

گروه ضمی اعداد به صورت (Z_n^*)

پارسا تسبیحی، دانشکده ریاضی - دانشگاه هرمن

- در این قسم به بررسی ساختار و خواص گروه Z_n^* به ویژه در حالتی که این گروه

دوستی است چیزی را داریم. در ادامه مسائل مربوط و خودبرهایی از گروه Z_n^* را اصلاح

چیزی نیم و تأثیر این گروه در ریاضیات را تحلیل چیزی نیم.

تعريف ۱: اگر n عددی طبیعی باشد آنهاه را \mathbb{Z}_n^* را چنین تعریف می‌نماییم:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n^+ \mid \gcd(a, n) = 1\}$$

و معلم روی \mathbb{Z}_n^* ، ضرب اعداد طبیعی به همراه n متراد معده است.

آنکه a در اصل عضویت \mathbb{Z}_n^* را صدق نماید باید $\gcd(a, n) = 1$ باشد.

I) \mathbb{Z}_n^* دارای مطفر حقیقی است.

برهان: $1 \in \mathbb{Z}_n^*$ و $\gcd(1, n) = 1$ بجهت تعریف ضرب روی اعداد طبیعی.

II) \mathbb{Z}_n^* دارای مطفر حقیقی می‌باشد.

برهان: برهان معمولی شود (از حالاباً و فاصله می‌دیم) برآست.

let $a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n^*$

برهان:

اگر $\gcd(a, b, n) = d > 1$ ، در توجه عدد اول p چنین

وجود داشت $d \mid a$ و $d \mid b$ ، مطابق تعریف \gcd می‌توانست

بعد از دست داشت مسلم می‌شوند $a \mid p$ و $b \mid p$ همین می‌دانیم

$a \cdot b \in \mathbb{Z}_n^*$ و $\gcd(a \cdot b, n) > 1$ باقی است. در توجه ممکن باشد

III) عمل. ریت پذیر است.

برهان: از تعریف حزب روی اعداد طبیعی نتیجه می شود، ریت پذیر است.

IV) هر عضو در \mathbb{Z}_n^* دلای وارون می باشد.

برهان: عضو a را به طور دخواه از \mathbb{Z}_n^* اختاب می نماییم، می توان نت $\text{gcd}(a,n)=1$ را ب داشت.

حال صدق نمایم برو اعداد x و y چنان موجود هستند که $ax+ny=1$.

این معادله بهینانه n نیز باید برقرار باشد، درنتیجه

همین ادعایی نمایم x است به n اول است زیرا:

$ax+ny=1 \Rightarrow d(\underbrace{ax+ny}_A) = 1$ ، آنکه $\text{gcd}(x,n)=d$ است:

$$\Rightarrow dA = 1.$$

از آنچه A عددی صحیح است پس ۱ عضوی صحیح از d است، لذا $d=1$ می باشد.

حالت صدق برای $d=1$ است.

$ax \equiv 1 \pmod{n}$ و $\text{gcd}(x,n)=1$ در نتیجه است.

◎ نشان دادم \mathbb{Z}_n^* در اصل مجموعه کروه صادق است، در نتیجه \mathbb{Z}_n^* کروه است.

لما بزد: مرض نیم $a, b \in \mathbb{Z}$ و $n, m \in \mathbb{N}$ باشد هستند

$$an + bm = \gcd(n, m)$$

$S = \{ an + bm \mid a, b \in \mathbb{Z} \wedge an + bm > 0 \}$ برمان: معرفی می نیم

حقیقی اصل خوش ترتیبی می دایم S دایی دوچیزین همچوی باشند، آنرا d می نامیم،

$d = \gcd(n, m)$ که S ناتیج است زیرا دستم $-al - bm$ هست)، اما می نیم

. $d = an + bm$ می نیم

. $d \mid m$, $d \mid n$ ثابت می نیم (I)

($0 \leq r < d$) $n = dq + r$ حقیقی الگوریتم تقسیم می دایم

$$\begin{aligned} r &= n - dq = n - (an + bm)q \\ &= n - anq + bmq = n(1 - aq) + m(bq) \\ \Rightarrow r &= 0 \vee r \in S \end{aligned}$$

نهیین دایم:

او $r \in S$ می نیم $d \mid n$ دلیل $d \mid r$ باشد

. $d \mid m$ ثابت می نیم

II) ثابت کنیم هر قسم ای مسیر m, n نظری صاری d است.

$$d = tua + tvb = t(u_a + v_b) \Rightarrow t | d \Rightarrow t \leq d.$$

هر قسم ای $m = tv, n = tu$ می باشد.

با این ترتیب معلم ثابت کنیم.

قضیه ۱: Z_n^* کروه آکلی است.

