

Talteori, algebraiska begrepp

Multiplikativ ordning, Cykliska Gruper, Fermats och Eulers satser

Jan Snellman¹

¹Matematiska Institutionen
Linköpings Universitet

Föreläsningsanteckningar på kurshemsidan <http://courses.mai.liu.se/GU/TATA54/>



TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Grupp teori

Definition

Multiplicativ ordning

Multiplikationstabeller

Ordning

Multiplikativ ordning

Cycliska grupper

Direkt produkt av grupper

Fermat, Euler

Euler's thm

Fermat

Beräkna $a^b \bmod n$

Kommutativa ringar

Grupp teori

Definition

Multiplicativ ordning

Multiplikationstabeller

Ordning

Multiplikativ ordning

Cycliska grupper

Direkt produkt av grupper

Fermat, Euler

Euler's thm

Fermat

Beräkna $a^b \bmod n$

Kommutativa ringar

Gruppteori

Definition

Multiplicativ ordning

Multiplikationstabeller

Ordning

Multiplikativ ordning

Cycliska grupper

Direkt produkt av grupper

Fermat, Euler

Euler's thm

Fermat

Beräkna $a^b \bmod n$

Kommutativa ringar

Definition

$(G, *, e)$ är en grupp om för alla $a, b, c \in G$,

1. $a * (b * c) = (a * b) * c$,
2. $a * e = e * a = a$,
3. finns unik $a^{-1} \in G$ så att $a * a^{-1} = a^{-1} * a = 1$.

Om $a * b = b * a$ alltid gäller, så är gruppen Abelsk (kommutativ).

Definition

Den delgrupp till en grupp G är en delmängd $H \subseteq G$ så att

1. $e \in H$,
2. om $h \in H$ så $h^{-1} \in H$,
3. om $h_1, h_2 \in H$ så $h_1 * h_2 \in H$.

Vi skriver $H \leq G$.

Teorem

*Om $(G, *, e)$ grupp och H delgrupp, så är $(H, *, e)$ en grupp. En delgrupp till en abelsk grupp är fortsatt abelsk.*

Exempel

- ▶ $(\mathbb{Z}, +, 0)$ är en abelsk grupp
- ▶ $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ är likaså abelska grupper under addition
- ▶ $\mathbb{C} \setminus \{0\}$ abelsk grupp under multiplikation
- ▶ $\mathcal{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ också abelsk grupp
- ▶ För varje positivt heltal n , $\{\exp(\frac{2k\pi i}{n}) \mid k \in \mathbb{Z}\}$ abelsk grupp under multiplikation
- ▶ För varje positivt heltal n , $\mathbb{Z}_n$ abelsk grupp under addition
- ▶ Den “typiska” ändliga, icke-abelska gruppen är gruppen S_n av bijektioner $\phi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ under funktionssammansättning

Exempel

Vi studerar additionstabellen för de abelska gruppen $(\mathbb{Z}_4, +, [0]_4)$ och $(\mathbb{Z}_5, +, [0]_5)$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Kom ihåg: i $\mathbb{Z}_n$ så har $g = [a]_n$ en multiplikativ invers om $\gcd(a, n) = 1$.

Definition

$\mathbb{Z} \ni n > 1$.

- ▶ $\mathbb{Z}_n^* = \{ [a]_n \mid \gcd(a, n) = 1 \}$.
- ▶ $\phi(n) = |\{ 1 \leq a < n \mid \gcd(a, n) = 1 \}| = |\mathbb{Z}_n^*|$.

$\mathbb{Z}_n$ är inte en grupp under multiplikation, eftersom det finns element som inte har någon invers, men:

Teorem

$\mathbb{Z}_n^*$ är en abelsk grupp.

