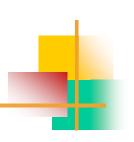


- گروه (Group)
- هر گروه G شامل مجموعهای از عناصر همراه با یک عمل دوتایی \circ است
 - عمل دوتایی •
 - جمع، ضرب و غيره
 - ویژگیها
 - بستار (Closure)
 - $a,b \in G$ برای هر
 - $a \circ b \in G$
 - شرکتپذیری (Associative)
 - $a,b,c \in G$ برای هر
 - $a \circ (b \circ c) = (a \circ b) \circ c$



- عنصر همانی یا خنثی (Identity Element)
- $a \in G$ وجود دارد به طوری که برای هر $e \in G$ عنصری مانند
 - $a \circ e = e \circ a = a$
 - عنصر وارون يا معكوس (Inverse Element)
- برای هر $a \in G$ عنصری مانند $a \in G$ وجود دارد به طوری که lacktriangle
 - $a \circ a^{-1} = a^{-1} \circ a = e \quad \bullet$
- مثال ا
- مجموعه اعداد صحیح $\{n-1\}$, ...,(n-1) و عمل جمع به پیمانه n یک گروه با عنصر همانی n است



- گروه آبلی (Abelian Group)
- $a,b \in G$ گروه (G,\circ) آبلی نامیده میشود اگر برای هر G,\circ
 - $a \circ b = b \circ a$
- با فرض این که Z_n^* مجموعه همه اعداد صحیح مثبتی باشد که از n کوچکتر بوده و نسبت به n اول هستند
 - است n یک گروه آبلی تحت عمل ضرب به پیمانه z_n^*
 - عنصر هماني
 - e=1 •
 - محاسبه معكوس ضربي
 - الگوريتم گسترشيافته اقليدس يا قضيه اويلر



- مثال •
- یک گروه آبلی تحت عمل ضرب به پیمانه 9 است Z_9^*
 - $Z_9^* = \{1,2,4,5,7,8\}$
 - Z_9^* جدول ضرب برای •

× mod 9	1	2	4	5	7	8
1	1	2	4	5 1 2 7 8	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1



- گروه متناهی (Finite Group)
- گروه (G,\circ) متناهی نامیده میشود اگر تعداد عناصرش متناهی باشد \bullet
 - کاردینالیتی یا مرتبه گروه
 - |G|
 - مثال •
 - $(Z_n,+)$ گروه متناهی lacktriangle
 - $|Z_n|=n$
 - $(Z_n^*, imes)$ گروه متناهی lacktriangle
 - $|Z_n^*| = \varphi(n)$
 - $(Z_9^*, imes)$ گروه متناهی \bullet
 - $|Z_9^*| = \varphi(9) = 3^2 3^1 = 6$



- مرتبه عناصر گروه
- است به $a\in G$ مرتبه هر عنصر $a\in G$ برابر با کوچک ترین عدد صحیح مثبت $a^k=a\circ a\circ \cdots \circ a=e$ طوری که
 - ord(a) = k
 - مثال ا
 - Z_{11}^st مرتبه عنصر 3 در گروه آبلی lacktree
 - ord(3) = 5 •

$$3^1 = 3 \equiv 3 \pmod{11}$$

$$3^2 = 9 \equiv 9 \pmod{11}$$

$$3^3 = 27 \equiv 5 \pmod{11}$$

$$3^4 = 81 \equiv 4 \pmod{11}$$

$$3^5 = 243 \equiv 1 \pmod{11}$$



- گروه دوری (Cyclic Group)
- گروه (G,\circ) دوری نامیده می شود اگر شامل حداقل یک عنصر g با حداکثر مرتبه |G| باشد
 - ord(g) = |G| •
 - عنصر g تمام گروه را تولید می کند lacktriangle
 - عناصر با حداکثر مرتبه
 - عناصر اوليه (Primitive Elements)
 - مولدها (Generators)
 - ریشههای اولیه (Primitive Roots)



- مثال م
- Z_{11}^st گروه دوری $lacktree \bullet$
- عنصر اوليه يا مولد
 - 2 •

$$2^1 \equiv 2 \pmod{11}$$
 $2^9 \equiv 6 \pmod{11}$

$$2^2 \equiv 4 \pmod{11}$$
 $2^{10} \equiv 1 \pmod{11}$

$$2^3 \equiv 8 \pmod{11}$$

$$2^4 \equiv 5 \pmod{11}$$

$$2^5 \equiv 10 \pmod{11}$$

$$2^6 \equiv 9 \pmod{11}$$

$$2^7 \equiv 7 \pmod{11}$$

$$2^8 \equiv 3 \pmod{11}$$



- برای هر عدد اول p گروه $(Z_p^*, imes)$ یک گروه دوری متناهی آبلی است
 - با فرض این که (G,\circ) یک گروه دوری متناهی باشد lacktream
- مرتبه هر عنصر $G \in G$ یعنی ord(a) مرتبه گروه یعنی $a \in G$ را میشمارد lacktriangle
 - مثال
 - Z_{11}^st گروه دوری lacktree
 - $|Z_{11}^*| = 10$

$$ord(1) = 1$$
 $ord(5) = 5$ $ord(9) = 5$
 $ord(2) = 10$ $ord(6) = 10$ $ord(10) = 2$
 $ord(3) = 5$ $ord(7) = 10$
 $ord(4) = 5$ $ord(8) = 10$