برهان: طبق معرفی ضرب روی اعداد طبیعی، ضرب جایه جایی می باشد، درنتیجه
• نیز جایه جایی است.

حال تعداد اعمت کروه Z_n^* را بررسی می کنیم.

تعريف ۲: تابع اویلر (Euler's totient function) را با $\varphi(n)$ نامی دهم و بهین شنل

تعريف می کنیم: (مجموعه اعداد طبیعی را ب N نامی دیم)
 $\varphi: N \rightarrow N$
 $\varphi(n) = |Z_n^*|$

این تابع را تابع اویلر توتین از آن جهت / دخشن بر اویلر در ۱۷۶۳ آزا معرفی کرد

و آزا با π نامی می داد. اما صرف ایندی کن وسط لاؤس در ۱۸۰۱ معرفی شد.

لازم به ذراست تابع φ دخشن بر برای بیان تعداد اعداد طبیعی که هم از آن

اول هستند معرفی شد.

قضیه 2: ارید برای محاسبه $\varphi(n)$ فرمول زیر را ارائه کرد.

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

برهان: مرض نیم

$A_i = \{k \in N \mid p_i^k | k \wedge k \leq n\}$ ، قاردمیم بازی هر $i \leq r$

$$\varphi(n) = n - |\bigcup_{i=1}^r A_i|$$

حق اصل سُعْل و عالم سُعْل داریم:

$$= n - \sum |A_i| + \sum |A_i \cap A_j| + \dots + (-1)^r |\bigcap_{i=1}^r A_i|.$$

از آنکه $|A_i| = \frac{n}{p_i}$ ، همین بازی هر $i \neq j$ مصادب p_i هستند،

$|A_i \cap A_j| = \frac{n}{p_i p_j}$ ، به همین ترتیب

$$|\bigcap_{k=1}^m A_{i_k}| = \frac{n}{\prod_{k=1}^m p_{i_k}} \quad \text{پس از } i_1 < \dots < i_m \text{ برای هر}$$

$$\Rightarrow \varphi(n) = n - \sum \frac{n}{p_i} + \sum \frac{n}{p_i p_j} + \dots + (-1)^r \frac{n}{p_1 p_2 \dots p_r}$$

$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \blacksquare$$

شاید: شاید زیر بسادی از قضیه 2 بدست چیزی

$$1) \varphi(n \cdot m) = \varphi(n)\varphi(m) \cdot \frac{\gcd(n, m)}{\varphi(\gcd(n, m))}$$

$$2) \varphi(p^k) = p^{k-1}(p-1).$$

- در قسمی ۱ سهان دادم Z_n^* آبی است، اما برای تاکت هر Z_n^* باید بدایم

که Z_n^* دوری است؟

شیش از بررسی دوری بودن Z_n^* خوب است به صوری معادل در نظریه اعداد پردازم

تعريف 3: اگر n عددی طبیعی باشیم کم از n اعداد $\{1, 2, \dots, n-1\}$ توسط رابطه R_n

به این شکل تعریف می شود: $a R_n b$ iff $a^n \equiv b$ به تعدادی لاس هم ارزی

اعزاز می شوند.

تعريف 4: اگر n عددی طبیعی باشیم و را یک ریشه اولیه (primitive root) برای n دویم

که $x \in R_n$ و $[x]_{R_n} \neq [0]_{R_n}$ و برای هر $k \in N$ $[x^k]_{R_n} \neq [0]_{R_n}$ عدد طبیعی k هر چاهه

چنان موجور باشند $x = g^k$. این صنوم تعریف اولیه صفر و مطابق

("Arithmetical Investigations" در تاب 1801 ("Disquisitiones Arithmeticae" لاتینی، آنلاینسی)

به طور لسترد بآن در راه است.

تعريف 5: می دایم که روده های دوری مرتبه n بُلِیت هستند.

روده دوری مرتبه n را در حالت C_n با C_n نامی دهم و علَّ آن است.

تعريف 6: روده چهارتایی لاین را با K_4 نامی می دیم.

قضیه 3: برای هر عدد n طبیعی C_n بازی هر زیر رود

d عضوی دارد، همین زیر رود دلیلی ندارد.

برهان: ابتدا ثابت می کنیم اگر $H \leq C_n$ آنها

برهان: حتم صحت قضیه لاراژ می باشد.

حال ثابت می کنیم برای هر زیر رود d عضوی داریم.

می دایم $\langle g^{\frac{n}{d}} \rangle = d$, $\langle g^{\frac{n}{d}} \rangle \leq C_n$ آنها $C_n = \langle g \rangle$

حال ثابت می کنیم $\langle g^{\frac{n}{d}} \rangle$ نهایی رود d عضوی است.