Exempel

$$\mathbb{Z}_2^* = \{[1]_2\}$$

$$\mathbb{Z}_3^* = \{[1]_3, [2]_3\}$$

$$\mathbb{Z}_4^* = \{[1]_4, [3]_4\}$$

$$\mathbb{Z}_5^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$$

$$\mathbb{Z}_6^* = \{[1]_6, [5]_6\}$$

$$\mathbb{Z}_7^* = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$

$$\mathbb{Z}_8^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$$

Exempel

Multiplikation i $\mathbb{Z}_5^*$ och i $\mathbb{Z}_8^*$

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Definition

- ▶ G ändlig grupp, $g \in G$.
- ▶ $g^2 = g * g$, $g^3 = g * g * g$, et cetera.
- ▶ $g^{-2} = g^{-1} * g^{-1} = (g * g)^{-1}$.
- ▶ $g^i * g^j = g^{i+j}$.
- ▶ $g \in G$ har ordning $o(g) = n$ om $g^n = 1$ men $g^m \neq 1$ for $1 \leq m < n$.
- ▶ Existerar ty $g^i = g^j$ medför $g^{i-j} = g^0 = 1$.
- ▶ $g^s = 1$ omm $n|s$.
- ▶ $g^i = g^j$ omm $i \equiv j \pmod n$.

Lemma

Om $o(g) = n < \infty$ och $a \in \mathbb{Z}_+$ så

$$o(g^a) = \frac{n}{\gcd(a, n)}.$$

Lemma

Om $gh = hg$, $o(g) = n < \infty$, $o(h) = m < \infty$ så $o(gh) | \text{lcm}(n, m)$.

Definition

Vi säger att $a \in \mathbb{Z}$ har multiplikativ ordning n modulo m om $o([a]_m) = n$, där $[a]_n \in \mathbb{Z}_n^*$. Med andra ord så är $a^n \equiv 1 \pmod{m}$ men ej för mindre potenser.

Exempel

- ▶ $3^2 = 9 \equiv 1 \pmod{8}$, så 3 har multiplikativ ordning 2 modulo 8.
- ▶ $3^2 = 9 \equiv 4 \pmod{5}$, $3^3 = 27 \equiv 2 \pmod{5}$, $3^4 = 81 \equiv 1 \pmod{5}$, så 3 har multiplikativ ordning 4 modulo 5.

Definition

- ▶ G grupp, $*$ operation, 1 enhet
- ▶ $g \in G$
- ▶ $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$
- ▶ "Delgrupp" till G , minsta som innehåller g
- ▶ Cyclisk delgrupp **genererad av** g
- ▶ Om $G = \langle g \rangle$ så G cyklisk grupp, g generator
- ▶ Additiv notation: $(G, +, 0)$,
 $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$

Lemma

- ▶ $o(g) = |\langle g \rangle|$
- ▶ $(\mathbb{Z}_n, +, [0]_n) = \langle [1]_n \rangle$
- ▶ $\mathbb{Z} = \langle 1 \rangle$
- ▶ $\mathbb{Z}_5^* = \langle [2]_5 \rangle$
- ▶ $\mathbb{Z}_8^*$ ej cyklisk

- ▶ G, H grupper
 - ▶ $f : G \rightarrow H$ bijektion,
 $f(g_1 * g_2) = f(g_1) * f(g_2)$
 - ▶ $G \simeq H$, G och H **isomorfa**
 - ▶ Samma struktur, andra namn på elementen
 - ▶ Alla egenskaper samma
- ▶ Speciellt, upp till iso, en enda cyklisk grupp av storlek n , kalla den C_n .
 - ▶ $(\mathbb{Z}_n, +) \simeq C_n$
 - ▶ $\{ \exp(\frac{2k\pi i}{n}) \mid k \in \mathbb{Z} \} \simeq C_n$
 - ▶ $(\mathbb{Z}, +) \simeq C_\infty$,
 - ▶ $(\mathbb{Z}_5^*, *) \simeq C_4$

Definition

- ▶ G, H grupper
- ▶ $G \times H = \{ (g, h) \mid g \in G, h \in H \}$
- ▶ Komponentvis addition och multiplikation

Lemma

1. G, H grupper
2. $g \in G, h \in H, o(g), o(h) < \infty$
3. $(g, h) \in G \times H$
4. Då $o((g, h)) = \text{lcm}(o(g), o(h))$

Teorem

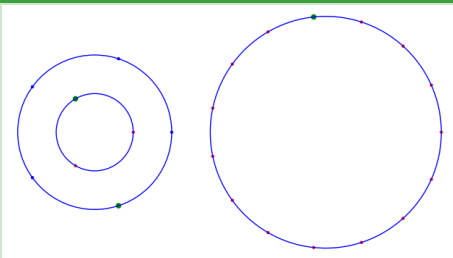
$$C_{mn} \simeq C_m \times C_n \text{ iff } \gcd(m, n) = 1$$

Bevis.

