

گنونیو هنه

(د اعداد تیوری)

Nummbertheory

$$k = n \pmod{m}$$

smakhan1946@gmail.com

Ketabton.com

لیکونیکی: جورج کوننبرویر

ژبیری: ډاکتر ماخان (میری) شینواری

دلوي څښتن په نامه

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

کتاب پيژندنه

د کتاب نوم: گڼونپوهنه
ليکونکی: پروفیسور جورج گوتنبرونر
ژباړی: ډاکتر ماخان،، میری،، شینواری
د خپریدو لړی:
خپرندوی: د افغانستان کلتوري ودې ټولته
جرمني
چاپ کال: ۲۰۱۲
د ژباړې برېښنا پته: smakhan1946@gmail.com

چاپ چاري

چاپ ته يې د هر چمتو هیوادوال مرسته په سترگو منل کيږي

پښتو موږ به او شمیرپوهنه پرې ساده ده

د ژباړې مننه

نيوليک

- د ژباړي سرريزه
- د ليکونکي سرريزه
- ۱ - ... خويونه ۱
- د.. د ا کسيومونو سيستم ۱
- د طبيعي اعدادو خای انخورونه ۸
- ۲- په ... وپشوروالي ۱۴
- پروپشوني (مقسوم عليه) 3۱
- د اويکلید يا اقلیدس له مخي ټاکل ۱۸
- خورا غټ گډ پروپشوني ۲۸
- ۳ - لومړني گڼونه ۳۲
- نور خويونه ۳۸
- (د خ غ ک او خ ک گ زياتخلي - - ۴۲
- ۴ - کونگروانخ ۵۱
- د کونگروانخ سره شمېرته ۵۱
- د پروپشوروالي قوانين ۵۸
- پاتي ټولگي ۶۳

۶۷	د پاتي ټولگې کړی یا - رینګ
۷۵	۵ - الجبري کونګروانڅ
۷۵	د کرښيزو کونګروانڅو حلوروالی
۸۱	سیمولتان کونګروانت
۸۷	الجبري کونګروانت
۸۹	۶- د حلونوو عملي شمېرڼه
۹۸	د الجبري کونګرواینڅو دحلونو ګڼون یا تعداد
۱۰۱	- لومړني پاتي ټولګي کروپونه
۱۰۱	د ابل ګروپ
۱۰۳	د $\varphi(m)$ شمېرڼي ته
۱۱۰	د اوپلر جمله
۱۱۶	د (\mathbb{Z}_m^*, \cdot) جوړښت
۱۲۶	د حقيقي اعدادو g - اديکي وديزيڼه
۱۲۶	ټولزه وديزيڼه
۱۳۳	کله $\alpha \in \mathbb{Q}^+$ دوه g - اديکي انځورونه لري؟
۱۳۵	کوم $\alpha \in \mathbb{Q}^+$ یوه پای g - اديکي انځورونه لري؟

- ۱۳۸ پریودیکی وده
- ۱۴۵ خأنگری حالت: سوچه پریودیکی وده
- ۱۴۹ تولیز حالت: نه سوچه - پریودیکی وده
- ۱۵۰ ۸ - N-م توان
- ۱۵۰ په خأنگری حالت بیرته اړول
- ۱۵۳ د... د حل لپاره تگلار
- ۱۵۸ د حل ساده متودونه
- ۱۵۸ خأنگری حالت
- ۱۶۵ د $x^n \equiv a(2^k), k \geq 3$ لپاره د حل متودونه
- ۱۶۹ خلوریز پاتی (که غواری: مربع باقیمانده)
- ۱۶۹ خأنگری حالت
- ۱۷۴ خلوریز پاتی (که غواری: مربع باقیمانده)
- ۱۷۴ خأنگری حالت
- ۱۷۹ لژندر-سومبول
- ۱۸۰ ساده خوږونه:
- ۱۸۶ د گاوس لیما یا جملگی
- ۱۹۶ Legendre-Symbo لپاره د خلوری - یا ...
- ۲۰۱ جاکوبی سومبول
- ۲۰۵ خأنگری حالتونه

د ژباړې سریزه

گرانو لوستونکو!

د لیکونکي سریزه راوړل شوي هلته اړین څه شته دی، خو زه غواړم دومره یادونه وکړم، چې گڼوښوونه یا د اعدو تیوري یو له بنسټیزو درسونو څخه گڼل کیږي، چې ما یې ډېر وخت د یوې داسې لیکني لټه کوله. ښه دی، دا می یو ډېرښه سکریپت پیدا کړ او بیا دا د ویانا د پوهنتون هم دی، چې ما هلته درس ویلی. دا په گوته کوم، چې د ویانا پوهنتون کې ډېر ښه او مشهور گڼوښووهان تیر شوي او لا هم شته.

دا ما له دې امله هم اړینه وبلله، چې زما په اند دا درس د افغانستان پوهنتونونو کې نه شته. هیله ده، چې دابه د گرانو هیوادوالو په گټه وځوري.

په دې هیله هم، چې گڼوښوونه به دپه درسي پروگرام کې خوندي شي.

ستاسو ماخان

سریزه:

په هغه وخت کې گاوس گڼونپوهنه یا د عددونو تیوري د ماتماتیک د ملکې (پاچاګۍ) په نوم ونوموله. د دې لپاره چې د شمیرپوهنې په دې ساحې بڼه وپوهیږو، مختلفې پیلونې – همداسې مخ ته تللي لکچرونه وړاندې کيږي.

گڼونتیوري د ډېرو داسې ساده برېښیدونکو پرابلمونو، بڼوونه او یا د هغوي تضاد تر څیرني 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 گڼونپوهنې دې خویونو یو د شمیر پوهنې تیوري ودې خورا ستر د تغذیې ورشو وموندله، چې د خپل دسختیلین ډپولي زیاته ور اخواته رسیدونکې ده. په دې اړوند دې دا هم په گوته شوې وي، چې د ساده پرابلمونو یو ډکې (حجم) شتون لري، د کومې له مخې چې هر څوک په خوښه ازمايلي شي ([Guy94] وگورئ).

، د گڼونتیوري یوه غټه معنا، چې د دې ساحې یا ورشو د یوه قهرمان څخه نږدې ۳۰۰ نا روښانه کلونو وروسته حل شوې: د فرمات Fermat گومان چې په بڼه 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 او ریچارد تیلور جملې څخه په سختی لیدل کيږي، بیا هم گڼونپوهنه 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 گڼونو ته اړتیا پېښيږي.

په ۶/۳ برخه کې لنډې پرابلم ته پام شوی دی، د گڼونپوهنې د بنسټیز د استعمالووالي دې دلته انتظار نه کيږي، ځکه چې بنسټیزه تیوري، نه مګر د هغې استعمال د دې سکریپت په ککره کې ځای لري. علاقمند لوستونکی دې په دې هکله نورو د گڼونتیوري 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 بڼه خو ده، چې د الجبري جوړښت او کلیمو سره بلدتیا شتون ولري. لکچر پروفیسر میچ او اړونده تمرینونه یې ډاکتر شویزنگایر مخ ته بیول. دا سکریپت د لکچر په لیکنو ولاړ دی او د تکمیل ادعا نه کوي.

جورج گوتنبرونر اپریل ۲۰۰۲

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

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::

$$a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Z} \text{ اسوځياتيو قانون}$$

ب-

$$\exists 0 \in \mathbb{Z} (, Null) : a + 0 = 0 + a = a \quad \forall a \in \mathbb{Z} \text{ (بي اغيزه يا ناپيلی توکی)}$$

پ -

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

ت -

$$a + b = b + a \quad \forall a, b \in \mathbb{Z} \text{ (کموټاتيو يا د بدلېدو قانون)}$$

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

الف-

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

ب -

ګڼونپوهنه

ناپېلی توکی) $(, , Ems)$ د $\exists 1 \in \mathbb{Z}, 1 \neq 0$ د $1 \cdot a = a \cdot 1 = a \forall a \in \mathbb{Z}$ (بی اغیزه یا

پ-

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

ت-

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

دریم: نسبت و نظم, \leq ته باور لري:

الف - $a \leq a \forall a \in \mathbb{Z}$ رفلکسیوي

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

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

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

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

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

څلوم- برخدېری $\mathbb{N} = \{a \in \mathbb{Z} \mid a > 0\}$ پوره منظمه ده، دا په دې معنا چې د \mathbb{N}

هره ناتش برخدېری 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 جمعی یا زیاتون د څلور خوینو لپاره $(\mathbb{Z}, +)$ یو ابل ګروپ

جوړوي، د ضرب د خوینو سره په ګډه د $(\mathbb{Z}, +, \cdot)$ سره په اړوند د یوه

ګموتاتیو رینګ څخه غږیرو، د یوې (واحد) توکي سره.

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

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

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

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

ښوونه:

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

$$a \leq b \xrightarrow{3f} a \cdot (-c) \leq b \cdot (-c) \stackrel{UE}{=} -(ac) \leq -(bc) \xrightarrow{3e} (1.3)$$

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

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

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

کښونپوهنه

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

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

(\Leftarrow)

ښوونه:

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

(\Rightarrow)

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

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

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

د سره

لاس ته راوړنه ۱ . ۱ . ۵ : $\dots - 2 < -1 < 0 < 1 < 2 \dots$

جمله گۍ ۱ . ۱ . ۶ : د \mathbb{N} لپاره د اندکشن اصول باور لري، دا په دې معنا چې

$$\exists \emptyset \neq A \subseteq \mathbb{N} \quad \text{د لاندې سره:}$$

$$1 \in A$$

1.

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

نو باور لري $A = \mathbb{N}$.

ښوونه: وي دې $\emptyset \neq A \subseteq \mathbb{N}, A$ په خوښه دواړو خوښو سره ورکړ شوي، ښايي:

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

نیسو $A \neq \mathbb{N}$. راوړو .

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

له دې امله $T \neq \emptyset$. د اکسیم 4 له مخې T یو کوچنی توکی $n_0 \in T$ لري.. دی $n_0 \neq 1$ ، ځکه چې د A خوی 1 له مخې:

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

د 1.1.4 پسي $n_0 > 1$ لرو ، داسې چې د 3e پسي باور لري:

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

(د \mathbb{N} تعريف وگورئ) د

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

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

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

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

کینونپوهنه

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

بڼوونه: وي دي

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

وښايه: $M \neq \emptyset$

که $a \geq 0$ وي، نو دی

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

پس $n \in M$ ، که $a < 0$ وي، نو $0 < -a$ او له $a \leq b$ څخه د [3f](#) له مخې لاس ته راځي

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

دا په دې معنا، جي

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

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

د له مخې دا دېری یو کوچنی توکی r لري 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

$$0 \leq r. \text{ چیرته چې } a = b \cdot x_0 + r; \quad (1.22)$$

نور غواړو وښايو: $r < b$

نیسو $r \geq b$ (3d)، د 1.1.4 پسي $x_0 < x_0 + 1$ باور لري، له دې

سره $-(x_0 + 1) < -x_0$ ، د $b > 0$ له امله د 3f پسي لرو:

$$-(x_0 + 1)b < -x_0b \stackrel{3e}{\Rightarrow} a - (x_0 + 1)b < a - x_0b = r; \quad (1.23)$$

باور لري

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

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 گن یا عدد دی.

$$a = -42, b = 32 : 1.1.8 \text{ بېلگه}$$

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

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

د پښې یادونه:

... غوره 1.1

سری هم وایي، تر ایزومورفي پوري، .

د طبیعي ګڼونو یا - اعدادو خای انخورونه

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

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

جملگی 1.2.1 : وي دې $a \in \mathbb{N}, b \in \mathbb{N}, b \geq 2$ ، نو یواځنی ټاکلی ګڼ یا عدد $n \geq 0, a_i \in \mathbb{N}_0$ شتون لری د لاندې سره:

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

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

بنوونه:

شتون:

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

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

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

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

$$\vdots (1.29)$$

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

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

$$: i = 1$$

نيسو $q_1 < 0$ ، نو باور لري

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

- تضاد يا مخامخوالی!

$$: i \rightarrow i + 1$$

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

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

نو

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

- تضاد!

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

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

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

کینونپوهنه

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

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

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

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

یواځیوالی:

نیسو، چې دوه مختلفې انځورونې شتون لري. وي دې

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

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

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

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

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

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

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

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

د b سره لنډونې له لارې لاس ته راځي:

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

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

$$a_n b^{n-(m+1)} + \dots + a_{m+1} = 0 \quad (n \geq m) \quad (1.40)$$

که $n > m$ وي له $a_n > 0, b > 0 \Rightarrow$ سره وي، نو لاس ته تری راځي: کينه لور له صفر لويه ده، تضاد.

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

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

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

ګڼونپوهنه

که $b = 10$ وي، نو له دیکادیکي *dekadischen* یا لسميزي انځوروني غبریزو، د $b > 0$ سره له بینار یا دوه بیزي انځوروني غبریزو. که وي، نو سری لیکي $A = 10, B = 11, \dots$ (د دې لپاره چې له $1 \ 0$ څخه یې توپیر وکړای شو).

یادونه 1.2.3: د a ځای انځورونه نسبت $b \geq 2$ ته کېدی شي د 1.2.1 د بنووني په بنسټ و ټاکل شي 1.2.

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

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

$$q_2 = q_3 b + a_2 \quad 0 \leq a_2 < b \Rightarrow a_2 \quad \text{ټاکلی} \quad (1.44)$$

بېلګه 1.2.4: وي دې $a = 731, b = 10$ ، غوښتنه: د انځورونه $731 : 10 = 73 + 1$ ، نو

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

بېلګه 1.2.5: وي دې $a = 367, b = 2$ ، غوښتنه یا ثبوت: د بینار-یا دوه بیزه انځورونه $367 = 183 \cdot 2 + 1 = \dots$ سری داسې لیکي:

$$\begin{array}{c|c|c|c|c|c|c|c|c|c} 367 : 2 & 183 : 2 & 91 : 2 & 45 : 2 & 22 : 2 & 11 : 2 & 5 : 2 & 2 : 2 & 1 : 2 & 0 \\ \hline 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & \end{array}$$

ګڼونپوهنه

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

ازماښت:

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

په \mathbb{Z} کې توپه ونه \mathbb{Z} Teilbarkeit in \mathbb{Z}

لاندې برخه (خوړا غټ ګډ پروېشونى ggT)

- پروېشونى او $\text{ggT}(a, b)$ (مقسوم عليه او) يا

د اوکلید له مخې د ggT ټاکنه

د

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

خوړا غټ ګډ پروېشونى (بزرګترین مقسوم عليه مشترک)

Georg Gutenbrunner 2002-10-04

پروېشونى او خوړا غټ ګډ پروېشونى $\text{ggT}(a, b)$

پېژند(تعريف) 2.1.1 : وي دې $a \in \mathbb{Z}$ ، سړى وايي $b \in \mathbb{Z}$ وېشي، که د يوه

$$q \in \mathbb{Z} \text{ لپاره باور ولري } a = b \cdot q$$

ګڼونپوهنه

سومبولیک: $b \mid a$ ، b د a پروېشوني بلل کيږي، q د b پوره کېدونکي يا کمپلمنتار پروېشوني بلل کيږي. که b د a پروېشوني (مقسوم عليه) نه وي، نو لیکو $b \nmid a$.

د 1 پروېشوني د \mathbb{Z} یونونه يا واحدونه بلکيږي (دا فقط $\{1, -1\}$ دي).

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

لېما جمله ګوتي 2.1.3:

$$b \mid a \Rightarrow b \cdot c \mid a \cdot c \quad \forall c \in \mathbb{Z} \quad .1$$

$$bc \mid ac, c \neq 0 \Rightarrow b \mid a \quad .2$$

$$a \mid b, b \mid c \Rightarrow a \mid c \quad .3$$

$$a \mid b, b \neq 0 \Rightarrow |a| \leq |b| \quad .4$$

$$|a| = |b| \quad a \mid b, b \mid a \Rightarrow a = \pm b \quad .5$$

(also) (نو)

$$b \mid a_1, \dots, b \mid a_n \quad a_1, \dots, a_n, b \in \mathbb{Z} \quad .6$$

که $\forall c_1, \dots, c_n \in \mathbb{Z} :$ سره، نو باور لري

$$b \mid \sum_{i=1}^n c_i a_i \quad .(2.1)$$

بڼونه:

ad [4](#)

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

$$\text{نو } |q| \geq 1 \text{ او } |a| \cdot |q| \geq |a| \text{ هم } |b| = |a| \cdot |q| \geq |a| > 0 \text{ پرتله له دې } b = 0.$$

ad [5](#)

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

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

$$|a| \leq |b| \quad \text{او} \quad |b| \leq |a|, \text{ له دې سره } |a| = |b| \text{ دی، داپه دې معناچې } a = \pm b.$$

دی .

ad [6](#)

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

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

لاس ته راوړنه 2.1.4 : هر $a \in \mathbb{Z}, a \neq 0$ ، پای دېرې پروېشونې b لري، ځکه چې د(4) 2.1.3 پسي باور لري: ، نو $|b| \leq |a|$ ، له دې امله $-|a| \leq b \leq |a|$ ،

کڼونپوهنه

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

دا فقط پای ډېر دي.

$$0 = b \cdot 0 \quad \forall b \in \mathbb{Z}$$

مگر : $a = 0$ ټول گڼونه يا ټول عددونه د پروېشونو په څېر لري :
 ، دا په دې معنا چې a ناپای ډېر پروېشوني لري.

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

پروېشونو د ټاکلو له امله کېدی شي سړی ځان په هغه د $1 \leq b \leq \sqrt{a}$ سره رابند يا محدود کړي.

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

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

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

بېلگه 2.1.6 : $a = 80$ ، ټول پروېشوني غوښتونوي دي. د $\sqrt{80} < 9$ له امله ټول

زياتيز يا مثبت پروېشوني b دي د $1 \leq b \leq \sqrt{80} < 9$ سره وټاکل شي:

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

له دې سره ټول پروېشوني دي:

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

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

ياودونه 2.1.8 : که $a \in \mathbb{Z}, a \neq 0$ وي، نو a د 2.1.4 پسي يا له مخي فقط پای ډېر پروېشونى لري. که $b \in \mathbb{Z}$ په خوښه وي، نو a او b فقط پای ډېر پروېشونى لري. د اکسيوم 3d له مخي \mathbb{Z} توتالي (ټول يا بېخي) منظم دى، يعنى د a, b ګډ پروېشونى يو خورا لوي توکى دى. نو سړى کړى شي تعريف کړي:

پېژند يا تعريف 2.1.9 : (خورا غټ ګډ پروېشونى يا بزرګترين مقسوم عليه Greatest Common Divisor) وي دي $a, b \in \mathbb{Z}$ ، نه دواړه صفر، نو $\text{ggT}(a, b)$ (انګرېزي بې $\text{gcd}(a, b)$) د ټولو ګډ پروېشونو خورا لوى (يعنى تر ټولو لوي) دى . دا يواځنى ټاکلى دى. دى، که $\text{ggT}(a, b) = 1$ وي، نو نسبي لومړني يا پريم بلل کيږي يا پروېش پردې (ګډ اصلي پروېشونى نه لري).

ياودونه 2.1.10 : که $a, b \in \mathbb{Z}$ دواړه صفر نه وي. نو کېدى شي سړى د $\text{ggT}(a, b)$ ټاکلو لپاره په زياتيزو يا مثبتو ګډو پروېشونو ځنونه محدود کړي، ځکه چې 1 يو ګډ پروېشونى دى، يعنى باور لري:

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

بېلګه 2.1.11 : $a = 12, b = -8$

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

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

کنونپوهنه

د اویکلید یا اقلیدس له مخې د ggT ټاکنه

جمله 2.2.1 : د اویکلید الگوریتم (Euklidische [2.1](#) Algorithmus) وي دي

$a, b \in \mathbb{N}$ او بي له ټوليزو بندیزونو $b \leq a$. که $b \mid a$ وي، نو ردو $r_0 = b$ ،
 که $b \nmid a$ باور لري، ځکه چې که د وېش له لارې د پاتې سره $q_i, r_i \in \mathbb{Z}$ سری په
 لاندې توگه ټاکي:

$$a = q_0 b + r_1, \quad 0 \leq r_1 < b$$

$$b = q_1 r_1 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3, \quad 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{m-1} = q_m r_m + r_{m+1}, \quad 0 \leq r_{m+1} < r_m$$

$$\vdots$$

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

بڼوونه : که $b \mid a$ وي، نو باور لري

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

$$a = b \cdot q_0 + r_1 \quad \text{د لپاره.}$$

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

$$r_1 > r_2 > \dots > r_i > r_{i+1} > \dots \quad (2.7)$$

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

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

$$r_n = \text{ggT}(a, b) \quad \text{وښايی:}$$

• $r_n \mid a, b$: اخرنی مساوات يا برابرېون 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 $r_n \mid r_{n-1}, r_{n-2}$

کینونپوهنه

- که په ورته توگه مخ ته لار شو، نو ترې لاس ته راځي
 $r_n \mid r_2, r_n \mid r_1, r_n \mid b$ او له دې امله

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

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

t دې په خوښه یو د مثبت پروېشونی وي. نو د لومړي مساوات څخه لرو:

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

له 2 مساوات:

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

او همداسې پسي، تر

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

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

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

مور د a, b د مثبت پروېشونو پیدا کیدل غواړو (پام $\text{ggT}(a, b) \geq 1$).

بېلگه 2.2.3: $a = 97, b = -44$ ، نو باور لري: $|b| = 44 \leq 97 = a$ ، نو لاس ته راځي:

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

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

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

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

بېژند يا تعريف 2.2.4: (ګرښيز کمپوزېشن يا - يوځای اېښوونه): وي دي $a, b \in \mathbb{Z}$

، نو يو $c \in \mathbb{Z}$ د a, b ګرښيز کمپوزېشن بلل کيږي، که $c = xa + yb$ وي د $x, y \in \mathbb{Z}$ ځانګړو سره.

که $a, b \in \mathbb{Z}$ د c, d ګرښيز ښيز کمپوزېشنونه وي، په دي پسي $\alpha c + \beta d$ ، $\forall \alpha, \beta \in \mathbb{Z}$

هم ګرښيز کمپوزېشن دي..

جمله 2.2.5: (اوکلید) که وي $a, b \in \mathbb{Z}$ ، نه دواړه صفر، نو $\text{ggT}(a, b)$ د a, b :

$\text{ggT}(a, b) = xa + yb$ يو ګرښيز کمپوزېشن دي، د ټاکلو $x, y \in \mathbb{Z}$ لپاره.

ښوونه:

لومړی $b > 0$: نو $0 < b \leq a$ ، يعني $a, b \in \mathbb{N}$ ، داسي چي د اوکلید الګوريتم [2.2.1](#) سره باور لري:

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

دویم . له دې سره باور لري

$$r_{n-2} = q_{n-1}r_{n-1} + r_n, \dots, a = q_0b + r_1$$

$r_1 = a - q_0b,$ نو	$a, b \mid r_1$ دایه دې معنا چې کمپوزېشن دی
$\Rightarrow r_2 = b - q_1r_1,$	$a, b \mid r_2$ دایه دې معنا چې کمپوزېشن دی
$\dots \Rightarrow \underbrace{r_n}_{\text{ggT}(a,b)} = r_{n-2} - q_{n-1}r_{n-1},$	$a, b \mid r_n$ دایه دې معنا چې کمپوزېشن دی

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

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

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

$$-b > 0 \quad b < 0 \quad .3$$

دې او له ۱ . حالته باور لري نو :

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

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

□

یادونه 2.2.6: ښوونه بېرته جوړځتیزه ده، دا یو متود راګوي د $x, y \in \mathbb{Z}$ ټاکلو لپاره په $\text{ggT}(a, b) = xa + yb$ 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 د [2.2.1](#) 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 $\text{ggT}(a, b)$ د ټاکلو لپاره، که a او b د یوې اووښتونې یا متحولې په واک کې وي یا تابع وي. غواړو پیدا کړو:

کڼونپوهنه

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

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

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

(x, y داسې ټاکل سوي دي، چې له هغې سره اووښتونې يا متحوله لري کيږي، دا

زیات وخت ممکن دی، ځکه چې $\forall x, y \in \mathbb{Z} \quad d = xa + yb$ د .

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

که $d = 17$ وي، نو دا په دې معنا چې $17 \mid 2k - 1, 17 \mid 9k + 4$ ، يعني،

$$k = \frac{1}{2}(17t + 1) \quad t \in \mathbb{Z} \quad 2k - 1 = 17 \cdot t$$

د یوه لپاره، له دې امله .

له دې امله باید t ناجوره يا طاق وي (پرتله له دې $k \in \mathbb{Z}$ دی)، يعني $t = 2n - 1, n \in \mathbb{Z}$. 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 یوه $n \in \mathbb{Z}$ لپاره $k = 17n - 8$ وي، نو بلاور لري:

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

دا په دې معنا چې $17 \mid 2k - 1$.

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

دا په دې معنا چې $17 \mid 9k + 4$.

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 يا جملگی 2.2.9: وي دې $a, b \in \mathbb{Z}$ ، نه دواړه صفر، نو باور لري:

$$d = \text{ggT}(a, b) \Rightarrow \text{ggT}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \quad .1$$

$$\text{ggT}(a, b) = |t| \text{ د } \text{ggT}\left(\frac{a}{t}, \frac{b}{t}\right) = 1 \text{ سره، نو دى } t \mid a, t \mid b \quad .2$$

$$\text{ggT}(a \cdot m, b \cdot m) = |m| \cdot \text{ggT}(a, b) \text{ نو، } m \in \mathbb{Z}, m \neq 0 \quad .3$$

ښوونه: ad 1:

[2.2.5](#) له مخې باور لري: $d = xa + yb$ د ټاکلو $x, y \in \mathbb{Z}$ لپاره، يعنې $1 = x\frac{a}{d} + y\frac{b}{d}$ ($d \neq 0$) داسې چې باور لري، 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 $|t| \leq 1$ ، يعنې $t \leq 1$ ، له دې سره $t = 1$ نو $\text{ggT}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

ad 2:

له [2.2.5](#) سره د معلومو $\alpha, \beta \in \mathbb{Z}$ لپاره $1 = \alpha\frac{a}{t} + \beta\frac{b}{t}$ ، يعنې $t = \alpha a + \beta b$ د وړاندنيونو(فرضيو) وروسته $|t|$ راكوي a, b يو ګډ پروېشونى دى. 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 $|s| \leq |t|$ دى، دا په دې معنا چې $s \leq |t|$. يعنې $\text{ggT}(a, b) = |t|$ دى.

ad 3:

$$\begin{aligned}
 & \text{د } 1 \text{ له مخې د } d = \text{ggT}(a, b) \text{ لپاره باور لري، چې } \text{ggT}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \text{ ، د} \\
 & \text{له امله د } 2.1.3 \text{ پسي لاس ته راځي } d \mid a, b \text{ ، له دې سره لاس ته} \\
 & \text{راځي } \text{ggT}\left(\frac{a}{d}, \frac{b}{d}\right) = \text{ggT}\left(\frac{ma}{md}, \frac{mb}{md}\right) = 1 \text{ ، د } 2 \text{ پسي لاس ته راځي} \\
 & \quad \quad \quad |md| = \text{ggT}(ma, mb)
 \end{aligned}$$

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

$$\begin{aligned}
 & \text{يادونه 2.2.10 : که } \frac{a}{b} \in \mathbb{Q} \text{ وي (ريښتوني يا راشنل)، نو د} \\
 & \text{تولو } d = \text{ggT}(a, b) : \text{ لپاره } \frac{\frac{a}{d}}{\frac{b}{d}} = \frac{a}{b} \text{ باور لري. د } 2.2.9 \text{ (1) له مخې باور لري:} \\
 & \text{، دا په دې معنا چې } \frac{1}{b} \text{ کېدی شي په } \frac{c}{d} \text{ بڼه د } \text{ggT}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \\
 & \text{سره وليکل شي } (c, d) \text{ حتی يواځني ټاکلي دي). } \text{ggT}(c, d) = 1
 \end{aligned}$$

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

$$\begin{aligned}
 & \text{وي دې } a, b \in \mathbb{Z} \text{ ، نه دواړه صفر، نو باور لري: } d \in \mathbb{N} \text{ گڼ يا عدد ټيک هلته خرا} \\
 & \text{غټ پروېشونى (لنډ:خ غ پggT = gcm) دى، که } \text{ggT}(a, b) \\
 & \quad \quad \quad d \mid a, d \mid b \quad (1)
 \end{aligned}$$

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

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 پروېشونې، نو له $d = xa + yb$ ($x, y \in \mathbb{Z}$) لاس ته

راځي (جمله 2.2.5 دې وکتل شي)، چې $c \mid d$ دی (2.1.3) ، دا په دې معنا چې (2) باور لري.

 (\Leftarrow)

د (1) له مخې d د a, b ګډ پروېشونې دی. وي دې $c \in \mathbb{Z}, c \geq 1$ په خوښه د

پروېشونې، نو د (2) له مخې لاس ته راځي $c \mid d$ ، دا په دې معنا چې د 2.1.3

پسي $|c| \leq |d|$ دی ، له دې سره $c \leq d$. يعني d د a, b خورا غټ ګډ پروېشونې (بزرګترین مقسوم علیه مشترک؟) دی

□

جمله 2.2.12 : (بنسټيزه lemma) مرستندوی جمله چې د ښوونې يا ثبوت په جريان کې په کار راځي)) وي دې $a, b, c \in \mathbb{Z}, a \neq 0, \text{ggT}(a, b) = 1$ ، نو د $a \mid b \cdot c$ له مخې لاس ته راځي، چې $a \mid c$ دی.

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

$1 = xa + yb$	(2.18)
---------------	--------

ګڼونپوهنه

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

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

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

دینې یادون: اوکلید د 200-365 ز ک څخه له مخه.

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

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

پېژند یا تعریف :

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

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

دریم : که $\text{ggT}(a_1, \dots, a_n) = 1$ وي، نو a_1, \dots, a_n نسبي لومړني (وروسته به دا پروېش پردې وبلل شي) بلل کيږي.

څلورم : a_1, \dots, a_n جوړه (حفت) نسبي لومړني ګڼونه یا عددونه بلل کيږي، که $\text{ggT}(a_i, a_j) = 1$ وي د ټولو $\forall i \neq j$ لپاره.

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

څټ کېدنه يې باور نه لري:

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

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

جمله 2.3.3: وي دې $a_1, \dots, a_n \in \mathbb{Z}$ ، نه ټول صفر او $d = \text{ggT}(a_1, \dots, a_n)$ نو باور لري:

$d = \sum_{i=1}^n x_i a_i$	(2.20)
----------------------------	--------

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

ښوونه: وي دې

$M := \{c_1 a_1 + \dots + c_n a_n \in \mathbb{Z} \mid c_i \in \mathbb{Z} \ i = 1, \dots, n\},$	(2.21)
--	--------

نو $a_i \in M, i = 1, \dots, n$ ($c_i = 1, c_j = 0$) 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 معنا چې هم M طبيعي يا پيداېښتي ګڼونه يا عددونه لري. د \mathbb{N} د ټولنظم له مخې په M کې د ټولو طبيعي اعدادو ډېری يا ست يو خوا کوچنی توکی d^* لري، دا په دې معنا چې

$d^* = x_1 a_1 + \dots + x_n a_n$	(2.22)
-----------------------------------	--------

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

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

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

نو $r_i = a_i - q_i d^*$ او $r_i \in M$ د a_1, \dots, a_n کرښيز کمبېنېشن دی،
همداسې a_i ، په تعقيب کمبنت يا تفريق هم. له دې سره له
څخه لرو. يعنې:

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

وي دې a_1, \dots, a_n, t د $t \geq 1$ يو په خوښه ګډپروېشونې، نو t هر کرښيز
کمبېنېشن وېشي يعنې دا لاندې هم

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

$$d^* = \text{ggT}(a_1, \dots, a_n) = d.$$

له دې سره د [2.2.11](#) پسې لرو، چې

□

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

د $n = 2$ لپاره: د اویکلید الګوریتم، جمله [2.2.1](#).