فرض کنیم $\langle g^{\alpha} \rangle$ زیر رود d عضوی باشو. صدق الورت قسم می توان فت

$$\begin{aligned} (g^{\alpha})^d &= (g^{q^{\frac{n}{d}} + r})^d = (g^{q^{\frac{n}{d}}} * g^r)^d = g^{qn} * g^{rd} = e \\ \overline{g^{qn} = e} &\Rightarrow e * g^{rd} = e \xrightarrow{rd \leq n} rd = 0 \xrightarrow{d \neq 0} r = 0 \Rightarrow g^{\alpha} = (g^{\frac{n}{d}})^q \Rightarrow g^{\alpha} \in \langle g^{\frac{n}{d}} \rangle \\ &\text{بنهادن} \Rightarrow \langle g^{\alpha} \rangle = \langle g^{\frac{n}{d}} \rangle. \end{aligned}$$

s.a.m

قضیه ۴: اگر فضای \mathbb{C} را رو به باس و $H \leqslant \mathbb{C}_n$ موجود باشی طوی داشته باشیم، آنها \mathbb{C} دوری نیست. (با صفاتی باشند)

برهان: فضای \mathbb{C} را رو به باس، $\mathbb{C} \cong \mathbb{C}_n$ ، صدق قضیه ۳، \mathbb{C} تنها یک زیرگروه از مرتبه 2 می باشد.

$a^2 = b^2 = c^2 = e$, $H \cong \mathbb{K}_4$, $H = \{e, a, b, c\} \leqslant \mathbb{C}$ درستی، اما از آنکه \mathbb{C} دارای باس است،

پس \mathbb{C} دستم 3 زیرگروه $\langle a \rangle, \langle b \rangle, \langle c \rangle$ را از مرتبه 2 دارد، لذا فضای \mathbb{C} خلف باظل است و \mathbb{C} دوری نیست.

تعريف ۷: اگر \mathbb{C} را رو به فضای \mathbb{C} تابع Ψ را چنین تعریف کنیم،

$$\Psi(m) = |\{x \in \mathbb{C} \mid \text{ord}(x) = m\}|$$

$$\sum_{d|n} \Psi(d) = n \quad : \text{قضیه ۵}$$

برهان: \mathbb{C}_n را در نظر بگیریم هر عضو c_n مرتبه صحیحی دارد که صدق قضیه لاگرانژ را می نماید.

در نتیجه در حاصل جمع فضای \mathbb{C}_n دقیقاً یکبار سواری سود و تعداد اعضاء است پس

حاصل جمع فوق با n برابر است.

قضیه 6: $C_n = \langle g^n \rangle$ سازنده دارد.

برهان: ابتدا ثابت می‌کنیم تعداد سازنده‌های C_n لست $\{g^k\}$ مساوی است.

$$(t > 0) \cdot m \mid t \quad \text{که } x^t = e, \text{ ord}(x) = m \text{ از } H \text{ در رو رده.}$$

$$\begin{aligned} x^t &= x^{mq+r} = x^{mq} * x^r, (r < m) \quad t = mq + r \\ &= (x^m)^q * x^r = e * x^r = x^r = e \\ \xrightarrow{r < m} \quad r &= 0 \implies t = mq \xrightarrow{t > 0} m \mid t. \end{aligned}$$

- فرض نیم سازنده برای C_n باشد در نتیجه $g^k \in C_n$ (که $k < n$)

$$\begin{aligned} (g^k)^{\frac{n}{d}} &= (g^{\frac{k}{d}})^n = (g^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e, \text{ حال می‌توان نوشت:} \\ \Rightarrow \text{ord}(g^k) &\leq \frac{n}{d} \Rightarrow n \leq \frac{n}{d} \Rightarrow d = 1. \end{aligned}$$

پس توان هر سازنده C_n بست به n اول است.

حال ثابت می‌کنیم اگر $\text{gcd}(k, n) = 1$ آنها g^k

- فرض نیم سازنده C_n باشد، $n \mid km$ ثابت شود، $g^k = e$ در نتیجه $\text{ord}(g^k) = m$ از آنها

هر طرفی مرتبه هر عضو در رو رده لست $\{g^k\}$ مساوی است.

$C_n = \langle g^k \rangle$ است یعنی $\text{ord}(g^k) = m = n$ در نتیجه $m \leq n$ پس $n \mid m$ و $\text{gcd}(k, n) = 1$

به این روش حکم ثابت شد.

$$\sum_{d|n} \Psi(d) = n \quad \text{طبقه 7}$$

برهان: C_n را در نظر بگیریم، هر عضو آن صفر و زیرگرهی صفر $\langle x \rangle$ تولید می‌نماید.

