphi(7)}{2}} = 8 \equiv 1(7) \Rightarrow \qquad (8.62)$$

د 8.2.5 له مخې باور لري 2 د 4–م توان د سره اینکونګروانت حلونه دی

$$\Rightarrow x_1 = 2, x_2 = 5 \quad x^4 \equiv 177(2^5)$$

.

$$\Rightarrow x^4 \equiv 17(2^5) : n = 4$$

$17^{\frac{2^3}{4}} = 17^2 \equiv 1(32)$ ، $a = 17 \equiv 1(4)$ جوړه مګر

او همداسي د 8.2.7 له مخې : 17 د 4-م توان $\mod 32$ دی د $8 \bmod 32$ سره اینکونګروانت حلونه $y_1, y_2, \cdots, y_8$ دي.

(د $\overline{a} = \overline{(-1)^j 5^l}$ سره سم او $nx \equiv j(2)$ کرښیزکوګروانت همداسي

$nx \equiv l(2^{k-2}) \Rightarrow$ څخه لاس ته راځي توله α ، توله $\beta \Rightarrow$ څخه لاس ته راځي

توله $\overline{y} = \overline{(-1)^\alpha 5^\beta}$.)

د حینایيي پاتې جملې سره سم:

$$\left.\begin{array}{rcl} x & \equiv & x_i(7), \\ x & \equiv & y_s(32) \end{array}\right\} \qquad i = 1, 2, s = 1, \ldots, 8, \qquad (8.63)$$

یعنې 16 سیستمي له دې لاس ته راځي 16 حلونه.

څلوريز پاتې(که غواړئ: مربع باقيمانده)Quadratische Reste

ځانګړی حالت

مونږ اوس يوځانګړی حالت رااخلو، او د هده حلوړوالی ټيک تر څيړنې لاندې نيسو:

$n = 2$ دا په دې معنا،چې

$$x^2 \equiv a(m) \tag{9.1}$$

د څيړنې دی. د دې د حلوړولو لپاره ساده قضيې تر څيړنې لاندې نيول زمونږموخه ده.

پيژند 9.1.1 : $m \in \mathbb{N}, a \in \mathbb{Z}, \mathrm{ggT}(a,m) = 1$ مربعيز توانپاتې $\mathrm{mod}\, m$ 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

$$x_0 = 2k + 1 \ (k \in \mathbb{Z}) \tag{9.2}$$

حلوړ $\mathrm{mod}\, 2$ دی.

ښوونه: $x_0^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 1(2) \ (\equiv 2n + 1 \equiv a(2))$.

د عمومي قضيې 8.2.5 (هلته $n \in \mathbb{N}$ په خوښه)، څيکليکي يا تل بيرته راګرځيدونکی حالت له مخې:

جمله 9.1.3 : وي دي $m \in \mathbb{N}, m \geq 3; a \in \mathbb{Z}$ د $\mathrm{ggT}(a,m) = 1$ سره ټيک هلته مربع پاتي $\bmod m$ دی، که

$$a^{\frac{\varphi(m)}{2}} \equiv 1(m); \qquad (9.3)$$

د $x^2 \equiv a(m)$ د حلونو تعداد يا گنون 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 مخي باور لري،:

لومړی: که د m په لومړني ضريبتجزيه کي يو ناجوړه(طاق) p_i رامنځ ته شي، نو $p_i - 1$ جوړه يا جفت دی او له دي امله $\varphi(m) \equiv 0(2)$ دی.

دويم: که نه ، نو بيا ۲-م توان دی، يعني $\varphi(m) = \frac{m}{2}$ جوړه دی.

($m = 2^\alpha$ د $\alpha \geq 2$ سره ، ځکه چې $m \geq 3$)

جملګی ۴ . ۱ . ۹ : (اويلر)

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

په پای کي لکه نور چې ويلي مو وو د $m = 2^k, k \geq 3,$

حالت $\mathbb{Z}_{2^k}^*$ د نه څيکليکي، سره ځانونه په کار اچوو:

جمله 8.2.7: وي دي $k \geq 3, a \in \mathbb{Z}$ ، د $\mathrm{ggT}(a, 2^k) = 1$ سره ټيک هلته n – م توان $\bmod 2^k$ دی، که د $d = \mathrm{ggT}(n, 2^{k-2})$ لپاره باور ولري:

4. $a^{\frac{2k-2}{d}} \equiv 1(2^k)$,

.5 $a \equiv 1(4)$ یا n ناجوړه یا طاق دی.

.6

د $x^n \equiv a(m)$ د $\mathrm{mod}\, 2^k$ انکوګروانتو حلونو ګڼ،ن(تعداد) نو بیا 1 دی د n ناجوړه یا طاق لپاره، او $2d$ د جوړه n لپاره.

د $x^n \equiv a(2^k)$ د حل(نو) پیداکول له ښوونې 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 یواځنې ډول د 6.2.16له مخې انځور کړئ، راوړو

(8.56)	$nx \equiv j(2)$ همداسې $nx \equiv l(2^{k-2})$;

کړښیز کونګروانت دي، که α د $nx \equiv j(2)$ راکمشوی حل وي او β د $nx \equiv l(2^{k-2})$ راکم شوی حل، نو دی

$$\overline{x_0} = \overline{(-1)^\alpha 5^\beta} \tag{8.57}$$

د $x^n \equiv a(2^k)$ حل دی. له دې سره سړی ټول حلونه لاس ته راوړي.

بیلګه 8.2.8 :

$$x^3 \equiv 9(32) : N = 3, a = 9, m = 2^5 (k = 5)$$

.2

.

و ښایئ: $a = 9$.توانپاتي $\mathrm{mod}\, 32$ دی (راوړو: $\mathbb{Z}_{32}^*$ د ګاوس له مخې څیوکلیکي نه دی ، ځکه چې $k \geq 3, p = 2$) د 8.2.7سره سم:

$$d = \mathrm{ggT}(n, 2^{k-2}) = \mathrm{ggT}(3,8) = 1 \Rightarrow \tag{8.58}$$

$$a^{\frac{2^{k-2}}{d}} = 9^{2^{5-2}} = \left(9^4\right)^2 = \left(81^2\right)^2 \equiv 1(32), \qquad (8.59)$$

۳ . 9 نو دري 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:

$$\overline{a} = \overline{9} = \overline{(-1)^j 5^l}, \qquad j \in \{0,1\}, l \in \{1,\ldots,2^{k-2}\} \qquad (8.60)$$

: $\bmod 324$.
$$5^0 \equiv 1, 5^1 \equiv 5, 5^2 \equiv -7, 5^3 \equiv -3, 5^4 \equiv -15, 5^5 \equiv -11, 5^6 \equiv 9(32),$$

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 $\bmod 32$ دی.

$$\overline{x_0} = \overline{(-1)^\alpha 5^\beta} = \overline{25}. \qquad (8.61)$$

$$x^4 \equiv 177(224) : n = 4, a = 177, m = 224 = 7 \cdot 2^5,$$
$$, \text{ggT}(177, 224) = 1$$
.
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 څيوکليکي دی، د8.2.5 سره سم:

$$\varphi(7) = 6, d = \text{ggT}(n, \varphi(7)) = 2; a^{\frac{\varphi(7)}{2}} = 8 \equiv 1(7) \Rightarrow \qquad (8.62)$$

د 8.2.5 له مخې باور لري 2 د 4–م توان د سره اينکونګروانت حلونه دی

$$\Rightarrow x_1 = 2, x_2 = 5$$

.

$$x^4 \equiv 177(2^5)$$

$$\Rightarrow x^4 \equiv 17(2^5) : n = 4$$

$$17^{\frac{2^3}{4}} = 17^2 \equiv 1(32) \quad a = 17 \equiv 1(4)$$ جوړه مګر ،

او همداسي د 8.2.7 له مخي : 17 د 4-م توان $\bmod 32$ دی د $8 \bmod 32$ سره اینکونګروانت حلونه $y_1, y_2, \cdots, y_8$ دي.

$\overline{a} = \overline{(-1)^j 5^l}$ (د سره سم او $nx \equiv j(2)$ کربنیزکوګروانت همداسي

$nx \equiv l(2^{k-2}) \Rightarrow$ څخه لاس ته راځي ټول α ، ټول $\beta \Rightarrow$ څخه لاس ته راځي

$\overline{y} = \overline{(-1)^\alpha 5^\beta}$ ټول .)