د $d \geq 1$ له امله کېدی شي سری ټول ونیسي (فرض کړي) پرته له دې

مطلق ارزښت، a_i ، چې صفر دي، (لري) پریرودي. سری اوس د a_1, \dots, a_n لاندې

هغه خورا کوچنی لټوي، دا دې بي له توليزو بنديزونو a_1 وي (کېدی شي نمره بدل شي). د پاتي سره د a_2, \dots, a_n وېش د a_1 له لارې راكوي:

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

$$d = \text{ggT}(a_1, \dots, a_n) = d' = \text{ggT}(a_1, r_2, \dots, r_n) \quad \text{وېنایی:}$$

وي دې

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

نو باور لري $d \mid a_1, \dots, a_n$ ، يعني ، $d \mid a_1$ ، او له $r_i = a_i - q_i a_1$ لاس ته راځي $d \mid r_i \quad (i = 2, \dots, n)$ ، دا په دې معنا چې d د a_1, r_2, \dots, r_n يو گډ پروېشونی دی. d' خورا لويه ده له دې لاس تخ راځي $\Rightarrow d \leq d'$

برعکس يا په څټ باور لري: d' وېشي،، يعني داسي $a_1, d' \mid r_i \quad (i = 2, \dots, n)$

لاس ته راځي $a_i = q_i a_1 + r_i : d' \mid a_i \quad (i = 2, \dots, n)$ (د ليما يا جملگی

[2.1.3](#) پسې)، يعني d' د a_1, \dots, a_n گډپروېشونی دی. d خورا لوی دی له دې لاس ته راځي $\Rightarrow d' \leq d \stackrel{3b}{\Rightarrow} d = d'$.

يادونه : په پام کې دې وي: د دې تئلاړ سره گڼونه يا غددونه تل کوچني کيږي ($0 \leq r_i < a_1$) او د امکان په حالت کې حتی کميږي (کېدی شي $r_i = 0$ وي).

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

ګڼونپوهنه

$a_1 = 114$ ، وېش له پاتې سره :

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

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

$$d = \text{ggT}(114, 37, 43)$$

له دې سره:

$$\bar{a}_1 = 37$$

، وېش له پاتې سره:

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

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

$$d = \text{ggT}(37, 3, 6)$$

له دې سره:

$$\bar{a}_1 = 3$$

، وېش له پاتې سره:

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

۳ - لومړني ګڼونه (اعداد) Primzahlen

لومړني ګڼونه \mathbb{P}

Die Menge der Primzahlen \mathbb{P} بنسټونه *Grundlagen*

پېژند(تعريف) 3.1.1 : يو طبيعي گڼ 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 ډېری د \mathbb{P} سره په نخښه کوو. جمله : (اویکلید) ناپای ډېر لومړني گڼونه شته.

بنوونه: نیسو، چې p_1, \dots, p_n ټول لومړني اعداد دي چې شتون لري. جوړوو

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

ترڅېړني نیسو

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

نو $M \neq \emptyset$ دی، ځکه چې $N \in M$ (په ساده توگه $N \mid N, N > 1$). د ټول نظم

اصولو سره يو خورا کوچنی توکی q شتون لري، دا په دې معنا، چې $q > 1$

او $q \mid N$. وینایي: يو لومړنی عدد دی:

وي دې $t \mid q$ د $t > 1$ سره، نو د [2.1.3](#) پسي لاس ته راځي،

چې $t \mid N \Rightarrow t \in M$ له $q, t \leq q$ د $M \Rightarrow t = q$ خورا کوچنی توکی دی.

يعني q لومړنی گڼ دی، له نيوني څخه لاس ته راځي: $\exists j : q = p_j$. له دې

سره $q \mid N (q \in M)$ باولري او په ساده توگه :

کڼونپوهنه

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

- تضاد \square

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

ټوله 1 تر n پورې ټول گڼونه وليکه، که ټول لومړني اعداد $\leq \sqrt{n}$ پېژندل شوي وي، نو سړی دې د ټولو دې لومړنيو گڼونو په ډېرواره کرښه راکاږي (تر پخپله لومړني $\leq \sqrt{n}$ عدد پورې)، اوس فقط لومړني گڼونه پاتې دي.

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

2, 3, 5, 7, ~~9~~, 11, 13, ~~15~~, 17, 19, ~~21~~, 23, ~~25~~, ~~27~~, 29, 31, ~~33~~, ~~35~~,
37, ~~39~~, 41, 43, ~~45~~, 47, ~~49~~

ټول اعداد چې کرښه په راکښل شوي نه ده لومړني اعداد دي او ≤ 50 دي.

يادوني 3.1.4:

لومړی: د دې لپاره چې ایا یو عدد پريم دی، که نه، یوه اغیزمنه – یا اقتصادي تڼلار نه شته (لږ تر لږه تر اوسه، وگورئ [Gut02b, Rie94])، کارونه یا استعمالیې په کریپتولوژي Kryptologie کې کيږي.

دویم: د لومړنیو ګڼونو جمله:

که $\pi(x)$ د لومړنیو ګڼونو ګڼون یا تعداد وي، نو باور لري

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

دریم: د لویې $x \in \mathbb{N}$ لپاره

نږدې:

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

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

له بلې خوا د دوه لومړنیو اعدادو ترمنځ په خوښه لویې تشياوي شتون لري: وي دي

$$(n+1)! + 2, \dots, (n+1)! + (n+1) \quad n \in \mathbb{N}$$

ګڼونه

همدا اوس n يو په بل پسې اعداد دي، چې لومړني اعداد نه دي، ځکه چې:

$$2 \leq k \leq n+1 \quad g = (n+1)! + k$$

سره وي، نو باور لري

$$\stackrel{2.1.3}{\Rightarrow} k \mid g \quad k \mid k, k \mid (n+1)!$$

له دې لاس ته راځي، کوم ته چې

کڼونپوهنه

او $k \neq 1 (2 \leq k)$ $k \neq g (g = (n+1)! + k > k)$ (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 چیرته چې $27 \ll (4+1)! + 2$ (دی).

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

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

ناپای ډېر لومړني اعداد. (د اریتمیتیکی پروګرشن لپاره د لومړنیو اعدادو جمله، تولیزه بنوونه ډېره پېچلې ده!)

د $\{4k + 1 \mid k = 1, 2, \dots\}$ لپاره، همداسې $\{4k + 3 \mid k = 1, 2, \dots\}$ لپاره لږ څه وروسته بنايو (جمله [9.2.8](#) همداسې جمله [3.1.10](#) وګورئ).

شپږم: د $2^{2^n} + 1 (n \in \mathbb{N})$ بنې عدد د فرمات عدد [3.3](#) Fermat'sche Zahl بلل کېږي، د $n = 0, 1, 2, 3, 4$ لپاره په رېښتوني 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 څوک

ترتیبولی نه شي F_{33} دی.

اوم : يو د $2^n - 1$ ($n \in \mathbb{N}$) ښي عدد د مرزن عدد [3.4](#) *Mersenne'sche Zahl* 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 عدد د مرزن عدد دی، داسې

$$p = 2^{134066917} - 1$$

ناميز

اتم: د ګولډباين ګومان : هر جوړه عدد له څلور سره برابر يا ترې لوی وي د دوه لومړنيو اعدادو د زياتون يا جمعې په څېر انځوروي دی. (د بېلګې په توګه

$$4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, \dots$$

د عدد 1742 په هکله ګومان کېدی

شي نه تراوسه وښوول شي او نه رد شي.

جمله 3.1.5: که $a_1, \dots, a_n \in \mathbb{Z}$ وي او p يو لومړنی عدد د $p \mid a_1 \cdots a_n$ سره

وي، نو لږ تر لږه p د ضريبونن يا څلوونو $a_i, 1 \leq i \leq n$ څخه يو وېشي.

ښوونه: د n پسي ايندکشن:

: $n = 1$ ساده دی.

: $n \rightarrow n + 1$

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:

$$\text{ggT}(p, a_{n+1}) = 1 \quad p \nmid a_{n+1}$$

دی، داسې چې د بنسټيزې جملهګۍ [2.2.12](#)

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.

□

ګڼونپوهنه

لاس ته راورنه 3.1.6 : د $n = 2$ لپاره باور لري: د $a_1 \cdot a_2$ یو پروپینونی 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،،

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

، نو g بیا یو لومړنی ګڼ دی.

ښوونه: نیسو، چې g لومړنی عدد نه دی، نو g بیا اصلي پروپینونی لري، دا په دې

معنا چې $g = a \cdot b$ ، چېرته چې $1 < a < g, 1 < b < g$ دي . نو باور لري:

$g \mid a \cdot b$ ، یعنی د نیونی 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 $g = \pm b \Rightarrow g$ ، چې باید لومړنی وي.

□

نور خوښونه Weitere Eigenschaften

جمله 3.1.7 : (لومړني ضربیتوته ونه یا په لورنیو ضربیونو توتته کونه) هر طبیعي

عدد $n > 1$ کېدی شي په یواځني ډول د لومړنیو عددونو د ضرب په څېر ولیکل شي) دا په دې معنا ، چې لومړني ګڼونه د \mathbb{N} ضربیي جوړښتڅښتنی دي).

ښوونه:

شتونوالی:

په n پسې د (توليز شوي) ايندکشن Induktion له لارې:

$$: n = 2$$

ساده

$$: n - 1 \rightarrow n :$$

بنايو: جمله د $2, 3, \dots, n - 1$ لپاره ټيک ده.

نسيده، نيسو چې $\exists k : 2 \leq k \leq n - 1$ ، کوم چې د لومړنيو گنونو يا عددونو ضرب نه دی. وي دي k_0 د دوی ترمنځ خورا کوچنی عدد. نو k_0 لومړنی عدد نه دی. يعنې که باور ولري $k_0 = a \cdot b$ ، چېرته چې $a < b < k_0$ ، له دي سره لاس ته راځي: a او b هر يو د لومړنيو گنونو ضرب دی، له دي امله k_0 هم د لومړنيو گنونو ضرب دی - تضاد!

وښايي: n د لومړنيو عددونو ضرب نه دی.

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

که n لومړنی عدد نه وي، نو $n = cd$ باور لري د $1 < c, d < n$ سره. د پورته پام کوني څخه جمله د c, d لپاره ټيک ده، دا په دي معنا چې c, d هر يو د لومړنيو عددونو ضرب دی، يهني هم $n = c \cdot d$.

يواخپوالی يا يواځنوالی:

وي دي $n > 1$ او

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

کنونپوهنه

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

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

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

که $s > r$ وی نو باور لري چې q_{r+1} بنی خوا وېشي: $q_{r+1} \mid 1$ ، یعنی $q_{r+1} \leq 1$ ، و q_{r+1} ته تضاد چې لومړنی عدد دی له دې لاس ته راځي $s = r \Rightarrow$ 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 ضربونو لپاره، یعنی

$$g = -p_1 \cdots p_r$$

یادونه 3.1.9: که د $n > 1$ د لومړنیو ضربونو توپه 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 راځي، یعنی

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

که دا دلته نه شتون لرونکو لومړنيو 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 لومړنيو عددونو ضرب، فقي پای ډېر $\alpha_p \neq 0$) له دې سره

هم لیکلی شو. يعني د په ټوليزه توګه د ټول $g \in \mathbb{Z}, g \neq 0$ لپاره باور لري:

$$1 = \prod_{p \in \mathbb{P}} p^0$$

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

جمله 3.1.10 (ډيرينليت) د $4k + 3$ ($k = 0, 1, \dots$) بني ناپای ډېر لومړني
 گڼونه شتون لري، دا به دې معنا، چې د $\{3, 7, 11, 15, 19, \dots\}$ عدونو په ډېری کې ناپای ډېر لومړني عددونه شتون لري..

بنوونه: نيسو چې په دې ډول ډېر لومړني عددونه شتون لري، چې د p_1, \dots, p_s سره يې سړی په نخښه کولی شي. سړی جوړوي

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

کنونپوهنه

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

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

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

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

مګر $4k + 2$ او $4k + 0$ لومړني عددونه نه دي. که همدا اوس ترې
 $N = 4k + 3$
 دباندي دی. 2 د ضرب په حیث نه رامنځ ته کيږي، ځکه چې
 دى.)
 ناچوره

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

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

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

□

د ggT او kgV ترمنځ اړیکې (د x او y کک زیاتځلي - -

جمله 3.2.1: وي دی ، $b = \prod_{p \in \mathbb{P}} p^{\beta_p}$ ، $a = \prod_{p \in \mathbb{P}} p^{\alpha_p}$ ، نو باور لري

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

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

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

(\Rightarrow) يا له نډې لاس ته راځي

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

د $z = \prod_{p \in \mathbb{P}} p^{\tau_p}$ سره په لومړنيو ضربونو توته 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 لومړنيو ضربونو توته کوني د يواځيوالي په بنسټ لاس ته راځي عددونو په

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

کڼونپوهنه

د [1.1.4](#) پسي لاس ته راځي $\rho_p \leq \sigma_p \forall p \in \mathbb{P}$

(\Leftrightarrow)

نو د [1.1.4](#) پسي باور لري: $\rho_p \leq \sigma_p \forall p \in \mathbb{P}$

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

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

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

$xz = y \Rightarrow x \mid y$
يعني

وي دي $d := \text{ggT}(a, b)$ 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 . برعکس له

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

څخه لاس ته راځي، چي عدد $c := \prod_{p \in \mathbb{P}} p^{\min(\alpha_p, \beta_p)}$ عددونه a, b ويشي، د

جملې [2.2.5](#) او جملگي يا کورولار [2.2.11](#) څخه $c \mid d$ لاس ته راځي، دا په دې معن،

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

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

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

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

بېلګه 3.2.2 : وي دې ، نو د ناشتونو
لومړنيو ګڼونو د پوره کېدنې له امله د 0 اکسپننټ له لارې باور لري:

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

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

کورولار يا جمګي 3.2.3 :

لومړی :

وي دې $a_i \in \mathbb{N}$, sei $a_i = \prod_{p \in \mathbb{P}} p^{\alpha_{i,p}}$, $i = 1, \dots, n$
د لومړنيو ضربيونو ټوټه
کونه، نو باور لري

$$\text{ggT}(a_1, \dots, a_n) = \prod_{p \in \mathbb{P}} p^{\min_{1 \leq i \leq n} (\alpha_{i,p})}. \quad (3.23)$$

ګڼونپوهنه

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

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

تعريف 3.2.4 : وي دي، نو $a, b, v \in \mathbb{Z}$ د ګډ ډېرځله (مضرب مشترک) بلل کيږي،
که $a | v$ او $b | v$ وي (دا په دي معناچي $v = xa = yb$ د ځنو $x, y \in \mathbb{Z}$ سره).

يادونه 3.2.5 : $a \cdot b$ او $|a| \cdot |b|$ هر يو د a, b ګډ ډېرځله دي، دا په دي معنا، چي 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 ډېری په پام کې ونيسو، نو دا ډېری د پورته يادونو په بنسټ هم تشه نه ده، دا د اکسيم 4 په بنسټ هم دا ډېری کوچنی توکی لري. نو کړی شو تعريف کړو:

پېژند (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 $\text{kgV}(a, b)$ سره په نڅښه کوو.

$$\text{kgV}(a, b) := 0$$

که له دي ګڼونو يو صفر وي، يا دواړه، نو تعريفوو .

يادونه 3.2.7 : شرايط (مثبت) مهم دي، ځکه چي پرته له دي بايد نه دی، چي خورا کوچنی ګډ زياتځله شتون ولري. وي دي $a = 2, b = 3$ ، نو ټول $v = -6, -12, -18, \dots$ د a, b ګډ پروېشوني دي.

جمله 3.2.8 : $b = \prod_{p \in \mathbb{P}} p^{\beta_p}$ ، $a = \prod_{p \in \mathbb{P}} p^{\alpha_p}$ ، دي ورکړ شوي وي، نو باور لري

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

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

$\alpha_p, \beta_p \leq \max(\alpha_p, \beta_p)$	(3.26)
--	--------

امله د جملې [3.2.1](#) بنوونه پسي باور لري، چې

$a v, b v.$	(3.27)
-----------------	--------

که $c = \prod_{p \in \mathbb{P}} p^{\gamma_p}$ د a, b يو ګډ زیاتځله وي (c په خوښه، زیاتيز)، نو له $a | c$ ، $\alpha_p \leq \gamma_p, \beta_p \leq \gamma_p \mid c$ او $\max(\alpha_p, \beta_p) \leq \gamma_p \forall p \in \mathbb{P}$ لاس ته راځي. یعني باور لري: ، دا په دي معنا، چې $(c > 0, v > 0, v \leq c)$ د ليما(5) [2.1.3](#) له لاري دي. نو له دي سره v د a, b خورا کوچنی ګډ زیاتځله دی، یعني

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

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

$$a = 2^3 3^2 5^{17^0}, b = 2^2 3^3 5^0 7^1$$

کنونپوهنه

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

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

$$1. \quad a | v, b | v$$

$$2. \quad a | c, b | c \Rightarrow v | c$$

د a_1, \dots, a_n لپاره په ټوليزه توگه:

تعريف 3.2.11: وي دي $a_1, \dots, a_n \in \mathbb{Z}$ ، نو $v \in \mathbb{Z}$ د a_1, \dots, a_n يو گډ

زياتخه بلل کيږي، که $a_i | v, i = 1, \dots, n$.

وي دي $a_i \neq 0, i = 1, \dots, n$ ، نو دا د ټول مثبتو خورا کوچنيو گډزياتخه د

$$\text{kgV}(a_1, \dots, a_n)$$

سره په نخښه کوو (شتون و حالت $n = 2$ ته ورته مدلل وړ

دی)

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

يادونه 3.2.12: د $\text{kgV}(a_1, \dots, a_n) = \text{kgV}(|a_1|, \dots, |a_n|)$ له امله کېدی

شي دا حالت په باندې $a_1, \dots, a_n \in \mathbb{N}$ محدود شي.

$$a_1, \dots, a_n \in \mathbb{Z}, a_i = \prod_{p \in \mathbb{P}} p^{\alpha_{i,p}}$$

کورولار (حمله گئی) 3.2.13: وي دي په لږمړنی

ضريب ټوټه کونه، نو باور لري ($a_i \neq 0 \forall i$):

$$\text{kgV}(a_1, \dots, a_n) = \prod_{p \in \mathbb{P}} p^{\max_{1 \leq i \leq n} (\alpha_{i,p})}. \quad (3.28)$$

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

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

$$\text{kgV}(a_1, \dots, a_n) \cdot \text{ggT}(A_1, \dots, A_n) = a_1 \cdots a_n. \quad (3.29)$$

ښوونه: وي دي $a_i = \prod_{p \in \mathbb{P}} p^{\alpha_{i,p}}, i = 1, \dots, n$ نو باور لري.

$$A_i = \prod_{p \in \mathbb{P}} p^{\sum_{j \neq i} \alpha_{j,p}}, i = 1, \dots, n$$

او

$$\text{ggT}(A_1, \dots, A_n) = \prod_{p \in \mathbb{P}} p^{\min_{1 \leq i \leq n} (\sum_{j \neq i} \alpha_{j,p})}, \quad (3.30)$$

$$\text{kgV}(a_1, \dots, a_n) = \prod_{p \in \mathbb{P}} p^{\max_{1 \leq i \leq n} (\alpha_{i,p})}, \quad (3.31)$$

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

وي دي $\alpha_{i_0,p} = \max_{1 \leq i \leq n} (\alpha_{i,p})$ ، نو باور لري، $\alpha_{i,p} \leq \alpha_{i_0,p}, i = 1, \dots, n$ يعنې

$$-\alpha_{i,p} \geq -\alpha_{i_0,p} \quad \text{او}$$

کنونپوهنه

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

$$\sum_{j \neq i} \alpha_{j,p} \geq \sum_{j \neq i_0} \alpha_{j,p}, \quad i = 1, \dots, n$$

دا په دې معنا، چې

$$\min_{1 \leq i \leq n} \left(\sum_{j \neq i} \alpha_{j,p} \right) = \sum_{j \neq i_0} \alpha_{j,p}$$

نو له دې سره:

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

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

$\text{kgV}(a_1, \dots, a_n)$

جملگی 3.2.15: دا یو امکان دی، چې د لویو گڼو یا عددونو

لپاره و شمېرو () $\text{ggT}(A_1, \dots, A_n) = \frac{a_1 \cdots a_n}{\text{ggT}(A_1, \dots, A_n)}$ ، چېرته چې د وېش له لارې د پاتې سره شمېرل کېږي.

$$\text{kgV}(6, 8, 15) = ?$$

بېلگه 3.2.16: ؟

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

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

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

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

لاس ته راوړنه 3.2.17 :

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

$$\text{kgV}(a_1, a_2) \text{ggT}(a_1, a_2) = a_1 a_2$$

، نو لاس ته راځي:

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

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

یادونه 3.2.18 : په ټولیزه وګه: که $a_1, \dots, a_n \in \mathbb{N}$ وي، نو

$\text{kgV}(a_1, \dots, a_n) = a_1 \cdots a_n$ ټیک هلته دی، که $a_i, i = 1, \dots, n$ جوړه یو بل ته نسبي لومړني عددونه وي. (بنوونه د لومړنیو فاکتورونو ټوټه کوني سره کيږي)

Kongruenzen

د ګونګروانځ سره شمېرنه Rechnen mit Kongruenzen

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

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

کنونپوهنه

$$m \mid a - r$$

$$a - r = qm$$

یعني ، دا به دې معنا، چې

بیژند(تعریف) 4.1.1 : که وي $a, b \in \mathbb{Z}, m \in \mathbb{N}$ په خوښه، نو a, b کونگروانڅ

مودولو m بلل کيږي، که $m \mid a - b$ ، سومبولیک یا لیکندود $a \equiv b(m)$

بېلگه 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 ټیک هلته کونگروانټ مودولو

m دي، که a, b د m له لارې د پاتې سره په وېش کې دا یو د بل پاتې برابر دي.

بنوونه : 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). بنایو:

$$(\Leftrightarrow)$$

$$r = r' :$$

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

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

(\Rightarrow) $a \equiv b(m) :$

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

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

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

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

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

يادونه : \equiv له لارې په \mathbb{Z} د $m \in \mathbb{N}$ لپاره يو ورته اړيکي ، په خوښه مگر
 کره ټاکلي، تعريف دي:

لومړی :)

1. Reflexivität (هندارونه) $a \equiv a(m) \forall a \in \mathbb{Z}$ ، ځکه

$$m \mid a - a = 0$$

2. (Symmetrie سيوتري)

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

3. (Transitivität).

کینونپوهنه

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

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

ختی لا ډېر باور لري ($\equiv d$ او $\equiv d$ سره زعمور دی، د ،، کونگروانڅ ،، کلمه دي
پع الجبر کې 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. $ka \equiv kb(m)$ $k \in \mathbb{Z}, d = \text{ggT}(k, m) \Rightarrow a \equiv b(\frac{m}{d})$
für ein
6. $a \equiv b(m), a \equiv b(n), n \in \mathbb{N} \Rightarrow a \equiv b(\text{kgV}(m, n))$

ښوونه:

1. $a \equiv b(m), c \equiv d(m) \Rightarrow m \mid a - b, m \mid c - d$
- $$t \stackrel{2.1.3}{\Rightarrow} m \mid (a - b) + (c - d) \Rightarrow (a + c) \equiv (b + d)(m)$$

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

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

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

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

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

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

1. لپاره $s \in \mathbb{Z}$ يوهد

$$\Rightarrow \frac{k}{d}(a - b) = \frac{m}{d} \cdot s \frac{m}{d} \mid \frac{k}{d}(a - b), \quad (4.5)$$

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

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

نو د بنسټيزي ليما 2.2.12 څخ لاس ته راځي:

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

کنونپوهنه

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

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

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

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 ترنو یا کارونو یا عملیو سره زغور دی (د ورته اړیکو یا کونګروانځ اړیکو په هکله دتر مخه تېرې یادونې 4.1.4 وګورئ).

دویم:

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

(بنوونه د ایندکشن له لارې).

دریم:

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

$$c_i \in \mathbb{Z} \quad a \equiv b(m), f(x) = c_0 + c_1x + \dots + c_kx^k$$

د سره، نو باور

لري

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

څلورم :

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

$$3 \equiv 2(4) \quad 4 \cdot 4 \equiv 4 \cdot 2(4) \quad \text{لاس ته نه اځي} \quad \text{مگر له} \quad \text{. (!!!)}$$

پنجم :

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

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 لومړنيو ضربيونو توپه كونه

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

$$(p_i^{\alpha_i} \mid m \text{ ځكه چې})$$

اتم :

$$a \equiv b(p_i^{\alpha_i}), i = 1, \dots, k, p_i$$

مختلف لومړني گڼونه

کنونپوهنه

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

د پروبشنور والي قوانین Teilarkeitsregeln

هر یا یوه یا بل د پروبشنور قوانین پیژني. د دې قوانینو څخه زیات یې به روښانه ت وگه د لاندې جملې په بنسټ ولاړ دي.

جمله 4.2.1 : $n = (a_k a_{k-1} \dots a_1 a_0)$ دې د $n \in \mathbb{N}$ دیکادیکي یا لسمیزه انځوره وي. نو باور لري

1. $n \equiv a_0 (2)$,
2. $n \equiv a_0 + \dots + a_k (3)$,
3. $n \equiv a_0 + 10 \cdot a_1 (4)$,
4. $n \equiv a_0 (5)$,
5. $n \equiv (a_0 + 10a_1 + 10^2 a_2) - (a_3 + 10a_4 + 10^2 a_5) + \dots (7)$,
- resp. (13) ,
6. $n \equiv a_0 + 10a_1 + 10^2 a_2 (8)$,
7. $n \equiv a_0 + a_1 + \dots + a_k (9)$,
8. $n \equiv a_0 - a_1 + a_2 - \dots + (-1)^k a_k (11)$.

ښوونه:

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

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

دویم:

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

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

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

دریم:

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

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

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

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

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

پنځم :

1. د ۱ - له امله

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

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

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

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

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

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

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

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

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

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

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

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

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

$$n = a_0 + 10a_1 + \dots + 10^k a_k \equiv \quad (4.23)$$

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

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

جمله گي 4.2.2 : (پروېشنور 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. $3 \mid n \Leftrightarrow 3 \mid a_0 + \dots + a_k$ ،
3. $4 \mid n \Leftrightarrow 4 \mid (a_1 a_0)_{10}$ ،
4. $5 \mid n \Leftrightarrow 5 \mid a_0$ ،
5. $7, 13 \mid n \Leftrightarrow 7, 13 \mid (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - + \dots$ ،
6. $8 \mid n \Leftrightarrow 8 \mid (a_2 a_1 a_0)_{10}$ ،

کڼونپوهنه

7. $9 \mid n \Leftrightarrow 9 \mid a_0 + \dots + a_k$
8. $11 \mid n \Leftrightarrow 11 \mid a_0 - a_1 + a_2 - \dots + (-1)^k a_k$

ښوونه : د بېلگې په توگه د دې لومړنيو درې راورل شوي قوانین ښايو، نو ټول کېدی شي په ورته توگه وښوول شي.

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

$$\Leftrightarrow^1 a_0 \equiv n \equiv 0(2) \quad (4.27)$$

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

يادونه 4.2.3 : سړی کړی شي د معلومو پروېشقوانينو پسې و غزوي، که مودول نسبي لومړني وي.

$$m = 2, n = 3 \Rightarrow \text{لکه}$$

لاس ته راځي او

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

Beispiel 4.2.4

$$n = 97234382 \mid n \quad 2 \mid 8 \quad 3 \mid n \quad 3 \mid 36 \quad 4 \nmid n$$

, da ; , da ; ,

$$4 \nmid 38 \quad 5 \nmid n \quad 5 \nmid 8 \quad 6 \mid n \quad 2 \mid n, 3 \mid n \wedge \text{ggT}(2, 3) = 1$$

da ; , da ; , da ;

$$7 \nmid n \quad 7 \nmid (438 - 723 + 009) = -276 \quad 8 \nmid n \quad 8 \nmid 438 \quad 9 \mid n$$

, da ; , da

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

; , da ; ,

$$4 \nmid n$$

da ; ...

پاتې ټولګي Restklassen

د [4.1.3](#) له مخې باور لري: $a \equiv b(m)$ ټيک هلته يا 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 خويونو سره د يوې ډېرې په توګه سره يوځای کړو، نو سرې داسې په نامه، پاتې ټولګي، لاس ته راوړي، فورمال د [4.1.4](#) پسې ، ، \equiv ، په \mathbb{Z} يو ورته اړيکه ده، يعنې له دې سره د \mathbb{Z} يو پارټيشن يا ټوټه کونه ورکړ شوي د پرديو $\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a(m)\}$ سره، داسې په نامه ورته ټولګي *disjunkte Äquivalenzklassen*، دا په دې معنا، چې

$$\begin{aligned} \bar{a} &\neq \emptyset & 1. \\ \bar{a} \cap \bar{b} &= \emptyset \vee \bar{a} = \bar{b} & 2. \\ \bigcup_{a \in \mathbb{Z}} \bar{a} &= \mathbb{Z} & 3. \end{aligned}$$

باور لري:

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

کنونپوهنه

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

د یوه

لپاره . له دې سره

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

په خوښه

دویم: $\forall a \in \mathbb{Z} : \bar{a} = \bar{r}$ د کوم سره چې $r \in \mathbb{Z}$ په m باندې د a د

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

$$\begin{aligned} a = qm + r, 0 \leq r < m &\Leftrightarrow a - r = qm \Leftrightarrow \\ &\Leftrightarrow m \mid a - r \Leftrightarrow a \equiv r(m) \Leftrightarrow \bar{a} = \bar{r} \end{aligned}$$

بېژند(تعریف) 4.3.1: وي دی $m \in \mathbb{N}$ په خوښه، نو ورته یا اکویوانت ټولگی $\text{mod } m$ یو پاتې ټولگی $\text{mod } m$ بلل کیږي. هر د \bar{a} توکی د ټولگی \bar{a} نماینده بلل کیږي. د ټول پاتې ټولگیو $\text{mod } m$ ډېری د \mathbb{Z}_m سره په نڅېنه کیږي.

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

بنوونه: که \bar{a} په خوښه پاتې ټولگی 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 $r \equiv r'(m) \quad \bar{r} = \bar{r'}, 0 \leq r \leq m - 1, 0 \leq r' \leq m - 1$ باور ولري، نو

باور لري ، په m باندې د r, r' د وېشني څخه r همداسې r' پاتې (که غواړی: باقي) پاتې کيږي، دا باید د [4.1.3](#) پسې باور ولري: $r = r'$. برعکس: $r = r' \Rightarrow \bar{r} = \bar{r}'$. نو ټیک m ټولګي شتون لري.

بېلګه 4.3.3: $m = 5 : \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ ، څه:

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

ځانګړې توګه

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

پېژند (تعريف) 4.3.4: د \mathbb{Z} یوه برخه ډېری کومه چې له هر پاتې ټولګي ټیک یو توکی خوندي لري، نو پوره مودولو m پاتې سیستم بلل کيږي.

بېلګه 4.3.5: $m = 4, \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}; \{0, 1, 2, 3\}$ یو پوره پاتې

سیستم $\text{mod } 4$ دی، همداسې $\{4, -3, -2, 4\}$ یا $\{100, 99, 98, 97\}$.

لیما 4.3.6: یوه برخه ډېری $\{r_1, \dots, r_m\} \subseteq \mathbb{Z}$ ټیک هلته یو پوره پاتې سیستم

مودولو m دی، که $r_i \not\equiv r_j(m) \forall i, j = 1, \dots, m : i \neq j$ وي.

بنوونه:

(\Rightarrow)

که $\{r_1, \dots, r_m\}$ یو پوره پاتې سیستم وي، نو r_i ، $i = 1, \dots, m$ په مختلفو پاتې ټولگيو $\text{mod } m$ کې پراته دي، نو باور لري

$$\forall i \neq j \quad r_i \not\equiv r_j(m)$$

(\Leftarrow)

که باور ولري $r_i \not\equiv r_j \quad \forall i \neq j$ ، نو r_i په مختلفو پاتې ټولگيو کې پراته

دی، او ټول مختلف دي، نو $\{r_1, \dots, r_m\}$ یو پوره پاتې سیستم دی.

کورولار یا جمله گۍ 4.3.7: وي دي $\{r_1, \dots, r_m\} \subseteq \mathbb{Z}$ یو پوره پاتې سیستم

مودولو m او $a, b \in \mathbb{Z}$ دي د $\text{ggT}(a, m) = 1$ سره وي، نو

$$\{ar_1 + b, \dots, ar_m + b\}$$

هم یو پوره پاتې سیستم مودولو m دی.

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

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

او له دي سره د [4.1.6\(4\)](#) له امله:

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

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

نو له دې سره لاس ته راځي

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

او له [4.3.6](#) سره غوښتنه لرو.