طبقه قسمی لادران (یا قسمه 3) می‌دانیم $t = |\langle x \rangle|/n$ ، همین برای هر عضو جزء x

$H \notin C_n$ ، طبقه قسمه 3 $\langle y \rangle = \langle x \rangle$ ، از این بعد زیرگرهی $\langle y \rangle | t$

می‌نایم و می‌دانیم H بیانات، طبقه قسمه 6 $\Psi(t)$ بازنشده دارد،

از آنکه بارای هر d برای $\text{ord}(x)|n$ ، $x \in C_n$ دارد

پس هر عضو در حاصل جمع بالا در حقیقت ۱ میلیار تا شصت سرمه را همچنین ۸ عضور عجود دارد،

$$\sum_{d|n} \Psi(d) = n \quad \text{نحو 5}$$

$$\sum_{d|n} \Psi(d) = \sum_{d|n} \Psi(d) \quad \text{شبه 1: از قسمه 5 و 7 شبه می‌بینیم}$$

عَصَمَ Z_n^* مَاهِيَّةٌ $n = 2^k$, $k > 2$, $k \in N$: 8 دری بیت.

برهان: کوہا \mathcal{L} را چنین تعریف میں دیں
 $\mathcal{L} = \{1, (-1 \equiv 2^{k-1}), 2^{k-1}-1, 2^{k-1}+1\}$

$\mathcal{L} \cong k_4$ ، حال سُنان میں دهم
 وسیع است

$$(2^{k-1}-1)^2 \stackrel{n}{=} 2^{2k} - 2 \cdot 2^k + 1 \stackrel{n}{=} 0 - 0 + 1 = 1$$

$$(2^{k-1}-1)^2 = 2^{2k-2} - 2^k + 1 \stackrel{n}{=} 2^k \cdot 2^{k-2} - 2^k + 1 \stackrel{n}{=} 0 - 0 + 1 = 1$$

$$(2^{k-1}+1)^2 = 2^{2k-2} + 2^k + 1 \stackrel{n}{=} 2^k \cdot 2^{k-2} + 2^k + 1 = 0 + 0 + 1.$$

حال طبق عَصَمَ 4 می قلن تبیہ درست Z_n^* دری بیت.

قضیه 6: در \mathbb{Z}_p^* به ازای هر دایم $\Psi(d) = \Psi(d)$

برهان: اگر هجع $a \in \mathbb{Z}_p^*$ صورت باشد که $\text{ord}(a) = d$ پس

حال فرض می کیم $\text{ord}(a) = d$. از اینجا مطابله قضیه 10

نمایش $a^d \equiv 1$ دارد، هم اکنون دنباله $D: a, a^2, \dots, a^d$ مصادارت داشت

(خاصیت زیرده دوری) لذا تمامی جواب های مطابله T

در میان دنباله D هستند، در تبیه هر معنی $\text{ord}(b) = d$ پس دو آن تبیه رفته

$b \in D$

از تعریف دنباله D روش است داشتن اعضا $\langle a \rangle$ هستند و لذا d

همیشی هر عضوی دارند $\text{ord}(b) = d$ پس $b \in \mathbb{Z}_p^*$ است، با توجه به

قضیه 6 می توان نت $\Psi(d), \langle a \rangle$ لازمه دارد: در تبیه در \mathbb{Z}_p^* معنی از

از مرتبه d موجود است، پس $\Psi(d) = \Psi(d)$

تبیه 2: از تبیه 1 و قضیه 6 می توان تبیه رفت در \mathbb{Z}_p^* $\Psi(\mathbb{Z}_p^*) = \Psi(d)$

پس $\Psi(\mathbb{Z}_p^*) \neq 0$ دارای طغیتی می باشد و از مرتبه 1 \mathbb{Z}_p^* است

پس $\mathbb{Z}_p^* = \langle g \rangle$ در تبیه \mathbb{Z}_p^* درست است.

قضیه 10: مرضن کیم $f(x)$ یک چندجمله ای از مرتبه n به بیناند \mathcal{P} باشد (ک اول است)

آنفاه $f(x)$ در میان مجموعه $A = \{1, 2, \dots, p-1\}$ دارد.

برهان: حلم را ب استقراء روی n ثابت می کنیم.

$$f(x) = a_0 + a_1 x + \dots + a_n x^n, n=0, \text{ آنفاه}$$

فرض کیم حلم بدای همه مقادیر x از n برقرار است.