د حینایيي پاتي جملي سره سم:

$$\left.\begin{array}{rcl} x & \equiv & x_i(7), \\ x & \equiv & y_s(32) \end{array}\right\} \quad i = 1, 2, s = 1, \ldots, 8, \tag{8:63}$$

یعني 16 سیستمي له دي لاس ته راځي 16 حلونه.

څلوریز پاتي(که غواړئ: مربع باقیمانده) ځانګړی حالت

مور اوس یوځانګړی حالت رااخلو، او د هده حلوروالی ټیک تر څیړني لاندي نیسو:

$n = 2$ دا په دې معنا،چې

$$x^2 \equiv a(m) \quad (9.1)$$

د څيړنې دی. د دې د حلورولي لپاره ساده قضيې تر څيړنې لاندې نيول زمورږموخه ده.

پيژند 9.1.1 : $m \in \mathbb{N}, a \in \mathbb{Z}, \text{ggT}(a,m) = 1$ مربعيز توانپاتې $\text{mod}\, m$ بلل کيږي، او هم لنډ مربعيز پاتې، که $x^2 \equiv a(m)$ حلور وي.

دا لاندې د $m = 2$ لپاره باور لري:

ليما يا جملګئ 9.1.2: وي دې $a \in \mathbb{Z}$ د $\text{ggT}(a,m) = 1 \Rightarrow a$ سره ناجوړه(طاق)، دا په دې معنا،چې $2n+1$. نو باور لري:

هر ناجوړه عدد

$$x_0 = 2k + 1 \ (k \in \mathbb{Z}) \quad (9.2)$$

حلور $\text{mod}\, 2$ دی.

ثبوونه: $x_0^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 1(2) \ (\equiv 2n + 1 \equiv a(2))$.

د عمومې قضيې 8.2.5 (هلته $n \in \mathbb{N}$ په خوښه)، څيکليکي 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 $\text{ggT}(a,m) = 1$ سره ټيک هلته مربع پاتې $\text{mod}\, m$ 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.

ثبوونه: ځکه چې $d = \text{ggT}(2, \varphi(m))$ 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 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 –توان دی، یعني $\varphi(m) = \frac{m}{2}$، جوړه.

($m = 2^\alpha$ د $\alpha \geq 2$ سره ځکه چې $m \geq 3$)

کورولار ۹ . ۱ . ۴ (اویلر **(Euler)**): وي دي $p > 2$ لومړنی عدد، $a \in \mathbb{Z}$ د $\mathrm{ggT}(a,p) = 1$ (خورا غټ پروبشوی یا بزرکترین قاسم مشترک) سره ټیک هلته مربعیز باقي یا پاتي $\bmod p$ دی، که

$$a^{\frac{p-1}{2}} \equiv 1(p). \quad (9{:}4)$$

ښوونه: د ګاوس 6.2.15 له مخ او د $p \neq 2$ له امله $(\mathbb{Z}_p^*, \cdot)$ تل بیرته راګرځیدنې یا څیکلیکي دی.

جملګی ۹ . ۱ . ۵ - وي دي $p > 2$ یو لومړنی عدد، له $a \in \mathbb{Z}$ $\mathrm{ggT}(a,p) = 1$ سره ټیک هلته مربع باقي یا پاتي $\bmod p^\alpha \ \forall \alpha \in \mathbb{N}$ دی، که a مربع باقي $\bmod p$ وي

ښوونه:

$(\Rightarrow)$

ساده دی.

$(\Leftarrow)$

$a^{\frac{p-1}{2}} \equiv 1(p) \mod p$ که a مربع باقي وي، نو د جملګي 9.1.4 له مخي باور لري:

$a^{\frac{p-1}{2}} = 1 + tp$ ، يعني $t \in \mathbb{Z}$ د يوه $\alpha \in \mathbb{N}$ لپاره. له دي امله د هر لپاره باور ري:

$$a^{\frac{\varphi(p^\alpha)}{2}} = a^{\frac{1}{2}p^{\alpha-1}(p-1)} = \left(a^{\frac{p-1}{2}}\right)^{p^{\alpha-1}} = (1+tp)^{p^{\alpha-1}} \equiv 1(p^\alpha), \quad (9.5)$$

ځکه: (ايندکشن په α پسي).

$$\alpha = 1$$

$$(1+tp)^{p^{\alpha-1}} = 1 + tp \equiv 1(p). \quad (9.6)$$

$$\alpha \to \alpha + 1$$

$$(1+tp)^{p^\alpha} = \left[(1+tp)^{p^{\alpha-1}}\right]^p = (1+rp^\alpha)^p = \quad (9.7)$$

$$= 1 + \underbrace{\binom{p}{1}}_{=p} rp^\alpha + \cdots + r^p p^{\alpha p} \equiv 1(p^{\alpha+1}). \quad (9.8)$$

$$= \underbrace{\qquad\qquad\qquad\qquad}_{=1+sp^{\alpha+1}}$$

د جملي 9.1.3 پسي لرو($m = p^\alpha$ لپاره): $a \in \mathbb{Z}$ مربع پاتي $\mod p^\alpha$ دی. □

د ناڅيکليکي حالت لپاره، يعني $m = 2^k, k \geq 3$ بايد $a \in \mathbb{Z}$ ناجوړه(طاق) وي، لکه لاندي جمله چې ښايي:

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 ټیک یو حل لري.

دویم - د $k \geq 3$ لپاره حلوړ دی، د 4 حلونو سره، که $a \equiv 1(8)$ وي، پرته له ي نه.

ښوونه: لومړی- پورته وګوری: $m = 2 = 2^1$ ، دا چې ټول ناجوړه ګڼونه یا اعداد $\mathbf{mod}\, 2$ دي، نو ټیک یو حل شتون لري.

دویم: د ګاوس 6.2.15 له مخې ، $(\mathbb{Z}_4, \cdot)$ تلبیرته راګرځیدونی یا څیکلیکي دی، یعنې د $a \in \mathbb{Z}$ ناجوړه مربع پاتې $\mathbf{mod}\, 4 \ldots$ دی. 9.1.3 له مخې:

(9.9)	$\ldots \Leftrightarrow a^{\frac{\varphi(4)}{2}} \equiv 1(4) \Leftrightarrow a^{\frac{2}{2}} \equiv 1(4) \Leftrightarrow a \equiv 1(4).$

دریم: په همدې ترتیب د 9.1.3 پسې: د $x^2 \equiv a(4)$ د حلونو ګڼون یا تعداد 2 دی.

. وي دي $m = 2^k, k \geq 3$ حلوړ، نو دی

(9.10)	$x_0^2 \equiv a(2^k)$

څلورم- د یوه $x_0 \in \mathbb{Z}$ لپاره، له دې سره $x_0^2 \equiv a(8)$ ، ځکه چې $8 \mid 2^k \ (k \geq 3)$ ، پسې د 8.1.6 له مخې باور لري: خورا غټ ګډ پروېشونی(بزرګترین مقسوم علیه) $\mathrm{ggT}(x_0, 2^k) = 1$ ، نوله دې سره $\mathrm{ggT}(x_0, 8) = 1 \ (8 \mid 2^k, k \geq 3)$ دا په دې معنا، چې $x_0 \in \mathbb{Z}$ نسبت و 8 ته نسي لومړنی عدد دی، یعنې : $x_0 = 1, 3, 5, 7(8)$ ، له دې سره $x_0^2 \equiv 1(8)$.

په تولیزه توګه:

$a \equiv x_0^2 \equiv 1(8).$	(9.11)

پنځم- وي دي په څټ یا برعکس $a \equiv 1(8)$ ، یعني هم $a \equiv 1(4)$ ، پسې باور لري

$a^{2^{k-3}} \equiv 1(2^k)\ \ (k \geq 3).$	(9.12)

شپږم- ایندکشن: د نیونې یا قرضیې له مخې.