جمله گي 4.3.8: وي دي $\{r_1, \dots, r_m\} \subseteq \mathbb{Z}$ يو پوره پاتي سيستم مودولو m ،
 $\{s_1, \dots, s_n\} \subseteq \mathbb{Z}$ يو پوره پاتي سيستم مودولو n او $\text{ggT}(m, n) = 1$ ، نو

$\{nr_1 + ms_1, \dots, nr_m + ms_n\}$	(4.33)
---------------------------------------	--------

$$\{nr_1 + ms_1, \dots, nr_m + ms_n\} \quad (4.33)$$

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 همدا سي $i \neq k$ $j \neq l$ لپاره يا دواړه. د $m \mid m \cdot n$ له امله لاس ته راځي:

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

$$nr_i \equiv nr_k(m)$$

له دې سره

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

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

ګڼونپوهنه

د 4.3.6 له مخې . له دې سره نيوڼه داسې 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 د 4.3.6 له امله - تضاد دی □

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

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

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

په $\mathbb{Z}_m = \{\bar{a} \mid a \in \mathbb{Z}\}$ (m توکي دي) یو زیاتون یا جمعه \oplus او یو ضرب یا

خُل \odot تعریفوو د لاندې سره:

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

بڼایو : دا تعریفونه د وکیلانو (Repräsentanten) خپلواک دي، دا په دې معنا،

چې ، نو $\bar{a} = \bar{a'}, \bar{b} = \bar{b'}$ هم باور لریاو همداسې $\overline{ab} = \overline{a'b'}$ هم

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

نو:

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

نسبت جمعې \oplus ته باور لري: (\mathbb{Z}_m, \oplus) یو کموتاتیو ګروپ دی. ځکه چې:

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

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

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

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

ځکه چې ،

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

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

پوره کوي

$$4. \quad \overline{a} \oplus \overline{-a} = \overline{-a} \oplus \overline{a} = \overline{0} \quad \forall \overline{a} \in \mathbb{Z}_m$$

و ته زیلتیز یا مثبت معکوس دی، ځکه چې

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

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

نسبت ضرب \odot ته باور لري: (\mathbb{Z}_m, \odot) یو نیم ګروپ دی د 1 سره. ځکه چې:

کنونپوهنه

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

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

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

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

$$\bar{a} \odot \bar{1} = \bar{1} \odot \bar{a} = \bar{a} \quad \forall \bar{a} \in \mathbb{Z}_m \quad \bar{1} \in \mathbb{Z}_m \quad 3. \quad \text{پوره کوي}$$

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

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

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

له دې سره $(\mathbb{Z}_m, \oplus, \odot)$ یو کموتاتیو رینګ (کری) دی د 1 سره، داسې په نامه
 ،،پاتې ټولګي رینګ یا — (کری) 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:

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

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

په کړی یا رینګ $(\mathbb{Z}, +, \cdot)$ (کموتاتیو کړی د 1 سره) کې باور لري:

4.1 $ab = 0 \Rightarrow a = 0 \vee b = 0$. په ټولیزه توګه دا په $(\mathbb{Z}_m, +, \cdot)$ کې ټیک نه دی، دا د $m = 6$ لپاره باور لري $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ ، چېرته چې $\bar{2}, \bar{3} \neq \bar{0}$ دی.

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

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

دویم : یو R انټیګریتی کړی (صفرپروېشونی ازاد یا بی صفرپروېشونی) بلل کيږي، که په R کې صفرپروېشونی شتون ونه لري.

کنونپوهنه

دریم: یو $a \in R$ یوون یا واحد بلل کیري، که یو $b \in R$ شتون ولري، د $ab = 1$ سره، a د b معکوس یا په څنټ بلل کیري (نسبت و ضرب 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 کیري (انگریزي).

بېلگه 4.4.2:

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

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

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

پېژند (تعریف) 4.4.3: یو $\bar{a} \in \mathbb{Z}_m$ لومړنی پاتي سیستم $\text{mod } m$ بلل کیري، که $\text{ggT}(a, m) = 1$ وي، دا په دې معنا، چې a و m ته نسبي لومړنی دی.

لېم 4.4.4: هر $\bar{a} \in \mathbb{Z}_m$ د لومړني پاتي ټولگي توکي و مودول m ته نسبي لومړنی دی.

بنوونه: وي دې $\bar{a} \in \mathbb{Z}_m$ لومړنی پاتي سیستم او $\text{ggT}(a, m) = 1$ (پرتله له دې بیا سړی بل نماینده سیستم ټاکي). وي دې $b \in \bar{a}$ په خوښه، و دې بنوول شي: $\text{ggT}(b, m) = 1$.

$p \mid b$ شته د $p \in \mathbb{P}$ ، داپه دېمعنا، چې يو لومړنی گڼ $\text{ggT}(b, m) \neq 1$ نيسو، چې
 او $p \mid m$ سره (که وي $c \mid b, c \mid m \Rightarrow$ له دې څخه د c په لومړنيو ضريبونو
 توپه کونه د $p \mid b, p \mid m$ سره لاس ته راځي). د $b \in \bar{a}$ له امله باور لري:

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

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

$$p \mid a \Rightarrow \text{ggT}(a, m) \geq p \quad (4.44)$$

-- تضاد \square

جمله : په $(\mathbb{Z}_m, +, \cdot)$ کې يوونونه يا واحدونه ټيک لومړني پاتېتولگي دي.

بنوونه:

لومړی: که $\bar{a} \in \mathbb{Z}_m$ لومړنی پاتې تولگی وي له دې لاس ته راځي $\Rightarrow \text{ggT}(a, m) = 1$ ، د [2.2.5](#) پسي لاس ته راځي $1 = \alpha a + \beta m$ د ځنو $\alpha, \beta \in \mathbb{Z}$ لپاره . له دې امله

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

دويم: \bar{a} يوون يا واحد دی.

درېم: که $\bar{a} \in \mathbb{Z}_m$ يوون يا واحد وي، نو يو $\bar{b} \in \mathbb{Z}_m$ شتون لري د $\bar{a}\bar{b} = \bar{1}$ سره،
 دا په دې معنا، چې $\bar{a}\bar{b} = \bar{1}$ ، له دې سره $ab \equiv 1(m)$ ، دا په دې معن،
 چې $ab - 1 = km$ نيسو چې $\text{ggT}(a, m) \neq 1$ ، نو
 $\exists p \in \mathbb{P} : p \mid a, p \mid m \Rightarrow p \mid 1$

-- تضاد \square

جمله 4.4.6: $(\mathbb{Z}_m, +, \cdot)$ ټيک هلته يو بدن دی، که m يو لومړنی گن وي.

بنوونه

(\Leftarrow)

وي دې $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$. دا چې $1, 2, \dots, p-1$ نسبت p ته نسبي لومړنی دی،
 نو $\bar{1}, \bar{2}, \dots, \overline{p-1}$ باور لري، چې ټول پاتې ټولگي لومړني دي، نو هر يو په
 خوبنه $\bar{a} \in \mathbb{Z}_p$ هم.

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

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

نيسو يا فرضوو، چې m 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 $m \leq r$ او $m \mid r$ --تضاد يا مخامخوالی .

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

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

پینه نوټ::

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

په الجر کې همدا خوي د، صفر پروېشنی ازاد، بلل کيږي.

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

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

الجبري کونګروانځ Algebraische Kongruenzen

د کرښیزو کونګروانځو حلوروالی

د جملې 4.4.5 پسی یو \bar{a} په \mathbb{Z}_m کې ټیک هلته یوون یا واحد دی ، که $\bar{a} \in \mathbb{Z}_m$ $\text{ggT}(a, m) = 1$ لومړنی پاتې سیستم وي. د داسې یوه \bar{a} لپاره له دې

امله یو $\bar{x} \in \mathbb{Z}_m$ شتون لري د $\bar{ax} = \bar{1}$ سره ، دا په دې معنا، چې $\bar{ax} = \bar{1}$

او $ax \equiv 1(m)$ د $\bar{x} \in \mathbb{Z}_m$ غوښتنه: $ax \equiv 1(m)$ سره.

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

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

سره داسې کرښیز کونګروانځ یا ورته والی.

جمله 5.1.1: یو کرښیز کونګروانځ $ax \equiv b(m)$ ټیک هلته حل وړ دی، که

$\text{ggT}(a, m) \mid b$ وي. که دا حالت وي، نو ټیک ناګونګروانځ حل

$$d = \text{ggT}(a, m) \bmod m$$

لرو.

$$\Leftrightarrow \text{ggT}(a, m) \mid b$$

شوونه : په یوه لومړي پل یا قدم کې بنایو: حلور

\Rightarrow

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

\Leftarrow

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

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

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

اوس ځانونه د (اینکونگروانڅ) حلونو سره ځان مصروفوو:

وینایي: 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 یوه $k \in \mathbb{Z}$ لپاره باور لري:

کنونپوهنه

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

$$ax_1 \equiv b(m) \quad \text{نو هم.}$$

له دې امله غوښتنه :

وي دې $x_0 \in \mathbb{Z}$ حل، دا په دې معنا، چې $x \in \mathbb{Z}$ او $ax_0 \equiv b(m)$ په خوښه نو

حلونه دي، نو $ax \equiv b(m)$. له دې امله د کمښت يا تفریق له لارې:

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

نو .

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

د [4.1.5\(5\)](#) 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 دې معنا، چې $\frac{m}{d} \mid \frac{a}{d} (x - x_0)$. د [2.2.9](#) له امله باور $\text{ggT}(\frac{m}{d}, \frac{a}{d}) = 1$ لري:

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

د یوه $t \in \mathbb{Z}$ لپاره . له دې امله لاس ته راځي:

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

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

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

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

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

پورته لورته $x = x_0 + t\frac{m}{d}$ دی د يوه $t \in \mathbb{Z}$ لپاره. د d سره د پاتي سره وېشني

له امله سړی $t = qd + r$ د $0 \leq r < d$ 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 $0 \leq r < d$ سره.

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

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

$$(l-k)\frac{m}{d} \equiv 0(m) \Rightarrow m \mid (l-k)\frac{m}{d}. \quad (5.9)$$

، نو $l-k \equiv 0\left(\frac{m}{d}\right)$ ، $\text{ggT}(m, \frac{m}{d}) = \frac{m}{d}$ ، دا په دي معنا، چې

، له دي سره $l-k \equiv 0(d)$

کڼونپوهنه

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

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

یادونه 5.1.2: د $ax \equiv b(m)$ دتولو اینکونگروانت حلونو ته بسیا کوي، چې یو

خانگړی حل x_0 پیدا کړو. ټول اینکونگروانت حلونه دا لاندې څپره لري

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

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

د حل عملي شمېرنه:

بېلگه 5.1.3: د $32x \equiv 20(14)$; $\text{ggT}(32, 14) = 2 \mid 20$ له امله یو حل

شتون لري.

را کمونه:

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

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

د اکلید په لار: $2 = \text{ggT}(4, 14) = (-3) \cdot 4 + 1 \cdot 14$ ، 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: $\text{mod } 14$ اینګونګروانت 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 $5, 12, 19, 26, \dots$

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

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

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

پنځم: د بڼې بدلون له لارې:

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

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

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

کونپوهنه

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

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

$$x \equiv 5(7)$$

شپږم: دويم حل: $5 + 7 = 12$

بېلگه 5.1.4: غوښتنه يا ثبوت د $\bar{3} \pmod{16}$ معکوس (نسبت ضرب ته) غواړو پيدا

کړو. د 4.4.5 پسي $\bar{3}^{-1} \in \mathbb{Z}_{16}$ شتون لري، ځکه چې $\text{ggT}(3, 16) = 1$ ، نو $\bar{3}$

يو لومړنی پاتي ټولگی دی. غواړو يو x پيدا کړو، د $3x \equiv 1(16)$ سره، له دې امله

، نو $3x \equiv -15(16)$ او $x \equiv -5(16)$ ، داپه دې معن، چې $x \equiv 11(16)$

$$\bar{3}^{-1} = \bar{11}$$

سيمولتان کونگروانټ Simultane Kongruenzen

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

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

ځانگړی حالت: $a_i = 1 \quad \forall i$ د لاندې نینونو یا فرضیو له مخې

لومړی: m_1, \dots, m_k جوړه نسبي لومړني.

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

جمله 5.2.1: (چینایي پاتېجمله 5.1) یعنی د پاتو یا باقي مانده وو جمله)) : وي دي

$a_1, \dots, a_k \in \mathbb{Z}$ جوړه نسبي لومړني او $m_1, \dots, m_k \in \mathbb{N}$ په خوښه. نودا لندي حلور دی

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

او دا په حقیقت کې مودولو $m_1 \cdots m_k$ یواځنی.

$$M := m_1 \cdots m_k, M_i := \frac{M}{m_i}, i = 1, \dots, k$$

بنوونه: وي دي

نو $\text{ggT}(M_i, m_i) = 1$ باور لري، ځکه چې: که p یو لومړنی عدد وي د

$p \mid M_i, p \mid m_i$ سره د یوه $1 \leq i \leq k$ لپاره، نو:

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

تضاد، ځکه چې m_i جوړه لومړني وو د نینوني 1 له مخې.

له دي امله $M_i x \equiv 1(m_i)$ د 5.1.1 پسي یو حل $y_i \in \mathbb{Z}, 1 \leq i \leq k$ لري.

راورو یا ترڅپرني نیسو:

کنونپوهنه

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

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

وي 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 سیستم د k کونگروانتو هر يو پوره کوي.

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

$$\alpha - \beta \equiv 0(m_i) \quad \text{باور لري، نو} \quad \alpha \equiv a_i(m_i), \beta \equiv a_i(m_i) \quad \forall i$$

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

د (6) 4.1.5 پسي $\text{kgV}(a_1, \dots, a_k) = m_1 \cdots m_k$ باور لري او

تيک يو حل شتون لري. $\alpha \equiv \beta \pmod{m_1 \cdots m_k}$ ، دا په دې معنا، چې

□

بېلګه 5.2.2 : لاندې سيستم ورکړ شوی:

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

دا چې $3, 5, 7$ جوړه نسبي لومړني دي، نو $\text{mod } 3 \cdot 5 \cdot 7 = 105$ يو يواځنی حل لري

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

لومړی : د بنووني سره سم:

$$35x \equiv 1 \pmod{3} \Rightarrow y_1 = 2,$$

$$21x \equiv 1 \pmod{5} \Rightarrow y_2 = 1,$$

$$15x \equiv 1 \pmod{7} \Rightarrow y_3 = 1$$

$$\Rightarrow x_0 = \sum_{i=0}^3 a_i M_i y_i = 2 \cdot 35 \cdot 2 + 3 \cdot 21 + 2 \cdot 15 = 233 \equiv 2 \pmod{105}$$

دويم: د سکڅيسيف پرځای کولو سره:

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

کینونپوهنه

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

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

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

نو

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

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

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

نو

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

د دې ځانګړي حالت تر څنګ، اوس د کرښیزو کونګروانتو تولیز سیستم تر څپرني لاندې نيسو

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

نیونه یا فرضیه :

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

سری کړی شي وښايي:

جمله 5.2.3 : که کرښیزو کونګروانتو یو ټولیز [5.2](#) سیستم د پورته نیونو سره مخ ته ولرو، نو یواځنی ټاکلی حل $\text{mod } m_1 \cdots m_k$ شتون لري .

د لاندې یو په بل پسې ایښوونې له لارې عملي شمېرنې ته

بېلګه 5.2.4 : لاندې د کرښیزو کونګروانتو سیستم دې ورکړ شوی وي:

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

لکه ساده چې لیدل کیږي، دواړه نیونې پوره دي، د جملې [5.2.3](#) پسې د حلونو شتون تضمین دی.

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

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

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

نو

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

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

نو

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

کښونپوهنه

$$\overline{11}, \overline{25}, \overline{39}, \overline{53} \in \mathbb{Z}_{50}.$$

د سیستم حل (5.20). د ټول ځلونو ټولګه:

پښې یادونه:

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

.... ټولیز 5.2

د، ټولیز،، لاندې د 5.19 ډول یا تیوې سیستم پوهیرو، چېرته چې ټول $\alpha_i = 1$ نه دي.

الجبري کونګروانت Algebraische Kongruenzen

پېژند(تعریف) 5.3.1 : وي دي

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

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

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

يو الجبري کونګروانت یل کيږي د درجي n . غوښتونې: ټول $x_0 \in \mathbb{Z}$ د لاندې سره

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

یادونه 5.3.2 :

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

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

نو : حلونه د پولینومون صفر ځایونه دي

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

په \mathbb{Z}_m کې.

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

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

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

د لاس ته راوړنو سره (3) 4.1.6 :

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

$$\Rightarrow x_1$$

بېلګه 5.3.4 : لومړی: $x^3 - x \equiv 0(3)$: ټول حلونه دي پيدا شي.

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

کونپوهنه

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

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

پېژند(تعریف) : که

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

وي، نو

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

د $f(x)$ (فورمال) مشتق بلل کيږي.

یادونه 5.3.6 : د تول $\forall x, a \in \mathbb{Z}$ 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، چېرته چې $g(a) = f'(a)$ باور لري..

) $\lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a} = f'(a)$ ، ځکه چې f پولینوم دی، دا په دې معنا، چې

مشتق $\lim_{x \rightarrow a} g(x) = g(a)$ ، ځکه چې g پولینوم دی له دې لاس ته راځي، چې ناپربکېدونکی دی.)

د حلونو عملي شمېرنه Praktische Berechnung der Lösungen

لومړی : لیمما 5.3.7 : $f(x) \equiv 0(m)$ تیک هلته حلور دی، که $f(x) = 0(p_i^{\alpha_i})$ حلور وي د ټولو $i = 1, \dots, k$ لپاره او که $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ د لومړنی ضرب توتنه ونه وي.

بنوونه :

(\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، یعنی $f(x) \equiv 0(p_i^{\alpha_i}) \forall i = 1, \dots, k$ هم حلور دی ځکه چې $p_i^{\alpha_i} \mid m$ (4.1.5(3))

(\Leftarrow)

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

دا لاندې سیستم تر څپرني نیسو

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

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

ګڼونپوهنه

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

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

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

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

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

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

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

$$f(x) \equiv 0 (p) \quad \text{د } 0, 1, \dots, p-1 \text{ څا په ځای کوني يا ايښووني له لارې د}$$

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

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

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

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

بنونه:

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

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

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؟

لېما 5.3.9 : $x_0 = a + tp^{n-1}$ د $a, t \in \mathbb{Z}$ او $f(a) \equiv 0(p^{n-1})$ سره ټيک

هله د $f(x) \equiv 0(p^n)$ يو حل دی، که $t \in \mathbb{Z}$ د کرښيز کونگروانخ يا ورته والي حل وي؟

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

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 دي: دا t د کرښيز گونگرواينځ 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 $\text{ggT}(p^{n-1}, p^n) = p^{n-1}$ له امله لاس ته راځي:

$$\frac{f(a)}{p^{n-1}} + tg(x_0) \equiv 0(p). \quad (5.38)$$

دا چې $x_0 = a + tp^{n-1}$ دی، نو $p \mid x_0 - a$ باور لري: ، يعني $x_0 \equiv a(p)$ ، د(3) [4.1.6](#) پسي $g(x_0) \equiv g(a)(p)$ باور لری (ځکه چې g پولينوم دی)، دا په دې م عنا، چې

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

 (\Leftarrow)

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

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

بنايو؛ $f(x) \equiv 0(p^n)$ د $x_0 = a + tp^{n-1}$ 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 چي

$$f(x_0) - f(a) = (x_0 - a)g(x_0) \equiv tp^{n-1}f'(a)(p^n). \quad (5.42)$$

له دي سره $f(x_0) \equiv 0(p^n)$ ، دا په دي معنا، چي

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

د $f(x) \equiv 0(p^n)$ حل دی.

کنونپوهنه

لومړی : $f(x) \equiv 0(p_i^{\alpha_i}) \quad a_i \in \mathbb{Z}$ د ټول حلونه د هر
 $i = 1, \dots, k \quad (m = p_1^{\alpha_1} \cdots p_k^{\alpha_k})$
 لپاره معلوم دي، نو بیا سری په خوښه یو k -
 $f(a_i) \equiv 0(p_i^{\alpha_i}) \quad \forall i$
 ټول یا k -گون جوړوي، چېرته چې ، او دا سیستم باورلري:

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

یم : نو دا سیستم بیا د ضرب $p_1^{\alpha_1} \cdots p_k^{\alpha_k} = m$ مودولو یواځنی حل $a \in \mathbb{Z}$
 $f(x) \equiv 0(m) \quad a \in \mathbb{Z}$ هم د 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 $\text{mod } 5^1$:

$$x^3 + 2x^2 - 2x - g \equiv 0(5) \quad \text{فقط حل } 1(-0, -2, -3, -4) \text{ لري، دا په دې}$$

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

دویم: حل $\text{mod } 3^3$:لومړی $\text{mod } 3^1$:

$$x^3 + 2x^2 - 2x - 6 \equiv 0(3)$$

حل 0, 2 لري.

له دې څخه $\text{mod } 3^2$:

د $a = 0$ مخ ته تلنه :

$$f(a) = f(0) = -6, f'(a) = -2$$

يعني بايد حل شي:

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

$$-2x + (-2) \equiv 0(3) \Rightarrow t = -1$$

دا په دې معنا، چې او

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

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

له دې څخه $\text{mod } 3^3$:

$$f(-3) = -9, f'(-3) = 13 \Rightarrow 13x - \frac{9}{3^2} \equiv 0(3)$$

دا په دې معنا، چې

$$13x \equiv 0(3) \quad \text{يعني ،} \quad x \equiv 1(3) \quad \text{يعني ،} \quad t = 1$$

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

بېرته $\text{mod } 3^2$:

ګڼونپوهنه

د $a = 2$ مخ ته بیونه یا مخ ته تلنه:

$$a_1 = a + tp^{2-1}$$

، چېرته چې t د

$$f'(a)x + \frac{f(a)}{p^{a-1}} \equiv 0(p); \quad (5.47)$$

حل دی.

$$f'(2) = 18, f(2) = 0$$

، یعنی حل کوو: $18x + \frac{6}{3} \equiv 0(3)$ ، دا په دې معنا، چې

$$18x \equiv -2(3)$$

$$\text{ggT}(18, 3) = 3 \nmid -2$$

د له امله لاس ته راځي:

کومه $t \in \mathbb{Z}$ شتون نه لري، ینی هم a_1 شتون نه لري، داپه دې معنا، چې د $a = 2$ و یو $\text{mod } 3^2$ حل ته مخ ته بیونه نه شته، یعنی هم $\text{mod } 3^3$ حل شتون نه لري.

$$\begin{array}{cc} \text{mod } 5^1 & \text{mod } 3^1 \\ : & : \\ 1 & 0 \quad 2 \end{array}$$

↓ ↓

$$\begin{array}{c} \text{mod } 3^2 \\ : \\ -3 \end{array}$$

مخ ته بیونه ناشوني ده

↓

$$\begin{array}{l} \text{mod } 3^3 \\ : \\ 6 \end{array}$$

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

$$\left. \begin{array}{l} x \equiv 1(5) \\ x \equiv 6(3^3) \end{array} \right\} (5.48)$$

وېم:

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

له دې سره: $x = 1 + 5t = 1 + 5 \cdot 1 = 6 \Rightarrow x = 6$ یواځنې $\text{mod } 135$
ناګونګروانځ حل دی.

د الجبري کونګرواینځو دحلونو ګڼون یا تعداد
بېلګه 5.3.11:

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

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

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

کڼونپوهنه

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

یادونه 5.3.12: په څرگنده توگه په ټولیز ډول ناشوني دی، چې د الجبري ویناو د حلونو په تعداد څه ووايو. او همداسي لاندې جمله هم د تعجب وړ ده، هغه چې د ځانگړي حالت لپاره، چې د لومړني عدد مودولو دی، مگر سره له دې پوښتنې ته ځواب، چې څومره حلونه شتون لري، ولرو:

جمله (لاگرانژ (1736-1813) (5.3) 5.3.13 : وي دي

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

د $grad f = n$ ($i = 1, \dots, n$) سره او یو لومړنی عدد p دي ورکړ شوی وي. که p ټول $a_i, i = 1, \dots, n$ ونه وېشي، نو $f(x) \equiv 0(p)$ خورا زیات $grad f = n(p)$ اینکونگرواینټ حلونه لري.

ښوونه: سری 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 کونگرواینټ ه یو کوچنی درجه ولري.

$n = 1$:

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

که $\text{ggT}(a_1, p) \mid -a_0$ ، نو باور لري، چې اینکونگرواینټ حلونه شتون لري.

$n - 1 \rightarrow n$:

$$a_n x^n + \dots + a_1 x + a_0 \equiv 0(p) \quad \text{mit} \quad (5.50)$$

$$\text{ggT}(a_n, p) = 1, p \nmid a_n.$$

یا حل نه شته، چې بیا کار تمامدی.

یا: $a \in \mathbb{Z}$ دې له هغو څخه یو حل وي، د پورته پسي 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 ورپسي حل $x_0 \in \mathbb{Z}$ لپاره، یعنی:

$$(x_0 - a)g(x_0) \equiv 0(p) \Rightarrow p \mid (x_0 - a)g(x_0); \quad (5.52)$$

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 پسي اینکونگروانت 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

$\text{grad } g = n - 1$ باور لري. پسي a_n د خوراجک ضریب هم دی! د

وراندنیوني له مخې باور لری $p \nmid a_n$.

ګڼونپوهنه

د ایدکشن وړاندنیونې له مخې د $x_0 \in \mathbb{Z}$ لپاره زیات له زیاته $n - 1$ امکانات)
 $f(x) \equiv 0(p) \pmod{p}$ شتون لري. له دې سره زیات له زیاته
 $(n - 1) + 1 = n \pmod{p}$ اینګونګروانت حلونه لري.

لومړني پاتي ټولګي ګروپونه \pmod{m}

Die prime Restklassengruppe \pmod{m}

د ابل ګروپ (\mathbb{Z}_m^*, \cdot) Die abelsche Gruppe

د 4.4.5 پسي یونونه یا واحدونه (دا په دې معنا، چې د معکوس کیدونکو توکو

ضرب) ټیک د لومړنی پاتي ټولګي $\bar{a} \in \mathbb{Z}_m$ دي، دا په دې معنا، چې هر د
 $\text{ggT}(a, m) = 1$ سره. وي دې په \mathbb{Z}_m^* کې د ټولو واحدونو ډېری یا ست. نو
 باور لري:

لېما 6.1.1 : (\mathbb{Z}_m^*, \cdot) یو ابل ګروپ جوړوي.

بنوونه:

لومړی: که $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$ وي، نو $\bar{a} \cdot \bar{b} \in \mathbb{Z}_m^*$ دی، نو $\bar{a} \cdot \bar{b} \in \mathbb{Z}_m^*$ دی، خکه
 $\bar{a}' \cdot \bar{b}' \in \mathbb{Z}_m$ د ځنو لپاره، یعنی
 $\bar{a} \cdot \bar{a}' = \bar{1}, \bar{b} \cdot \bar{b}' = \bar{1}$
 $(\bar{a} \cdot \bar{a}') \cdot (\bar{b} \cdot \bar{b}') = \bar{1} \cdot \bar{1} = \bar{1}, (6.1)$

دویم: دا په دې معنا، چې $(\overline{ab})(\overline{a'b'}) = \bar{1}$ ، همداسې

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

$$\overline{a} \cdot \overline{b} \in \mathbb{Z}_m^*$$

دويم: يعنې د تعريف له مخې باور لري

درېم: اسوحياتيويټي روښانه ده، ځکه چې په $(\mathbb{Z}_{m,}^*)$ کې پوره ده، او باور لري:

$$\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$$

څلورام: کموتاتيويټي روښانه ده، ځکه چې همداسې له $(\mathbb{Z}_{m,}^*)$ را پاتې ده.

پنځم: وي دي $\overline{a} \in \mathbb{Z}_m^*$ ، نو يو $\overline{b} \in \mathbb{Z}_m$ شتون لري، د $\overline{a}\overline{b} = \overline{1}$ سره، يعنې

$\overline{b}\overline{a} = \overline{1}$ (د کموتاتيويټي له امله)، دا په دي معنا، چې \overline{b} هم د \mathbb{Z}_m يو يوون يا واحد دی، او له دي سره لاس ته راځي:

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

پېژند (تعريف) 6.1.2: د ابل گروپ $(\mathbb{Z}_{m,}^*, \cdot)$ لومړنی پاتېټولگي گروپ $\text{mod } m$ بلل کيږي.

بېلگه:

$$\mathbb{Z}_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}, \mathbb{Z}_{12}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$$

څومره توکي لري؟ \mathbb{Z}_m^*

ګڼونپوهنه

په ټوليزه توګه د يوه ګروپ (G, \cdot) د توکو تعداد يا ګڼون د G نظم بلل کيږي. سومبولیک $|G|$.

پېژند يا تعريف 6.1.4: د (\mathbb{Z}_m^*, \cdot) نظم د $\varphi(m)$ سره ښوول - يا په نڅښه کيږي، تابع يا بلواک

$$\varphi : \mathbb{N} \rightarrow \mathbb{N}, \varphi(n) \mapsto |\mathbb{Z}_m^*| \quad (6.4)$$

د اوپلر Euler φ - تابع بلل کيږي.

ليما 6.1.5: وي دي $m \in \mathbb{N}$ په خوښه، نو د $k \in \mathbb{N}$ ګڼون يا تعداد $\varphi(m)$ دی د $\text{ggT}(k, m) = 1$ او د $1 \leq k \leq m$ سره .

$$\mathbb{Z}_m = \{\bar{1}, \bar{2}, \dots, \bar{m} = \bar{0}\}$$

ښوونه:

$$\bar{k} \in \mathbb{Z}_m^* \stackrel{4.4.5}{\Leftrightarrow} \text{mod } m \text{ لومړنی پاتي ټولگی } \bar{k} \text{ دی}$$

$$\Leftrightarrow \text{ggT}(k, m) = 1,$$

دا په دي معنا، چي په \mathbb{Z}_m^* کي د توکو تعداد يا ګڼون د k د تعداد سره برابر دی، $\text{ggT}(k, m) = 1$ د $k \in \mathbb{N}, 1 \leq k \leq m$ سره . \square

پسې راتلنه يا نتيجه 6.1.6 : وي دي $p \in \mathbb{P}$ يو په خوښه لومړنی گڼ يا عدد، نو
 $\varphi(p) = p - 1$
 باور لری:

د شمیرني ته $\varphi(m)$ *Zur Berechnung von*
 پېژند يا تعريف 6.1.7 : د ټولو اعداد يا د ټول اعدادو يوه ډېری لومړنس پاتي سيستم $\text{mod } m$ بلل کيږی، که دا له هر لومړنی ټولگي $\text{mod } m$ ټيک يو توکی ولري.

ليما 6.1.8 : يو لومړنی پاتي سيستم ټيک $\text{mod } m$ ټيک $\varphi(m)$ توکي لري، ځکه
 چې د 6.1.5 پسې ټيک يوونونه يا واحدونه $\varphi(m) = |\mathbb{Z}_m^*|$ ، يعنی لومړني پاتي
 ټولگي $\text{mod } m$ شتون لري.

بېلگه 6.1.9 :

لومړی : $m = 6\{0, 1, \dots, 5\}$ يو پوره پاتي سيستم دی، $\{1, 5\}$ يو لومړنی پاتي
 سيستم دی، يعنی : $|\mathbb{Z}_6^*| = 2$ ، دا په دې معنا، چې $\varphi(6) = 2$.

دويم:

$$m = 5\{0, 1, \dots, 4\}$$

يو پوره پاتي سيستم دی، $\{1, 5\}$ يو لومړنی پاتي سيستم دی، يعنی $|\mathbb{Z}_6^*| = 2$ ، دا
 په دې معنا، چې $\varphi(6) = 2$.

کنونپوهنه

جمله 6.1.10 : وي دي $\{r_1, \dots, r_{\varphi(m)}\}$ ، $m, n \in \mathbb{N}, \text{ggT}(m, n) = 1$ يو

لومړنی پاتي سیستم $\text{mod } m$ دی، او $\{s_1, \dots, s_{\varphi(n)}\}$ يو لومړنی پاتي سیستم $\text{mod } n$ دی، نو

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

يو لومړنی پاتي سیستم $\text{mod } m \cdot n$ دی.