فرض کیم $f(x)$ دست کم n ریشه داشته باشد و x_1, x_2, \dots, x_n ریشه های آن

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \quad \text{باشد. مکاری از فرض کیم}$$

$$g(x) = f(x) - a_n(x-x_1)(x-x_2)\dots(x-x_n) \quad \text{مکاری دهم}$$

روشن است که درجه $g(x)$ و العدا لفتر از n است، در حالی که به ازای هر x_i

$g(x) \equiv 0$ یعنی $(x-x_1)(x-x_2)\dots(x-x_n) \equiv 0$ و $f(x) \equiv 0$ نیز است

$f(x) \equiv a_n(x-x_1)(x-x_n)$ داریم: پس $f(x)$ یک چندجمله ای ثابت \mathcal{P} است

در نتیجه از اینکه $f(x) \equiv 0$ اول است $f(x) \equiv 0$ از و فقط از دست کم یک پرائیز از است

راست \mathcal{P} سود یعنی $f(x) \equiv 0$ لذا هر ریشه x_i به بیناند \mathcal{P} می از

است، پس $f(x)$ به بیناند \mathcal{P} دارد، پس حمل ثابت \mathcal{P} است

- برهان ارائه شده در قضیه ۹، اینجا وجودی برای دوری بعدن \mathbb{Z}_p^* است.

اما در قضیه ۱۱ اینجا ساختی برای دوری بعدن \mathbb{Z}_p^* ارائه نیم که مسلم
در دست راسن بجزیه $|Z_p^*| = \varphi(p) = p-1 = \prod q_i^{\alpha_i}$ به عوامل اول است.

قضیه ۱۱: فرض نیم /
 $|Z_p^*| = \varphi(p) = p-1 = \prod q_i^{\alpha_i}$ (جزیه ها اول هستند)
 Z_p^* دوری است.

برهان: قضیه را در دو قسمت ثابت می نیم.

$\text{ord}(q_i) = q_i^{\alpha_i}$ /
(I) به ازای هر q_i ، $q_i^{\alpha_i}$ صفات عضو \mathbb{Z}_p^* موجود است و

(II) مرتبه محاصل حرب همه q_i ها $|Z_p^*| = p-1$ باشند.

قضیه ۱۰: $x^{\frac{p-1}{q_i}} \equiv 1$ در معادله ۱ و در عباره $g \in \mathbb{Z}_p^*$ /
I. فرض نیم

$h^{q_i^{\alpha_i}} \equiv g^{\frac{p-1}{q_i}}$ در نتیجه $h \equiv g^{\frac{p-1}{q_i^{\alpha_i}}}$ و موجود است، مرار می دهیم

$h^{q_i^{\alpha_i-t}} \equiv g^{\frac{p-1}{q_i^t}}$ (تکرار) زیرا $h^{q_i^{\alpha_i-t}} \not\equiv 1$ اما، $g^{\frac{p-1}{q_i^t}} \equiv 1$ نمی داشته باشد

$g^{\frac{p-1}{q_i^t}} \equiv 1$ و اگر $g^{\frac{p-1}{q_i^t}} \equiv 1$ آنهاه $g^{\frac{p-1}{q_i^t}} \equiv 1$

اذا هست است نز باید با 1 همیست سود که فرض کردیم نز سود پس $q_i^{\alpha_i} \equiv 1 \pmod{p-1}$

در نتیجه q_i را قارچی دهیم و

II. فرض کنیم $t \mid p-1$ ، می دایم $t < p-1$ ، $\text{ord}(Q_1 \cdot Q_2 \cdots \cdot Q_r) = t$

پس $\frac{P-1}{t}$ عددی صحیح و بزرگتر از 1 است، می توان نفت q_i موجود است

$Q = \prod Q_i$ پس $t \mid \frac{P-1}{q_i}$ در نتیجه $q_i \mid \frac{P-1}{t}$ به طوری که

به قوانین $\frac{P-1}{q_i} \equiv 1 \pmod{p-1}$ برابر 1 است، در نتیجه

زیرا بازای هر $i \neq j$ ، $q_i^{\alpha_j} \mid \frac{P-1}{q_i}$

در نتیجه $q_i^{\alpha_{i+1}} \mid \frac{P-1}{q_i}$ پس $\text{ord}(Q_i) = q_i^{\alpha_i} \mid \frac{P-1}{q_i}$ شنا

که با فرض اینه 1- است $q_i^{\alpha_i} \mid p-1$ در صناعهن است، پس $q_i^{\alpha_i} \in \mathbb{Z}_p^*$ دری است.

قضیه 12: اگر n عدی مرتبه باشد Z_n^* ریشه اولیه دارد اگر و تنها اگر Z_{2n}^* ریشه اولیه داشته باشد.

برهان: مرضی نیم و عدی مرتبه باشد، در نتیجه برای هر $k \in \mathbb{N}$ $g^k \equiv 1$ همواره برقرار

است، لذا صدق قضیه باقی مانند چنین $1 \equiv g^{2n}$ و اگر و تنها اگر $1 \equiv g^n$

در نتیجه و ریشه اولیه Z_n^* است اگر و تنها اگر و ریشه اولیه Z_{2n}^* باشد.