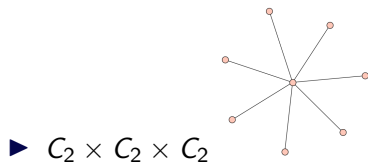
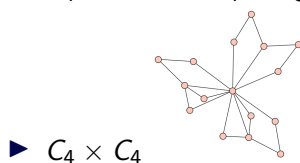
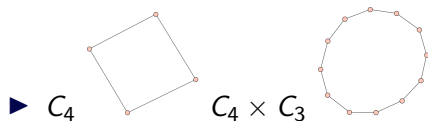
$C_{mn} \simeq (\mathbb{Z}_{mn}, +, [0]_{mn})$. $[a]_{mn} \mapsto ([a]_m, [a]_n)$ isomorfi enligt Kinesiska restsatsen. $\square$

Exempel

$$C_3 \times C_5 \simeq C_{15}, \text{ iso } ([4]_3, [4]_5) \longleftrightarrow [4]_{15}.$$



- ▶ Shanks, "Solved and Unsolved Problems in Number Theory"
- ▶ Rita varje cykel $1 \rightarrow g \rightarrow g^2 \rightarrow \dots \rightarrow g^n = 1$
- ▶ Ta bort delcykler



Teorem (Lagrange)

Om

- ▶ G grupp
- ▶ $|G| = n < \infty$
- ▶ $H \leq G$ delgrupp, $|H| = m$

så $m|n$. Speciellt, om $g \in G$, så $o(g)|n$.

Bevis.

Inte svårt, men behöver begreppet "sidoklasser"



Vi kommer visa detta för $G = \mathbb{Z}_n^*$ med elementära metoder.

Teorem (Euler)

Om $\gcd(a, n) = 1$ så

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad (*)$$

Ekvivalent, $[a]_n^{\phi(n)} = [1]_n \in \mathbb{Z}_n^*$.

Bevis.

Sätt $s = \phi(n)$. Låt $T = \{t_1, \dots, t_s\}$ vara ett val av precis ett element från varje klass i $\mathbb{Z}_n^*$.

Hävdar: aT innehåller också precis ett element från varje klass. Alla at_i icke-kongruenta modulo n , visat tidigare. Eftersom $\gcd(t_i, n) = 1$ och $\gcd(a, n) = 1$ så $\gcd(at_i, n) = 1$.

Nu har vi att

$$1 * (t_1 t_2 \cdots t_s) \equiv (at_1)(at_2) \cdots (at_s) \equiv a^s (t_1 t_2 \cdots t_s) \pmod{n}$$

Stryk $t_1 t_2 \cdots t_s$, det får du!



Exempel

- ▶ $n = 8, T = \{1, 3, 5, 7\},$
- ▶ $a = 5, aT = \{5, 15, 25, 35\} \equiv \{5, 7, 1, 3\} \pmod{8},$
- ▶ $5t_1 * 5t_2 * 5t_3 * 5t_4 \equiv 5 * 7 * 1 * 3 \equiv 1 * 3 * 7 * 5 \equiv 1 \pmod{8}$
- ▶ $5t_1 * 5t_2 * 5t_3 * 5t_4 \equiv 5^4 * t_1 t_2 t_3 t_4 \equiv 5^4 * 1 * 3 * 5 * 7 \equiv 1 * 1 \pmod{8}$
- ▶ $n = 3, T = \{1, 2\},$
- ▶ $a = 2, aT = \{2, 4\} \equiv \{2, 1\} \pmod{3},$
- ▶ $2t_1 * 2t_2 \equiv 2 * 1 \equiv 1 * 2 \equiv 2 \pmod{3}$
- ▶ $2t_1 * 2t_2 \equiv 2^2 * t_1 * t_2 \equiv 2^2 * 1 * 2 \equiv 2^2 * 2 \pmod{3}$