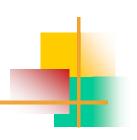


- با فرض این که (G, \circ) یک گروه دوری متناهی باشد lacktriangle
 - تعداد عناصر اولیه G برابر با $\varphi(|G|)$ است
 - مثال •
 - Z_{11}^* گروه دوری lacktree
 - $|Z_{11}^*| = 10$
 - $\varphi(10) = (5-1)(2-1) = 4$
 - عناصر اوليه
 - 2
 - 6
 - 7 •
 - 8

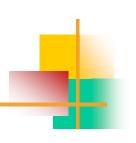


- زيرگروه (Subgroup)
- زیرمجموعهای از گروه (G,\circ) که خودش تحت عمل \circ یک گروه است
 - با فرض این که (G,\circ) یک گروه دوری متناهی باشد lacktriangle
- s هر عنصر $a \in G$ با مرتبه s یک عنصر اولیه از یک زیرگروه دوری با $a \in G$ عنصر است
 - مثال
 - Z_{11}^st گروه دوری lacktree lacktree
 - ord(3) = 5 •
 - $H = \{1,3,4,5,9\}$ زیرگروه دوری
 - عنصر اوليه
 - 3

× mod 11	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4



- قضيه لاگرانژ
- با فرض این که (G, \circ) یک گروه دوری متناهی باشد lacktream
- مرتبه هر زیرگروه $G \subseteq H$ یعنی $H \subseteq G$ مرتبه گروه یعنی G
 - مثال •
 - Z_{11}^st گروه دوری lacktree
 - $|Z_{11}^*| = 10 = 1 \times 2 \times 5$
 - زیرگروههای دوری
 - $H_1 = \{1\} \bullet$
 - $H_2 = \{1,10\}$ •
 - $H_3 = \{1,3,4,5,9\}$ •



- با فرض این که (G,\circ) یک گروه دوری متناهی و g یک عنصر اولیه برای این گروه باشد
- برای هر عدد صحیح k که مرتبه گروه یعنی |G| را میشمارد تنها یک زیرگروه دوری $H\subseteq G$ از مرتبه k وجود دارد
 - زیرگروه دوری H توسط $g^{|G|/k}$ تولید میشود lacktriangledown
 - مثال
 - Z_{11}^st گروه دوری lacktree
 - عنصر اوليه
 - 8
 - عنصر اولیه یا مولد برای زیرگروه دوری از مرتبه 2
 - $8^{10/2} = 8^5 \equiv 10 \pmod{11}$



- تمرين ا
- ثابت کنید عدد صحیح x یک عنصر اولیه برای گروه دوری Z_{97}^* است اگر $x^{48} \not\equiv 1 \pmod{97}$ و فقط اگر $x^{48} \not\equiv 1 \pmod{97}$ و فقط اگر $x^{48} \not\equiv 1 \pmod{97}$

مساله لگاریتم گسسته

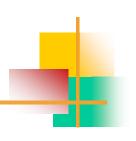


- با فرض این که p یک عدد اول، Z_p^* یک گروه دوری متناهی و $g \in Z_p^*$ یک عنصر اولیه برای این گروه باشد
- هدف مساله لگاریتم گسسته یافتن عدد صحیح $x \leq p-1$ است هدف مساله لگاریتم گسسته $g^x \equiv oldsymbol{eta} \pmod{p}$ به طوری که $g^x \equiv oldsymbol{eta} \pmod{p}$
 - عدد صحیح x
 - g لگاریتم گسسته $oldsymbol{eta}$ به مبنای

 $x = \log_q \beta \mod p$

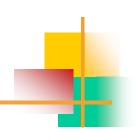
- مثال '
- Z_{47}^st گروه دوری ullet
- مساله لگاریتم گسسته
- $5^x \equiv 41 \pmod{47}$ يافتن عدد صحيح مثبت $1 \leq x \leq 46$ يافتن عدد صحيح مثبت ullet

مساله لگاریتم گسسته



- محاسبه لگاریتمهای گسسته به پیمانه یک عدد اول یک مساله سخت است
- در صورتی که مرتبه گروه اول باشد، از حمله پولیگ هلمن جلوگیری میشود
 - مرتبه گروه دوری Z_p^* اول نیست lacktream
 - $\left|Z_{p}^{*}\right|=p-1$ •
- برای جلوگیری از حمله پولیگ-هلمن، اغلب مساله لگاریتم گسسته به جای Z_p^* در زیرگروههایی از Z_p^* با مرتبه اول استفاده می شود

مساله لگاریتم گسسته



- مثال •
- Z_{47}^st گروه دوری lacktriangle
- $|Z_{47}^*| = 46$ •
- مرتبه زیرگروههای Z_{47}^st با توجه به قضیه لاگرانژlacktriangle
 - $|H_1| = 1$ •
 - $|H_2|=2$
 - $|H_3| = 23$ •
 - H_3 عنصر اولیه یا مولد برای زیرگروه دوری
 - g=2 •
 - $oldsymbol{eta}=36$ با فرض این که $oldsymbol{\bullet}$
 - مساله لگاریتم گسسته
- $2^x\equiv 36\ (\mathrm{mod}\ 47)$ يافتن عدد صحيح مثبت $1\leq x\leq 23$ به طوری که ullet