حال توجه می‌کنیم که هر ریشه اولیه Z_{2n}^* حتماً خواست اما صدق است که ریشه اولیه

$[h+n]_{R_n} = [h]_{R_n}$ باشد و h نیز باشد، اما $h+n$ لزماً نباشد و از آنجا که Z_n^*

سپس $h+n$ نیز ریشه اولیه Z_n^* می‌باشد.

قضیه 13: فرض کنیم و رسم اولیه Z_p^* باشد، $p > 2$) $g^{p-1} \not\equiv 1$ و $g^{p^2} \not\equiv 1$ اول است

$$\forall k \geq 1: g^{\varphi(p^k)p^{k+1}} \not\equiv 1$$

برهان: حمل را به اسفار روی k تابت می‌کنیم.

باشه: $k=1$ ، در فرض صدق فته شد.

فرض کنیم حمل برای k برقرار است ، برای $k+1$ هنوز تابت می‌کنیم:

$$g^{\varphi(p^k)p^k} \equiv 1 \Rightarrow g^{\varphi(p^k)} = 1 + mp^k \quad (p \nmid m) \quad - \text{طبق قضیه اولیه:}$$

$$\varphi(p^{k+1}) = \varphi(p^k) \cdot p \quad \text{از} \quad \varphi(m, n) = \varphi(m)\varphi(n) \frac{\gcd(m, n)}{\varphi(\gcd(m, n))} \quad - \text{مح دایم}$$

$$\Rightarrow g^{\varphi(p^{k+1})} = g^{\varphi(p^k) \cdot p} = (1 + mp^k)^p \stackrel{p}{\equiv} 1 + mp^{k+1}$$

و، به این ترتیب حمل تابت می‌شود.

قضیه 14: عرض نیم و ریشه اولیه در $\mathbb{Z}_{p^k}^*$ باشد آنگاه $(g+p)$ دارای است.

برهان: ابتدا عرض نیم $g^{p-1} \not\equiv 1$ باشد می توانیم $\text{ord}(g)_{\mathbb{Z}_{p^k}^*} = \varphi(p^k) = p^{k-1} \cdot (p-1)$

با استعاضه کردیم:

پایه: برای $k=1$ برقرار است.

عرض نیم برای عواید فریبا صادری K برقرار است برای $K+1$ هم ثابت می شود.

فرض نیم $g^m \equiv 1$ در نتیجه $g^{m \cdot p} \equiv 1$ در نتیجه $\text{ord}(g)_{\mathbb{Z}_{p^{K+1}}^*} = m$

طبق قضیه اسکرین $\varphi(p^k) = p^{k-1}(p-1) | m$ و $\text{ord}(g)_{\mathbb{Z}_p^*} = \varphi(p^k)$

قضیه نظر از $m | \varphi(p^{k+1}) = p^k(p-1)$ از آنجا که p اول است

اما طبق قضیه 13 $m = p^k(p-1) = \varphi(p^{k+1})$ و $m \neq p^{k-1}(p-1)$ هر لذا $\text{ord}(g)_{\mathbb{Z}_{p^{k+1}}^*} \neq \varphi(p^k)$

و ریشه اولیه $\mathbb{Z}_{p^{k+1}}^*$ است و حمل ثابت شد.

$[g]_{R_p} = [g+p]_{R_p}$ بجای g و $g+p$ را در صورت نیم، از آنجا که $g^{p-1} \equiv 1$ داشتیم

و $g+p$ نیز نیز ریشه اولیه برای \mathbb{Z}_p^* است.

اراده قضیه 14: همین با استفاده از قضیه دوچله ای

$$(g+p)^{p-1} p^2 \equiv g^{p-1} + g^{p-2} p(p-1)$$

$$\equiv 1 - g^{p-2} p$$

از آنکه $(g+p)^{p-1} p^2 \equiv 1 - g^{p-2} p \neq 1$ و اراده حل یسان باشد

$$p-1 \neq 1$$

نتیجه 3: از نتیجه 2، قضیه 14 و قضیه 12 نتیجه می‌شود که n به علی از صورت

های زیر باشد، Z_n^* دری است. (که $p > 2$ ، اول، $p \neq 2$)

قضیه 15: اگر Z_n^* دری باشد، $n = p^k$

برهان: فرض کنیم $n = mp^k$ باشد. شان می‌شود که $m > 3$.

$\varphi(p^k), \varphi(m), \varphi(n) = \varphi(m)\varphi(p^k)$ می‌شوند. فرض کنیم Z_n^* دری است.

هر دو زوج هستند، برای هر $a \in Z_n^*$ داشته باشند $a^n \equiv 1$

$$a^{\frac{\varphi(n)}{2}} \equiv (a^{\varphi(m)})^{\frac{\varphi(p^k)}{2}} \equiv 1$$

$$a^{\frac{\varphi(n)}{2} p^k} \equiv (a^{\varphi(p^k)})^{\frac{\varphi(m)}{2}} \equiv 1$$

(قضیه اولیه)

و در نتیجه $\varphi(n) \mid \text{ord}(a) < \varphi(n)$ می‌شود که $a^{\frac{\varphi(n)}{2}} \equiv 1$ باشد.