نیسو چې د لپاره سم دی، د لپاره باور لري:

$a^{2^{(k+1)-3}}$ =	
$\left(a^{2^{k-3}}\right)^2 = (1+t2^k)^2 = 1+2t2^k+t^2 2^{2k} = 1+s2^{k+1} \equiv$	(9.13)
$\equiv \quad 1(2^{k+1}).$	(9.14)

اوم- له دې سره لرو او $a \equiv 1(4)$ $(d = \text{ggT}(2, 2^{k-2}) = 2)$

$a^{\frac{2^{k-2}}{d}} = a^{2^{k-3}} \equiv 1(2^k);$	(9.15)

اتم- نو د 8.2.7 له مخې لرو، چې $a \in \mathbb{Z}$ مربع پاتې یا باقي $\mod 2^k$ دی. له دې سره $2d = 4$ حلونه باور لري. □

بیلګه ۹ . ۱ . ۷ : ایا $x^2 \equiv 110(211)$ حلور دی؟ (⇔110مربع پاتې $\mod 211$ دی؟)

دا چې 211 يو لومړنی ګڼ يا عدد دی، او $ggT(110,211)=1$ د اويلر 9.1.4 پسې بار لري، ټيک هلته حلوړ دی، که وي:

$a^{\frac{p-1}{2}} = 110^{105} \equiv 1(211)$	(9.16)

- ډير کار غواړي!

لژندر-سومبول(1752-1833) Legendre-Symbol:

د $x^2 \equiv a(m), ggT(a,m)=1$ د حلوړوالي لپاره نوي لار.

پيژند يا تعريف ۹ . ۲ . ۱ : (لژندر سيمبول [9.1]): وي دي $p>2$ يو لومړنی ګڼ يا عدد، $a \in \mathbb{Z}$ د لژندر سومبول له مخې مربع پاتې د دې لاندې له لارې تعريف دی:

(9.17)	a مربع باقي mod p دی. P|a anه 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

$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right).$	(9.18)

بنوونه:

$\left(\frac{a}{p}\right) = 1 \mod p$ مربع باقي	(9.19)
$\Leftrightarrow \quad x^2 \equiv a(p)$	(9.20)
$\Leftrightarrow \quad x^2 \equiv a'(p)$	(9.21)
$\Leftrightarrow \quad \left(\frac{a'}{p}\right) = 1.$	(9.22)

جملګی ۹ . ۳ – وېش له باقي يا پاتې سره:

$a = p \cdot s + r$	(9.23)

د $0 \leq r < p$ سره، له دې امله دی $a = ps + r \equiv r(p)$ ، نو د 9.2.2 پسې:

$\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right) \ldots$ لنډونه	(9.24)

جمله ۹ . ۲ . ۴ : وي دي $p > 2$ يو لومړنی عدد او $a \in \mathbb{Z}$ د(خورا غټ ګډ پروېشونی) $ggT(a,p) = 1$ سره ، نو باور لري

(9.25)	$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (p).$

بنوونه:

- که $\left(\frac{a}{p}\right) = 1$ وي، نو a مربع پاتي $\bmod p$ دی او د 9.1.4 پسي يا له $a^{\frac{p-1}{2}} \equiv 1(p)$ مخي: ، له دي 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 $\bmod p$ نه دی او د 9.1.4 له مخي يا $a^{\frac{p-1}{2}} \not\equiv 1(p)$ $a^{\frac{p-1}{2}} - 1 \not\equiv 0(p)$ پسي: ، دا په دي معنا، چي . د 6.1.18 له مخي باور لري

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

نو $a^{p-1} - 1 \equiv 0(p)$ ، د اسي چي په بدن (انګريزي يي فيلډ) $(\mathbb{Z}_p, +, \cdot)$ کي (p لومړنی ګڼ يا عدد) باور لري:

(9.28)	$\overline{0} = \overline{a^{p-1} - 1} = \overline{(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)} = \overline{\underbrace{a^{\frac{p-1}{2}} - 1}_{\neq \overline{0}}}\,\overline{a^{\frac{p-1}{2}} + 1};$

دا چي بدن صفر نه لري، لرو

(9.29)	$\overline{a^{\frac{p-1}{2}} + 1} = \overline{0}.$

له دي سره $a^{\frac{p-1}{2}} + 1 \equiv 0(p)$ او $a_1, \ldots, a_n \in \mathbb{Z}$ ، دا په دي معنا، چي

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (p).$	(9.30)

کورولار ۹ . ۲ . ۵: $p > 2$ دي لومړني عدد وي او $a_1, \ldots, a_n \in \mathbb{Z}$ د خ غ ګ يعني $(i = 1, \ldots, n)\ \mathrm{ggT}(a_i, p) = 1$ سره، نو باور لري

$\left(\frac{a_1 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdots \left(\frac{a_n}{p}\right).$	(9.31)

ثبوت: $\mathrm{ggT}(a_1 \cdots a_n, p) = 1$ ، ځکه چې پرته له دې به $p \mid a_1 \cdots a_n$ ، داسې چې د يوه $1 \leq i \leq n$ لپاره د 3.1.5 له مخې $p \mid a_i$ لرو. – تضاد يا مخمخوالی! له دې سره $\left(\frac{a_1 \cdots a_n}{p}\right)$ تعريف دی.

$\left(\frac{a_1 \cdots a_n}{p}\right) \equiv (a_1 \cdots a_n)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdots a_n^{\frac{p-1}{2}} \equiv \left(\frac{a_1}{p}\right) \cdots \left(\frac{a_n}{p}\right) (p).$	(9.32)

له دې امله p کمښت وېشي، يعني $p \mid (\pm 1) - (\pm 1)$. دا کمښت صفر دی، که دواړه عددونه برابر وي، او پرته له دې ± 2 .

له $p > 2$ امله باورلري: $p \nmid \pm 2 \Rightarrow$ يعني لاس ته راځي کمښت $\neq 0 \Rightarrow$ لاس ته راځي (9.26). □

لاس ته راوړنه ۹ . ۲ . ۶ :

لومړی- $a = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ دي د $a \in \mathbb{Z}\ (a \neq 0)$ په لومړنيو ضريبونو ټوټه کونه يا تجزيه وي. نو د 9.2.5 له مخې باور لري:

$\left(\frac{a}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{p_1^{\alpha_1}}{p}\right)\cdots\left(\frac{p_k^{\alpha_k}}{p}\right),$	(9.33)

دویم: نو شمیرو: $\left(\frac{-1}{p}\right)$ او $\left(\frac{q^\alpha}{p}\right)$ د خ غ پ(قاسم بزرگ مشبرک) $\gg\mathrm{T}(p,q^\alpha)=1$ سره، دا په دې معنا، چې $p\neq q$.

دریم: $\left(\frac{q^2}{p}\right)=1$ ، ځکه چې $x^2\equiv q^2(p)$ د حل په حیث $x_0=q$ 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 یا ثبوت دی.

پنځم: له ې امله فقط د شمیرلو لپاره: $\left(\frac{-1}{p}\right)$ او $\left(\frac{q}{p}\right)$ د $p\neq q$ سر لومړنی عدد $2<$ دی، ځکه چې

$\left(\frac{q^{2k}}{p}\right)=\left(\frac{(q^k)^2}{p}\right)=1.$	(9.34)

کورولار یا 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 ټیک هلته مربع باقي $\bmod p$ دی، که $p\equiv 1(4)$ وي.

ښوونه:

لومړی- د له مخې باور لري:

$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}(p);$	(9.35)

دویم: نو p کمښت یا تفریق وېشي، دا 0 یا ± 2 دی. د $p > 2$ له امله دی

$p \nmid \pm 2 \Rightarrow$ (له دې لاس ته راځي)

$\Rightarrow$ کمښت $= 0 \Rightarrow$

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$	(9.36)

دویم: مربع پاتې دی

$\ldots \overset{1.}{\Leftrightarrow} \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$	(9.37)
$\Leftrightarrow \frac{p-1}{2}$ جوړه	(9.38)
$\Leftrightarrow \frac{p-1}{2} = 2k \ (k \in \mathbb{N})$	(9.39)
$\Leftrightarrow p - 1 = 4k$	(9.40)
$\Leftrightarrow p = 4k + 1$	(9.41)
$\Leftrightarrow p \equiv 1(4).$	(9.42)

لاندې جمله د دیریښلت د جملې څوکه انځوروي، چې نوره غوارو وښایو:

جمله ۹ . ۲ . ۸ : د $4k+1\ (k\in\mathbb{N})$ بڼې ناپای ډې لومړني ګڼونه شتون لري.

ښوونه: ناسيده، نيسو چې د دې بڼې پای ډېر ګڼونه شتون لري:

$p_1,\cdots,p_n$ وي دې.