بنوونه: $\{r_1, \dots, r_{\varphi(m)}\}$ و يوه پوره سیستم $\text{mod } m$ ته پوره يا تکميل کړی:

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

او $\{s_1, \dots, s_{\varphi(n)}\}$ و يوه پوره پاتي سیستم $\text{mod } n$ ته پوره کړی:

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

د [4.3.8](#) پسي

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

يو پوره پاتي سیستم $\text{mod } m \cdot n$ دی، په ځانگړې توگه ټول گڼونه يا عددونه له R يعنې هم له T ټول عددونه، انکونگروانځ $\text{mod } mn$ دي.

و بنايي:

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

د $a \in R$ له امله $a = nr_i + ms_j$ باور لري د څنو $1 \leq i \leq m, 1 \leq j \leq n$ 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 شتون لري 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).

وښایي:

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

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

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

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

گنونه پوهنه

بي له ټوليزو بنديزونو يا محدوديتونو دي $p \mid m$ وي (ورته $p \mid n$). نو $p \mid ms_j$
 او $p \mid a$ باور لري، يعني $p \mid nr_i$ ، 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 $\text{ggT}(m, n) \neq 1$ له دې امله $p \mid r_i$
 لاس ته راځي، د $p \mid m$ سره لاس ته راځي $\text{ggT}(r_i, m) \neq 1$ - تضاد، ځکه چې
 T_i د لومړني پاتي سيستم $\text{mod } m$ توکي دی.

يعني: T يو لومړنی پاتي سيستم $\text{mod } mn$ دی. \square

کورولار 6.1.11 : وي دي $\text{ggT}(m, n) = 1$ د $m, n \in \mathbb{N}$ سره، نو باور لري:

$$\varphi(mn) = \varphi(m)\varphi(n). \quad (6.12)$$

بنوونه: د [6.1.10](#) له مخې

$$T = \{nr_i + ms_j \mid i = 1, \dots, \varphi(m), j = 1, \dots, \varphi(n)\} \quad (6.13)$$

يو لومړنی پاتي سيستم $\text{mod } mn$ دی، نو $\varphi(m) \cdot \varphi(n)$ توکي لري. دا چې
 هر پاتي سيستم همدا اوس $\varphi(mn)$ توکي لري، نو لاس ته راځي:
 $\varphi(m) \cdot \varphi(n) = \varphi(m \cdot n)$
 \square

يادونه 6.1.12 : يو تابع $f : \mathbb{N} \rightarrow \mathbb{N}$ د لاندې خويونو سره

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

ضریبي یا خلیزه تابع بیلیري.

له دې سره د اویلر φ -تابع د یوه ضریبي تابع بېلگه ده (کاپیتل یا برخه 11 وګورئ).

پسې راتلنه یا ترې لاس ته راوړنه 6.1.13 : وي دې $m \in \mathbb{N}$ او

$$\text{ggT}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1 \quad m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

د لومړنیضریب توتنه ونه، نو باور لري

، یعنی

$$\varphi(p_i^{\alpha_i} \cdot p_j^{\alpha_j}) = \varphi(p_i^{\alpha_i}) \cdot \varphi(p_j^{\alpha_j}). \quad (6.15)$$

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 کیري، د لومړني عدد p او $n \in \mathbb{N}$ لپاره.

جمله 6.1.14 : وي دې p یو لومړنی ګڼ یا عدد، $k \in \mathbb{N}$ ، نو باور لري::

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

کڼونپوهنه

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

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

\Rightarrow

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

$$p \mid a$$

\Rightarrow

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

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

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

د $1 \leq a \leq p^k$ ($a \in R$) له امله باور لري $1 \leq pt \leq p^k$ ، يعني
 بايد $1 \leq t \leq p^{k-1}$ باور ولري.

برعکس هر $t \in \mathbb{N}$ د $1 \leq t \leq p^{k-1}$ سره هم $p \mid pt = a$ پوره کوي. يعني
 تیک p^{k-1} گڼونه $a \in R$ شتون لري د $p \mid a$ سره، يعني

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

$$\Rightarrow \exists p^k - p^{k-1}a \in R : \text{ggT}(a, p^k) = 1$$

□ . له دې سره د پيژند له مخې هم باور لري: $\varphi(p^k) = p^k - p^{k-1}$.

کورولار يا وره جمل 6.1.15: وي دې $m \in \mathbb{N}, m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ په لومړنيو
 ضريبونو ټوټه کونه ، نو باور لري:

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

(دا په دې معنا، چې په په پاتېټولگي کړی (رين، حله) $\text{mod } m$ کې د يونونو يا
 واحدونو گڼون يا تعداد شتون لري).

بېلگه :

لومړی :

$$m = 25m = 5^2 \Rightarrow \varphi(25) = 25 - 5 = 20$$

يعني $|\mathbb{Z}_{25}^*| = 20$ ، دا په دې معنا، چې په \mathbb{Z}_{25} کې تیک 20 يونونه يا واحدونه
 شتون لري.

دويم:

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

يعني $|\mathbb{Z}_{72}^*| = 24$ دا په دې معنا، چې په \mathbb{Z}_{72} کې ټيک 24 يونونه يا واحدونه شتون لري.

د اويلر جمله

Der Satz von Euler

ليما 6.1.17: وي دې $G = \{g_1, \dots, g_n\}$ يو پای، ابل گروپ، نو باور لري:

لومړی: د هر $a \in G$ لپاره باور لري ، $ag_i \neq ag_j \forall i \neq j$

دويم: د هر $a \in G : a^n = e$ لپاره باور لري، د کوم سره چې e د (G, \cdot)

يوون يا واحد دی، او $n = |G|$ دی.

بنوونه:

يو ته :

وړاندنيونه $ag_i = ag_j$ د يوه $a \in G, i \neq j$ لپاره، نو د $a^{-1} \in G$: سره د ضربولو له لارې لاس ته راځي:

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

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

دويم ته:

د لومړي ټکي له مخي $ag_i \neq ag_j$ باور لري، يعنې د $e(g_1 \cdots g_n) = g_1 \cdots g_n$ لپاره بېرته n مختلف توکي لاس ته راځي. له دې سره باور لري $i = 1, \dots, n$

$$g_1 \cdots g_n = (ag_1)(ag_2) \cdots (ag_n) = a^n(g_1 \cdots g_n), \quad (6.22)$$

همداسي

$$e(g_1 \cdots g_n)(g_1 \cdots g_n)^{-1} = a^n(g_1 \cdots g_n)(g_1 \cdots g_n)^{-1}. \quad (6.23)$$

له دې سره ترلې $e = a^n, n = |G|$ راكوي . □

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

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

بنوونه: د $\text{ggT}(a, m) = 1$ له امله باور لري: $\bar{a} \in \mathbb{Z}_m$ لومړنی پاتي ټولگی $\text{mod } m$ دی، يعنې $\bar{a} \in \mathbb{Z}_m^*$ باور لري . د $|Z_m^*| = \varphi(m)$ له امله د تعريف له مخي، د 6.1.17 له مخي لاس ته راځي:

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

ګڼونپوهنه

$$a^{\varphi(m)} \equiv 1(m) \quad \square \text{ باور لري. داسې چې}$$

يو ځانګړی غوره حالت او د [6.1.18](#) مشهور غوره حالت غواړو په لاندې کې ځانله تر څېړنې لاندې ونیسو:

کوروار 6.1.19: (کوچنی فرمات) د ټولو $a \in \mathbb{Z}, p \in \mathbb{P}$ لپاره باور لري:

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

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

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

نو په ځانګړې توګه $a^p \equiv a(p)$.

که وي $\text{ggT}(a, p) \neq 1$ ، 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 پیدایښتي ګڼ یا طبیعي عدد p لپاره باور لري:

$$\begin{aligned} & \text{لومړنی عدد دی } p \\ & (6.28) \\ & \Leftrightarrow (p-1)! \equiv -1(p). \end{aligned}$$

ښوونه:

(\Rightarrow)

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

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

نو غوښتنه ټيک ده.

وي دي $p > 2$ ، نو د ټولو $a \in \mathbb{N}$ لپاره باور لري د

سر. د [6.1.19](#) له مخي دي a لپاره لاس

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

ته راځي:

له دي سره ټول عددونه $1 \leq a \leq p - 1$ د الجبري کونگروانځ

حلونه دي. د [5.3.13](#) له مخي کونگروانځ خورازيات $x^{p-1} \equiv 1(p)$ د

پولينوم درجه ده $\text{mod } p$ بنکونگروانټ حلونه، له دي سره لاس ته راځي:

همدا اوس ټول انکونگروانټ $1, 2, \dots, p - 1$ $\text{mod } p$ حلونه دي.

پسي الجبري کونگروانځ

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

انکونگروانټ حلونه $1, 2, \dots, p - 1$ لري. د $\text{grad} = p - 1$ له امله

ټيک $1, 2, \dots, p - 1$ $\text{mod } p$ انکونگروانټ حلونه دي (د [5.3.13](#) سره د

کڼونپوهنه

ضریب دی، نو x^{p-1} یو دی، نو د p له لارې پروېشوني نه ده. د ضربولو وروسته
سری یو د $p-1$ درجې پولینوم د مطلق لري

$$c_0 = (-1)(-2) \cdots (-(p-1)) = (-1)^{p-1}(p-1)! = (p-1)! \quad (6.30)$$

سره لاس ته راوړي، ځکه چې $p > 2$ ، نو ناجوره یا طاق دی.

له $x^{p-1} \equiv 1(p)$ څخه د دې کونگروانتونو کمون له لارې سری یو الجبري
کونگروانت لاس ته راوړي

$$f(x) \equiv 0(p), \quad \text{grad } f \leq p-2 \quad (6.31)$$

او مطلق غری $-1 - c_0 = -1 - (p-1)!$
دا کونگروانت زیات له زیاته .
انگروانت $\text{grad } f \leq p-2 \pmod p$ حلونه لري، که p نه د f ټول ضریبونه
وېشي (5.3.13) مگر: $1, 2, \dots, p-1$ $p-1$ انگروانت $\pmod p$ حلونه دي
له دې سره لاس ته راځي: f د p ټول کونگروانتونه وېشي، په ځانگړې توگه
 $-1 - c_0$ ، دا په دې معنا، چې

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

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

(\Leftarrow)

وي دي $n \in \mathbb{N}$ د $(n-1)! \equiv -1(n)$ سره نيسو، چي $n \notin \mathbb{P}$ له دي .
 سره يو لومړنی ګڼ p د $p | n$ سره او $2 \leq p \leq n-1$ سره شتون لري، له دي سره

$$p | (n-1)! \Rightarrow (n-1)! \equiv 0(p). \quad (6.33)$$

د $(n-1)! \equiv -1(n)$ له امله د $p | n$ سره لاس ته راځي، چي
 د $(n-1)! \equiv -1(p)$ له دي سره لاس ته راځي .

$$0 \equiv (n-1)! \equiv -1(p) \Rightarrow p | 0 - (-1) = 1 \quad (6.34)$$

--- تضاد) $p > 1, p \in \mathbb{P}$ (\square

يادونه 6.1.21 : د ويلسن (6.1.20) 1741-1793) جملې له امله دا تروسه يواځنی څرګنده يا معلوم د لومړنيو ګڼو قضيه انځوروي!

د (\mathbb{Z}_m^*, \cdot) جوړښت Struktur von (\mathbb{Z}_m^*, \cdot)

د (\mathbb{Z}_m^*, \cdot) نظم د اويلر φ تابع په څخه معلوم دی: $|\mathbb{Z}_m^*| = \varphi(m)$

د ګروپ تيوري له مخې خورا ځانګړي ګروپونه داسې په نامه ،، ځيوکليکي،، ګروپونه دي:

پيژند(تعريف) 6.2.1 : يو پای ګروپ (G, \cdot) ځيوکليکي دی، که

کنونپوهنه

$$G = \{a, a^2, \dots, a^{|G|} = e\} \quad (6.35)$$

د لږ تر لږه یوه $a \in G$ لپاره باور ولري. یو توکی $a \in G$ د دې خوي سره د (G, \cdot) تولیدېدونکی توکی بلل کیږي.

یادونه 6.2.2:

لومړی: د یوه ځیوکلیکي گروپ (G, \cdot) هر توکی g کیدی شي د یوه کره یا همغه کلک توکی $a \in G$ د توان په توگه ولیکل شي: $g = a^n$ د یوه $n \in \mathbb{N}$ لپاره د $1 \leq n \leq |G|$ سره.

دویم: هر ځیوکلیکي گروپ (G, \cdot) د ابل گروپ دی.

$$\begin{aligned} & \text{د یوه تولیدي توکي لپاره } (g, h \in G \Rightarrow g = a^m, h = a^n) \\ & a \in G \Rightarrow g \cdot h = a^m \cdot a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m = h \cdot g \end{aligned}$$

بیلگه 6.2.3:

لومړی: (\mathbb{Z}_5^*, \cdot) ځیوکلیکي دی:

$$\mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} \quad (\varphi(5) = 4) \quad \bar{2}^1 = \bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{3}, \bar{2}^4 = \bar{1} \Rightarrow a = \bar{2}$$

د (\mathbb{Z}_5^*, \cdot) یو تولیدي سیستم دی.

همداسي: $\bar{3}^1 = \bar{3}, \bar{3}^2 = \bar{4}, \bar{3}^3 = \bar{2}, \bar{3}^4 = \bar{1}$
 توليدي سيستم دی. (\mathbb{Z}_5^*, \cdot) يو همدا $a = \bar{3}$ نو د

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

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

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

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

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

$\mathbb{Z}_2^* = \{\bar{1}\}$ - trivial; $\mathbb{Z}_4^* = \{\bar{1}, \bar{3}\}, \bar{3}$ ساده دی،
 $\mathbb{Z}_2^* = \{\bar{1}\}$ - trivial; $\mathbb{Z}_4^* = \{\bar{1}, \bar{3}\}, \bar{3}$ توليدي توکی دی)

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

پيژند(تعريف) 6.2.4: يو تول گن يا - عدد $g \in \mathbb{Z}$ ساده ريښه $\text{mod } m$ بلل کيږي،
 که $\bar{g} \in \mathbb{Z}_m^*$ لومړنی پاتي تولگيگروپ (\mathbb{Z}_m^*, \cdot) توليد کړي.

بيلگه 6.2.5:

لومړی: 2 يو ساده ريښه $\text{mod } 5$ دی (پورته بيلگه وکوری: $\bar{2} \in (\mathbb{Z}_5^*, \cdot)$ توليدوي)،
 همداسي: $g = 3$ ساده ريښه $\text{mod } 5$ دی.

گنونپوهنه

دویم: کومه ساده ریښه $\text{mod } 8$ شتون نه لري (همداسې: (\mathbb{Z}_8^*, \cdot) څیوکلیکي نه دی).
دریم: 1 ساده ریښه $\text{mod } 2$ ، 3 ساده ریښه $\text{mod } 4$ دی.

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

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

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

$$a^k = e \quad k \in \mathbb{N} \Leftrightarrow \text{ord } a \mid k. \quad (6.36)$$

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

جمله 6.2.8: وي دې p یو لومړنی عدد، نو (\mathbb{Z}_p^*, \cdot) څیوکلیکي یا تل بېرته راگرځېدونی دی.

(دایه دې معنا، چې ذات وخت ساده ریښې $\text{mod } p$ شتون لري، خو شمېرنو ته یې ټولیز متود شتون نه لري؟)

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

جمله 6.2.10: وي دي $p > 2$ لومړنی عدد، نو $(\mathbb{Z}_{p^\alpha}^*, \cdot) \forall \alpha \in \mathbb{N}$ خيکليکي دي (څيکليکي دي) دا په دي معنا، چپوه ساده ريښه شتون لري). $\text{mod } p^\alpha \forall \alpha \in \mathbb{N}$

ښوونه: له ښووني: که g ساده ريښه $\text{mod } p$ وي، نو باور لري:

$$g^{p-1} \not\equiv 1(p^2) \vee (g+p)^{p-1} \not\equiv 1(p^2). \quad (6.37)$$

پام؛ $g+p$ ساده ريښه $\text{mod } p$ دي. ($\Rightarrow \exists$) له دي لاس ته راځي تل يو g شتون لري لکه په [6.2.9](#) کي غوښتل شوي). \square

بيلگه 6.2.11: وي دي $p = 5$ ، د [6.2.3](#) له مخي $g = 2$ يوه ساده ريښه $\text{mod } 5$ دي، د

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

له امله $g = 2$ يوه ساده ريښه $\text{mod } 5^\alpha \forall \alpha \in \mathbb{N}$ ده، دا په دي معنا، چي $\text{mod } 25, 125, 625, \dots$

په همدې توگه: $g = 3$ يوه ساده ريښه $\text{mod } 5$ ده، د

$$g^{p-1} = 3^{p-1} = 3^4 = 81 \not\equiv 1(25) \quad (6.39)$$

له امله 3 هم يوه ساده ريښه $\text{mod } 5^\alpha \forall \alpha \in \mathbb{N}$ دي.

گنونپوهنه

جمله 6.2.12: $p > 2$ دې یو لومړنی عدد وي، نو $(\mathbb{Z}_{2p^\alpha}, *)$ څیوکلیکي دی $\forall \alpha \in \mathbb{N}$ (دا په دې معنا، چې یوه ساده ریښه شتون لري).

ښوونه: له ښوونې څخه: g دې ناجوره وي، $g \in \mathbb{Z}$ ، او یوه ساده ریښه $\forall \alpha \in \mathbb{N}$ $g \pmod{2p^\alpha}$ ده، نو هم یوه ساده ریښه $g \pmod{p^\alpha}$ ده، که g جوړه وي، نو $g + p^\alpha$ ناجوره دی او ساده ریښه $\pmod{p^\alpha}$. □

بیلگه 6.2.13: وي دې $p = 5$ ، د 6.2.11 له مخې $g = 3$ یوه ساده ریښه

$\forall \alpha \in \mathbb{N}$ $g \pmod{5^\alpha}$ ده او ناجوره، نو لاس ته راځي: 3 یوه ساده ریښه $\forall \alpha \in \mathbb{N}$ $g \pmod{2 \cdot 5^\alpha}$ ده، دا په دې معنا، چې

د 6.2.11 له مخې $g = 2$ هم ساده ریښه $\forall \alpha \in \mathbb{N}$ $g \pmod{5^\alpha}$ ده، مگر جوړه، بیا هم $g' = 2 + 5^\alpha$ ناجوره او ساده ریښه $\pmod{5^\alpha}$ ده، نو هم ساده ریښه $\pmod{2 \cdot 5^\alpha}$ ده.

لیما 6.2.14: د $\alpha \geq 3$ لپاره $(\mathbb{Z}_{2^\alpha}^*, *)$ څیوکلیکي نه دی. (دا په دې معنا، چې ساده ریښه $\pmod{2^\alpha}$ شتون نه لري د $\alpha \geq 3$ لپاره).

جمله: (گاوس 1777-1855). $(\mathbb{Z}_m^*, *)$ ټیک هلته څیوکلیکي دی، که

د $m \in \{2, 4, p^\alpha, 2p^\alpha\}$ $p > 2, p \in \mathbb{P}$ سره او $\alpha \in \mathbb{N}$ په خوښه وي

(6.40)

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

جمله 6.2.16: هر $\bar{a} \in \mathbb{Z}_{2^m}^*$ ته يو يواځنی ټاکلی $j \in \{0, 1\}$ او
 $n \in \{1, 2, \dots, 2^{\alpha-2}\}$ شته دی د لاندې سره.

$\bar{a} = \overline{(-1)^j 5^n}$.	(6.41)
-------------------------------------	--------

کارونه: کریپتولوژيKryptologie Anwendung:

د خبررسوني لپاره تل اړين همداسي غوښتنور دی، چې معلومات فقط نیونکي B او نه بل چا ته ورسیري. کریپتولوژي د متودونو پوهنه ده، چې د خورا کم یا مینیمال ورزیات معلومات له مخي (د له B لاري ورکړشوی) څوک د $A \rightarrow B$ څخه خبر پرانستلی نه شي، چې دا معلومات ونه لري.

بیلگه 6.3.1: (،Caesar“) الفبي: A, B, \dots, Z ، په خوښه ټاکل $n \in \mathbb{N}$ شوی، تعریفوو:

$A = n$ -ter Buchstabe, م توری

$B = (n+1)$ -ter Buchstabe, م توری

⋮

$Y = (n-2)$ -ter Buchstabe, م توری

$Z = (n-1)$ -ter Buchstabe. م توری

ګڼونپوهنه

له دې سره د $n=6$ لپاره بریدتی قلفیری و FSLWNKK ته وازېدنه ښوونې ده، که $n = 6$ معلوم وي.

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

فکر یا اند

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

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

تلنلار

که A و B به ته یو خبر استول غواړي، نو دوه ډېر ستر ګڼونه p, q ټاکي او یو عدد $e > 1, e \in \mathbb{N}$ چې $\varphi(n) \mid n = p \cdot q$ ته نسبي لومړني عدد دی، او په (څرګند ډول) n او e معلوم ورکوي. دلته غوره ټکی: که سړی n, e هم وپېژني، د n دواړه لومړني ضریبونه (په ټولیزه توګه) p, q نه ټاکل کيږي. دا عددونه p, q باید سړی وپېژني 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 کرښیز کونګرواینڅ

$\text{mod } \varphi(n)$
حل یا اوبیونه).

د یوه خبر د قلفولو یا شفر کولو لپاره $\text{mod } \varphi(n)$ دا د یوه عدد ښه (لکه په بینار ښه)

اړوي او پیدایښتي بیت طبیعي عدد $w \in \mathbb{N}$ لاس ته راوړي. سړی کړی شي

لاس ته راوړي، داسې چې خبر په بلوکونو برخو یا سترو توتو د $w < n = p \cdot q$
 اوږدوالي سره توتې کړي، او دا ځانله یو پېه ګوني ډول ولیري. دا قلف شوی $l < n$
 لغات w د یوه کوچني بافي c په توګه تعریف دی، کوم چې د $w^e \in \mathbb{N}$ سره د وېشنې
 سره د $n = pq$ له لارې منځ ته راځي، داپه دې معنا، چې $w^e \equiv c(n)$. A اوس $c \in \mathbb{N}$
 ورلیري. د دې لپاره چې w وټاکي، له دې امله الجبري کونګرواینڅ

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

باید حل شي (w یو حل یا اوبی دی) .

دا چې $n \in \mathbb{N}$ ډېر لوي دی، امکان شتون لري، چې دا فقط په لومړنیو ضریبونو توتې شي، او $x^e \equiv c$ د یوګونو اعدو مودولو پسي حل شي (پېسي د چيني پاتي جمله [5.2.1](#) وکتل شي) . له دې سره باید د n دواړه لومړنیو ضریبونه p, q وټاکل شي. (نتشفر کیدی. دا د p, q لپاره ډېر لوي دی،، ناشونی،،) نو له $n, e, c \in \mathbb{N}$ څخه خبر په ټولیزه توګه نه شي وازیدی یا اشفري کیدی.نت

د $c \in \mathbb{N}$ وازول (د $w \in \mathbb{N}$ ټاکولپاره) کیدی شي په لاندې توګه لاس ته راشي:
 $d \in \mathbb{N}$ د $\text{mod } \varphi(n)$ یواځنی لاندې کرښیز کونګرواینڅ زیاتیز- یا مثبت حل دی

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

کنونپوهنه

نو باور لري، چې $w^{ed} \equiv w(n) : w \in \mathbb{N}$ خورا کوچنی څلوری یا مربع باقی دی،
 $w^{ed} \in \mathbb{N}$ کوم چې n له لاری د په وېش منځ ته راځي. (دا چې $c \equiv w^e$ یعنی
 $w \in \mathbb{N}$ 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).

د $ex \equiv 1(\varphi(n))$ له امله کرښیز کونگرواینڅ $\text{ggT}(e, \varphi(n)) = 1$ ښوونه: د
 $\text{mod } \varphi(n)$ ناگونگرواینڅ حل لري: d . [5.1.1](#) له مخې ټیک یو

وښایی:

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

د $\text{ggT}(p, q) = 1$ او $n = pq$ له امله دې فقط وښوول شي، چې

$w^{ed} \equiv w(p) \wedge w^{ed} \equiv w(q)$	(6.47)
--	--------

باور لري (د [4.1.5\(6\)](#) له مخې لاس ته راځي، چې $w^{ed} \equiv w(pq)$ ځکه چې

$$\text{kgV}(p, q) = pq$$

دې، نو هم $p \mid w$ ، یعنی $p \mid w^{ed} - w$ ، داسې چې $w^{ed} \equiv w(p)$
 باور لري. $p \nmid w$ دی: دا چې $ed \equiv 1(\varphi(n))$ (حل دی) بار لري

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

د یوه لپاره $e, d, 1, \varphi(n)$ $k \in \mathbb{N}$ زیاتیز یا مثبت دي. دا چې $\text{ggT}(w, p) = 1$ ، د کوچني فرمات، [6.1.19](#) له مخې باور لري.

$w^{p-1} \equiv 1(p),$ دا په دې معنا چې	$w^{\varphi(n)} \equiv 1(p),$ (6.49)
--	---

له دې سره لرو:

$w^{ed} = w^{1+k\varphi(n)} = w^{1+k(p-1)(q-1)} =$ $w \cdot (w^{p-1})^{k(q-1)} \equiv w \cdot 1^{k(q-1)} = w(p).$	(6.50)
--	--------

ورته: $w^{ed} \equiv w(q) \Rightarrow$ غوښتنه. \square

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

بیلگه 6.3.3 (گنونه په رښتیا ډېر واره دي!)

$n = 23 \cdot 3 = 69, \varphi(n) = 2 \cdot 22 = 44$ $p = 3, q = 23$ B
غوره ټاکي، یعنی
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 یا کود یا پت خبر
 $c = 12$ تر لاسه کوي.

کنونپوهنه

حلونه یا اوبیونه یې: $ex \equiv 1(\varphi(n))$ ، دا په دې معنا، چې $3x \equiv 1(44)$ ،
 $e^d \equiv w(n)$ ، دا په دې معنا، چې $\text{mod } 44$ یواځنی ټاکلی حل: $d = 15$. له دې سره ،
 $12^{15}(69)$ چې

$$12^{15} : 12^2 \equiv 6(69), 12^4 \equiv 6^2 = 36(69), 12^5 \equiv 36 \cdot 12 \equiv 18(69),$$

$$, 12^{10} \equiv 18^2 = 324 \equiv 48(69), 12^{15} = 12^{10} \cdot 12^5 \equiv 48 \cdot 18 \equiv 36(69)$$

نو $w \equiv 12^{15} \equiv 36(n)$ ، دا پټ لغات 36 وو.

۷- د حقیقي اعدادو g - ادیکي وديزیننه

g -adische Entwicklung reeller Zahlen

تولزه وديزیننه 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 $a_n > 0, 0 \leq a_i \leq g (i = 0, \dots, n-1)$ شتون لري د

$$a = a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0 \quad (7.1)$$

سره

د $a \in \mathbb{N}$ -ادیکي وده) g .

د صفر سره نابرابرو حقیقي عددونو ته ټولیزونه:

د $\pi = 3,1415\dots$ لپاره باور لري:

$$\pi = 3 \cdot 10^0 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + \dots = \sum_{i=0}^{\infty} a_i 10^{-i}. \quad (7.2)$$

جمله 7.1.1: $\alpha > 0$ د یو حقیقي عددوي او $g \in \mathbb{N}, g \geq 2$ نو $a_i \in \mathbb{N}_0$ ($i = 0, 1, 2, \dots$) شتون لري د $0 \leq a_i \leq g$ ($i = 1, 2, \dots$)

سره، داسې چې دي

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

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

ښوونه: د یوه داسې انځوروني یواځنوالی:

که $\alpha \in \mathbb{R}^+$ ناراشنل وي، نو $[\alpha]$ د α پسي خورا کوچنی عدد په گوته کوي.

د ټوليزې ښوونې روښانهونه یا تشریح:

$\pi = 3,1415\dots$ ، تعريف کړئ، $a_0 = [\pi] = 3$ ، $a_1 = \pi - [\pi]$ جوړ کړئ او $a_1 = [10a_1] = [1,415\dots] = 1$ تعريف کړئ،

کینونپوهنه

$$\alpha_2 = 10\alpha_1 - [10\alpha_1] = 0,415\dots$$

$$a_2 = [10\alpha_2] = 4$$

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

$$\alpha_1 = \alpha - [\alpha], \dots, \alpha_{i+1} = g\alpha_i - [g\alpha_i], \quad (7.4)$$

او له دې سره تعریف کړئ

$$a_0 = [\alpha], \dots, a_i = [g\alpha_i]. \quad (7.5)$$

باور لري: $0 \leq a_i \leq g \quad \forall i > 0$ ، ځکه چې

$$0 \leq \alpha_i = g\alpha_{i-1} - [g\alpha_{i-1}] < 1 \stackrel{g \geq 0}{\Rightarrow} 0 \leq g\alpha_i \leq g \Rightarrow \quad (7.6)$$

$$\Rightarrow 0 \leq [g\alpha_i] = a_i < g. \quad (7.7)$$

باور لري

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

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

و بنایي:

$$\alpha = a_0 + a_1g^{-1} + \cdots + a_n g^{-n} + \alpha_{n+1}g^{-n} \quad \forall n \in \mathbb{N}$$

$$n = 1 :$$

$$\alpha = a_0 + a_1g^{-1} + \alpha_2g^{-1}$$

پورته لور ته واز دی

$$n \rightarrow n + 1 :$$

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

$$\Rightarrow \alpha = a_0 + a_1g^{-1} + \cdots + a_n g^{-n} + \alpha_{n+1}g^{-n} = \quad (7.9)$$

$$= a_0 + a_1g^{-1} + \cdots + a_n g^{-n} + (a_{n+1}g^{-1} + \alpha_{n+2}g^{-1})g^{-n} = \quad (7.10)$$

$$= a_0 + a_1g^{-1} + \cdots + a_n g^{-n} + a_{n+1}g^{-(n+1)} + \alpha_{n+2}g^{-(n+1)} \quad (7.11)$$

\Rightarrow

چې د $n + 1$ لپاره هم ټيک دی.

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

وینایی: دا لړۍ د α په لور ځي یا α ته کونورکنت کیري.

کڻونپوهنه

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

n - مه ٽوٽه - يا پارشل جمعه (زياتون)

$$s_n = \sum_{i=0}^n a_i g^{-i} = a_0 + a_1 g^{-1} + \dots + a_n g^{-n} \quad (7.13)$$

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

پوره کوي

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

$$0 \leq \alpha_{n+1} g^{-n} < g^{-n} \quad \forall n \in \mathbb{N}; \quad (7.14)$$

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

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

α په لور هڅيري.
يو اڻنوالی (يو اڻيوالی):

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

(7.15)

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

سره، چیرته چې $a_i \neq b_i$ د یوه i لپاره، وي دي خورا کوچنی عدد د $a_{i_0} \neq b_{i_0}$ سره. بي له تولیز محدودیت دي $a_{i_0} > b_{i_0}$ وی.

یعني

(7.16)

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

او لاس ته راځي $\sum_{i=i_0}^{\infty} a_i g^{-i} = \sum_{i=i_0}^{\infty} b_i g^{-i}$ ، له دي سره (د تولیز پولې ته تلني له امله کیدی شي سره راټول شي)

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

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

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

$$= \frac{2-g}{-1+g}$$

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

له دي سره باید په دي تخمین کې هر چیرته برابروالی باور ولري، نو له دي لاس ته راځي:

کنونپوهنه

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

دا په دې معنا، چې

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

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

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

له دې سره ټول زیتوني یا د جمعې اجزای د a_i په انځورونه کې د $i > i_0$ سره
صفر دي، دا په دې معنا، چې

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = a_0 + a_1 g^{-1} + \dots + a_{i_0} g^{-i_0} = a_0 + \frac{a_1}{g} + \dots + \quad (7.23)$$

تضاد دی! نو: a_i فقط یوه g -ادیکي وده لري. \square

یادونه 7.1.2: دی $g = 10$ (لسمیز سیستم)، نو سری د $\alpha = \sum_{i=0}^{\infty} a_i g^{-i}$ لپاره
لیکي هم

$$a_0, a_1 a_2 \dots \quad 0 \leq a_i < 10 \quad \forall i \geq 1. \quad (7.24)$$

کورولار 7.1.3: $\alpha > 0$ یو راشنل عدد دی، نو a_i خورا زیات دوه g -ادیکي
انځوروني، داسې په نامه

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

د کوم سره چې

$$a_i = 0 \quad \forall i > i_0 \quad .1$$

$$b_i = g - 1 \quad \forall i > i_0 \quad \text{او} \quad b_{i_0} = a_{i_0} - 1 \quad .2$$

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

پېژند(تعریف) 7.1.4: سری وایي، $\alpha \in \mathbb{Q}, \alpha = \frac{a}{b}$ یو پای انځورونه لري، که وي

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

$$a_i = 0 \quad \forall i > i_0 \quad \left(\frac{a}{b} = a_0 + a_1 g^{-1} + \dots + a_{i_0} g^{-i_0} \right)$$

د کږم سره چې

7.1.5: کورولار $\frac{a}{b} \in \mathbb{Q}^+$ ټیک دوه مختلف g -ادیکي ودې لري، که $\frac{a}{b}$ یو یواځنی انځورونه ولري.