رسون است دارای دویی هسته همین باد روش

معنی 15 و شعبه 3 درم:

عنه ریشه اولیه دویی دارای Z_n^* است (primitive root theorem)

$$n \in \{1, 2, 4, p^k, 2p^k \mid k \geq 1, p \text{ prime}\}$$

حال ن تاحدی با ساختار Z_n^* آسانیم به کاربردها و عوامل مربوط به آن می پردازیم.

مسئلہ: میں دایم $p^k Z$ دوری است، روئی ازانہ لیند براہی محاسبہ یعنی از سازنہ های Z_n^* .

- تاب امروز یعنی روش طاری اعوی (الگوریتم با پیچیدگی چند جملہ ای) براہی حل این مسئلہ
یافت شدہ و این مسئلہ در تاریخ مسئلہ لایام لستہ کہ به آن حواہم پرداخت و مسئلہ جزئیه

اعواد صحیح در دستہ ای از عوامل بنام NP-Intermediate تواریح لیرند.

با این حال با توجه به برهان قضیہ ۱۱ میں قوان الگوریتم چند جملہ ای ازانہ کردہ مسئلہ

دانش جزئیہ $p-1$ میں باسہدہ

اھمیت این الگوریتم از آنها است کہ ثابت میں نہ مسئلہ یا چن سازنہ از نظر

پیچیدگی محاسباتی حد اکثر بہ اندازہ جزئیه اعواد سنت است.

الگوریتم ۱: برای محاسبه یک سازنده برای Z_p^* .

for $i \leftarrow 1$ to r :

while $\beta \neq 1$:

choose $\alpha \in Z_p^*$ at random

$$\beta \leftarrow \alpha^{(p-1)/q_i}$$

$$\gamma_i = \alpha^{(p-1)/q_i \cdot \alpha_i}$$

$$\gamma \leftarrow \gamma \gamma_i$$

output γ

- درستی این الگوریتم از برهان قضیه ۱۱ به ساده‌ی ترین شکر است.

و اسیدریاضی پیچیدگی زمانی آن $O(r(\log p)^3)$ است، به برشب اندازه ورودی

چیز جمله‌ای است، اما در این متن از خلیل آن صرف نظر نمی‌شیم.

حال نشان می‌دهیم که توان الگوریتم احتمالاتی برای یافتن سازنده با اسیدریاضی ثابت یافت.

قضیه ۱۶: برای هر $3 < n$ داریم:

نلا ثابت او بیر-حاسکروی می‌باشد.

قضیه ۱۷: از آنچه $\frac{n}{m} < \Psi(n)$ ، $m \in \mathbb{R}$ ، $\lim_{n \rightarrow \infty} \log \log n = \infty$

نتیجه برقرار است. لذا هم ران پائی ثابتی برای اعواد سازنده های یک روک م وجود نیست.

مسئله لگاریتم سه‌تایی (Discrete logarithm problem) مسئله لگاریتم سه‌تایی است:

فرض نسخه Z_n^* دری باشد و g کارزنه آن باشد.

روشی از آن نسخه بازی هر $\alpha \in Z_n^*$ ، x را طبق محاسبه لگاریتم $\log_g \alpha$ را محاسبه نماید.

به عبارت دیگر $x = \log_g \alpha$ را محاسبه نماید.

- همان طرد در توصیفات مسدود قبل اشاره شد، برای حل این مسئله الگوریتم

با پیچیدگی چندجمله‌ای درست است، اما الگوریتم‌های زیر-نمایی (Sub-exponential)

برای حل معمول وجود ندارند از قبیل جستجو طالع، مردم بزرگ/عدم بُرچد (Baby step/Giant step)

از آنکه جستجو طالع بسیار ساده و در مقایسه با BS/GS بسیار نظرآفرین است،

در این متن نیز BS/GS را بررسی می‌نماییم.

الgoritم 2 (Baby step / Giant step) برای محاسبه β^{-1} است.

ایده اصلی این الgoritم بهینه سازی الgoritم جستجو طائل با استفاده از تبادل زمان / حافظه است. (Time / space trade-off)

در این الgoritم Z_n^* را که $(n) = O(\Phi(n^{1/2}))$ مفهودار در m بازه، برای تعادل $\frac{\Phi(n)}{m} = O(\Phi(n^{1/2}))$ عضو آن بازه تقسیم می کنیم و سری از یا من بازه مناسب از میان $\frac{\Phi(n)}{m}$ تعیین کنیم.