$N := (2p_1\cdots p_n)^2+1,$	(9.43)

$N=2m+1$ ، يعني ناجوړه، ا په دې معنا، چې $2\nmid N$.

نو باور ري: د $N>1$ له امله يو لومړنی عدد p د $p\mid N$ شتون لري، داپه دې معنا، چې $N\equiv 0(p)$. نو:

$(2p_1\cdots p_n)^2\equiv -1(p).$	(9.44)

دا په دې معنا چې -1 مربع پاتې يا باقي $\bmod p$ دی. د 9.2.7 له مخې لرو يا لاس ته راځي:

$p\equiv 1(4),$	(9.45)

دا په دې معنا چې $p=4k+1$. د نيونې يا فرضيې له مخو لاس ته راځي: $p=p_i$ د يوه $1\le i\le n$ لپاره. له دې امله باور لري

$p\mid (2p_1\cdots p_n)^2;$	(9.46)

د $p\mid N$ له امله لاس ته راځي:

$p\mid N-(2p_1\cdots p_n)^2=1,$	(9.47)

نو $p\le 1$ ـ تضاد يا ردونه. □

د ګاوس لیما یا جملګی

جمله ۹ ، ۲ . ۹ : (د ګاوس جمله ګی) وي دي $p > 2$ لومړنی عدد، $a \in \mathbb{Z}$ د خورا غټ ګد پروېشوني (بزرګترین مقسوم علیه 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

$\left(\frac{a}{p}\right) = (-1)^{n(a)},$	(9.48)

چیرته چې $n(a)$ سره د باتې یا باقي ګنون یا تعداد په نخښه کیږي، چې له $\frac{p}{2}$ لوی دي.

ښوونه: د $i = 1, 2, \ldots, \frac{p-1}{2}$ لپاره دي وي:

$ia = pq_i + t_i \quad 0 \leq t_i < p$	(9.49)

(د پاتې سره ېش). نو $t_i \neq 0 \ \forall i$ باور لري، پرته له دې $ia = pq_i$ ، یعنې $p \mid ia$ ، داسې چې(د 3.1.5 له مخې): $p \mid i$ یا $p \mid a$ ، داچې $\mathrm{ggT}(a,p) = 1$ (خ غ ګ) ، باید باور ولري ($\Rightarrow p \leq i$) ،د $1 \leq i \leq \frac{p-1}{2} < p$ له مخې یو مخامخوالی یا تضاد لاس ته راځي!

په ځانګړي ډول باور لري:

$t_i \equiv ia(p) \ \forall i = 1, 2, \ldots, \frac{p-1}{2}.$	(9.50)

وي دي $r_1, \ldots, r_{n(a)}$ پورتنۍ پاتې له $\frac{p}{2} < t_i < p, s_1, \ldots, s_k$ سره پاتې 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!)

(9.51)	$\Rightarrow n(a) + k = \frac{p-1}{2}.$

وښايي: $r_1, \ldots, r_{n(a)}, s_1, \ldots, s_k$ ټول سره توپير لري.

نيسو $t_i = t_j$ د $i > j$ لپاره، نو

(9.52)	$ia - ja = pq_i - pq_j = p(q_i - q_j);$

$q_i - q_j = 0$ دی، نو $ia - ja = 0$ ، دا په دې معنا چې $(i-j)a = 0$ ، يعنې $i = j \ (a \neq 0)$ -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 $\mathrm{ggT}(p,a) = 1$ (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

(9.53)	$\alpha_i = p - r_i \ (i = 1, \ldots, n(a)),$

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 :

(9.54)	$\alpha_i = p - r_i = s_j \ \Rightarrow \ r_i + s_j = p \equiv 0(p)$

i,j	
$\Rightarrow \quad ia+ja\equiv 0(p)\ \ (t_i\equiv ia(p)\ \forall i)$	(9.55)
$\Rightarrow\ p\mid (i+j)a \overset{3.1.5}{\Leftrightarrow} p\mid i+j\ (\mathrm{ggT}(a,p)=1);$	(9.56)

$1\le i,j\le \frac{p-1}{2}$ د $1\le i+j\le p-1<p$ له امله باور لري: -تضاد!

$\alpha_1,\ldots,\alpha_{n(a)},s_1,\ldots,s_k$	(9.57)

ټول مختلف دي يا توپير لري.

$0<\alpha_i\le \frac{p-1}{2}$

باور لري: ، ځکه چې

$\frac{p}{2}<r_i<p\Rightarrow -p<-r_i<\frac{p}{2}\Rightarrow 0<p-r_i=\alpha_i<\frac{p}{2};$	(9.58)
$0<s_j<\frac{p-1}{2}$	(9.59)

د پيژند له مخې باور لري.

له دې سره هم

$1\le s_j\le \frac{p-1}{2};\quad 1\le \alpha_i\le \frac{p-1}{2}$ او	(9.60)

دا چې

$n(a)+k=\frac{p-1}{2}$	(9.61)

(ټول باقي يا پاتې توپير لري) $\alpha_1, \ldots, \alpha_{n(a)}, s_1, \ldots, s_k$ تيک $\frac{p-1}{2}$ طبيعي اعداد دي د 1 او $\frac{p-1}{2}$ ترمنځ. له دې سره: ټيک اعداد $\alpha_1, \ldots, \alpha_{n(a)}, s_1, \ldots, s_k$ دي.

له دې لاس ته راځي:

$$\alpha_1 \cdots \alpha_{n(a)} s_1 \cdots s_k = 1 \cdot 2 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)! \tag{9.62}$$

$$\Rightarrow (p - r_1) \cdots (p - r_{n(a)}) s_1 \cdots s_k = \left(\frac{p-1}{2}\right)! \tag{9.63}$$

$$\Rightarrow (-1)^{n(a)} r_1 \cdots r_{n(a)} s_1 \cdots s_k \equiv \left(\frac{p-1}{2}\right)!(p) \tag{9.64}$$

$$\Rightarrow (-1)^{n(a)} t_1 \cdots t_{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)!(p) \tag{9.65}$$

(9.66) (د r_i, s_j له تعريف څخه)

$$\Rightarrow (-1)^{n(a)} 1 \cdot a \cdots \left(\frac{p-1}{2}\right) \cdot a \equiv \left(\frac{p-1}{2}\right)!(p) \tag{9.67}$$

(9.68) (د تعريع له مخې: $ia = pq_i + t_i \equiv t_i(p)$)

$$\Rightarrow (-1)^{n(a)} a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(p). \tag{9.69}$$

باور لري $ggT((\frac{p-1}{2})!, p) = 1$ ، ځکه چې پرته له دې به وی

$$p \left| \left(\frac{p-1}{2}\right)! = 1 \cdot 2 \cdots \frac{p-1}{2}, \right. \tag{9.70}$$

يعني د 3.1.5 له مخې:

$$\exists k : 1 \leq k \leq \frac{p-1}{2} < p \quad : \quad p \mid k \quad \text{- اتضاد!} \tag{9.71}$$

$$\Rightarrow \quad (-1)^{n(a)} a^{\frac{p-1}{2}} \equiv 1(p) \tag{9.72}$$

$$\Rightarrow \quad a^{\frac{p-1}{2}} \equiv (-1)^{n(a)}(p) \tag{9.73}$$

$$\overset{9.2.4}{\Leftrightarrow} \left(\frac{a}{p}\right) \equiv (-1)^{n(a)}(p) \tag{9.74}$$

$$\Rightarrow \quad p \quad \text{کمښت وېشي} \quad \in \{0, \pm 2\} \text{ د} \tag{9.75}$$

$$\Rightarrow \quad \begin{matrix} \text{کښت باید صفر} \\ \text{وي } (p > 2, p \nmid 2!) \end{matrix} \tag{9.76}$$

$$\Rightarrow \quad \left(\frac{a}{p}\right) = (-1)^{n(a)}. \tag{9.77}$$

بیلګه 9.2.10 . ایا 7 څلورې پاتې یا مربع باقي $\bmod 13$ دی؟

$p = 13, a = 7, ggT(a, p) = 1$ (ggT خورا غټ ګډ پروېشونې) ;جوړ کړئ :

$1 \cdot 7, \ldots, 6 \cdot 7$

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 ګنون یا 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 –یا څلوریپاتې $\bmod 13$ نه دی.