بنوونه:

(\Rightarrow)

دوه انځورونې لري، نو له دوي څخه یو د [7.1.3](#) له مخې پای دی. $\alpha = \frac{a}{b}$

(⇐)

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

وي دي يوه پای انځورونه، نو باور لري

$$\frac{\alpha}{b} = \sum_{i=0}^{i_0-1} a_i g^{-i} + a_{i_0} g^{-i_0} = \sum_{i=0}^{i_0-1} a_i g^{-i} + (a_{i_0} - 1) g^{-i_0} + g^{-i_0} = (7.27)$$

$$= \sum_{i=0}^{i_0-1} a_i g^{-i} + (a_{i_0} - 1) g^{-i_0} + \sum_{i=i_0+1}^{\infty} (g-1) g^{-i}, \quad (7.28)$$

دا چې

$$-g^{-i_0} + \sum_{i=i_0+1}^{\infty} (g-1) g^{-i} = -g^{-i_0} + (g-1) g^{-(i_0+1)} \underbrace{\sum_{i=0}^{\infty} g^{-i}}_{\rightarrow \frac{g}{g-1}} = (7.29)$$

$$= -g^{-i_0} + (g-1) g^{-(i_0+1)} \frac{g}{g-1} = (7.30)$$

$$= -g^{-i_0} + g^{-i_0} = 0. \quad (7.31)$$

نو له دې 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 $\alpha, b \in \mathbb{N}$ او $\text{ggT}(a, b) = 1$ سره،

نو α تیک هلته یوو پای (او له دې سره 2 مختلف) g - ادیکي وده لري، که هر د مخرج لومړنی پروپشوني بنسټ وېشي.

بڼونه:

(\Rightarrow)

وي دې

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

نو باور لري

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

له دې سره $b \mid a g^n$. وي دې p په خوښه د b لومړنی پروپشونی، 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 $\text{ggT}(a, b) \geq p > 1$ -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 دې

$$b = p_1^{\alpha_1} \cdots p_m^{\alpha_m} \quad (7.34)$$

د ماتلاندې يا مخرج په لومړني ضريبونو ټوټه کونه، نو $p_i | b$ باور لري ، نو د وړاند
 نيونې له مخې $p_i | g \forall i = 1, \dots, k$ له دې سره $p_i^{\alpha_i} | g^{\alpha_i} (i = 1, \dots, k)$
 وي دې $m := \max\{\alpha_1, \dots, \alpha_n\}$ نو باور لري .

$$p^{\alpha_i} | g^m (i = 1, \dots, k), \quad (7.35)$$

دا چې $m \geq \alpha_i$

د $\text{ggT}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1 \forall i \neq j$ له امله باور لري

$$\text{kgV}(p_1^{\alpha_1}, \dots, p_k^{\alpha_k}) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = b; \quad (7.36)$$

د تمريني بيلگې 24 له مخې باور لري: $b | g^m$. له دې سره دې $\frac{a}{b}g^m \in \mathbb{N}$ او وي دې

$$\frac{a}{b}g^m = a_0 + a_1g + \cdots + a_n g^n \quad (7.37)$$

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

له دې لاس ته راځي:

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

دا په دې معنا، چې $\frac{a}{b}$ یوه پای g -ادیکي وده لري. □

لاس ته راوړنه 7.1.7: وي دې

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

دا چې لومړنۍ پروپوشوني همداسې لري، باید مخرج د لپاره وي، له دې سره شرایط پوره دي. له دې سره په ل

دا چې $g = 10$ فقط لومړنۍ پروپوشوني $p = 2$ همداسې $p = 5$ لري، باید د

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

$$\alpha = \frac{a}{b}, \text{ggT}(a, b) = 1$$

که یو پای (او له دې سره دوه مختلف) انځورونه ولری \Leftrightarrow

$$\Leftrightarrow b = 2^\alpha 5^\beta, \alpha, \beta \in \mathbb{N}_0$$

له دې سره هم: $\exists p : p \mid b$ او $p \nmid 10 \Rightarrow$ (له دې لاس ته راځي) چې فقط یوه لسميزه انځورونه شتون لري.

بیلگه:

لومړی: $\alpha = \frac{287}{100} \in \mathbb{Q}^+$ ، د $b = 2^2 5^2$ له امله α یوه پای او له دې سره دوه لسميز انځورونه لري:

$$\alpha = 2.870000\dots = 2.869999\dots$$

کینونپوهنه

دویم: $\alpha = \frac{5}{3} \in \mathbb{Q}^+$ ، دا چې $b = 3^1$ د $2^a 5^b$ په بڼه نه دی، نو α فقط یوه لسمیزه انځورونه لري. یاد وپشنې له لارې، یاد [7.1.1](#) د بنوونې سره سم (α_i, a_i) :

$$\alpha = 1.6666\dots$$

دریم: $\alpha = 1 \in \mathbb{Q}^+$ د $\alpha = \frac{1}{1}$ او $\text{ggT}(1,1) = 1$ 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 $(\text{ggT}(a,b) \neq 1\dots)$:

$$\alpha = 1.0000\dots = 0.9999\dots$$

$$0.999\dots = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \dots = 9 \left[\underbrace{\sum_{i=0}^{\infty} \left(\frac{1}{10}\right)^i}_{\rightarrow \frac{1}{1-\frac{1}{10}} = \frac{10}{9}} - 1 \right] = \quad (7.39)$$

$$= 9 \left[\frac{10}{9} - 1 \right] = 10 - 9 = 1. \quad (7.40)$$

پریودیکی وده

د یوه حقیقی عدد په لسمیزه وده کې کله کله ځنې عددونه منظم منځ ته راځي، لکه $\alpha = 1.70714285714285\dots$ ،

پوښتنه: کوم حقیقی اعداد دا خویونه لري؟

پيژند (تعريف) 7.2.1: د يوه حقيقي عدد $\alpha > 0$ يوه g -اديکي يا g -ايزه وده

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = a_0 + a_1 \frac{1}{g} + a_2 \frac{1}{g^2} + \dots \quad (7.41)$$

تل بيرته راگرځيدونې يا پريوديکي بلل کيږي، که $n, e \in \mathbb{N}$ شتون ولري د لا ندي سره

$$a_{n+i} = a_{n+e+i} \quad \forall i = 0, 1, 2, \dots \quad (7.42)$$

که n مينيمال يا خورا کوچنی ټاکلی وي، نو $a_1 a_2 \dots a_{n-1}$ ترمخ پريود يا - راگرځيدنه بلل کيږي او $n-1$ د هغه اوږدوالی، که $n=1$ وي (داپه دې معنا، چې \mathbb{N} ترمخ پريود)، نو وده سوچه پريودیک بلل کيږي.

که e خورا کوچنی ټاکلی وي، نو $a_n a_{n+1} \dots a_{n+e-1}$ تلبيرونه راگرځيدونې بلل کيږي او e د هغه اوږدوالی.

د $g = 10$: لپاره سومبول يا نخبن:

$$\alpha = a_0 \cdot \underbrace{a_1 a_2 \dots a_{n-1}}_{\text{Vorperiode}} \underbrace{a_n a_{n+1} \dots a_{n+e-1}}_{\text{Periode}} \underbrace{a_{n+e}}_{=a_n} \dots \underbrace{a_{n+2e-1}}_{=a_{n+e-1}} \dots \quad (7.43)$$

بيلگه 7.2.2:

د الماني پښتو: اوږدوال Länge ;

تل بيرته راگرځيدنه، له مخه تل بيرته راگرځيدنه = periode; Vor periode

کنونپوهنه

$$\alpha = 1. \underbrace{714285}_{\text{Periode}} \underbrace{70}_{\text{Vorperiode}}$$

Länge 2 Länge 6714285...

1.

$$. \alpha = 2.87000 \dots = 2.86999 \dots . 2$$

له مخ پرېود 87 نسبت 86 ته، اوږدوالی 2 ، پرېود 0 ، نسبت 9 ته، اوږدوالی 1

جمله 7.2.3: یو مثبت (زیاتیز) عدد α د یوه $g \geq 2$ لپاره (او له دې سره د $g \geq 2$ لپاره) ټیک هلته یو پرېودیکی g -ایزه وده لري، که α راشنل وي.

بنوونه:

$$(\Leftrightarrow)$$

وي وي $\alpha = \frac{a}{b}, \text{ggT}(a, b) = 1, b > 0$ او $g \geq 2$ لکه د [7.1.1](#) په بنوونه کې وي دی

$$\alpha_1 = \alpha - [\alpha],$$

$$\alpha_0 = [\alpha],$$

$$\vdots$$

$$\alpha_{i+1} = g\alpha_i - [g\alpha_i],$$

$$a_i = [g\alpha_i].$$

$b\alpha_i \in \mathbb{Z}$ و بنایئ :

$i = 1 :$

$$b\alpha_1 = b(\alpha - [\alpha]) = b\alpha - b[\alpha] = b \cdot \frac{a}{b} - \underbrace{\left[\frac{a}{b} \right]}_{\in \mathbb{Z}} \cdot b \in \mathbb{Z}$$

$i \rightarrow i + 1 :$

$$b\alpha_{i+1} = b(g\alpha_i - [g\alpha_i]) = \underbrace{(b\alpha_i)}_{\text{Ind.VS:} \in \mathbb{Z}} g - \underbrace{b[g\alpha_i]}_{\in \mathbb{Z}} \in \mathbb{Z}$$

$b_i \equiv g^{i-1}b_1(b) \forall i \in \mathbb{N}$ ، و بنایئ: $b_i := b\alpha_i \forall i \in \mathbb{N}$ پیژند (تعریف)

$i = 1 :$

$$g^{1-1}b_1 = b_1 \equiv b_1(b)$$

$i \rightarrow i + 1 :$

$b_{i+1} =$	
$b\alpha_{i+1} = b(g\alpha_i - \underbrace{[g\alpha_i]}_{=a_i}) = \underbrace{(b\alpha_i)}_{=b_i} g - \underbrace{ba_i}_{\equiv 0(b)} \equiv g^{i-1}b_1g$	(7.44)

$= g^i b_1.$	(7.45)
--------------	--------

د $0 \leq \alpha_i < 1$ له امله باور لري

$$0 \leq b\alpha_i = b_i < b \quad (b > 0) \quad \forall i \in \mathbb{N}; \quad (7.46)$$

نو فقط پای دېر $b_i, i \in \mathbb{N}$ شته دی، له دې سره باید د دوي ترمنځ برابري 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:

$$g^{n-1} b_1 \equiv b_n = b_{n+e} \equiv b_1 g^{n+e-1}(b), \quad (7.47)$$

د g^i سره د ضرب له لاري $(i \in \mathbb{N})$ په خوښه لاس ته راځي:

$$g^{n-1+i} b_1 \equiv g^{n-1+e+i} b_1(b), \quad (7.48)$$

دا په دې معنا، چې دپورته لور ته: $b_{n+i} \equiv b_{n+e+i}$ ، يعني $b \mid b_{n+e+i} - b_{n+i}$.

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

$$b_{n+e+i} = b_{n+i} \quad \forall i \in \mathbb{N}; \quad (7.49)$$

$$b_{n+e+i} = b_{n+i} \quad \forall i \in \mathbb{N}_0$$

د $b_n = b_{n+e}$ له امله (پورته) باور لري

له دې سره:

$$b\alpha_{n+e+i} = b\alpha_{n+i} \quad (b \neq 0) \quad (7.50)$$

او

$$g\alpha_{n+e+i} = g\alpha_{n+i} \quad \forall i \in \mathbb{N}_0, \quad [g\alpha_{n+e+i}] = [g\alpha_{n+i}] \quad \forall i \in \mathbb{N}_0, \quad (7.51)$$

$$a_{n+e+i} = a_{n+i} \quad \forall i \in \mathbb{N}_0$$

نو

له دې سره د $\alpha = \frac{a}{b}$ - ایزه وده تل بیرته راګرځیدوني ده. g

(\Rightarrow)

وي دې حقيقي د پرېودیګي ودې سره، داپه دې معنا، چې $n, e \in \mathbb{N}$ شتون لري د $\alpha > 0$

$$a_{n+e+k} = a_{n+k} \quad \forall k \in \mathbb{N}_0$$

سره؟

$$a_{n+e+k} = a_{n+k} \quad \forall k \in \mathbb{N}_0$$

بنوول کيږي: $\alpha \in \mathbb{Q}$:

کنونپوهنه

$$\alpha = \sum_{i=0}^{\infty} a_i g^{-i} = a_0 + a_1 g^{-1} + \dots + a_n g^{-n} + a_{n+1} g^{-(n+1)} + \dots + \quad (7.52)$$

$$+ a_{n+e-1} g^{-(n+e-1)} + \underbrace{a_{n+e}}_{=a_n} g^{-(n+e)} + \underbrace{a_{n+e+1}}_{=a_{n+1}} g^{-(n+e+1)} + \dots + \quad (7.53)$$

$$+ \underbrace{a_{n+2e-1}}_{=a_{n+e-1}} g^{-(n+2e-1)} + \dots = \quad (7.54)$$

$$= \sum_{i=0}^{\infty} a_i g^{-i} + a_n g^{-n} \underbrace{(1 + g^{-e} + g^{-2e} + \dots)}_{\sum_{k=0}^{\infty} (g^{-e})^k \rightarrow \frac{1}{1-g^{-e}} = \frac{g^e}{g^e-1}} + \dots + \quad (7.55)$$

$$a_{n+e-1} g^{-(n+e-1)} \underbrace{(1 + g^{-e} + g^{-2e} + \dots)}_{\sum_{k=0}^{\infty} (g^{-e})^k \rightarrow \frac{1}{1-g^{-e}} = \frac{g^e}{g^e-1}} = \quad (7.56)$$

$$= \sum_{i=0}^{\infty} a_i g^{-i} + \frac{g^e}{g^e-1} (a_n g^{-n} + \dots + a_{n+e-1} g^{-(n+e-1)}) \in \mathbb{Q}. \quad (7.57)$$

بیلګه 7.2.4: $g = 10, \alpha = 0.1342\overline{158}$ ، داچې دا یوه پریودیګي لسمیزه وده ده،

لاس ته راځي: α یو راشنل عدد دی، کوم؟

$n = 4, e = 4$ ، د ترمخپریود اوږدوالی: $\Rightarrow n - 1 = 3$ د [7.2.3](#) د بنوونې له

مخې:

$$\alpha = \frac{134}{1000} + \frac{10^4}{10^4 - 1} \left(2 \cdot \frac{1}{10^4} + \frac{1}{10^5} + 5 \cdot \frac{1}{10^6} + 8 \cdot \frac{1}{10^7} \right) = \dots = (7.5)$$

ځانگړی حالت: سوچه پریودیکی وده

پوښتنه: کله د $\alpha \in \mathbb{R}^+$ g - ایزه وده سوچه - پریودیکی ده؟

د [7.2.3](#) له مخې باید α راشنل وي، د $g = 10$ لپاره هر $\alpha \in \mathbb{Q}^+$ د

$$\alpha = a_0.\overline{a_1 a_2 \dots a_e} \quad (7.59)$$

سره غواړو پیدا کړو.

جمله 7.2.5: که $\frac{a}{b} \in \mathbb{Q}^+$ وي د $ggT(a, b) = 1, b > 0$ سره، نو د g -

ایزه وده ټیک هلته سوچه پریودیکی ده، که $ggT(b, g) = 1$ وي. که دا حالت وي، نو

د e پریودیکی اوږدوالی د $\bar{g} \in \mathbb{Z}_b^*$ د نظم سره برابر دی (دا په دې معنا، چې د خورا

کوچني طبيعي گڼ k سره برابر دی، د $\bar{g}^k = \bar{1} \in \mathbb{Z}_b^*$ سره).

ښوونه:

(\Rightarrow)

وي دې $\frac{a}{b} \in \mathbb{Q}^+, ggT(a, b) = 1, b > 0$ د سوچه-پریودیکی 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

$$g^{n+\varepsilon-1}b_1 \equiv g^{n-1}b_1(b), \quad (7.60)$$

نو د $n = 1$ له امله $g^\varepsilon b_1 \equiv b_1(b)$ دی.

$$\text{ggT}(b, b_1) = 1$$

وښایي:

نیسو چې $\exists p \in \mathbb{P}$ د لاندې سره

$$p \mid b, p \mid b_1 \stackrel{7.1.1}{=} b\alpha_1 = b \left(\frac{a}{b} - \underbrace{\left[\frac{a}{b} \right]}_{\in \mathbb{N}} \right) = a - b \underbrace{\left[\frac{a}{b} \right]}_{\in \mathbb{N}},$$

له دې سره لاس ته راځي $p \mid a$ - تضاد و $\text{ggT}(a, p) = 1$ ته.

له دې سره د $g^\varepsilon b_1 \equiv b_1(b)$ څخه د [4.1.5\(5\)](#) له مخې لاس ته راځي

$$g^\varepsilon \equiv 1(b). \quad (7.61)$$

وښایي: $\text{ggT}(b, g) = 1$. نیسو چې $\exists p \in \mathbb{P}$ د $p \mid b, p \mid g$ سره، نو باور لري

$$p \mid b, p \mid g^\varepsilon = 1 + tb \quad (t \in \mathbb{N}), \quad (7.62)$$

نو هم $p \mid 1$ - تضاد.

وي دي $\frac{a}{b}$ سوچه پريوديكي، نو وبنايي په (\mathbb{Z}_b^*, \cdot) کې. $e = \text{ord } \bar{g}$ پورته لور ته باور لري:

$$g^e \equiv 1(b) \wedge \text{ggT}(b, g) = 1; \quad (7.63)$$

) $\text{ord } \bar{g} \leq e$ دا په دي معنا، چې $\bar{g} \in \mathbb{Z}_b^*$ او $\bar{g}^e = \bar{1}$ په (\mathbb{Z}_b^*, \cdot) کې دي. يعني $\bar{g}^k = \bar{1}$ د پيژند له مخي خورا کوچني طبيعي عدد k دي د $\text{ord } \bar{g}$ سره.

وي دي $\text{ord } \bar{g} = k$ ، نو په (\mathbb{Z}_b^*, \cdot) کې باور لري $\bar{g}^k = \bar{1}$ ، دا په دي معنا، چې $g^{k+i} b_1 \equiv g^i b_1(b)$ او $g^k \equiv 1(b)$ له دي سره هم $g^{k+i} \equiv g^i(b) \forall i \geq 0$ باور لري د b_1 سره د [7.2.3](#) بنووني له مخي $\forall i \geq 0$. له دي بنووني لاس ته راخي:

$$b_{k+i+1} \equiv b_{k+i}(b), \quad (7.64)$$

نو $b_{k+i+1} = b_{k+i}$ ، او

$$a_{1+k+i} = a_{1+i} \forall i \geq 0. \quad (7.65)$$

دا چې e د $a_{1+e+i} = a_{1+i} \forall i \geq 0$ ($n = 1$) سره خورا کوچني ده، لاس ته راخي $e \leq k = \text{ord } \bar{g}$. له دي امله په (\mathbb{Z}_b^*, \cdot) کې باور لري $e = k = \text{ord } \bar{g}$.

(⇐)

وي دي $gg\Gamma(b, g) = 1$ ، د بنوولو دی: د $\frac{a}{b}$ - ایزه وده سوچه پریودیکی ده.

دا چې $\frac{a}{b} \in \mathbb{Q}^+$ د [7.2.3](#) له مخې یو پریودیکی اونخورونه شتون لري، یعنی د لاندي سره:

$$g^{n-1}b_1 \equiv g^{n+e-1}(b). \quad (7.66)$$

دا چې $gg\Gamma(b, g) = 1$ ، نو $gg\Gamma(b, g^{n-1}) = 1$ هم شتون لري، یعنی دپورته

کونگروانخ څخه لاس ته راځي $b_1 \equiv g^e b_1(b)$. یعنی د ټولو

$$i \geq 0: g^i b_1 \equiv g^{e+i} b_1(b)$$

لپاره، نو د جملې [7.2.3](#) د بنوونې له مخې لرو:

$$b_{i+1} \equiv b_{e+i+1}(b) \quad , \quad \text{له دې سره} \quad b_{i+1} = b_{e+i+1} \quad \forall i \geq 0$$

دا په دې معنا، چې د $\frac{a}{b}$ - ایزه یا g - ایدیکی انخورونه $a_{1+i} = a_{1+e+i} \quad \forall i \geq 0$

پریودیکی ده د $n = 1$ سره، یعنی سوچه تل بیرته راگرځیدونې یا پریودیکی. □

یادونه [7.2.6](#): ایا د $\frac{a}{b} \in \mathbb{Q}^+$ - ایزه وده د $gg\Gamma(a, b) = 1, b > 0$ سره،

سوچه پریودیکی ده، او هم د پریود اوردوالی د ماتلاندي یا مخرج b په واک کې دی!

بیلگه [7.2.7](#):

$$g = 10, \alpha = \frac{3}{7} \in \mathbb{Q}^+ \quad . \quad 1.$$

دا چې $gg\Gamma(3, 7) = 1$ د [7.2.5](#) له مخې باور لري: $\frac{a}{b} = \frac{3}{7}$ سوچه پریودیکی لسمیزه

وده لري ($\text{ggT}(7, 10) = 1$)، د کوم سره چې د بريود اوږدوالی $e = \text{ord } \overline{10}$ په (\mathbb{Z}_7^*, \cdot) کې دی:

$$10^1 \not\equiv 1(7), 10^2 \not\equiv 1(7), \dots, 10^6 \equiv 1(7)$$

(د لومړي ځل لپاره)....

. $e = 6$ also $\Rightarrow \text{ord } \overline{10} = 6$

$$\left(\frac{3}{7} = 0.\overline{428571}\right)$$

$$g = 10, \alpha = \frac{15}{7} \in \mathbb{Q}^+ \quad .2$$

$$\text{ggT}(15, 7) = 1$$

سوچه پريوديکي د $e = \text{ord } \overline{10} = 6$ سره.

$$\left(\frac{15}{7} = 2.\overline{142857}\right)$$

ټوليز حالت: نه سوچه - پريوديکي وده

جمله 7.2.8: وي دی $\frac{a}{b} \in \mathbb{Q}^+, \text{ggT}(a, b) = 1, b > 0$ دی.

$$g = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad (7.67)$$

د بنسټ $g \geq 2$ په لومړنيو ضريبونو ټوټه کونه او

$b = p_1^{\beta_1} \cdots p_k^{\beta_k} \cdot t$	(7.68)
--	--------

کنونپوهنه

(د همغه p_i سره!) د $\text{ggT}(g, t) = 1$ سره، نو د تر مخ پر یو اوږدوالی $n-1$ په g -ایز دوه کي خورا کوچنی طبیعي عدد γ دی، د کوم لپاره چې $\frac{b}{t} \mid g^\gamma$ دی، او د \bar{g} پر یو اوږدوالی د پر یو د نظم سره برابر دی په (\mathbb{Z}_t^*, \cdot) کي.

بیلگه 7.2.9: $g = 10, \frac{a}{b} = \frac{239}{140} \in \mathbb{Q}^+$ ، لسمیزه وده سوچه پر یو دیک نه ده، ځکه

$$\text{ggT}(b, g) = \text{ggT}(140, 10) \neq 1$$

چې

د پر یو اوږدوالی:

$$\left. \begin{array}{l} g = 10 = 2 \cdot 5 \\ b = 140 = 2^2 \cdot 5 \cdot 7 \end{array} \right\} \Rightarrow t = 7, \frac{b}{t} = \frac{140}{7} = 20$$

$$20 \nmid 10^1, 20 \mid 10^2 = 100 \Rightarrow \gamma = 2.$$

د پر یو اوږدوالی:

$e = \text{ord } \bar{g}$ په (\mathbb{Z}_t^*, \cdot) کي: $e = \text{ord } \overline{10}$ په (\mathbb{Z}_7^*, \cdot) کي، پورته لور ته لاس ته راځي $e = 6$.

$$\Rightarrow \frac{a}{b} = a_0 \cdot \underbrace{a_1 a_2}_{\text{Vorperiode}} \cdot \underbrace{a_3 a_4 a_5 a_6 a_7 a_8}_{\text{Periode}}; \quad \frac{239}{140} = 1.70\overline{714285}$$

n-te Potenzreste

په ځانگړي حالت بېرته اړول

دلته $x^m \equiv a(m)$ په

$x^m \equiv a(p^\alpha)$	(8.2)
--------------------------	-------

بیره اړول کیري د $\text{ggT}(a, p) = 1$ سره (یعني په $(\mathbb{Z}_{p^\alpha}^*, \cdot)$ کې شمیرنه).

لیما 8.1.2: $x^m \equiv a(m)$ د $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ سره ټیک هلته حولور ده، که

$$x^2 \equiv a(p_i^{\alpha_i}) \quad i = 1, 2, \dots, k \quad (8.3)$$

حلور وي (برخه 5 وگورئ)

لیما 8.1.3: $x^n \equiv a(p^\alpha), p \in \mathbb{P}, \alpha \in \mathbb{N}$ د $a = p^k a'$ لپاره د $\text{ggT}(p, a') = 1$ سره ټیک هلته حولور ده، که $n | k$ او $x^n \equiv a'(p^{\alpha-k})$ حلور وي $(0 \leq a < p^\alpha)$.

بنوونه:

(\Rightarrow)

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

$$x_0^n \equiv a(p^\alpha), \quad (8.4)$$

کنونپوهنه

دا په دې معنا، چې $x_0^n = a + rp^\alpha$ دی د یوه $r \in \mathbb{Z}$ لپاره.

وي دې $x_0 = p^\beta s$ د $\text{ggT}(p, s) = 1$ ($\beta \in \mathbb{N}_0$) سره، نو باور لري:

$$x_0^n = (p^\beta s)^n = p^{n\beta} s^n = a + rp^\alpha = p^k a' + rp^\alpha. \quad (8.5)$$

د $a = p^k a' < p^\alpha$ له امله باور لري: $k < \alpha$ ($a' > 0$)، یعنی، $p^k \mid p^\alpha$ ، له دې سره دپورته لور ته:

$$p^{n\beta-k} s^n = a' + rp^{\alpha-k}; \quad (8.6)$$

له دې سره باور لري: $p^k \mid p^{n\beta} s^n$ د $\text{ggT}(p, s) = 1$ له امله هم، $\text{ggT}(p^k, s^n) = 1$ دي، یعنی د [2.2.11](#) سره لاس ته راځي: $p^k \mid p^{n\beta}$ ، یعنی،

$$k \leq n\beta$$

که $k < n\beta$ وي، نو $n\beta - k > 0$ به وی او د

$$p^{n\beta-k} s^n = a' + rp^{\alpha-k} \quad (8.7)$$

له مخې به مو لروډی: $p \mid a'$ او $\text{ggT}(p, a') \neq 1$ چې تضاد دی.

له دې سره: $k = n\beta$ او $n \mid k$ ، پسي لاس ته راځي:

$$s^n = a' + rp^{\alpha-k}, \quad (8.8)$$

دا په دې معنا، چې $s^n \equiv a'(p^{\alpha-k})$ او $s \in \mathbb{Z}$ د $x^n \equiv a'(p^{\alpha-k})$ یو حل دی.

(⇐)

وي دي $x_0 \in \mathbb{Z}$ د $x^n \equiv a'(p^{\alpha-k})$ حل د $n | k$ او د $\text{ggT}(a', p) = 1$ 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 $n | k$ له امله باور لري $k = nt$ د يوه $t \in \mathbb{N}$ لپاره.

$$x_0^n p^{nt} \equiv a(p^\alpha) \Rightarrow (x_0 p^t)^n \equiv a(p^\alpha), \quad (8.9)$$

له دې سره $s = x_0 p^t \in \mathbb{Z}$ د کونګروانت $x^n \equiv a(p^\alpha)$ يو حل دی. □

يادونه 8.1.4: له دې سره د $x^n \equiv a'(p^{\alpha-k})$ له حل x_0 څخه د $\text{ggT}(a', p) = 1$

سره د $x^n \equiv a(p^\alpha)$ هر حل x_1 شميرل کیدی شي:

$$x_1 = x_0 p^t, \quad (8.10)$$

د کوم سره چې $k = nt$ باور لري.

لاس ته راوړنه 8.1.5: د مسألې $x^n \equiv a(p^\alpha)$ سره سرې کړی شي ځان په حالت

$\text{ggT}(a, p) = 1$ محدود کړي ($\Rightarrow \text{ggT}(a, p^\alpha) = 1$) ، دا په دې معنا، چې سرې

کړی شي په $(\mathbb{Z}_{p^\alpha}^*, *)$ کې شميرنه وکړي ($\bar{a} \in \mathbb{Z}_{p^\alpha}^*$).

ليما 8.1.6: x_0 د $x^n \equiv a(p^\alpha)$ حل دی د $\text{ggT}(a, p) = 1$ سره، نو

$\text{ggT}(x_0, p) = 1$ هم باور لري (دا په دې معنا، چې

$$(\bar{x}_0^n = \bar{a} \in \mathbb{Z}_m^* \Rightarrow \bar{x}_0 \in \mathbb{Z}_m^*).$$

کڼونپوهنه

ښوونه: د $x_0^m \equiv a(p^\alpha)$ له امله باور لري $p^\alpha \mid x_0^m - a$ ، دا په دې معنا، چې

$$x_0^m - a = tp^\alpha \quad (t \in \mathbb{N}) \Rightarrow a = x_0^m - tp^\alpha. \quad (8.11)$$

نیسو چې $\exists q \in \mathbb{P}$ د $q \mid x_0, q \mid p$ سره، نو $q = p$ او $q = p \mid a$ لرو له دې لرو: تضاد دی.

له دې سره موږ سرچینه ییزه مسأله په $(\mathbb{Z}_{p^\alpha}^*, \cdot)$ کې شمیرنه باندې بیرته وړوله.

پیژند(تعریف) 8.1.7: و ی د $\text{ggT}(a, m) = 1$ $m \in \mathbb{N}, a \in \mathbb{Z}$ سره، نو

$a \in \mathbb{Z}$ یو n -م توان مودولو m بلل کیږي، که $x^n \equiv a(m)$ حل وړ وي. (دا په دې معنا، چې $\bar{a} \in \mathbb{Z}_m^*$ د یوه توکي $\bar{x}_0 \in \mathbb{Z}_m^*$ n -م توان دی).

بیلگه 8.1.8: $m = 6, a = 0, 1, 3, 4$ دویمتوانپاتې $\text{mod } 6$ دی، $a = 2, 5$ دویم توانپاتې $\text{mod } 6$ نه دی (پورته وگورئ).