جواب را پیدا می کنیم. لذا الgoritم از دو بخش اصل شکل شده است:

(I) ساخت بازه ها. (Baby step)

(II) یا من جواب در میان بازه مناسب.

I. برای ساخت بازه ها، از داده ساختار T استفاده می کنیم که درستی به هر یک

از عناصر آن سریع باسر می باشد. ... hash table, Binary search tree

و تعریف می کنیم در ابتدا بازی هر $\beta \in Z_n^*$ (هیچ عضوی مقادیر می شود).

در پایان می خواهیم $T[\beta]$ همان $\beta \log \beta$ باشد.

حال الgoritم زیر را به صورت ساخت بازه ها و مقادیر می اولیه T اجرای نمی

$$\beta \leftarrow 1$$

for $i \leftarrow 0$ to $m-1$:

$$T[\beta] \leftarrow i$$

$$\beta \leftarrow \beta \cdot g$$

- پس از اجرا این الگوریتم بازه $\frac{\varphi(n)}{m}$ تایی ساخته شده / است ابتدا و این آنها مقادره شده.

و پس از اجرا این الگوریتم تابه اینجا $O(m \cdot \log n)$ می باشد.

II. حال برای یافتن $x = \log^\alpha \varphi(n)$ الگوریتم زیر را اجرایی نمایم.

$$\beta \leftarrow \alpha, j \leftarrow 0, i \leftarrow T[\beta]$$

while $i = 1$:

$$\beta \leftarrow \beta \cdot g^{-m}, j \leftarrow j+1, i \leftarrow T[\beta]$$

$$x \leftarrow jm + i$$

output x

- برای ابتدت درست این الگوریتم ضعف نیم $x = g^x$ / $\alpha = \varphi(n)$. حال طبق

ضعیف قسم می داریم $x = am + b$ و a, b بین صفحه های بیرون دهیم

$$0 < a < \frac{\varphi(n)}{m}$$

در زیر این تبار معنی داریم:

لذا صدق تعریف ۱ است اگر و تنها اگر $j = a$ و $i = b$ آنگاه $x = jm + i = am + b$

پس $x = \log^\alpha \varphi(n)$ و الگوریتم صحیح است و درست است / پس این طل الگوریتم همچنین

می باشد بر حسب اندازه و درجه $O(\frac{\varphi(n)}{m} \log n + m \log n)$

s.a.m

از معتبرین طاریه های Z_n^* می توان به پروتکل سادل لیور دیفی - هلمن اشاره کرد،
که سعی آن برای سختی حل مسئله لایریم مستمر می باشد.

(Diffie-Hellman key exchange protocol) پروتکل سادل لیور دیفی - هلمن

فرض نیم سمعی A و نیم B می خواهند نیو احتمالی مسئله کرا داشته باشند اما
امان سادل آن کاروی سبله موجود است. اگر $A, B, \alpha, \beta \in Z_n^*$ باشند

به طبقان نیو همانی روی سبله مسئله سر، اتفاقاً حقیقتی روی نیو کارا به طبقان
لیور احتمالی مسئله سازن.

ابتدا A، عدد α را انتخاب کرده و α^x را به طبقان تابع خود روی سبله مسئله نماید.

سپس B، عدد α را انتخاب کرده و β^y را به طبقان تابع خود روی سبله مسئله نماید.

حال $k_A = \alpha^x$ را دریافت کرده A فرمی عدد β^x را مترادی دهد،

$$k_B = k_A = \beta^x = (g^y)^x = g^{xy} = \alpha^y = k_B$$

نحو الفون

$x = \log_g \alpha, y = \log_g \beta$ / اگر نیم C بجهاد K را بدست آورد باید از α, β, α^y و β^x را محاسبه نماید

/ این طریق دست دم به اندازه صندل لایریم سه سمت است.

پروتول تبادل کلید دیفی- هلمن در بعده روش های رمزگاری مانند رمزگاری الجعل استاده می سود. (ElGamal crypto-system)

در این صن مطلب به خواص و مسائل کوچک پیش از اعداد به همانه π ، در حالی که این کوچک دوری است پرداخته ایم، در حالی که در حالت های غیر دوری بین این کوچک دارای خواص و خواص دیگر های سیاری می باشد؛ از جمله رمزگاری RSA (RSA crypto-system) RSA

از کوچک Z_{pq}^* استاده می شود.

منابع:

- Disquisitiones Arithmeticae (Investigations on Arithmetics)
Carl F. Gauss 1801 (1986, Springer)

- A Computational Introduction to Number Theory and Algebra (Ver. 2)
Victor Shoup (Non-commercial PDF version).

- The Primitive Root Theorem , Amin Witno
[WWW.witno.com/numbers/chap5.pdf](http://www.witno.com/numbers/chap5.pdf)