د $\left(\frac{q}{p}\right)$ شمیرنه:

د $\left(\frac{q}{p}\right)$ شمیرنې ته، د له ۲ لوي p, q مختلفو لومړنیو ګنونو سره.

جمله $11 : 2 : 9$: p, q مختلف لومړني ګنونه دي، $p > 2$ ، نو باور لري:

1. $q = 2$:

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}, \tag{9.80}$$

2. $q > 2$:

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right]}. \tag{9.81}$$

دریم: ($[x]$ د x پسې کوچنی عدد یا ګڼ په نخښه کوي)

ښوونه: د 9.2.9 ښوونې ته ورته (ټاکو $a = q$) باور لري:

$$iq = pq_i + t_i \ (i = 1, \ldots, \frac{p-1}{2}),\ 0 < t_i < p, q_i = \left[\frac{iq}{p}\right]. \quad (9.82)$$

جوړ کړی:

$$\sum_{i=1}^{\frac{p-1}{2}} iq = \sum_{i=1}^{\frac{p-1}{2}} (pq_i + t_i) = p\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right] + \sum_{i=1}^{\frac{p-1}{2}} t_i, \quad (9.83)$$

له دې سره:

$$q \cdot \underbrace{\sum_{i=1}^{\frac{p-1}{2}} i}_{=\frac{1}{2}(\frac{p-1}{2})(\frac{p-1}{2})} = q\frac{p^2-1}{8} = p\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right] + \sum_{i=1}^{n(q)} r_i + \sum_{i=1}^{k} s_i \quad (9.84)$$

($r_i \ldots$ پاتې (باقي) $> \frac{p}{2}$ ، $s_i \ldots$ پاتې $\leq \frac{p}{2}$). د 9.2.9 ښوونې له مخې باور لري:

$$\left\{1, 2, \ldots, \frac{p-1}{2}\right\} = \{p - r_1, \ldots, p - r_{n(q)}, s_1, \ldots, s_k\}; \quad (9.85)$$

نو باور لري:

$$\frac{p^2-1}{8}=\sum_{i=1}^{\frac{p-1}{2}} i=\sum_{i=1}^{n(q)}(p-r_i)+\sum_{i=1}^{k} s_i=p\cdot n(q)-\sum_{i=1}^{n(q)} r_i+\sum_{i} \quad (9.86)$$

د (9.64) او (9.66) کمون(تفريق) له لاري:

$$(q-1)\frac{p^2-1}{8}=p\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]-p\cdot n(q)+2\sum_{i=1}^{n(q)} r_i. \quad (9.87)$$

له دي سره $\mathbf{mod\,2}$:

$$(q-1)\frac{p^2-1}{8}\equiv\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]-n(q)(2). \quad (9.88)$$

- كه $q>2$ وي، نو q ناجوړه(طاق) دی، يعني $q-1$ جوړه(جفت)، نو $q-1\equiv 0(2)$. له دي سره:

$$0\equiv\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]-n(q)(2)\Rightarrow n(q)\equiv\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right](2). \quad (9.89)$$

- د 9.2.9 له مخي لرو يا لاس ته راځي:

$$\left(\frac{q}{p}\right)=(-1)^{n(q)}=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]}. \quad (9.90)$$

- که $q=2$ وي، نو $q-1=1$ ، او د $1 \leq i \leq \frac{p-1}{2}$ لپاره باور لري:

$$0<\frac{2}{p} \leq \frac{2i}{p} \leq \frac{p-1}{p}<1, \tag{9.91}$$

- نو $\left[\frac{2i}{p}\right]=0$ د $1 \leq i \leq \frac{p-1}{2}$ لپاره ، له دي سره پاتيږي

$$\frac{p^2-1}{8} \equiv -n(q)(2) \Rightarrow n(q) \equiv \frac{p^2-1}{8}(2). \tag{9.92}$$

د 9.2.9 له مخي لاس ته راځي:

$$\left(\frac{2}{p}\right)=(-1)^{n(q)}=(-1)^{\frac{p^2-1}{8}}. \tag{9.93}$$

جمله ګوتې 9.2.12 : وي دي $p>2$ يو لومړني ګڼ، نو باور لري: 2 تيک څلورئ پاتې يا مربع باقي ده، که $p=8k \pm 1(k \in \mathbb{Z})$ وي .

ښوونه: 2 څلورئ پاتې

$$\mathrm{mod}\, p \;\Leftrightarrow\; \left(\frac{2}{p}\right)=1 \tag{9.94}$$

$$\overset{9.2.11}{\Leftrightarrow} (-1)^{\frac{p^2-1}{8}}=1 \tag{9.95}$$

$$\Leftrightarrow \quad \frac{p^2-1}{8} \tag{9.96}$$

جوړه دی

$$\Leftrightarrow \quad \frac{p^2-1}{8} = 2n \qquad n \in \mathbb{N} \tag{9.97}$$

$$\Leftrightarrow \quad p^2 - 1 = 16n. \tag{9.98}$$

د $p > 2$ لومړنی کې $\mod 8$ لاندې بڼه لري

$$8k \pm 1, 8k \pm 2, 8k \pm 3, 8k \pm 4 \tag{9.99}$$

$p > 2$ لومړنی کې $\Rightarrow p$ ناجوړه کې $\Rightarrow 8k \pm 1, 8k \pm 3$

که وی $p = 8k \pm 3 \Rightarrow$

$$p^2 - 1 = 64k^2 \pm 48k + 9 - 1 \equiv 8(16) \not\equiv 0(16), \tag{9.100}$$

$p^2 - 1 \neq 16n$ تضاد یا په څټوالي

دا په دې معنا، چې

په څټ یا برعکس:

$$p = 8k \pm 1 \Rightarrow p^2 - 1 = 64k^2 \pm 16k + 1 - 1 \equiv 0(16), \quad (9.101)$$

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 څلورې – یا مربع ریځیپروسیټي قانون
reciprocity law

جمله 9.2.13 : (مربع ریځیپروخیتي): 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 ټیک $\frac{p-1}{2}\frac{p-1}{2}$ توکي لري. راوړو

$$M_1 = \{(i,j) \in M \mid qi > pj\}, \quad (9.105)$$

$$M_2 = \{(i,j) \in M \mid qi < pj\}. \quad (9.106)$$

باور لري $qi = pj$ ، لاس ته راځي $p \mid qi$ ، يعني $p \mid i \ (\mathrm{ggT}(p,q) = 1)$ -
تضاد یا مخمخوالی و $1 < i \leq \frac{p-1}{2} < p$ ته. له دې سره:

$$M = M_1 \cup M_2, M_1 \cap M_2 = \emptyset. \tag{9.107}$$

وښایی:

$$M_1 = \left\{ (i,j) \in \mathbb{N} \times \mathbb{N} \middle| 1 \leq i \leq \frac{p-1}{2}, 1 \leq j < \frac{qi}{p} \right\}, \tag{9.108}$$

$$M_2 = \left\{ (i,j) \in \mathbb{N} \times \mathbb{N} \middle| 1 \leq i < \frac{pj}{q}, 1 \leq j \leq \frac{q-1}{2} \right\}. \tag{9.109}$$

- د M_1 لپاره: د هر څه د مخه یا 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 یا برعکس: $\{\dots\} \subseteq M_1$ ، ځکه چې

$$1 \leq i \leq \frac{p-1}{2}, 1 \leq j < \frac{qi}{p} \Rightarrow \frac{qi}{p} \leq \frac{q}{p}\frac{p-1}{2} - \frac{q}{2}\frac{p-1}{p} < \frac{q}{2} \tag{9.111}$$

$$\Rightarrow \left[\frac{qi}{p}\right] \leq \left[\frac{q}{2}\right] \leq \frac{q-1}{2}, \tag{9.112}$$

$$1 \le j < \frac{qi}{p} \Rightarrow 1 \le j \le \left[\frac{qi}{p}\right] \le \frac{q-1}{2}, \qquad (9.113)$$

- دا په دې معنا، چې $(i,j) \in M$. بالاخره: $(i,j) \in M_1$ ، ځکه چې

$$1 \le j < \frac{qi}{p} \Rightarrow pj < qi. \qquad (9.114)$$

- 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)

توکي لري. د 9.2.11 له مخي باور لري:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{qi}{p}\right]}(-1)^{\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{pj}{q}\right]}=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{qi}{p}\right]+\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{pj}{q}\right]}= \quad (9.11$$

$$=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \quad (9.11$$

جمله کی 9.2.14 : p,q مختلف >2 لومړني ګڼونه يا اعداد دي، نو باور لري

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right) \quad (9.120)$$

ټيک هلته، که $p\equiv 1(4)$ يا $q\equiv 1(4)$ يا دواړه وي.