پسې: هر $a \in \mathbb{Z}$ دریم توانپاتې $\text{mod } 6$ دی (پورته وگورئ)

د $x^n \equiv a(p^\alpha), \text{ggT}(a, p) = 1$ د حل لپاره تگلار

لومړی: تولیز د الجبري کونگروانت لپاره له برخې 5 څخه (مفصل)

دویم: که د داسې په نامه اندکسجدول لهماځې یوه ساده ریښه $\text{mod } p^\alpha$ شتون ولري. پام دې وي: د گاوس 6.2.15 له مخې، د هر لومړني عدد $p \neq 2$ او هر $\alpha \in \mathbb{N}$ لپاره

یوه ساده ریښه $\text{mod } p^\alpha$ شتون لري، ورپسې د 2 او $4 = 2^2$ ته، مگر نه د 2^α لپاره د $\alpha \geq 3$ سره، د دې لپاره: ځانله پام په کار ی

پېژند 8.1.9: $m \in \mathbb{N}$ دې داسې وي، چې (\mathbb{Z}_m^*, \cdot) څپوکلیکي يا تل بیرته راگرځیدونی دی، دا په دې معنا، چې ساده ریښه شتون (\exists) لري، دا په دې معنا، چې \bar{g} تولیدوي (\mathbb{Z}_m^*, \cdot) او دی

$$\mathbb{Z}_m^* = \{\bar{g}, \bar{g}^2, \dots, \bar{g}^{\varphi(m)}\}. \quad (8.12)$$

که $\bar{a} \in \mathbb{Z}_m^*$ په خوښه وي، نو خورا کوچنی طبیعي عدد k یا 0 بلل کيږي، چې د هغې لپاره $\bar{a} = \bar{g}^k$ د a ایندکس دی نسبت g ته، سومبولیک: $I_g(a)$. یادونه 8.1.10: یواځنی ټاکلی دی، ځکه چې

$$\mathbb{Z}_m^* = \{\bar{g}, \bar{g}^2, \dots, \bar{g}^{\varphi(m)}\} \quad (8.13)$$

او د دوي څخه ټول توکي مختلف دي: ټیک یو ځل رامنځ ته کيږي. د ایندکی جدول د هر $\bar{a} \in \mathbb{Z}_m^*$ لپاره (څپکلیکي وړاندنیونه) $I_g(a) \in \mathbb{N}_0$ راکوي.

بیلگه 8.1.11: $m = 14 = 2 \cdot 7$ ، د گاوس 6.2.15 له مخې $(\mathbb{Z}_{14}^*, \cdot)$ له دې امله څپوکلیکي دی، یعنی یوه ساده ریښه $\text{mod } 14$ شتون لري.

$g = 3$ یوه ساده ریښه $\text{mod } 7$ ده، ځکه چې

$$\mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} \quad (8.14)$$

او $\bar{3} = \bar{3}, \bar{3}^2 = \bar{2}, \bar{3}^3 = \bar{6}, \bar{3}^4 = \bar{4}, \bar{3}^5 = \bar{5}, \bar{3}^6 = \bar{1}$ ، داپه دې معنا، چې $\bar{3}$ تولیدوي، \mathbb{Z}_7^*

کینونپوهنه

دا چې g ناجوره یا طاق دی، د [6.2.12](#) د بنوونې له مخې ترې لاس ته راځي: $g = 3$ هم ساده ریښه $\text{mod } 14$ دی.

$$\mathbb{Z}_{14}^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{9}, \bar{11}, \bar{13}\} \quad (8.15)$$

$$(\varphi(14) = \varphi(2 \cdot 7) = \varphi(2)\varphi(7) = 1 \cdot 6 = 6)$$

د $\bar{3} \in \mathbb{Z}_{14}^* : \bar{3} = \bar{3}, \bar{3}^2 = \bar{9}, \bar{3}^3 = \bar{13}, \bar{3}^4 = \bar{11}, \bar{3}^5 = \bar{5}, \bar{3}^6 = \bar{1}$ توان.

له دې سره لاندې ایندکس جدول راکوي:

\bar{a}	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{9}$	$\bar{11}$	$\bar{13}$
$I_g(a)$	0	1	5	2	4	3

(8.16)

لیما 8.1.12: وي دې g ساده ریښه $\text{mod } m$ ، 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

$$I_g(ab) \equiv I_g(a) + I_g(b)(\varphi(m)). \quad (8.17)$$

بنوونه:

لومړی: (\Rightarrow) (لاس ته راځي)

وي دي $g^i \equiv g^j(m)$ د $i > j$ لپاره، نو په (\mathbb{Z}_m^*, \cdot) کې $\bar{g}^i = \bar{g}^j$ باور لري،
يعنې د $\bar{g}^{-j} \in \mathbb{Z}_m^*$ سره د ضرب له مخې لرو:

$$\bar{g}^{i-j} = \bar{1}. \quad (8.18)$$

دا چې \bar{g} د (\mathbb{Z}_m^*, \cdot) گروپ توليدوي، $\text{ord } \bar{g} = \varphi(m)$ دی. د [6.2.7](#) له مخې لاس ته راځي

$$\varphi(m) \mid i - j, \quad (8.19)$$

داپه دي معنا، چې $i \equiv j(\varphi(m))$.

(\Leftarrow)

برعکس دي $i \equiv j(\varphi(m))$ وي، نو باور لري

$$\varphi(m) \mid i - j \Rightarrow i - j = t\varphi(m) \quad t \in \mathbb{Z}; \quad (8.20)$$

يعنې $i = j + t\varphi(m)$ او:

$$\bar{g}^i = \bar{g}^{j+t\varphi(m)} = \bar{g}^j (\bar{g}^{\varphi(m)})^t = \bar{g}^j, \quad (8.21)$$

دا په دي معنا، چې $\bar{g}^i = \bar{g}^j$ او له دي سره $g^i \equiv g^j(m)$.

ګڼونپوهنه

لومړۍ: د $\text{ggT}(a, m) = \text{ggT}(b, m) = 1$ له امله باور لري: $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$ يعنې

يعنې، $\bar{a}\bar{b} \in \mathbb{Z}_m^*$ او باور لري $I_g(ab)$

$$\bar{g}^{I_g(ab)} = \bar{a}\bar{b} = \bar{a}\bar{b} = \bar{g}^{I_g(a)+I_g(b)}, \quad (8.22)$$

$$\overline{g^{I_g(ab)}} = \overline{g^{I_g(a)+I_g(b)}}$$

دويم يعنې ، له دې سره

$$g^{I_g(ab)} \equiv g^{I_g(a)+I_g(b)}(m) \stackrel{1}{\Rightarrow} I_g(ab) \equiv I_g(a) + I_g(b) (\varphi(m)). \quad (8.23)$$

$$a_1, a_2, \dots, a_k \in \mathbb{Z}$$

ترې لاس ته راوړنه 8.1.13: وي دې

سره او $\text{ggT}(a_i, m) = 1$ ($i = 1, \dots, k$) دې يوه ساده ريښه $\text{mod } m$ وي،

نو د ايندکشن سره لاس ته راځي:

$$I_g(a_1 \cdots a_k) \equiv I_g(a_1) + \cdots + I_g(a_k) (\varphi(m)). \quad (8.24)$$

په ځانګړې توګه دې وي $a_i = a$ ($i = 1, \dots, k$) ، نو لاس ته راځي

$$I_g(a^k) \equiv kI_g(a) (\varphi(m)). \quad (8.25)$$

دا خويونه د هغه ورسره بلد لوګارېتم سره ورته دي، چې په اناليز کې څيرل شوي.

له دې امله I_g د اعدادو تيوريکي لوګارېتم بلل کيږي.

د حل ساده متودونه Einfache Lösungsmethode

ځانگړی حالت

له دې سره د ځنو الجبري کونگروانتونو د حل ساده امکانات شته، که یوه ساده ریښه شتون ولري:

$$g \text{ سره او } \text{ggT}(a, m) = \text{ggT}(b, m) = 1 \quad ax \equiv b(m) \quad \alpha) \text{ ورکړل شوي:}$$

ساده ریښه $\text{mod } n$ ده. په \mathbb{Z}_m^* کې حل کوو $\bar{ax} = \bar{b}$ ، یعنې:

$$\bar{g}^{I_g(ax)} = \bar{g}^{I_g(b)} \Leftrightarrow g^{I_g(ax)} \equiv g^{I_g(b)}(m) \quad (8.26)$$

$$\stackrel{8.1,12}{\Leftrightarrow} I_g(ax) \equiv I_g(b)(\varphi(m)) \quad (8.27)$$

$$\Leftrightarrow I_g(a) + I_g(x) \equiv I_g(b)(\varphi(m)) \quad (8.28)$$

$$\Leftrightarrow I_g(x) \equiv I_g(b) - I_g(a)(\varphi(m)). \quad (8.29)$$

دې له ایندکس جدول څخه وټاکل شي. x د دې کرښیز مساوات حل وي، نو $I_g(x)$ که

ليما 8.2.1: $3x \equiv 5(14); \text{ggT}(3, 14) = \text{ggT}(5, 14) = 1, g = 3$
ساده ریښه $\text{mod } 14$ ده، حل کوو:

$I_3(x) \equiv I_3(5) - I_3(3)(6).$	(8.30)
-------------------------------------	--------

$$I_3(x) \equiv 5 - 1 = 4(6) \Rightarrow I_3(x) = 4 ($$

(0 ≥ کوچنی حل)

$$\Rightarrow x = \overline{11}$$

β)

ورکړل شوي د $ax^n \equiv b(m)$ ساده g سره او $\text{ggT}(a, m) = \text{ggT}(b, m) = 1$

رېښه $\text{mod } m$ ده. د حل دی: $\overline{ax^n} = \overline{b}$ په (\mathbb{Z}_m^*, \cdot) کې، يعنې

$$\overline{g}^{I_g(ax^n)} = \overline{g}^{I_g(b)} \Leftrightarrow g^{I_g(ax^n)} \equiv g^{I_g(b)}(m) \quad (8.31)$$

$$\Leftrightarrow I_g(ax^n) \equiv I_g(b)(\varphi(m)) \quad (8.32)$$

$$\Leftrightarrow I_g(a) + I_g(x^n) \equiv I_g(b)(\varphi(m)) \quad (8.33)$$

$$\Leftrightarrow nI_g(x) \equiv I_g(b) - I_g(a)(\varphi(m)) \quad (8.34)$$

له دې لاس ته راځي: په نامعلومه $I_g(x)$ کې د دې کرښيز کونګروانت په حل بېرته اړوو، که دا حلور وي، نو $I_g(x)$ د اندکس جدول کې پيدا کړئ او اړونده $\overline{x} \in \mathbb{Z}_m^*$ وټاکئ.

بيلگه 8.2.2:

$$5x^2 \equiv 9(14), \text{ggT}(5, 14) = \text{ggT}(9, 14) = 1, g = 3$$

ساده رېښه $\text{mod } 14$ 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 $ggT(2, 6) = 2 \nmid -3$ له امله حل نه شته، او لهدې سره د پیل یا سرچینیز کونګروانت $5x^2 \equiv 9(14)$ حل هم نه شته.

$$5x^3 \equiv 9(14), ggT(5, 14) = ggT(9, 14) = 1, g = 3$$

ساده ریښه $\text{mod } 14$ ده، د حل دی:

$$3I_3(x) \equiv I_3(9) - I_3(5) = 2 - 5 = -3(6). \quad (8.36)$$

د $ggT(3, 6) = 3 \mid -3$ له امله یو حل شتون لري (حتا 3 انګوروانت حلونه):

$$I_3(x) = \begin{cases} 1 \\ 3 \\ 5 \end{cases} \Rightarrow \begin{cases} \bar{3} \\ \bar{5} \\ \bar{13} \end{cases} \quad (8.37)$$

د \bar{x} په حیث

۷)

$$ggT(a, m) = ggT(b, m) = ggT(c, m) = 1 \quad a \cdot b^x \equiv c(m) \quad \text{ورکړ شوي د}$$

سره او g ساده ریښه $\text{mod } m$ ده. د حل ده: $\bar{a} \cdot \bar{b}^x = \bar{c}$ په (\mathbb{Z}_m^*, \cdot) کې. یعنې:

کنونپوهنه

$$\bar{g}^{I_g(ab^x)} = \bar{g}^{I_g(c)} \Leftrightarrow g^{I_g(ab^x)}(m) \equiv g^{I_g(c)}(m) \quad (8.38)$$

$$\stackrel{8.1,12}{\Leftrightarrow} I_g(a) + xI_g(b) \equiv I_g(c)(\varphi(m)), \quad (8.39)$$

دا په دې معن، چې باټي دی په x کې یو کرښیز کونګروانت حل کړو.

بیلګه 8.2.3:

$$3 \cdot 5^x \equiv 11(14) \text{ ggT}(3, 14) = \text{ggT}(5, 14) = \text{ggT}(11, 14) = 1, g = 3$$

ساده ریښه دی، له دې سره حل کوو:

$$\underbrace{I_3(3)}_{=1} + x \underbrace{I_3(5)}_{=5} \equiv \underbrace{I_3(11)}_{=4} \underbrace{(6)}_{=\varphi(14)}, \quad (8.40)$$

دا په دې معنا، چې $5x \equiv 3(6)$ ، یعنی حل کوو ، له دې سره $5x \equiv 15(6)$ ،
 $x \equiv 3(6)$ ، دا په دې معنا، چې $x_0 = 3$.

تري لاس ته راتلنه 8.2.4 : $\text{ggT}(a, m) = 1$ د $x^n \equiv a(m)$ سره او ساده g ریښه $\text{mod } m$ حلور ده....

$$\dots \Leftrightarrow \bar{g}^{I_g(x^n)} = \bar{g}^{I_g(a)} \quad (Z_m^*, \cdot) \quad \text{په کې} \quad (8.41)$$

$$\stackrel{8.1,12}{\Leftrightarrow} I_g(x^n) \equiv I_g(a)(\varphi(m)) \quad (8.42)$$

$$\Leftrightarrow nI_g(x) \equiv I_g(a)(\varphi(m)) \quad (8.43)$$

$$\stackrel{5.1.1}{\Leftrightarrow} \text{ggT}(n, \varphi(m)) \mid I_g(a). \quad (8.44)$$

$\text{ggT}(a, m) = 1$ داچې سړی پورته لور ته په $m = p^\alpha, p \in \mathbb{P}, \alpha \in \mathbb{N}$ او په

خان محدودولی شي، نو ټول حالتون پرته له $m = 2^k$ څخه د $k \geq 3$ سره رانیول

شوي یا رانگارل شوي دي (پرته [6.1.10](#): د $p^\alpha, p \neq 2, \alpha \in \mathbb{N}$ لپاره په خوبه

$(\mathbb{Z}_{p^\alpha}^*, \cdot)$ څیکلیکي دی، دا په دې معنا، چې یوه ساده ریښه $\text{mod } p^\alpha$ شتون ري). دا په جمله [8.2.7](#) کې په ځانله ډول څیرل کيږي. د $n - m$ توان لپاره یوه بله قضیه لاندې نتیجه انځوروي:

جمله : $m \in \mathbb{N}$ دې د \mathbb{Z}_m^* سره څیکلیکي وي. د $a \in \mathbb{Z}$

$\text{ggT}(a, m) = 1$ سره ټیک هلته $n - m$ توان $\text{mod } m$ دی، که د

$d := \text{ggT}(n, \varphi(m))$ سره باور ولري:

$$a^{\frac{\varphi(m)}{d}} \equiv 1(m). \quad (8.45)$$

نو د $x^n \equiv a(m) \text{ mod } m$ انکونگروانت حلونو گنون یا تعداد d دی.

بنوونه:

(\Rightarrow)

کنونپوهنه

$$a^{\frac{\varphi(m)}{d}} \equiv (x_0^n)^{\frac{\varphi(m)}{d}} = \left(x_0^{\varphi(m)}\right)^{\frac{n}{d}} = 1^{\frac{n}{d}} = 1(m). \quad (8.46)$$

 (\Leftarrow)

وي دي $a^{\frac{\varphi(m)}{d}} \equiv 1(m)$ ، دا چې \mathbb{Z}_m^* څپوکلپکي دی پوه ساده رینه $g \bmod m$ شتون لري. یعنی

$\bar{a} = \bar{g}^{I_g(a)},$	(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)
--	--------

$$\bar{1} = \bar{g}^{\frac{\varphi(m)I_g(a)}{d}}$$

دا په دي معنا، چې [6.2.7](#) له مخي لاس ته راځي.

$$\underbrace{\text{ord}(\bar{g})}_{=\varphi(m)} \mid \frac{\varphi(m)I_g(a)}{d}, \quad (8.49)$$

$$d\varphi(m) \mid \varphi(m)I_g(a) \Rightarrow d \mid I_g(a)$$

دا په دي معنا، چې

له دي سره د [5.1.1](#) له مخي کرښيز کونگروانت

$$ny \equiv I_g(a)(\varphi(m)) \quad (8.50)$$

حلور دی، یعنی $a \in \mathbb{Z}$ -مه رینه ده.

پسي د [5.1.1](#) له مخي باور لري: دا کرښيز کونگروانت $d \bmod \varphi(m)$ انکونگروانت حلونه لري. د $y_0 \in \mathbb{Z}$ لپاره د

$$ny_0 \equiv I_g(a)(\varphi(m)) \quad (8.51)$$

سره ټيک يو $x_0 \in \mathbb{Z}$ شتون لري د $x_0^m \equiv a(m)$ سره، ځکه چې:

له $y_0 = I_g(x_0) = I_g(x_1)$ لاس ته راځي

$$\overline{x_1} = \overline{g^{I_g(x_1)}} = \overline{g^{I_g(x_0)}} = \overline{x_0}, \quad (8.52)$$

يعني ټيک يو $\overline{x_0} \in \mathbb{Z}_m^*$ شتون لري.

له دې سره هم ټيک $x^m \equiv a(m)$ انکونگروانت $d = \text{ggT}(n, \varphi(m)) \bmod m$ حلونه لري. \square

بيلگه 8.2.6: وي دې $x^5 \equiv 7(25)$ حلور، دا په دې معنا، چې:

ايا $a = 7$ پنځه توان $\bmod 25$ دی؟

د گاوس له مخي: $a = 7, n = 5, m = 25 = 5^2$ $\mathbb{Z}_{5^2}^*$ څيوکليکي د

$$\varphi(m) = \varphi(25) = 20$$

کنونپوهنه

$$\Rightarrow d := \text{ggT}(n, \varphi(m)) = \text{ggT}(5, 20) = 5 \quad (8.53)$$

$$\Rightarrow a^{\frac{\varphi(m)}{d}} = 7^{\frac{20}{5}} = 7^4 \equiv (-1)^2(25) = 1(25), \quad (8.54)$$

دا په دې معنا، چې 7 پنځم توان $\text{mod } 25$ دی.

ټول حلونه د د ساده ریښې $g = 2$ او اندکس جدول له مخې لاس ته راځي

$$\Rightarrow 5 \text{ mod } 25$$

انکونگوانت حلونه $2, 7, 12, 17, 22$.

د $x^n \equiv a(2^k), k \geq 3$ لپاره د حل متودونه
په پای کې لکه نور چې ویلي مو وو د

$$m = 2^k, k \geq 3,$$

حالت $\mathbb{Z}_{2^k}^*$ د نه ځیکلیکي، سره ځانونه په کار اچوو:

جمله 8.2.7: وي دې $a \in \mathbb{Z}, k \geq 3$ ، د $\text{ggT}(a, 2^k) = 1$ سره ټیک هلته n
—توان $\text{mod } 2^k$ دی، که د $d = \text{ggT}(n, 2^{k-2})$ لپاره باور ولري:

$$1. \quad a^{\frac{2^k-2}{d}} \equiv 1(2^k)$$

$$2. \quad a \equiv 1(4) \text{ یا } n \text{ ناجوره یا طاق دی.}$$

3.

د $x^n \equiv a(m) \text{ mod } 2^k$ انکوگروانتو حلونو گڼ، ن(تعداد) نو بیا 1 دی د n
ناجوره یا طاق لپاره، او $2d$ د جوړه n لپاره.

د $x^n \equiv a(2^k)$ حل (نو) پیدا کول له بنوونې 8.2.7 څخه:

$\bar{a} \in \mathbb{Z}_{2^k}$
په لاندې بڼه

$$\bar{a} = \overline{(-1)^j 5^l}, \quad j \in \{0, 1\}, l \in \{1, \dots, 2^{k-2}\} \quad (8.55)$$

په یواځني ډول د 6.2.16 له مخې انځور کړئ، راوړو

$$nx \equiv l(2^{k-2}); \text{ همداسې } nx \equiv j(2) \quad (8.56)$$

ګرښیز کونګروانت دي، که α د $nx \equiv j(2)$ راکم شوی حل وي او β د $nx \equiv l(2^{k-2})$ راکم شوی حل، نو دی

$\bar{x}_0 = \overline{(-1)^{\alpha\beta} 5^{\beta}}$	(8.57)
---	--------

د $x^n \equiv a(2^k)$ حل دی. له دې سره سرې ټول حلونه لاس ته راوړي.

بیلګه 8.2.8:

$$x^3 \equiv 9(32) : N = 3, a = 9, m = 2^5 (k = 5) \quad 1.$$

و بنایئ: $a = 9$. توانپاتي $\text{mod } 32$ دی (راوړو: \mathbb{Z}_{32}^* د ګاوس له مخې څپوکلیکي نه دی، ځکه چې $(k \geq 3, p = 2)$ د 8.2.7 سره سم:

$$d = \text{ggT}(n, 2^{k-2}) = \text{ggT}(3, 8) = 1 \Rightarrow \quad (8.58)$$

$$a^{\frac{2^k-2}{d}} = 9^{2^5-2} = (9^4)^2 = (81^2)^2 \equiv 1(32), \quad (8.59)$$

۳. 9 نو درې توانپاتي دی

حل: د $n = 3$ ناجوره یا طاق له امله فقط یو انکونگروانت $\text{mod } 32$ حلونه لري، د [8.2.7](#) بنووني سره سم:

$$\bar{a} = \bar{9} = \overline{(-1)^j 5^l}, \quad j \in \{0, 1\}, l \in \{1, \dots, 2^{k-2}\} \quad (8.60)$$

: $\text{mod } 324$.

$$5^0 \equiv 1, 5^1 \equiv 5, 5^2 \equiv -7, 5^3 \equiv -3, 5^4 \equiv -15, 5^5 \equiv -11, 5^6 \equiv 9(32),$$

4. يعني $j = 0, l = 6 \leq 2^{k-2} = 8$ له دې سره $\bar{9} = \overline{(-1)^0 5^6}$ ، 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 دې معنا، چې $3x \equiv 6(8)$ ، دا په دې معنا، چې $\beta = 2 \Rightarrow$ له دې لاس ته راځي یوگونی حل $\text{mod } 32$ دی.

$$\bar{x}_0 = \overline{(-1)^\alpha 5^\beta} = \overline{25}. \quad (8.61)$$

$$x^4 \equiv 177(224) : n = 4, a = 177, m = 224 = 7 \cdot 2^5,$$

$$\text{gg}\Gamma(177, 224) = 1$$

له دې جلا تر راوړو: $x^4 \equiv 177(7)$ او $x^4 \equiv 177(2^5)$

$$x^4 \equiv 177(7)$$

د 8.2.5 له مخې څپوکلیکي دی، د $x^4 \equiv 2(7) : n = 4, a = 2, p = 7$ د گاوس له مخې څپوکلیکي دی، د 8.2.5 سره سم:

$$\varphi(7) = 6, d = \text{ggT}(n, \varphi(7)) = 2; a^{\frac{\varphi(7)}{2}} = 8 \equiv 1(7) \Rightarrow \quad (8.62)$$

د 8.2.5 له مخې باور لري 2 د 4-م توان د سره اینکونگروانت حلونه دی

$$\Rightarrow x_1 = 2, x_2 = 5 \quad x^4 \equiv 177(2^5)$$

$$\Rightarrow x^4 \equiv 17(2^5) : n = 4$$

$$17^{\frac{2^3}{4}} = 17^2 \equiv 1(32), a = 17 \equiv 1(4) \quad \text{جوړه مگر}$$

او همداسې د 8.2.7 له مخې: 17 د 4-م توان mod 32 دی د $8 \bmod 32$ سره

اینکونگروانت حلونه y_1, y_2, \dots, y_8 دي.

$$\bar{a} = \overline{(-1)^j 5^l} \quad \text{د سره سم او کرښیزکوگروانت همداسې} \quad nx \equiv j(2)$$

$\Rightarrow nx \equiv l(2^{k-2})$ څخه لاس ته راځي ټول α ، ټول β څخه لاس ته راځي

$$\bar{y} = \overline{(-1)^{\alpha} 5^{\beta}} \quad \text{ټول (.)}$$

د چینایي پاتي جملې سره سم:

$$\left. \begin{aligned} x &\equiv x_i(7), \\ x &\equiv y_s(32) \end{aligned} \right\} \quad i = 1, 2, s = 1, \dots, 8, \quad (8.63)$$

یعنې 16 سیستمي له دې لاس ته راځي 16 حلونه.

څلوریز پاتې (که غواړئ: مربع باقیمانده) Quadratische Reste

ځانګړی حالت

مور اوس یوځانګړی حالت رااخلو، او د هده حلوروالی تیک تر څیرني لاندې نیسو:

$n = 2$ دا په دې معنا، چې

$$x^2 \equiv a(m) \quad (9.1)$$

د څیرني دی. د دې د حلوروالی لپاره ساده قضیې تر څیرني لاندې نیول زمورموخه ده.

پیژند 9.1.1: $m \in \mathbb{N}, a \in \mathbb{Z}, \text{ggT}(a, m) = 1$ مربعیز توانپاتې $\text{mod } m$ بلل

کیري، او هم لنډ مربعیز پاتې، که $x^2 \equiv a(m)$ حلور وي.

دا لاندې د $m = 2$ لپاره باور لري:

لیما یا جملگی 9.1.2: وي د $\text{ggT}(a, m) = 1 \Rightarrow a \in \mathbb{Z}$ سره

ناجوره (طاق)، دا په دې معنا، چې $2n + 1$ نو باور لري:

هر ناجوره عدد

$$x_0 = 2k + 1 \quad (k \in \mathbb{Z}) \quad (9.2)$$

حلور $\text{mod } 2$ دی.

بنوونه: $x_0^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1(2) \equiv 2n + 1 \equiv a(2)$.

د عمومي قضیې 8.2.5 (هلته $n \in \mathbb{N}$ په خوبنه)، څیکلیکي یا تل بیرته راګرځیدونکی حالت له مخي:

جمله 9.1.3: وي دي $a \in \mathbb{Z}, m \geq 3; m \in \mathbb{N}$ د $\text{ggT}(a, m) = 1$ سره ټيک هلته مربع پاتي $\text{mod } m$ دی، که

$$a^{\frac{\varphi(m)}{2}} \equiv 1(m); \quad (9.3)$$

د $x^2 \equiv a(m)$ د حلونو تعداد يا گنون 2 وي.

بڼونه: 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 د په لومړني ضريب تجزيه کې يو ناجوره (طاق) p_i رامنځ ته شي، نو $p_i - 1$ جوړه يا جفت دی او له دې امله $\varphi(m) \equiv 0(2)$ دی.

دویم: که نه، نو بيا ۲-م توان دی، يعنې $\varphi(m) = \frac{m}{2}$ جوړه دی.

$$(m = 2^\alpha \text{ د } \alpha \geq 2 \text{ سره، } \text{ځکه چې } m \geq 3)$$

جملگی ۹.۱.۴: (اويلر)

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

په پای کې لکه نور چې ويلي مو وو د

$$m = 2^k, k \geq 3,$$

حالت $\mathbb{Z}_{2^k}^*$ د نه ځيکليکي، سره ځانونه په کار اچوو:

جمله 8.2.7: وي دي $a \in \mathbb{Z}, k \geq 3$ ، د $\text{ggT}(a, 2^k) = 1$ سره ټيک هلته n - م توان $\text{mod } 2^k$ دی، که د $d = \text{ggT}(n, 2^{k-2})$ لپاره باور ولري:

$$a^{\frac{2^k - 2}{d}} \equiv 1(2^k) \quad .4$$

کنونپوهنه

5. $\alpha \equiv 1(4)$ یا n ناجوره یا طاق دی.

6.

د $x^n \equiv a(m) \pmod{2^k}$ انکوگروانتو حلونو گڼ، n (تعداد) نو بیا 1 دی د n ناجوره یا طاق لپاره، او $2d$ د جوړه n لپاره.د $x^n \equiv a(2^k)$ د حل (نو) پیدا کول له بنوونې 8.2.7 څخه: $\bar{a} \in \mathbb{Z}_{2^k}$
په لاندې بڼه

$$\bar{a} = \overline{(-1)^j 5^l}, \quad j \in \{0, 1\}, l \in \{1, \dots, 2^{k-2}\} \quad (8.55)$$

په یواځني ډول د 6.2.16 له مخې انځور کړئ، راوړو

$nx \equiv j(2) \pmod{2^{k-2}}$ همداسې؛ $nx \equiv l(2^{k-2})$	(8.56)
--	--------

کرښیز کونگروانت دي، که α د $nx \equiv j(2)$ راکم شوی حل وي او β د $nx \equiv l(2^{k-2})$ راکم شوی حل، نو دی

$$\bar{x}_0 = \overline{(-1)^{\alpha} 5^{\beta}} \quad (8.57)$$

د $x^n \equiv a(2^k)$ حل دی. له دې سره سرې ټول حلونه لاس ته راوړي.

بیلگه 8.2.8:

$$x^3 \equiv 9(32) : N = 3, a = 9, m = 2^5 (k = 5)$$

2.

و بنایئ: $a = 9$. توانپاتي $\pmod{32}$ دی (راوړو: \mathbb{Z}_{32}^* د گاوس له مخې څیوکلېکي نه دی، ځکه چې $k \geq 3, p = 2$) د 8.2.7 سره سم:

$$d = \text{ggT}(n, 2^{k-2}) = \text{ggT}(3, 8) = 1 \Rightarrow \quad (8.58)$$

$$a^{\frac{2^k-2}{d}} = 9^{2^5-2} = (9^4)^2 = (81^2)^2 \equiv 1(32), \quad (8.59)$$

۳. 9 نو درې توانپاتي دی
حل: د $n = 3$ ناجوره يا طاق له امله فقط يو انکونگروانت $\text{mod } 32$ حلونه لري، د [8.2.7](#) بنووني سره سم:

$$\bar{a} = \bar{9} = \overline{(-1)^j 5^l}, \quad j \in \{0, 1\}, l \in \{1, \dots, 2^{k-2}\} \quad (8.60)$$

: $\text{mod } 32$.

$$5^0 \equiv 1, 5^1 \equiv 5, 5^2 \equiv -7, 5^3 \equiv -3, 5^4 \equiv -15, 5^5 \equiv -11, 5^6 \equiv 9(32),$$

4. يعني $j = 0, l = 6 \leq 2^{k-2} = 8$ له دې سره $\bar{9} = \overline{(-1)^0 5^6}$ ، 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 دې معنا، چې $3x \equiv 6(8)$ ، دا په دې معنا، چې $\beta = 2 \Rightarrow$ له دې لاس ته راځي يوگونی حل $\text{mod } 32$ دی.

$$\bar{x}_0 = \overline{(-1)^{\alpha} 5^{\beta}} = \bar{25}. \quad (8.61)$$

$$x^4 \equiv 177(224) : n = 4, a = 177, m = 224 = 7 \cdot 2^5, \\ \text{ggT}(177, 224) = 1$$

$$\text{له دې جلا تر راوړو: } x^4 \equiv 177(7) \text{ او } x^4 \equiv 177(2^5) \\ x^4 \equiv 177(7)$$

د ګاوس له مخې څيوکليکي دی، د [8.2.5](#) $\Rightarrow x^4 \equiv 2(7) : n = 4, a = 2, p = 7$ سره سم:

$$\varphi(7) = 6, d = \text{ggT}(n, \varphi(7)) = 2; a^{\frac{\varphi(7)}{2}} = 8 \equiv 1(7) \Rightarrow \quad (8.62)$$

د [8.2.5](#) له مخې باور لري 2 د 4-م توان د سره اينکونگروانت حلونه دی

کنونپوهنه

$$\Rightarrow x_1 = 2, x_2 = 5$$

$$x^4 \equiv 177(2^5)$$

$$\Rightarrow x^4 \equiv 17(2^5) : n = 4$$

$$17^{\frac{2^3}{4}} = 17^2 \equiv 1(32) \quad \alpha = 17 \equiv 1(4)$$

جوړه مگر

او همداسې د [8.2.7](#) له مخې: 17 د 4-م توان mod 32 دی د 8 mod 32 سره

اینکونګروانت حلونه y_1, y_2, \dots, y_8 دي.

$$\bar{a} = \overline{(-1)^j 5^l} \quad nx \equiv j(2) \quad \text{د) سره سم او کرښیزکوګروانت همداسې}$$

$$\Rightarrow nx \equiv l(2^{k-2}) \Rightarrow \bar{y} = \overline{(-1)^{\alpha 5^{\beta}}} \quad \text{خڅه لاس ته راځي ټول } \alpha, \text{ ټول } \beta \Rightarrow \text{خڅه لاس ته راځي ټول} \quad \text{تول} \quad \text{تول} \quad \text{تول}$$

د چینایي پاتي جملې سره سم:

$$\left. \begin{aligned} x &\equiv x_i(7), \\ x &\equiv y_s(32) \end{aligned} \right\} \quad i = 1, 2, s = 1, \dots, 8, \quad (8:63)$$

يعنې 16 سيستمي له دې لاس ته راځي 16 حلونه.

څلوريز پاتي (که غواړئ: مربع باقیمانده)

ځانګړی حالت

مورن اوس یوځانګړی حالت رااخلو، او د هده حلوروالی ټیک تر څیرني لاندې نیسو:

$n = 2$ دا په دې معنا، چې

$$x^2 \equiv a(m) \quad (9.1)$$

د څیړني دې د دې د حلورولي لپاره ساده قضیې تر څیړني لاندې نیول زموږ موخه ده.

پېژند 9.1.1: $m \in \mathbb{N}, a \in \mathbb{Z}, \text{ggT}(a, m) = 1$ مربعیز توانپاتې $\text{mod } m$ بلل

کیري، او هم لنډ مربعیز پاتې، که $x^2 \equiv a(m)$ حلور وي.

دا لاندې د $m = 2$ لپاره باور لري:

لیما یا جملگی 9.1.2: وي دې $a \in \mathbb{Z}$ د $\text{ggT}(a, m) = 1$ سره

ناجوړه (طاق)، دا په دې معنا، چې $2n + 1$ نو باور لري:

هر ناجوړه عدد

$$x_0 = 2k + 1 \quad (k \in \mathbb{Z}) \quad (9.2)$$

حلور $\text{mod } 2$ دې.

بنوونه: $x_0^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1(2) \equiv 2n + 1 \equiv a(2)$.

د عمومي قضیې 8.2.5 (هلته $n \in \mathbb{N}$ په خوښه)، څیکلیکي یا تل بیرته راگرځیدونکی 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 ټیک هلته مربع پاتې $\text{mod } m$ دې، که

$$a^{\frac{\varphi(m)}{2}} \equiv 1(m); \quad (9.3)$$

د $x^2 \equiv a(m)$ د حلونو تعداد یا گنون 2 وي.

بنوونه: ځکه چې $d = \text{ggT}(2, \varphi(m))$ او دا چې $\varphi(m)$ د $m \geq 3$ لپاره دې تل جوړه دې، نو د 8.2.5 له مخې باور لري:

ګڼونپوهنه

لومړی: که د m په لومنیو ضربیتجزیه کې یو ناجوره 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 2 -م توان دی، یعنې $\varphi(m) = \frac{m}{2}$ ، جوړه.

($m = 2^\alpha$ د $\alpha \geq 2$ سره ځکه چې $m \geq 3$)

کورولار ۹. ۱. ۴ (اویلر) (Euler): وي دې $p > 2$ لومړنی عدد، $a \in \mathbb{Z}$ د

$$\text{ggT}(a, p) = 1$$

(خوړا غټ پروپشوی یا بزرګترین قاسم مشترک) سره ټیک هلته

مربعیز باقی یا پاتې $\text{mod } p$ دی، که

$$a^{\frac{p-1}{2}} \equiv 1(p). (9:4)$$

بڼوونه: د ګاوس 6.2.15 له مخ او د $p \neq 2$ له امله (\mathbb{Z}_p^*, \cdot) تل بیرته راګرځیدني یا ځیکلیکي دی.

جملگی ۹. ۱. ۵ - وي دې $p > 2$ یو لومړنی عدد، له $a \in \mathbb{Z}$ $\text{ggT}(a, p) = 1$

سره ټیک هلته مربع باقی یا پاتې $\text{mod } p^{\alpha} \forall \alpha \in \mathbb{N}$ دی، که a مربع باقی $\text{mod } p$ وي

بڼوونه:

(\Rightarrow)

ساده دی.

(\Leftarrow)

$a^{\frac{p-1}{2}} \equiv 1(p)$ که a مربع باقي $\pmod p$ وي، نو د جملګي 9.1.4 له مخې باور لري:

یعني، $a^{\frac{p-1}{2}} = 1 + tp$ د یوه $t \in \mathbb{Z}$ لپاره. له دې امله د هر $\alpha \in \mathbb{N}$ لپاره باور لري:

$a^{\frac{p(p^\alpha)}{2}} = a^{\frac{1}{2}p^{\alpha-1}(p-1)} = \left(a^{\frac{p-1}{2}}\right)^{p^{\alpha-1}} = (1 + tp)^{p^{\alpha-1}} \equiv 1(p^\alpha),$	(9.5)
--	-------

خُکه: (ایندکشن په α پسی).

$\alpha = 1$ $(1 + tp)^{p^{\alpha-1}} = 1 + tp \equiv 1(p).$	(9.6)
$\alpha \rightarrow \alpha + 1$ $(1 + tp)^{p^\alpha} = \left[(1 + tp)^{p^{\alpha-1}}\right]^p = (1 + rp^\alpha)^p =$	(9.7)
$1 + \underbrace{\binom{p}{1} rp^\alpha + \dots + r^p p^{\alpha p}}_{=p} \equiv 1(p^{\alpha+1}).$	(9.8)
$= \underbrace{\hspace{10em}}_{=1+sp^{\alpha+1}}$	

د جملې 9.1.3 پسی لرو ($m = p^\alpha$ لپاره): $a \in \mathbb{Z}$ مربع پاتي $\pmod{p^\alpha}$ دی. □

د ناڅیکلیکي حالت لپاره، یعنی $a \in \mathbb{Z}$ باید $m = 2^k, k \geq 3$ ناچوره (طاق) وي، لکه لاندې جمله چې ښایي:

کینونپوهنه

جمله ۹.۱.۶: وي دي $a \in \mathbb{Z}$ ناچوره، نو کونگر وانځ يا ورته والی دی $x^2 \equiv a(2^k)$

لومړۍ د $k = 1$ لپاره تل حلور دی او ټيک يو حل لري.

دويم - د $k \geq 3$ لپاره حلور دی، د 4 حلونو سره، که $a \equiv 1(8)$ وي، پرته له ې نه.

بنسونه: لومړۍ پورته وگورۍ: $m = 2 = 2^1$ ، دا چې ټول ناچوره گڼونه يا اعداد $\text{mod } 2$ دي، نو ټيک يو حل شتون لري.

دويم: د گاوس 6.2.15 له مخې، (\mathbb{Z}_4, \cdot) تلبيرته راگرځيدونۍ يا څيکلکي دي، يعنې د 9.1.3 له مخې: ناچوره مربع پاتي $\text{mod } 4 \dots$ دی.

$\dots \Leftrightarrow a \equiv 1(4) \Leftrightarrow a^{\frac{2}{2}} \equiv 1(4) \Leftrightarrow a \equiv 1(4).$	(9.9)
--	-------

دریم: په همدې ترتيب د 9.1.3 پسي: د $x^2 \equiv a(4)$ د حلونو گڼون يا تعداد 2 دی.

وي دي $m = 2^k, k \geq 3$ حلور، نو دی

$x_0^2 \equiv a(2^k)$	(9.10)
-----------------------	--------

څلورم- ديوه $x_0 \in \mathbb{Z}$ لپاره، له دې سره $x_0^2 \equiv a(8)$ ، ځکه چې $8 \mid 2^k (k \geq 3)$

، پسي د 8.1.6 له مخې باور لري: خورا غټ گډ پروپشونۍ)

بزرگترین مقسوم عليه) $\text{ggT}(x_0, 2^k) = 1$ ، نوله دې سره

$\text{ggT}(x_0, 8) = 1 (8 \mid 2^k, k \geq 3)$ $x_0 \in \mathbb{Z}$ دا په دې معنا، چې نسبت و 8 ته

نسي لومړنی عدد دی، يعنې: $x_0 = 1, 3, 5, 7(8)$ ، له دې سره $x_0^2 \equiv 1(8)$

په ټوليزه توګه:

$a \equiv x_0^2 \equiv 1(8).$	(9.11)
-------------------------------	--------

پنځم- وي دي په څټ يا برعکس $a \equiv 1(8)$ ، يعني هم ، $a \equiv 1(4)$ ، پسي باور لري

$a^{2^k-3} \equiv 1(2^k) \quad (k \geq 3).$	(9.12)
---	--------

شپږم- ايندګڼښ: د نيوني يا قرضيې له مخي.

نيسو چي د لپاره سم دي، د لپاره باور لري:

$a^{2^{(k+1)}-3}$	=
$(a^{2^k-3})^2 = (1 + t2^k)^2 = 1 + 2t2^k + t^22^{2k} = 1 + s2^{k+1} \equiv$	(9.13)
$\equiv 1(2^{k+1}).$	(9.14)

$$(d = \text{gg}\Gamma(2, 2^{k-2}) = 2) \quad a \equiv 1(4)$$

اوم- له دي سره لرو او

$a^{\frac{2^k-2}{d}} = a^{2^k-3} \equiv 1(2^k);$	(9.15)
--	--------

اتم- نو د [8.2.7](#) له مخي لرو، چي $a \in \mathbb{Z}$ مربع پاتي يا باقي $\text{mod } 2^k$ دي. له دي

سره $2d = 4$ حلونه باور لري. \square

$$x^2 \equiv 110(211)$$

بيلګه ۹ . ۱ . ۷ : ايا $\Leftrightarrow 110$ مربع پاتي $\text{mod } 211$ حلور دي؟

(دي؟)

کنونپوهنه

دا چې 211 یو لومړنی گڼ یا عدد دی، او $\text{ggT}(110, 211) = 1$ د اویلر 9.1.4 پسي بار لري، ټیک هلته حلور دی، که وي:

$a^{\frac{p-1}{2}} = 110^{105} \equiv 1(211)$	(9.16)
---	--------

- ډیر کار غواړي!

Legendre-Symbol (1752-1833) لژندر-سومبول:

د $x^2 \equiv a(m), \text{ggT}(a, m) = 1$ د حلوروالي لپاره نوې لار.

پیژند یا تعریف ۹ . ۲ . ۱ : (لژندر سیمبول 9.1): وي دي $p > 2$ یو لومړنی گڼ یا عدد،

$a \in \mathbb{Z}$ د لژندر سومبول له مخې مربع پاتي د دي لاندې له لاري تعریع دی:

$\left(\frac{a}{p}\right) = \begin{cases} 1 \\ 0 \\ -1 \end{cases}$	<p>a مربع باقي mod p دی.</p> <p>$P a$</p> <p>انه مربع باقي mod p دی.</p>	(9.17)
---	---	--------

ساده خویونه:

جملگی ۹ . ۲ . ۲ : که $a \equiv a'(p)$ وي، باور لري

$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right).$	(9.18)
---	--------

بڼوونه:

$\text{mod } p \quad \left(\frac{a}{p}\right) = 1$ <p style="text-align: center;">مربع باقي</p>	(9.19)
$\Leftrightarrow x^2 \equiv a(p)$	(9.20)
$\Leftrightarrow x^2 \equiv a'(p)$	(9.21)
$\Leftrightarrow \left(\frac{a'}{p}\right) = 1.$	(9.22)

جملگی ۹. ۳ - وېش له باقي يا پاتي سره:

$a = p \cdot s + r$	(9.23)
---------------------	--------

$a = ps + r \equiv r(p)$ $0 \leq r < p$ د سره، له دي امله دی ، نو د [9.2.2](#) پسي:

$\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right) \dots$ <p style="text-align: center;">لڼوونه</p>	(9.24)
---	--------

جمله ۹. ۲. ۴: وي دی $p > 2$ يو لومړنی عدد او $a \in \mathbb{Z}$ (د خورا غټ گډ پروېشونی) سره، نو باور لري $\text{ggT}(a, p) = 1$

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (p).$	(9.25)
--	--------

بنوونه:

- که $\left(\frac{a}{p}\right) = 1$ وي، نو a مربع پاتي $\text{mod } p$ دی او د [9.1.4](#) پسي يا له $a^{\frac{p-1}{2}} \equiv 1(p)$ مخي: ، له دې سره دی

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (p).$	(9.26)
--	--------

- که $\left(\frac{a}{p}\right) = -1$ وي، نو a مربع باقي $\text{mod } p$ نه دی او د [9.1.4](#) له مخي يا $a^{\frac{p-1}{2}} - 1 \not\equiv 0(p)$ پسي: ، دا په دې معنا، چي $a^{\frac{p-1}{2}} \not\equiv 1(p)$ مخي باور لري

$a^{p-1} \equiv 1(p),$	(9.27)
------------------------	--------

نو $a^{p-1} - 1 \equiv 0(p)$ ، د اسي چي په بدن (انگريزي يي فيلد) $(\mathbb{Z}_p, +, \cdot)$ کي p لومړنی گڼ يا عدد) باور لري:

$\bar{0} = \overline{a^{p-1} - 1} = \overline{(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)} = \underbrace{\overline{a^{\frac{p-1}{2}} - 1}}_{\neq \bar{0}} \overline{a^{\frac{p-1}{2}} + 1};$	(9.28)
---	--------

دا چي بدن صفر نه لري، لرو

$\overline{a^{\frac{p-1}{2}} + 1} = \bar{0}.$	(9.29)
---	--------

له دې سره $a^{\frac{p-1}{2}} + 1 \equiv 0(p)$ او $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ ، دا په دې معنا، چي

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (p).$	(9.30)
--	--------

کورولار ۹ . ۲ . ۵ : دې لومړني عدد وي او $p > 2$ د $a_1, \dots, a_n \in \mathbb{Z}$ د خ غ گ
 یعنی سره، نو باور لري $(i = 1, \dots, n) \text{ ggT}(a_i, p) = 1$

$\left(\frac{a_1 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdots \left(\frac{a_n}{p}\right).$	(9.31)
---	--------

ښوونه: $\text{ggT}(a_1 \cdots a_n, p) = 1$ ، ځکه چې پرته له دې به ، داسې ، $p \mid a_1 \cdots a_n$
 چې د یوه $1 \leq i \leq n$ لپاره د 3.1.5 له مخې $p \mid a_i$ لرو . – تضاد یا مخمخوالی! له دې
 سره $\left(\frac{a_1 \cdots a_n}{p}\right)$ تعریف 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، یعنی $p \mid (\pm 1) - (\pm 1)$. دا کمښت صفر دی، که دواړه
 عددونه برابر وي، او پرته له دې ± 2 .
 له $p > 2$ امله باور لري: $p \nmid \pm 2 \Rightarrow$ یعنی لاس ته راځي کمښت $= 0$ لاس ته راځي
 □ . (9.26).

لاس ته راوړنه ۹ . ۲ . ۶ :

لومړۍ- $a \in \mathbb{Z} (a \neq 0)$ دې د $a = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$
 په لومړنيو ضریبونو توپه کونه یا تجزیه وي. نو د 9.2.5 له مخې باور لري:

کینونپوهنه

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{p_1^{\alpha_1}}{p}\right) \cdots \left(\frac{p_k^{\alpha_k}}{p}\right), \quad (9.33)$$

دویم: نو شمیرو: $\left(\frac{-1}{p}\right)$ او $\left(\frac{q^x}{p}\right)$ د خ غ پ (قاسم بزرگ مشبرک) سره، دا په دې معنا، چې $\text{gg}\Gamma(p, q^a) = 1$ $p \neq q$.

دریم: $1 = \left(\frac{q^2}{p}\right)$ ، 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 دی. $\text{mod } p$

څلورم: ځانگړی حالت: $\left(\frac{1}{p}\right) = 1$ ($1 = 1^2 \Rightarrow$) مو غوښتنه یا ثبوت دی.

پنځم: له ی امله فقط د شمیرلو لپاره: او $\left(\frac{-1}{p}\right)$ د $\left(\frac{q}{p}\right)$ سر لومړنی عدد 2 < دی، ځکه چې

$$\left(\frac{q^{2k}}{p}\right) = \left(\frac{(q^k)^2}{p}\right) = 1. \quad (9.34)$$

کورولار یا جملگی ۹ . ۲ . ۷ : وي دې $p > 2$ لومړنی عدد، نو باور لري:

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

لومړی- -1 تیک هلته مربع باقي $\text{mod } p$ دی، که $p \equiv 1(4)$ وي.

ښوونه:

لومړی- د له مخي باور لري:

$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} (p);$	(9.35)
--	--------

دويم: نو p كمښت يا تفريق وېشي، دا 0 يا ± 2 دی. د $p > 2$ له امله دی
 $p \nmid \pm 2 \Rightarrow$ (له دې لاس ته راځي)
 \Rightarrow كمښت = 0

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$	(9.36)
---	--------

دويم: مربع پاتي دی

$\dots \Leftrightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$	(9.37)
$\Leftrightarrow \frac{p-1}{2}$ <p style="text-align: center;">جوړه</p>	(9.38)
$\Leftrightarrow \frac{p-1}{2} = 2k \quad (k \in \mathbb{N})$	(9.39)
$\Leftrightarrow p-1 = 4k$	(9.40)
$\Leftrightarrow p = 4k + 1$	(9.41)
$\Leftrightarrow p \equiv 1(4).$	(9.42)

لاندي جمله د ديربينلنت د جملې څوکه انځوروي، چې نوره غواړو وښايو:

کینونپوهنه

جمله ۹ . ۲ . ۸ : د $4k + 1$ ($k \in \mathbb{N}$) بڼې ناپای دې لومړني ګڼونه شتون لري. بنوونه: ناسیده، نیسو چې د دې بڼې پای ډېر ګڼونه شتون لري:

p_1, \dots, p_n وي دې .

$N := (2p_1 \cdots p_n)^2 + 1,$	(9.43)
---------------------------------	--------

نو باور ري: $N = 2m + 1$ ، يعنې ناجوره، ا په دې معنا، چې $2 \nmid N$.
 د $N > 1$ له امله يو لومړنی عدد p د $p \mid N$ شتون لري، د ا په 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 پاتي يا باقي \pmod{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 نيوني يا فرضيې له مخو لاس ته راځي: $p = p_i$
 د يوه $1 \leq i \leq n$ 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 $p \leq 1$ - تضاد يا ردونه. \square

د ګاوس لیمایا جملگی

جمله ۹، ۲، ۹: (د ګاوس جمله ګی) وي دي $p > 2$ لومړنی عدد، $a \in \mathbb{Z}$ د خورا

غټ ګډ پروېشوني (بزرګترین مقسوم علیه مشترک) سره $\text{ggT}(a, p) = 1$.

جوړووو: $1 \cdot a, 2 \cdot a, \dots, \frac{p-1}{2} \cdot a$ 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 پاتې یا باقي ګڼون یا تعداد په نڅښه کيږي، چې له $\frac{p}{2}$ لوی دي. بنوونه: د $i = 1, 2, \dots, \frac{p-1}{2}$ لپاره دي وي:

$ia = pq_i + t_i \quad 0 \leq t_i < p$	(9.49)
--	--------

(د پاتې سره وېش) نو $t_i \neq 0 \forall i$ باور لري، پرته له دي $ia = pq_i$ ، يعني $p \mid ia$ ، داسې چې (د 3.1.5 له مخې): $p \mid i$ يا $p \mid a$ ، دا چې $\text{ggT}(a, p) = 1$ ، (خ غ ګ)، بايد باور ولري ($\Rightarrow p \leq i$)، له مخې يو مخامخوالی يا تضاد لاس ته راځي! په ځانګړي ډول باور لري:

$t_i \equiv ia(p) \quad \forall i = 1, 2, \dots, \frac{p-1}{2}.$	(9.50)
--	--------

کڼونپوهنه

وي دي $r_1, \dots, r_{n(a)}$ پورتنی پاتي له $\frac{p}{2} < t_i < p, s_1, \dots, s_k$ سره پاتي له
 $1 \leq t_i \leq \frac{p-1}{2}$ سره دا په دي معنا، چي $1 \leq t_i \leq \frac{p-1}{2}$ (ناجوره!) p

$\Rightarrow n(a) + k = \frac{p-1}{2}.$	(9.51)
---	--------

وښايی: $r_1, \dots, r_{n(a)}, s_1, \dots, s_k$ ټول سره توپير لري.

نيسو $t_i = t_j$ د $i > j$ لپاره، نو

$ia - ja = pq_i - pq_j = p(q_i - q_j);$	(9.52)
---	--------

$ia - ja = 0$ دی، نو $q_i - q_j = 0$ ، دا په دي معنا چي $(i - j)a = 0$ ، يعني $i = j$ ($a \neq 0$)
 -تضاد يا مخامخوالی!

دی، نو $q_i - q_j \neq 0$ ، $p \mid (i - j)a$ ، د [3.1.5](#) له مخي لاس ته راخي $p \mid i - j$ يا $ggT(p, a) = 1$ ، $p \mid a$ (خ غ ک) له امله لرو - تضاد يا مخامخوالی!
 $0 \leq i - j < \frac{p-1}{2} < p$ ، له کوم به چي $i - j = 0$ لاس ته راغلی وی.)

جوړ کړی

$\alpha_i = p - r_i \ (i = 1, \dots, n(a)),$	(9.53)
--	--------

نو ټول $\alpha_1, \dots, \alpha_{n(a)}$ مختلف يا نابرابر دي (ټول $r_1, \dots, r_{n(a)}$ مختلف دي).
 پسي لرو $\alpha_i \neq s_j \ \forall i, j$ خکه چي :

$\alpha_i = p - r_i = s_j \Rightarrow r_i + s_j = p \equiv 0(p)$	(9.54)
--	--------

i, j	
$\Rightarrow ia + ja \equiv 0(p) \ (t_i \equiv ia(p) \ \forall i)$	(9.55)
$\Rightarrow p \mid (i+j)a \stackrel{3.1.5}{\Leftrightarrow} p \mid i+j \ (ggT(a, p) = 1);$	(9.56)

$1 \leq i+j \leq p-1 < p$ $1 \leq i, j \leq \frac{p-1}{2}$
 له امله باور لري: د
 تضاد!

$\alpha_1, \dots, \alpha_{n(a)}, s_1, \dots, s_k$	(9.57)
---	--------

ټول مختلف دي يا توپير لري.

$0 < \alpha_i \leq \frac{p-1}{2}$
 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

$1 \leq s_j \leq \frac{p-1}{2}; \quad 1 \leq \alpha_i \leq \frac{p-1}{2}$ او	(9.60)
---	--------

دا چې

$n(a) + k = \frac{p-1}{2}$	(9.61)
----------------------------	--------

کنونپوهنه

(ټول باقي يا پاتي توپير لري) $\alpha_1, \dots, \alpha_{n(a)}, s_1, \dots, s_k$ ټيک $\frac{p-1}{2}$ طبيعي اعداد دي د 1 او $\frac{p-1}{2}$ ترمنځ. له دې سره: ټيک اعداد $\alpha_1, \dots, \alpha_{n(a)}, s_1, \dots, s_k$ دي. له دې لاس ته راځي:

$$\alpha_1 \cdots \alpha_{n(a)} s_1 \cdots s_k = 1 \cdot 2 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)! \quad (9.62)$$

$$\Rightarrow (p-r_1) \cdots (p-r_{n(a)}) s_1 \cdots s_k = \left(\frac{p-1}{2}\right)! \quad (9.63)$$

$$\Rightarrow (-1)^{n(a)} r_1 \cdots r_{n(a)} s_1 \cdots s_k \equiv \left(\frac{p-1}{2}\right)! (p) \quad (9.64)$$

$$\Rightarrow (-1)^{n(a)} t_1 \cdots t_{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! (p) \quad (9.65)$$

$$(d \text{ ټيک } r_i, s_j \text{ له تعريف څخه}) \quad (9.66)$$

$$\Rightarrow (-1)^{n(a)} 1 \cdot a \cdots \left(\frac{p-1}{2}\right) \cdot a \equiv \left(\frac{p-1}{2}\right)! (p) \quad (9.67)$$

$$(d \text{ تعريف له مخې: } ia = pq_i + t_i \equiv t_i(p)) \quad (9.68)$$

$$\Rightarrow (-1)^{n(a)} a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! (p). \quad (9.69)$$

باور لري $ggT\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$ ، ځکه چې پرته له دې به وی

$$p \mid \left(\frac{p-1}{2}\right)! = 1 \cdot 2 \cdots \frac{p-1}{2}, \quad (9.70)$$

يعني د [3.1.5](#) له مخې:

$$\exists k : 1 \leq k \leq \frac{p-1}{2} < l : p \mid k \quad \text{اتضاد.} \quad (9.71)$$

$$\Rightarrow (-1)^{n(a)} a^{\frac{p-1}{2}} \equiv 1(p) \quad (9.72)$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv (-1)^{n(a)}(p) \quad (9.73)$$

$$\stackrel{9.2.4}{\Leftrightarrow} \left(\frac{a}{p}\right) \equiv (-1)^{n(a)}(p) \quad (9.74)$$

$$\Rightarrow p \in \{0, \pm 2\} \text{ د کمنبت وېشي } \quad (9.75)$$

$$\Rightarrow \text{کمنبت بايد صفر وي } (p > 2, p \nmid 2!) \quad (9.76)$$

$$\Rightarrow \left(\frac{a}{p}\right) = (-1)^{n(a)}. \quad (9.77)$$

بيلکه 9.2.10 . ايا 7 څلورۍ پاتې يا مربع باقي $\text{mod } 13$ دی؟

$p = 13, a = 7, ggT(a, p) = 1$ خورا غټ گډ پروېشونۍ؛ جور کړی :
 $1 \cdot 7, \dots, 6 \cdot 7$

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 گڼون یا تعداد $n(7)$ له $\frac{13}{2}$ لوي دي ، دا په دې معنا، چې $7 \geq 3$ برابر دی. له دې امله

$\left(\frac{7}{13}\right) = (-1)^3 = -1,$	(9.79)
--	--------

دا په دې معنا، چې $a = 7$ مربع یا څلورې پاتې $\text{mod } 13$ 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 گڼونو سره.

جمله $11 : 2 : 9 : p, q$ مختلف لومړني گڼونه دي، $p > 2$ ، نو باور لري:

1. $q = 2$:

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}, \quad (9.80)$$

2. $q > 2$:

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^{\frac{q-1}{2}} \left[\frac{ip}{q}\right]}. \quad (9.81)$$

دریم: $[x]$ د x پسي کوچنی عدد یا گڼ په نڅبنه کوي) (بنوونه: د [9.2.9](#) بنووني ته ورته (ټاکو $a = q$) باور لري:

$$iq = pq_i + t_i \quad (i = 1, \dots, \frac{p-1}{2}), \quad 0 < t_i < p, \quad q_i = \left[\frac{iq}{p} \right]. \quad (9.82)$$

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:

$$q \cdot \underbrace{\sum_{i=1}^{\frac{p-1}{2}} i}_{= \frac{1}{2} \left(\frac{p-1}{2} \right) \left(\frac{p-1}{2} \right)} = q \frac{p^2 - 1}{8} = p \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p} \right] + \sum_{i=1}^{n(q)} r_i + \sum_{i=1}^k s_i \quad (9.84)$$

($r_i \dots$ پاتي (باقي) $> \frac{p}{2}$ ، $s_i \dots$ پاتي $\leq \frac{p}{2}$). د [9.2.9](#) بنووني له مخې باور لري:

$$\left\{ 1, 2, \dots, \frac{p-1}{2} \right\} = \{p - r_1, \dots, p - r_{n(q)}, s_1, \dots, s_k\}; \quad (9.85)$$

نو باور لري:

کنونپوهنه

$$\frac{p^2 - 1}{8} = \sum_{i=1}^{\frac{p-1}{2}} i = \sum_{i=1}^{n(q)} (p - r_i) + \sum_{i=1}^k s_i = p \cdot n(q) - \sum_{i=1}^{n(q)} r_i + \sum_i (9.86)$$

د (9.64) او (9.66) کمون (تفریق) له لارې:

$$(q-1) \frac{p^2 - 1}{8} = p \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p} \right] - p \cdot n(q) + 2 \sum_{i=1}^{n(q)} r_i. \quad (9.87)$$

له دې سره $\text{mod } 2$:

$$(q-1) \frac{p^2 - 1}{8} \equiv \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p} \right] - n(q)(2). \quad (9.88)$$

- که $q > 2$ وي، نو q ناجوره (طاق) دی، یعني $q-1$ جوړه (جفت)، نو $q-1 \equiv 0(2)$ له دې سره:

$$0 \equiv \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p} \right] - n(q)(2) \Rightarrow n(q) \equiv \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p} \right] (2). \quad (9.89)$$

د 9.2.9 له مخې لرو یا لاس ته راځي:

$$\left(\frac{q}{p} \right) = (-1)^{n(q)} = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p} \right]}. \quad (9.90)$$

- که $q = 2$ وي، نو $q - 1 = 1$ ، او د $1 \leq i \leq \frac{p-1}{2}$ لپاره باور لري:

$$0 < \frac{2}{p} \leq \frac{2i}{p} \leq \frac{p-1}{p} < 1, \quad (9.91)$$

- نو $\left[\frac{2i}{p}\right] = 0$ د $1 \leq i \leq \frac{p-1}{2}$ لپاره، له دې سره پاتيري

$$\frac{p^2 - 1}{8} \equiv -n(q)(2) \Rightarrow n(q) \equiv \frac{p^2 - 1}{8}(2). \quad (9.92)$$

د [9.2.9](#) له مخې لاس ته راځي:

$$\left(\frac{2}{p}\right) = (-1)^{n(q)} = (-1)^{\frac{p^2-1}{8}}. \quad (9.93)$$

جمله ګوتي 9.2.12: وي دې $p > 2$ يو لومړني ګڼ، نو باور لري: 2 ټيک څلورۍ

پاتي يا مربع باقي ده، که $p = 8k \pm 1 (k \in \mathbb{Z})$ وي.

بڼونه: 2 څلورۍ پاتي

$$\text{mod } p \Leftrightarrow \left(\frac{2}{p}\right) = 1 \quad (9.94)$$

$$\stackrel{9.2.11}{\Leftrightarrow} (-1)^{\frac{p^2-1}{8}} = 1 \quad (9.95)$$

کونپوهنه

$$\Leftrightarrow \frac{p^2 - 1}{8} \quad (9.96)$$

جوړه دی

$$\Leftrightarrow \frac{p^2 - 1}{8} = 2n \quad n \in \mathbb{N} \quad (9.97)$$

$$\Leftrightarrow p^2 - 1 = 16n. \quad (9.98)$$

د $p > 2$ لومړنی گڼ $\text{mod } 8$ لاندې بڼه لري

$$8k \pm 1, 8k \pm 2, 8k \pm 3, 8k \pm 4 \quad (9.99)$$

$$\Rightarrow 8k \pm 1, 8k \pm 3 \Rightarrow p \text{ لومړنی گڼ } p > 2$$

ناجوړه گڼ

$$p = 8k \pm 3 \Rightarrow \text{که وی}$$

$$p^2 - 1 = 64k^2 \pm 48k + 9 - 1 \equiv 8(16) \not\equiv 0(16), \quad (9.100)$$

دا په دې معنا، چې $p^2 - 1 \neq 16n$ تضاد یا په څټوالي

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-Symbol لپاره د خلوری - یا مربع ریخیپروسیتی قانون reciprocity law

جمله 9.2.13: (مربع ریخیپروختی): وي دې p, q لومړني گنونه، ≥ 2 دواړه ، نو

$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$	(9.103)
---	---------

بنوونه: وي دې

$$M := \left\{ (i, j) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq i \leq \frac{p-1}{2}, 1 \leq j \leq \frac{p-1}{2} \right\}, \quad (9.104)$$

نو M تیک $\frac{p-1}{2} \frac{p-1}{2}$ توکي لري. راوړو

$$M_1 = \{(i, j) \in M \mid qi > pj\}, \quad (9.105)$$

$$M_2 = \{(i, j) \in M \mid qi < pj\}. \quad (9.106)$$

کینونپوهنه

- باور لري $qi = pj$ ، لاس ته راځي ، يعني ، $p \mid qi$ ، $p \mid i$ ($\text{ggT}(p, q) = 1$)
تضاد يا مخمخوالی و ته له دې سره: $1 < i \leq \frac{p-1}{2} < p$

$$M = M_1 \cup M_2, M_1 \cap M_2 = \emptyset. \quad (9.107)$$

وښايي:

$$M_1 = \left\{ (i, j) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq i \leq \frac{p-1}{2}, 1 \leq j < \frac{qi}{p} \right\}, \quad (9.108)$$

$$M_2 = \left\{ (i, j) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq i < \frac{pj}{q}, 1 \leq j \leq \frac{q-1}{2} \right\}. \quad (9.109)$$

- د M_1 لپاره: د هر څه د مخه يا لومړی باور لري $M_1 \subseteq \{\dots\}$ ، ځکه چې

$$(i, j) \in M_1 \Rightarrow qi > pj \Rightarrow 1 \leq j < \frac{qi}{p}. \quad (9.110)$$

- په څټ يا برعکس: $\{\dots\} \subseteq M_1$ ، ځکه چې

$$1 \leq i \leq \frac{p-1}{2}, 1 \leq j < \frac{qi}{p} \Rightarrow \frac{qi}{p} \leq \frac{qp-1}{p} - \frac{qp-1}{2p} < \frac{q}{2} \quad (9.111)$$

$$\Rightarrow \left[\frac{qi}{p} \right] \leq \left[\frac{q}{2} \right] \leq \frac{q-1}{2}, \quad (9.112)$$

$$1 \leq j < \frac{qi}{p} \Rightarrow 1 \leq j \leq \left[\frac{qi}{p} \right] \leq \frac{q-1}{2}, \quad (9.113)$$

- دا په دې معنا، چې $(i, j) \in M$. بالاخره: $(i, j) \in M_1$ ، ځکه چې

$$1 \leq j < \frac{qi}{p} \Rightarrow pj < qi. \quad (9.114)$$

- ورته د M_2 لپاره. ګڼل یې: د هر لپاره توکي شتون لري، له دې سره باور لري

$$(9.115) \quad \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p} \right] \quad \text{توکي لري} \quad M_1 \quad \text{تیک}$$

ورته

$$(9.116) \quad \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q} \right] \quad \text{توکي لري} \quad M_2 \quad \text{تیک}$$

نو $M = M_1 \cup M_2, M_1 \cap M_2 = \emptyset$ تیک

$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p} \right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q} \right] = \frac{p-1}{2} \frac{q-1}{2}$	(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 گي 9.2.14: p, q مختلف > 2 لومړني گڼونه يا اعداد دي، نو باور لري

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad (9.120)$$

تيک هلته، که $p \equiv 1(4)$ يا $q \equiv 1(4)$ يا دواړه وي.