ښوونه: د 9.2.13 له مخي يا پسي:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \quad (9.121)$$

د $\left(\frac{q}{p}\right)=\pm 1$ سره د ضرب له لارې لاس ته راوړو:

$$\left.\begin{array}{rrrr}\left(\frac{q}{p}\right)= & 1\Rightarrow & \left(\frac{p}{q}\right) & =(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)\\ \left(\frac{q}{p}\right)= & -1\Rightarrow & \left(\frac{p}{q}\right)(-1)^2 & =(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)\end{array}\right\}\Rightarrow\left(\frac{p}{q}\right) \quad (9.122)$$

له دې سره:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p} \Leftrightarrow (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2}\frac{q-1}{2}\right. \quad (9.123)$$

جوړه

$$\Leftrightarrow \frac{p-1}{2} \vee \frac{q-1}{2} \quad (9.124)$$

یا دواړه جوړه دي

$$\Leftrightarrow \frac{p-1}{2} = 2n \vee \frac{q-1}{2} = 2m \Leftrightarrow p-1 = 4n, q- \quad (9.125)$$

$$\Leftrightarrow p \equiv 1(4) \vee q \equiv 1(4) \vee \quad (9.126)$$

.دواړه

بیلګه 9.2.15 : ایا $a = -21$ څلورې پاتې یا مربع باقي $\mathbf{mod}\,\mathbf{61}$ دي؟

$x^2 \equiv -21(61)$ اوبیوړ یا حلوړ دی؟)

(دا په دې معنا چې

$p = 61 \in \mathbb{P}, \mathrm{ggT}(-21, 61) = 1$

له دې سره میژندر:

$$\left(\frac{-21}{61} = \left(\frac{(-1)\cdot 3\cdot 7}{61}\right) \overset{9.2.5}{=} \left(\frac{-1}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right) \overset{9.2.7}{=} 1\left(\frac{3}{6}\right.\right. \quad (9.127)$$

$$\overset{9.2.1}{=} \left(\frac{61}{3}\right)\left(\frac{7}{61}\right) \overset{Red.}{=} \left(\frac{1}{3}\right)\left(\frac{7}{61}\right) = 1\left(\frac{7}{61}\right) = \left(\frac{7}{61}\right) \quad (9.128)$$

$$\overset{Red.}{=} \left(\frac{5}{7}\right) \overset{9.2.14}{=} \left(\frac{7}{5}\right) \overset{Red.}{=} \left(\frac{2}{5}\right) \overset{9.2.12}{=} -1 \qquad (9.129)$$

$\Rightarrow -21$ څلوری پاتې $\bmod 61$ 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 دي $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ د m په لومړنیو ضریبونو یا ځله وونو ټوټه کیدنه.نو باور لري:

a مربع بقي $\bmod m \ldots$ دی.

$$\ldots \Leftrightarrow x^2 \equiv a(m) \qquad (9.130)$$

$$\Leftrightarrow x^2 \equiv a(p_i^{\alpha_i}) \quad i = 1, \ldots, k \qquad (9.131)$$

$$\overset{9.1.5}{\Leftrightarrow} x^2 \equiv a(p_i) \quad i = 1, \ldots, k \qquad (9.132)$$

$$\Leftrightarrow a \text{ څلوری پاتې } \bmod p_i \quad i = 1, \ldots, k \qquad (9.133)$$

$$\Leftrightarrow \left(\frac{a}{p_i}\right) = 1 \quad i = 1, \ldots, k. \qquad (9.134)$$

جاکوبي سومبول Jacobi-Symbol

په لاندې کې د $x^2 \equiv a(m)$ د اوبی یا حل د پرېکړې لپاره یو بل امکان څېړو، مګر د لږ واړه بندیز سره:

پیژند 9.3.1: (جاکوب[9.2] سومبول): m دې یو ناجوړه طبیعي ګڼ وي، چیرته چې $m = p_1 \cdots p_k$ نه اړین مختلف طبیعي لومړني ګڼونه دي. $p_1, \ldots, p_k$ دی د $a \in \mathbb{Z}$ سره، نو څلوری –یامربع باقي د جاکوب له مخې په $\mathrm{ggT}(a, m) = 1$ لاندې توګه تعریف دی

(9.135)	$\left(\frac{a}{m}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)_L$

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:

(9.136)	$\left(\frac{a}{m}\right) := \left(\frac{a}{|m|}\right).$

دا موږ نه پریږدو، د دې لارې لاندې تري لاس ته راتلنه په روښانه توګه ساده لاس ته راوړل کیږي.

یادونه 9.3.3

لومړی . $m \in \mathbb{N}$ جوړه دی، نو نو د $x^2 \equiv a(m)$ اوبیوړوالي – یا د حلوړوالی پرابلم په یوه ناجوړه مودل بیرته اړوو، ځکه چې: $m = 2^{\alpha}n$ د ناجوړه n سره(تل شونی دی)، نو باور لري :

(9.137)	$x^2 \equiv a(m) \quad \Leftrightarrow x^2 \equiv a(2^{\alpha}) \qquad x^2 \equiv a(n)$ او

دویم. دلته $x^2 \equiv a(2^{\alpha})$ له 9.1.6 سره پای شو او n ناجوړه دي

دریم: د پیژند یا تعریف له مخې دی

(9.138)	$\left(\frac{a}{m}\right)_J = \pm 1, \qquad \left(\frac{a}{p_i}\right)_L = \pm 1.$ ځکه چې

ځلورم: $\left(\frac{a}{m}\right)_J = -1$ دی، نو a ځلورې پاتې یا مربع باقي $\bmod m$ نه ده، ځکه چې د تعریف له مخې:

(9.139)	$-1 = \left(\frac{a}{m}\right)_J = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)_L,$

پنځم: ینې لږ تر لږه $\left(\frac{a}{p_i}\right)_L = -1$ یو دی، دا په دې معنا، چې د دې i لپاره a ځلورې پاتې $\bmod p_i$ نه دی. له دې سره a هم مربع باقي $\bmod m$ نه دی.

$$\left(x_0^2 \equiv a(m) \overset{p_i|m}{\Rightarrow} x_0^2 \equiv a(p_i)\right)$$

شپږم: $\left(\frac{a}{p_i}\right)_L = -1$ دی، نو a نه اړیین یو مربع باقي $\bmod p_i$ دی(کیدی شي وي، مګر باید نه دی، چې وي).

بیلګه : $\left(\frac{2}{15}\right)$ جاکوبي- سومبل دی($15 \in \mathbb{N}$ ناجوړه(طاق) $(2,15) = 1$) ، د تعریف له مخي:

(9.140)	$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right),$

له دي سره د 9.2.12 له مخي باور لري: $\left(\frac{2}{3}\right) = -1$ ځکه چې $3 \neq 8k \pm 1, \left(\frac{2}{5}\right) = -1$ ځکه چې $5 \neq 8k \pm 1$.

یعني:

(9.141)	$\left(\frac{2}{15}\right) = (-1)(-1) = 1,$

مګر 2 مربع باقي $\bmod 15$ نه دی. له دې امله په لومړنیو ضریبونو تجزیه.....

لومړی: $a \equiv a'(m)$ دی، نو باور لري

$\left(\frac{a}{m}\right)_J = \left(\frac{a'}{m}\right)_J.$	(9.142)

دويم: جمله ګې 9.2.5 ته ورته د ليجندر-سومبول لپاره او هم د جاکوبي سومبول لپاره باور لري

$\left(\frac{ab}{m}\right)_J = \left(\frac{a}{m}\right)_J \left(\frac{b}{m}\right)_J.$	(9.143)

څلورم: پسې باور لري:

$\left(\frac{a}{m_1 m_2}\right)_J = \left(\frac{a}{m_1}\right)_J \left(\frac{a}{m_2}\right)_J.$	(9.144)

يادونه: که په راتلونکي کې 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، چې جا کوبي سومبول د ليجندر – سومبول ضرب دی.

ځانګړي حالتونه: $a = -1, a = 2$

ليجندر ته ورته: د $a = -1$ همداسې د $a = 2$ لپاره جاکوبي-سومبول را اخلو:

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)	$\frac{m^2-1}{8} \equiv \sum_{i=1}^{k} \frac{m_i^2 - 1}{8} (2).$

ثبوونه : 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 ثبوول کیږي.

$k \to k+1$:

وي دي $m = m_1 \cdots m_k m_{k+1} \in \mathbb{N}$ 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 تولیزه توګه دا ضرب په 4 وېشوړ دی

(9.147)	$(m_1 \cdots m_k - 1)(m_{k+1} - 1) =$

$= \underbrace{m_1 \cdots m_k m_{k+1}}_{=m} - m_1 \cdots m_k - m_{k+1} + 1;$	

له دي املې: $m-1 \equiv m_1 \cdots m_k - 1 + m_{k+1} - 1 (4)$ ، کيږي او ښي لور ته جوړه ګڼ ځای دی، د $\mathrm{ggT}(4,2) = 2$ له املې د (5)4.1.5 له مخې لاس ته راځي:

$\frac{m-1}{2} \equiv \frac{m_1 \cdots m_k - 1}{2} + \frac{m_{k+1}-1}{2} (2).$	(9.148)

د ايندکشن پسې لرو:

$\frac{m-1}{2} \equiv \sum_{i=1}^{k} \frac{m_i - 1}{2} + \frac{m_{k+1}-1}{2} = \sum_{i=1}^{k+1} \frac{m_i - 1}{2} (2).$	(9.149)

وښايي: که $a \in \mathbb{N}$ ناجوړه وي، نو $8 \mid a^2 - 1$ باور لري:

$a = 2t+1 \Rightarrow$	
$a^2 = 4t^2 + 4t + 1 = 4t(t+1) + 1$	(9.150)
$\Rightarrow a^2 - 1 = 4t(t+1),$	(9.151)

جيرته جې يا t يا $t+1$ جوړه دی، دا په دې معنا، چې ضريب يا ځله وونی 2 لري.
له دې سره باور لري

$8 \mid a^2 - 1 \left(\Rightarrow \frac{m_i^2 - 1}{8} \in \mathbb{N} \right).$	(9.152)

۱ - ایندکشن:

۲ - $k = 1$:

۳ – دلته هم نه ښوول کیږي

$k \to k+1$

:

۴ – وي دي $m = m_1 \cdots m_k m_{k+1} \in \mathbb{N}$ ، ناجوړه، نو ټول m_i ناجوړه دي او $m_1 \cdots m_k$ هم، نو

(9.153)	$8 \mid m_1^2 \cdots m_k^2 - 1 \quad 8 \mid m_{k+1}^2 - 1.$ او

$m_1^2 \cdots m_k^2 - 1 \equiv 0(8), m_{k+1}^2 - 1 \equiv 0(8)$

۵ – له دي سره ، يعني د 4.1.5 له مخي

(9.154)	$(m_1^2 \cdots m_k^2 - 1)(m_{k+1}^2 - 1) \equiv 0(64).$

۶ - دا په دي 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

(9.155)	$m_1^2 \cdots m_k^2 m_{k+1}^2 - 1 \equiv m_1^2 \cdots m_k^2 - 1 + m_{k+1}^2 - 1(64),$

۷ – نو:

(9.156)	$\frac{m^2-1}{8} \equiv \frac{m_1^2 \cdots m_k^2 - 1}{8} + \frac{m_{k+1}^2 - 1}{8}(8),$

۸ – دا په دې معنا، چې د ایندکشن له مخې:

$\frac{m^2-1}{8} \equiv \sum_{i=1}^{k} \frac{m_i^2-1}{8} + \frac{m_{k+1}^2-1}{8} = \sum_{i=1}^{k+1} \frac{m_i^2-1}{8}(8).$	(9.157)

د دې پربکړې لپاره چې ایا -1 یا 2 څلورې پاتې (مربعباقي) دی که نه:

جمله : وي دي $m \in \mathbb{N}$ ناجوړه، نو باور لري:

۱ – $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}},$	(9.158)
۲ – $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$	(9.158)

ښوونه: وي دي $m = p_1 \cdots p_k$ ناجوړه، $p_i \in \mathbb{P}$، ټول p_i ناجوړه، یعنې > 2

۱ -

$\left(\frac{-1}{m}\right) \overset{Def.}{=} \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right)_L \overset{9.2.7}{=} \prod_{i=1}^{k} (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^{k} \frac{p_i-1}{2}}.$	(9.160)

۲ – دا چې د(1)9.3.5 له مخې باور لري:

$\sum_{i=1}^{k}\frac{p_i-1}{2}\equiv\frac{m-1}{2}(2)\Rightarrow\sum_{i=1}^{k}\frac{p_i-1}{2}=\frac{m-1}{2}+2t\ (t\in\mathbb{N}),$	(9.161)

۳ – 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 –

$\left(\frac{2}{m}\right)\overset{Def.}{=}$	(9.163)
$\prod_{i=1}^{k}\left(\frac{2}{p_i}\right)_L\overset{9.2.11}{=}\prod_{i=1}^{k}(-1)^{\frac{p_i^2-1}{8}}=(-1)^{\sum_{i=1}^{k}\frac{p_i^2-1}{8}}\overset{9.3.5(2)}{=}$	
$\overset{9.3.5(2)}{=}(-1)^{\sum_{i=1}^{k}\frac{m^2-1}{8}}.$	(9.164)

د جاکوبي-سومبول لپاره څلورې – یا مربع رڅیپروسیتي قانون

لیجندر- سومبول ته ورته د جاکوبپ-سومبول لپاره هم مربع ریڅیپروڅیتي قانون) باور لري:

جمله : (مربع رڅیپروڅیتي قانون) وې دي $m,n\in\mathbb{N}$ د ناجوړه(طاق) $\mathrm{ggT}(m,n)=1,m,n$ (خورا غټ ګډ پروېشونی) سره، نو با ور لري:

$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$	(9.165)

ښوونه: وي دي $m=p_1\cdots p_k,\ p_i\in\mathbb{P}$ ، 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 املې 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:

$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)\ =$	

$$\prod_{j=1}^{s}\prod_{i=1}^{k}\left[\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right] \overset{9.2.13}{=} \prod_{j=1}^{s}\prod_{i=1}^{k}\left[(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}\right] = \tag{9.168}$$

$$= (-1)^{\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right)}. \tag{9.169}$$

دا چې باور لري:

$$\sum_{i=1}^{k}\frac{p_i-1}{2} \equiv \frac{m-1}{2}(2), \tag{9.170}$$

او

$$\sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{n-1}{2}(2)$$

پسې لاس ته راځي

$$\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right) \overset{9.3.5(1)}{=}$$

$$\left(\frac{m-1}{2}+2t\right)\left(\frac{n-1}{2}+2n\right) = \tag{9.168}$$

$$= \frac{m-1}{2}\frac{n-1}{2}+2v. \tag{9.169}$$

له دې سره په تولیزه توګه باور لري:

$(-1)^{\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{r_j-1}{2}\right)}=(-1)^{\frac{m-1}{2}\frac{n-1}{2}+2v}=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$	(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 تري لاس ته راځي:

		$\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)\quad\Leftrightarrow$
(9.176)	جوړه(جفت)	$(-1)^{\frac{m-1}{2}\frac{n-1}{2}}=1\Leftrightarrow\frac{m-1}{2}\frac{n-1}{2}$
(9.177)	جوړه	$\Leftrightarrow\frac{m-1}{2}\vee\frac{n-1}{2}$

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 :

۱ - $x^2 \equiv -8(15)$ ابیوړ یا حل وړ دی؟

(دا په دې معنا، چې $a = -8$ مربعپاتې $\mathrm{mod}\,15$ دی؟)

$$m = -8 < 0, n = 15 \notin \mathbb{P}, \mathrm{ggT}(-8, 15) = 1, 15$$

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)
$(-1)\cdot 1\cdot 1 = -1$	(9.179)

۲ – (لرو چې) $\Rightarrow -8$ مربع باقي $\mathrm{mod}\,15$ نه دی.