بنوونه: 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 لاري لاس ته راوړو:

$$\left. \begin{aligned} \left(\frac{q}{p}\right) = 1 &\Rightarrow \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right) \\ \left(\frac{q}{p}\right) = -1 &\Rightarrow \left(\frac{p}{q}\right) (-1)^2 = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right) \end{aligned} \right\} \Rightarrow \left(\frac{p}{q}\right) \quad (9.12)$$

له دې سره:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \Leftrightarrow (-1)^{\frac{p-1}{2} \frac{q-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2} \frac{q-1}{2} \text{ جوړه} \quad (9.12 \quad 3)$$

$$\Leftrightarrow \frac{p-1}{2} \vee \frac{q-1}{2} \text{ يا دواړه جوړه دي} \quad (9.12 \quad 4)$$

$$\Leftrightarrow \frac{p-1}{2} = 2n \vee \frac{q-1}{2} = 2m \Leftrightarrow p-1 = 4n, q-1 = 4m \quad (9.12 \quad 5)$$

$$\Leftrightarrow p \equiv 1(4) \vee q \equiv 1(4) \text{ دواړه.} \quad (9.12 \quad 6)$$

بيلگه 9.2.15: ايا $a = -21$ څلورۍ پاتې يا مربع باقي $\pmod{61}$ دي؟

$$x^2 \equiv -21(61) \text{ (دا په دې معنا چې اوببور يا حلور دی؟)}$$

$$p = 61 \in \mathbb{P}, \text{ggT}(-21, 61) = 1 \text{ له دې سره ميژندر:}$$

$$\left(\frac{-21}{61}\right) = \left(\frac{(-1) \cdot 3 \cdot 7}{61}\right) \stackrel{9.2.5}{=} \left(\frac{-1}{61}\right) \left(\frac{3}{61}\right) \left(\frac{7}{61}\right) \stackrel{9.2.7}{=} 1 \left(\frac{3}{61}\right) \left(\frac{7}{61}\right) \quad (9.12 \quad 7)$$

$$\stackrel{9.2.1}{=} \left(\frac{61}{3}\right) \left(\frac{7}{61}\right) \stackrel{Red.}{=} \left(\frac{1}{3}\right) \left(\frac{7}{61}\right) = 1 \left(\frac{7}{61}\right) = \left(\frac{7}{61}\right) \quad (9.12 \quad 8)$$

کنونپوهنه

$$\stackrel{\text{Red.}}{\equiv} \left(\frac{5}{7}\right) \stackrel{9.2.14}{\equiv} \left(\frac{7}{5}\right) \stackrel{\text{Red.}}{\equiv} \left(\frac{2}{5}\right) \stackrel{9.2.12}{\equiv} -1 \quad (9.12)$$

9)

 $\Rightarrow -21$ څلورۍ پاتي $\text{mod } 61$ نه دي.

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

پام يا يادونه 9.2.16: ، چيرته چې m لومړنی گڼ نه دی، نو ليژندر

لومړنیو ضربيونو يا ځله وونو ټوټه کيدنه. نو باور لري: $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ د m په

سومبول تعريف ده دی يا پي-اند نه لري، مگر: وي دي

لومړنیو ضربيونو يا ځله وونو ټوټه کيدنه. نو باور لري:

$$a \pmod{m \dots} \text{ مربع بقي دی.}$$

$$\dots \Leftrightarrow x^2 \equiv a(m) \quad (9.130)$$

$$\Leftrightarrow x^2 \equiv a(p_i^{\alpha_i}) \quad i = 1, \dots, k \quad (9.131)$$

$$\stackrel{9.1.5}{\Leftrightarrow} x^2 \equiv a(p_i) \quad i = 1, \dots, k \quad (9.132)$$

$$\Leftrightarrow a \pmod{p_i} \text{ څلورۍ پاتي } i = 1, \dots, k \quad (9.133)$$

$$\Leftrightarrow \left(\frac{a}{p_i}\right) = 1 \quad i = 1, \dots, k. \quad (9.134)$$

جاکوبي سومبول Jacobi-Symbol

په لاندې کې د $x^2 \equiv a(m)$ د اوبی یا حل د پرېکړې لپاره یو بل امکان څیړو، مگر د لږ واړه بندیز سره:

پېژند 9.3.1: (جاکوب [9.2](#) سومبول): m دې یو ناجوره طبیعي ګڼ وي،
 $m = p_1 \cdots p_k$ چېرته چې p_1, \dots, p_k نه اړین مختلف طبیعي لومړني ګڼونه دي.
 $\text{ggT}(a, m) = 1$ $a \in \mathbb{Z}$ دی د سره، نو څلورۍ یامربع باقی د جاکوب له مخې په لاندې توګه تعریف دی

$\left(\frac{a}{m}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)_L$	(9.135)
---	---------

او $\left(\frac{a}{1}\right) = 1$ [\[9.3\]](#)

یادونه 9.3.2: زیات وخت دا سومبول د کمیزو یا منفي ګڼونو $m < 0$ لپاره هم تعریفیږي:

$\left(\frac{a}{m}\right) := \left(\frac{a}{ m }\right).$	(9.136)
---	---------

دا مور نه پریردو، د دې لارې لاندې ترې لاس ته راتلنه په روښانه توګه ساده لاس ته راوړل کیږي.

یادونه 9.3.3

کڼونپوهنه

لومړی . $m \in \mathbb{N}$ جوړه دی، نو نو د $x^2 \equiv a(m)$ اوبیوروالي - یا د حلوروالي پرابلم په یوه ناجوره مودل بیرته اړوو، ځکه چې: $m = 2^\alpha n$ د ناجوره n سره (تل شونی دی)، نو باور لري:

$x^2 \equiv a(m) \Leftrightarrow x^2 \equiv a(2^\alpha) \quad \text{او} \quad x^2 \equiv a(n)$	(9.137)
--	---------

دویم. دلته $x^2 \equiv a(2^\alpha)$ له 9.1.6 سره پای شو او n ناجوره دی

دریم: د پیژند یا تعریف له مخي دی

$\left(\frac{a}{p_i}\right)_L = \pm 1, \quad \text{ځکه چې} \quad \left(\frac{a}{m}\right)_J = \pm 1,$	(9.138)
---	---------

څلورم: $\left(\frac{a}{m}\right)_J = -1$ دی، نو a څلوری پاتي یا مربع باقي $\text{mod } m$ نه ده، ځکه چې د تعریف له مخي:

$-1 = \left(\frac{a}{m}\right)_J = \prod_{i=1}^k \left(\frac{a}{p_i}\right)_L,$	(9.139)
---	---------

پنځم: ینی لږ تر لږه $\left(\frac{a}{p_i}\right)_L = -1$ یو دی، دا په دي معنا، چې د دي i لپاره a څلوری پاتي $\text{mod } p_i$ نه دی. له دي سره a هم مربع باقي $\text{mod } m$ نه دی.

$$\left(x_0^2 \equiv a(m) \stackrel{p_i|m}{\Rightarrow} x_0^2 \equiv a(p_i) \right)$$

شپږم: $\left(\frac{a}{p_i}\right)_L = -1$ دی، نو a نه اړین یو مربع باقي $\pmod{p_i}$ دی (کیدى شي وي، مګر باید نه دی، چې وي).

بیلګه: $\left(\frac{2}{15}\right)$ جاکوبي-سومیل دی ($15 \in \mathbb{N}$ ناچوره (طاق) $(2, 15) = 1$)، د تعریف له مخې:

$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right),$	(9.140)
--	---------

له دې سره د [9.2.12](#) له مخې باور لري: $\left(\frac{2}{3}\right) = -1$ ځکه چې

$3 \neq 8k \pm 1$, $\left(\frac{2}{5}\right) = -1$ ځکه چې $5 \neq 8k \pm 1$

یعنې:

$\left(\frac{2}{15}\right) = (-1)(-1) = 1,$	(9.141)
---	---------

مګر 2 مربع باقي $\pmod{15}$ نه دی. له دې امله په لومړنیو ضریبونو تجزیه.....

لومړی: $\alpha \equiv \alpha'(m)$ دی، نو باور لري

کنونپوهنه

$\left(\frac{a}{m}\right)_J = \left(\frac{a'}{m}\right)_J.$	(9.142)
---	---------

دویم: جمله گۍ 9.2.5 ته ورته د لیجنډر-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: پسي 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)
---	---------

یادونه: که په راتلونکي کي د سومبول ډول غوره وي، نو د $\left(\frac{a}{p}\right)_L$ سره د لیجنډر-

سومبول او له $\left(\frac{a}{p}\right)_J$ سره د جاکوبي سومبول سره توپيروي. دا پورته تعريف له دې امله وايي، چې جاکوبي سومبول د لیجنډر - سومبول ضرب دی.

ځانگړي حالتونه: $a = -1, a = 2$

لیجنډر ته ورته: د $a = -1$ همداسي د $a = 2$ لپاره جاکوبي-سومبول را اخلو:

ليما يا وره جمله : $m = m_1 \cdots m_k \in \mathbb{N}$ ناچوره دی، نو باور لري:

لومړی:

$\frac{m-1}{2} \equiv \sum_{i=1}^k \frac{m_i-1}{2} (2),$	(9.145)
--	---------

دویم:

$\frac{m^2-1}{8} \equiv \sum_{i=1}^k \frac{m_i^2-1}{8} (2).$	(9.146)
--	---------

بنوونه : دا چې m ناچوره دی، باید هر m_i هم ناچوره 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 بنوول کيږي.

$k \rightarrow k+1$

:

وي دی $m = m_1 \cdots m_k m_{k+1} \in \mathbb{N}$ ناچوره، نو هر m_i ناچوره دی، او هم $2 \mid m_{k+1} - 1$ ناچوره دی او همداسې $2 \mid m_{k+1} - 1$ هم، نو په ټوليزه توگه دا ضرب په 4 وپشور دی

$(m_1 \cdots m_k - 1)(m_{k+1} - 1) =$	(9.147)
---------------------------------------	---------

کنونپوهنه

$= \underbrace{m_1 \cdots m_k m_{k+1}}_{=m} - m_1 \cdots m_k - m_{k+1} + 1;$	
--	--

له دې امله: $(4) m - 1 \equiv m_1 \cdots m_k - 1 + m_{k+1} - 1$ ، کين او بنې لور ته جوړه گڼ ځای دی، د $\text{ggT}(4, 2) = 2$ له امله 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 ایندکشن پسي 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 $a \in \mathbb{N}$ ناجوره 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)

جوړه دی، دا په دې معنا، چې ضريب يا ځله وونی 2 لري. $t+1$ يا t 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 بنوول کيږي

$k \rightarrow k + 1$

:

۴ - وي دي $m = m_1 \cdots m_k m_{k+1} \in \mathbb{N}$ ، ناجوره، نو تول m_i ناجوره دي او $m_1 \cdots m_k$ هم، نو

$8 \mid m_{k+1}^2 - 1.$ او $8 \mid m_1^2 \cdots m_k^2 - 1$	(9.153)
--	---------

۵ - له دي سره $m_1^2 \cdots m_k^2 - 1 \equiv 0(8), m_{k+1}^2 - 1 \equiv 0(8)$ ، يعني د [4.1.5](#) له مخي

$(m_1^2 \cdots m_k^2 - 1)(m_{k+1}^2 - 1) \equiv 0(64).$	(9.154)
---	---------

۶ - دا په دي معنا، چي $64 \mid m_1^2 \cdots m_k^2 m_{k+1}^2 - m_1^2 \cdots m_k^2 + 1 - m_{k+1}^2$ ، نو

$m_1^2 \cdots m_k^2 m_{k+1}^2 - 1 \equiv m_1^2 \cdots m_k^2 - 1 + m_{k+1}^2 - 1(64),$	(9.155)
---	---------

۷ - نو:

$\frac{m^2 - 1}{8} \equiv \frac{m_1^2 \cdots m_k^2 - 1}{8} + \frac{m_{k+1}^2 - 1}{8} (8),$	(9.156)
--	---------

۸ - دا په دې معنا، چې د ایندکشن له مخې:

$\frac{m^2 - 1}{8} \equiv \sum_{i=1}^k \frac{m_i^2 - 1}{8} + \frac{m_{k+1}^2 - 1}{8} = \sum_{i=1}^{k+1} \frac{m_i^2 - 1}{8} \quad (8).$	(9.157)
---	---------

د دې پرېکړې لپاره چې ایا -1 یا 2 څلورۍ پاتې (مربعباقي) دی که نه:

جمله : وي دې $m \in \mathbb{N}$ ناجوره، نو باور لري:

$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}},$	- ۱ (9.158)
$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$	- ۲ (9.158)

ښوونه: وي دې $m = p_1 \cdots p_k$ ناجوره، $p_i \in \mathbb{P}$ ، ټول p_i ناجوره، يعنې > 2

- ۱

$\left(\frac{-1}{m}\right) \stackrel{Def.}{=} \prod_{i=1}^k \left(\frac{-1}{p_i}\right)_L \stackrel{9.2.7}{=} \prod_{i=1}^k (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^k \frac{p_i-1}{2}}.$	(9.160)
--	---------

۲ - دا چې د(1) [9.3.5](#) له مخې باور لري:

$$\sum_{i=1}^k \frac{p_i - 1}{2} \equiv \frac{m-1}{2} (2) \Rightarrow \sum_{i=1}^k \frac{p_i - 1}{2} = \frac{m-1}{2} + 2t \quad (t \in \mathbb{N}), \quad (9.161)$$

۳- او $(-1)^{2t} = 1$ ، لاس ته راځي:

$$(-1)^{\sum_{i=1}^k \frac{p_i - 1}{2}} = (-1)^{\frac{m-1}{2}}. \quad (9.162)$$

۴-

$$\left(\frac{2}{m} \right) \stackrel{Def.}{=} (9.163)$$

$$\prod_{i=1}^k \left(\frac{2}{p_i} \right)_L \stackrel{9.2.11}{=} \prod_{i=1}^k (-1)^{\frac{p_i^2 - 1}{2}} = (-1)^{\sum_{i=1}^k \frac{p_i^2 - 1}{2}} \stackrel{9.3.5(2)}{=} (9.164)$$

$$\stackrel{9.3.5(2)}{=} (-1)^{\sum_{i=1}^k \frac{m^2 - 1}{2}}.$$

د جاکوبي-سومبول لپاره څلورۍ - يا مربع رځپېروختي قانون

ليجنډر-سومبول ته ورته د جاکوبپ-سومبول لپاره هم مربع رځپېروختي قانون) باور لري:

جمله : (مربع رځپېروختي قانون) وي دي $m, n \in \mathbb{N}$ د ناچوره(طاق)
 $ggT(m, n) = 1, m, n$
 (خورا غټ ګډ پروېشونۍ) سره، نو با وړ لري:

$\binom{m}{n} \binom{n}{m} = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}$	(9.165)
--	---------

بنسونه: وي دي $m = p_1 \cdots p_k, p_i \in \mathbb{P}$ ، نه په اړينه توگه مختلف،
 له $\text{ggT}(m, n) = 1$ نه په اړينه توگه مختلف. د $n = q_1 \cdots q_s, q_j \in \mathbb{P}$
 امله باور لري: $\text{ggT}(p_i, q_j) = 1, p_i, q_j > 2 \forall i, j$. پسي .

$\binom{n}{m} \stackrel{Def.}{=} \prod_{j=1}^s \binom{m}{q_j}_L = \prod_{i=1}^s \binom{p_1 \cdots p_k}{q_j} \stackrel{9.2.5}{=} \prod_{j=1}^s \left(\prod_{i=1}^k \binom{p_i}{q_j} \right);$	(9.166)
$\binom{n}{m} \stackrel{Def.}{=} \prod_{i=1}^k \binom{n}{p_i}_L = \prod_{i=1}^k \left(\frac{q_1 \cdots q_s}{p_i} \right) \stackrel{9.2.5}{=} \prod_{i=1}^k \left(\prod_{j=1}^s \binom{q_j}{p_i} \right);$	(9.167)

نو:

$\binom{m}{n} \binom{n}{m} =$	
-------------------------------	--

$\prod_{j=1}^s \prod_{i=1}^k \left[\binom{p_i}{q_j} \binom{q_j}{p_i} \right] \stackrel{9.2.13}{=} \prod_{j=1}^s \prod_{i=1}^k \left[(-1)^{\frac{p_i-1}{2} \frac{q_j-1}{2}} \right] =$	(9.168)
$= (-1)^{\left(\sum_{i=1}^k \frac{p_i-1}{2} \right) \left(\sum_{j=1}^s \frac{q_j-1}{2} \right)}.$	(9.169)

دا چې باور لري:

$\sum_{i=1}^k \frac{p_i - 1}{2} \equiv \frac{m - 1}{2} (2),$	(9.170)
او	
$\sum_{j=1}^s \frac{q_j - 1}{2} \equiv \frac{n - 1}{2} (2)$	

پسې لاس ته راځي

$\left(\sum_{i=1}^k \frac{p_i - 1}{2} \right) \left(\sum_{j=1}^s \frac{q_j - 1}{2} \right) \stackrel{9.3.5(1)}{=}$	
$\left(\frac{m - 1}{2} + 2t \right) \left(\frac{n - 1}{2} + 2n \right) =$	(9.168)
$= \frac{m - 1}{2} \frac{n - 1}{2} + 2v.$	(9.169)

له دې سره په ټوليزه توگه باور لري:

$$(-1)^{\left(\sum_{i=1}^k \frac{n_i-1}{2}\right)\left(\sum_{j=1}^s \frac{r_j-1}{2}\right)} = (-1)^{\frac{m-1}{2} \frac{n-1}{2} + 2v} = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}. \quad (9.173)$$

پايله 9.3.8 : $a < 0$ دی، نو

$$\left(\frac{a}{m}\right) = \left(\frac{-|a|}{m}\right) = \left(\frac{-1}{m}\right) \left(\frac{a}{m}\right), \quad (9.174)$$

د هغه سره چې $\left(\frac{-1}{m}\right)$ د 9.3.6 له مخې ټاکلی، او $|a| > 0$.

پايله 9.3.9 : (ورته و 9.2.14 ته)

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) (-1)^{\frac{m-1}{2} \frac{n-1}{2}}, \quad (9.175)$$

نو ترې لاس ته راځي:

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \Leftrightarrow (-1)^{\frac{m-1}{2} \frac{n-1}{2}} = 1 \Leftrightarrow \frac{m-1}{2} \frac{n-1}{2} \text{ جوړه (جفت)}$$

$$\Leftrightarrow \frac{m-1}{2} \vee \frac{n-1}{2} \text{ جوړه} \quad (9.177)$$

جاکوبي-سومبول دا کره کوي، چې ایا a مربع باقي $\text{mod } m$ دی (که جاکوبي-سومبول 1 وي، نو پرېکره نه شته).

بیلگه 9.3.10 :

$$x^2 \equiv -8(15) \pmod{15} \quad \text{۱- ابيور يا حل وړ دی؟}$$

(دا په دې معنا، چې $a = -8$ مربعپاتي $\pmod{15}$ دی؟)

$$m = -8 < 0, n = 15 \notin \mathbb{P}, \text{ggT}(-8, 15) = 1, 15$$

ناجوړه له دې لاس ته راځي جاکوبي

$\left(\frac{-8}{15}\right)_J =$	(9.178)
$\left(\frac{-1}{15}\right) \left(\frac{8}{15}\right) \stackrel{9.3.6}{=} (-1) \left(\frac{8}{15}\right) = (-1) \underbrace{\left(\frac{4}{15}\right) \left(\frac{2}{15}\right)}_{=1} \stackrel{9.3.6}{=}$	(9.179)
$\stackrel{9.3.6}{=} (-1) \cdot 1 \cdot 1 = -1$	(9.179)

۲- (لرو چې) $\Rightarrow -8$ مربع باقي $\pmod{15}$ نه دی.

$$x^2 \equiv 59(125) \pmod{125} \quad \text{۳- اوبيور يا حل وړ دی؟}$$

$$\text{ggT}(59, 125) = 1, a \in \mathbb{Z}, m \in \mathbb{N}$$

، دواړه ناجوړه، جاکوبي:

$\left(\frac{59}{125}\right)_J \stackrel{9.3.7}{=}$	
---	--

$\left(\frac{125}{59}\right) \stackrel{Red.}{=} \left(\frac{7}{59}\right) \stackrel{9.3.7}{=} - \left(\frac{59}{7}\right) \stackrel{Red.}{=} - \left(\frac{3}{7}\right) \stackrel{9.3.7}{=} \left(\frac{7}{3}\right) =$	(9.180)
$= \left(\frac{1}{3}\right) = 1 \dots$	(9.180)

وینا نه شته

۴ - مگر (تل کیری): $m = 125 = 5^3$ ، یعنی $p_1 = 5$ ، وشمیره:

$\left(\frac{59}{5}\right)_L = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$	(9.182)
---	---------

۵ - $59 \stackrel{9.1.5}{\Rightarrow}$ مربع باقي $\text{mod } 125$ دي.

۶ - ایا $x^2 \equiv 15(67)$ اوبیور یا حلور دی؟ (دا په دی معنا، چي $a = 15$ خلوری - یا مربع پاتي $\text{mod } 67$ دی؟)

$$\left(\frac{15}{67}\right) \stackrel{9.3.7}{=} \left(\frac{67}{15}\right) (-1) \stackrel{Red.}{=} (-1) \left(\frac{7}{15}\right) \stackrel{9.3.7}{=} (-1) \left(\frac{15}{7}\right) (-1) \stackrel{Red.}{=} \left(\frac{1}{7}\right) = 1.$$

مگر دا چي $\left(\frac{15}{67}\right)$ یو لیجنر - سومبول دی، لاس ته رځي: 15 مربع باقي $\text{mod } 67$ دی.

۷ - ایا $x^2 \equiv 67(77)$ اوبیور دی؟

$77 \notin \mathbb{P} \Rightarrow$ لاس ته راځي جاکوبي $77 \notin \mathbb{P} \Rightarrow$ نسبي لومړنی، ناجوره،

$\left(\frac{67}{77}\right) \stackrel{9.3.7}{=} \left(\frac{77}{67}\right) (-1)^{\text{gerade}} = \left(\frac{77}{67}\right) \stackrel{\text{Red.}}{=} \left(\frac{10}{67}\right).$	(9.184)
---	---------

۸ - جوړه دی، $\notin \mathbb{P} \Rightarrow$

نه [9.2.13](#) او نه [9.3.7](#) استعمال وړ د کارونې وړ دی! له دې لاس ته راځي:

په لومړنيو گنونو ټوټه کونه:

$\left(\frac{10}{67}\right)_L = \left(\frac{2}{67}\right) \left(\frac{5}{67}\right) = (-1)(-1) = 1 \dots$	(9.185)
وینا نه ده!	
$67 \not\equiv \pm 1(8); \quad \left(\frac{2}{67}\right)_L \stackrel{9.2.12}{=} -1,$ <p style="text-align: center;">ځکه چې</p>	(9.186)
$\left(\frac{5}{67}\right)_L \stackrel{9.2.13}{=} \left(\frac{67}{5}\right) \stackrel{\text{Red.}}{=} \left(\frac{2}{5}\right) \stackrel{9.2.12}{=} -1,$ <p style="text-align: center;">ځکه چې</p>	(9.187)
$5 \not\equiv \pm 1(8).$	

۹ - مگر د پیژند له مخې:

$\left(\frac{67}{77}\right) = \left(\frac{67}{7}\right) \left(\frac{67}{11}\right) = \left(\frac{4}{7}\right) \left(\frac{1}{11}\right) = 1 \cdot 1.$	(9.188)
---	---------

۱۰ - دا چې دواړه (!) لیجنډر - سومبولونه برابر 1 دي، لاس ته راځي، چې 67 مربع باقي mod 77 دی.

د ډاکټر ماخان شینواري چاپ شوي لیکنې:

1988 Vienna (Austria):

لومړۍ:

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 پښتوتول 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 بنوونکو او زده کوونکو لپاره (دا کتاب په ۹۰۰ مخونو کې چاپ
او دا نوې لیکنه به یې ځنو ځایونو غزېدلې او ځنې ځایونه ترې لرې شوي دي)

2003 Bonn (Germany):

څلورم: ځمکچپوهنه (هندسه) ، په سلو، زرو کې شمیرنه، د گټې – او کټې د کټې
شمیرنه ، د احتمالي شمیرنه کتاب د بنوونځي ټولې اړتیاوې پوره کوي

2003 Bonn (Germany):

پنځم: الجبرونه (د الجبر بنسټونه دي)

2003 Bonn (Germany):

شپږم: د شمیرپوهنې انګرېزي - پښتو ډکشنري.

2003 Bonn (Germany):

اووم: د شمیرپوهنې الماني - پښتو - او پښتو الماني ډکشنري

Mathematical dictionary German/ Pashto and Pashto/German

2003 Bonn (Germany):

اتم: دفرنځيال برابرېون (دا کتاب په دې څانګه کې يو پيل دی، ساده ليکل 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

آبادولو ټولنه،، له خوا درې ساسي مجلې هم را وستلې.

د ډاکتر ماخان ،،میري،، شینواري لیکنې او ژباړې چې په چاپیدو یې پیل کیږي

2012 Bonn; Germany; Kabul Afghanistan

ژباړې:

: Prof. Brinkmann. (From Brinkmann.du.de)

لاندې د برينګمن ليکنې چې له برينګمن ن ج څخه ژباړل شوي دي.

- ۱ - شميرپوهنه د بنوونځي لپاره لومړی ټوک
- ۲ - شميرپوهنه د بنوونځي لپاره دويم ټوک
- ۳ - شميرپوهنه د بنوونځي لپاره دريم ټوک
- ۴ - د احتمالوالي شميرنه د بنوونځي لپاره
- ۵ - احصايه يا ستاتيستيک د بنوونځي لپاره

لاندې کتابونه د شتوتګارت د پوهنتون د استادانو د لکچرونو څخه چې د شتوتګارت پوهنتون ن ج څخه خپاره شوي را ژباړل شوي.

۶ - اناليزی ۱

۷ - اناليزي ۲

۸ - کرښيز الجبر

۹ - د شميرپوهني بنسټونه

۱۰ - د فرمولونو ټولګه

۱۱ - فنکشنل اناليز

۱۲ - وکتور شميرنه

نوري ژباړې

۱۳ - له www.grundstudium.info/linearealgebra څخه: کرښيز الجبر

۱۴ - Georg Gutenbrunner ګڼونپوهنه يا د اعدادو تيوري

زما ليکنې

Bonn (Germany):

۱۵ - د شميرپوهنې ستر کتاب دويم چاپ د پوره تغيراتو سره : دا کتاب د شميرپوهنې برخې برسیره د

انجنري، فزيک او اقتصاد لپاره ، همداسې د بنوونکو او زدهکوونکو لپاره پوره گټور دی. په کتاب کې د اړتيا سره زياتونه او کونه راغلي

۱۶ - ځمکچپوهنه (هندسه) دويم چاپ د پوره تغيراتو سره

۱۷ - الجبر بنسټونه دويم چاپ له تغيراتو سره

۱۸ - ډېری پوهنه يا ست تيوري

۱۹ - د شميرپوهنې سم اند (منطق رياضي)

۲۰ - د يو څو شميرپوهانو ژوندليک

۲۱ - د شمير پوهنې گډې وډې ليکنې

۲۲ - داهم ژباړه ده، خو ليکونکی يې متأسفانه راڅخه نابلد شوی: د مشتق او انتيگرال شميرنو ته تمرينونه او اوبيوني يا حلونه يې

۲۳ - د شميرپوهنې انگرېزي پښتو او عربي + دري ډکشنري

۲۴ - د شميرپوهنې پښتو انگرېزي ډکشنري

۲۵ - د شميرپوهنې پښتو ډکشنري د شميرپوهنيزو ويونو په پښتو روښانه ونه

۲۶ - د زره له کومې (دا هغه ليکنې دي، چې ځنې يې په نړيول جالونو کې خپرې شوي دي.)

۲۷ - د افغانستان په هکله سپينې خبرې، چې وبه غزيرې.

ګڼونپوهنه

نوري ليکنې، چې په ژباړه يې پيل شوی، خو لا پوره نه دي

– د شتوتګارت پوهنتون لکچرنوتونو څخه ، چې د شتوتګارت پوهنتون ن ج څخه خپريري:

د ګروپونو تيوري

- د بنوونځي لپاره فزيک د برينګمن ليکنه

له پنځم ټولګي څخه تر اووم ټولګي پورې ژباړل شوی (دا چې زما دويم مسلک فزيک دی، دا ليکنې ژباړم. دا هم د دې ليکوال يوه ډېره ښه ليکنه ده، چې د شميرپوهنې په څير- دلته هم زيات تمرينونه د حل يا اوبيوني سره په کې راغلي او ماته زيات ګټور برېښي)

د ليکوال ژوند ته لنډه کتنه



د ۱۹۶۶ تر سپټمبر د کابل طب پوهنځۍ له ۱۹۶۶ سپټمبر څخه د اتریش برس، چې هلته یې د شمیرپوهنې ډاکټري په پوره ستونځو تر لاسه کړه.

د ۱۹۸۷ ش ک تر ۱۹۸۸ د فبروري تر پای د دباندنيو چارو وزارت کي مامور.

د ۱۹۸۸ مارچ څخه تر ۱۹۹۲ جون پورې په بن کي د افغانستان جمهوریت سفارت شارژد افیر (صفر نه وو).

له هغې وروسته په جرمني کي سیاسي پناه. له ۲۰۰۸ مارچ څخه د ۲۰۰۹ دسمبر پورې د د ریاضي څانگه کي د پوهنې وزارت درسي نساب کي دنده.

ماخان ميړي په ۱۹۷۲ کي له لري د ميرمن ښاپيري سره واده شوی، چې د واده خبر ورته اتریش ته راغی.

ده د ميرمن ښاپيري سره په ۱۹۶۳ ز ک کي کوزده کړې وه.

دوي ته لوي څښتن په اتریش وينا کي د مای په شلم ۱۹۷۹ ز ک دوه بچيان وبخښل، چې څانگه او اباسين نوميري. څانگه په المان کي د پوهنتون علمي همکاره وه او د حقوقو ډاکټره ده او اباسين ملي اقتصاد او ټولنيزه ساپکولوژي لوستلي.

Thank you for reading

Find more e-books and articles on Ketabton - your multilingual digital library.

www.ketabton.com

Ketabton - Pashto, Farsi, Arabic & English