۳ – $x^2 \equiv 59(125)$ اوبیوړ یا حلوړ دی؟

$\mathrm{ggT}(59, 125) = \mathbf{1}, a \in \mathbb{Z}, m \in \mathbb{N}$

، دواړه ناجوړه، جاکوبي:

$\left(\frac{59}{125}\right)_J \overset{9.3.7}{=}$	

$\left(\frac{125}{59}\right) \overset{Red.}{=} \left(\frac{7}{59}\right) \overset{9.3.7}{=} -\left(\frac{59}{7}\right) \overset{Red.}{=} -\left(\frac{3}{7}\right) \overset{9.3.7}{=} \left(\frac{7}{3}\right) =$	(9.180)
$= \left(\frac{1}{3}\right) = 1 \ldots$ وینا نه شته	(9.180)

۴ – مګر(تل کیږي:) $m = 125 = 5^3$، یعني $p_1 = 5$ ، وشمیره:

$\left(\frac{59}{5}\right)_L = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$	(9.182)

۵ - $59 \overset{9.1.5}{\Rightarrow}$ مربع باقي $\bmod 125$ دي.

۶ – ایا $x^2 \equiv 15(67)$ اوبیوړ یا حلوړ دی؟ (دا په دې معنا، چې $a = 15$ څلورۍ – یا 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 $\left(\frac{15}{67}\right)$ یو لیجندر – سومبول دی، لاس ته رځي: 15 مربع باقي $\bmod 67$ دی.

۷ – ایا $x^2 \equiv 67(77)$ اوبیوړ دی؟

نسبي لومړنی، ناجوړه، $77 \notin \mathbb{P} \Rightarrow$ لاس ته راځي جاکوبي $77 \notin \mathbb{P} \Rightarrow$

$$\left(\frac{67}{77}\right) \overset{9.3.7}{=} \left(\frac{77}{67}\right)(-1)^{gerade} = \left(\frac{77}{67}\right) \overset{Red.}{=} \left(\frac{10}{67}\right). \tag{9.184}$$

$\notin \mathbb{P} \Rightarrow$ ۸ - جوړه دی،

نه 9.2.13او نه 9.3.7 استعماوړ د کاروني وړ دی! له دې لاس ته راځي:

په لومړنیو ګنونو توټه کونه:

$$\left(\frac{10}{67}\right)_L = \left(\frac{2}{67}\right)\left(\frac{5}{67}\right) = (-1)(-1) = 1\ldots \tag{9.185}$$

وینا نه ده!

$$\left(\frac{2}{67}\right)_L \overset{9.2.12}{=} -1, \tag{9.186}$$

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

$$5 \not\equiv \pm 1(8). \tag{9.187}$$

۹ - مګر د پیژند له مخې:

$$\left(\frac{67}{77}\right) = \left(\frac{67}{7}\right)\left(\frac{67}{11}\right) = \left(\frac{4}{7}\right)\left(\frac{1}{11}\right) = 1 \cdot 1. \tag{9.188}$$

۱۰ – دا چې دواړه (!) لیجندر – سومبولونه برابر 1 دي، لاس ته راځي، چې 67 مربع باقي $\bmod 77$ دی.

د ډاکتر ماخان شینواري چاپ شوې لیکنې:

1988 Vienna (Austria):

لومړی:

H.K. Kaiser , M. Shinwari : Aproximation compact pological algebra : general algebra 6 ; Page 117 – 122 contributions to

1987 Vienna (Austria):

دویم:

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 شمیرپوهنې پښتوټول کتابونه په المان کې د ،، افغانستان کلتوري ودې ټولنه،،له خوا چاپ شوي دي

2000 Bonn (Germany):

دریم: د شمیرپوهنې ستر کتاب : د شمیرپوهنې برسیره د انجنري، فزیک او اقتصاد لپاره ، همداسې د ښوونکو او زده کوونکو لپاره (دا کتاب په ۹۰۰ مخونو کې چاپ او دا نوې لیکنه به یې ځنو ځایونو غزېدلې او ځنې ځایونه تري لرې شوي دي)

2003 Bonn (Germany):

څلورم: ځمککچپوهنه(هندسه) ، په سلو، زرو کې شمیرنه، د ګټې – او کټې د کټې شمیرنه ، د اختمالوالي شمېرنه کتاب د ښوونځي ټولې اړتیاوې پوره کوي

2003 Bonn (Germany):

پنځم: الجبرونه (د الجبر بنسټونه دي)

2003 Bonn (Germany):

شپږم: د شمیرپوهنې انګریزي – پښتو ډکشنري.

2003 Bonn (Germany):

اووم: د شمیرپوهنې المانې - پښتو- او پښتو المانې ډکشنري

Mathematical dictionary German/ Pashto and Pashto/German

2003 Bonn (Germany):

اتم: دفرنځیال برابرون (دا کتاب په دې څانګه کې یو پیل دی، ساده لیکل شوی)

Differential equation Translation; An Introduction

Bonn (Germany): 2003

نهم: د شمیر پوهنې فرمولونو ټولګه

Mathematical Formulas

2003 Bonn (Germany):

لسم: شمیرپوهنه له عربي په پښتو

1997 Bonn (Germany):

یوولسم: د افغانستان په هکله سپینې خبرې: په المان کې

،،د افغانستان روغې او بیا ابادولو ټولنه،، له خو

یادونه: له ۲۰۰۰ کال دمخه ډاکتر ماخان شینواري د ،،د افغانستان روغې او بیا ابادولو ټولنه،، له خوا دري ساسي مجلې هم را وستلې.

د ډاکتر ماخان ،،میرې،، شینواري لیکنې او ژباړې چې په چاپیدو یې پیل کیږي

2012 Bonn; Germany; Kabul Afghanistan

ژباړې:

: *Prof. Brinkmann. (From Brinkmann.du.de)*

لاندې د برینکمن لیکنې چې له پرینکمن ن ج څخه ژباړل شوي دي.

۱ - شمیرپوهنه د ښوونځي لپاره لومړی ټوک

۲ – شمیرپوهنه د ښوونځي لپاره دویم ټوک

۳ – شمیرپوهنه د ښوونځي لپاره دریم ټوک

۴ - د احتمالوالي شمیرنه د ښوونځي لپاره

۵ – احصایه یا ستاتیستیک 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 – انالیزی ۱

۷ – انالیزې ۲

۸ – کرښیز الجبر

۹ - د شمیرپوهنې بنسټونه

۱۰ - د فرمولونو ټولګه

۱۱ – فنکشنل انالیز

۱۲ – وکتور شمیرنه

نورې ژباړې

۱۳ – له www./grundstudium.info/linearealgebra څخه:کرښیز الجبر

۱۴ – Georg Gutenbrunner ګټونپوهنه 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 - ډېرې پوهنه یا ست 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.

نوري لیکنې، چې په ژباړه یې پیل شوی، خو لا پوره نه دي

– د شتوتکارت پوهنتون لکچرنوټونو څخه ، چې د شتوتګارت پوهنتون ن ج څخه خپریږي:

د ګروپونو تیوري

- د ښوونځي لپاره فزیک د برینکمن لیکنه

له پنځم ټولګي څخه تر اووم ټولګي پورې ژباړل شوی (دا چې زما دویم مسلک فزیک دی، دا لیکنې ژباړم. دا هم د دې لیکوال یوه ډېره ښه لیکنه ده، چې -د شمیرپوهنې په څیر- دلته هم زیات تمرینونه د حل یا اوښیونې سره په کې راغلي او ماته زیات ګټور برېښي)

د لیکوال ژوند ته لنډه کتنه

ماخان په اولني نوم میرې شینواری د اروابنادې پستو او اروابناد نوررحمان زوي په ۱۳۲۰ ؟ ه لمریز کې د شینوارو هسکه مینه کې دې نړۍ ته سترګې راغړولي.

د هسکې مینې د لومړنې ښوونځي (د لومړنیو زده کوونکو څخه) څخه وروسته د رمحمان بابا لیسه له ۱۹۵۴ تر ۱۹۶۵ پورې(ښوونځي له لومړي ټولګي پیل او د دویم ټولګي څخه ګام 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 جرمنې کې سیاسي پناه. له ۲۰۰۸ مارچ څخه د ۲۰۰۹ دسمبر پورې د د ریاضي څانګه کې د پوهنې وزارت درسي نساب کې دنده.

ماخان میرې 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 څانګه او اباسین نومیږي. څانګه په المان کې د پوهنتون علمي همکاره وه او د حقوقو ډاکتره ده او اباسین ملي اقتصاد او ټولنیزه سایکولوژي لوستلي.