Teorem (Fermat)

Låt p vara ett primtal och a ett heltal så att $p \nmid a$. Då gäller att

$$a^{p-1} \equiv 1 \pmod{p} \quad (**)$$

Med andra ord: $[a]_p^{p-1} = [1]_p \in \mathbb{Z}_p^*$.

Bevis.

$$\phi(p) = p - 1.$$



Exempel

Vad blir resten då 1247^{1231} delas med 7?

$$\begin{aligned}1248^{1231} &\equiv (178 * 7 + 2)^{205*6+1} \pmod{7} \\&\equiv 2^{205*6+1} \pmod{7} \\&\equiv 2^{205*6} * 2^1 \pmod{7} \\&\equiv (2^6)^{205} * 2^1 \pmod{7} \\&\equiv 1^{205} * 2^1 \pmod{7} \\&\equiv 2 \pmod{7}\end{aligned}$$

Exempel (Upprepad kvadrering)

Vad blir 3^{19} modulo 23?

$$3^0 \equiv 1 \pmod{23}$$

$$3^1 \equiv 3 \pmod{23}$$

$$3^2 \equiv 3^2 \equiv 9 \pmod{23}$$

$$3^4 \equiv (3^2)^2 \equiv 81 \equiv 12 \pmod{23}$$

$$3^8 \equiv (3^4)^2 \equiv 12^2 \equiv 6 \pmod{23}$$

$$3^{16} \equiv (3^8)^2 \equiv 6^2 \equiv 13 \pmod{23}$$

så

$$3^{19} = 3^{16+2+1} = 3^{16} * 3^2 * 3^1 \equiv 13 * 9 * 3 \equiv 6 \pmod{23}$$

Exempel (Fermat)

Beräkna 3^{19} modulo 17

$$3^{19} = 3^{16+3} = 3^{16} * 3^3 \equiv 3^3 \equiv 10 \pmod{17}$$

Exempel (Kinesiska restsatsen)

Vad blir $x = 3^{19}$ modulo $17 * 23 = 391$?

$$x \equiv 10 \pmod{17}$$

$$x \equiv 6 \pmod{23}$$

så

$$x \equiv 230 \pmod{391}$$

Definition

En kommutativ, unitär ring $(R, +, 0, *, 1)$ är en abelsk grupp $(R, +, 0)$ med en extra associativ och kommutativ operation $*$, för vilken elementet 1 är en enhet. Vi kräver också att följande distributiva lag gäller:

$$x * (y + z) = x * y + x * z \quad \text{för alla } x, y, z \in R.$$

Definition

En kommutativ, unitär ring R är ett integritetsområde om $a, b \neq 0$ medför att $a * b \neq 0$.

R är en kropp om varje $a \neq 0$ har en multiplikativ invers a^{-1} så att $aa^{-1} = 1$.

Varje kropp är ett integritetsområde.

Exempel

- ▶ $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ kommutativa, unitära ringar. $\mathbb{Z}$ område, ej kropp. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ kroppar.
- ▶ $\mathbb{Z}_n$ kommutativ, unitär kropp.
- ▶ Om R ring så $R[x]$ ring.

Teorem

$\mathbb{Z}_n$ kropp om n primtal, integritetsområde om n komposit.

Definition

Om R kommutativ, unitär ring så är enhetsgruppen

$$R^* = \{ a \in R \mid a \text{ har multiplikativ invers} \}$$

Teorem

Enhetsgruppen är en grupp.

Vi har sett $\mathbb{Z}_n^*$ tidigare. Vad är $\mathbb{Z}^*$?

Definition

- ▶ R, S kommutativa, unitära ringar
- ▶ $T = R \times S = \{ (r, s) \mid r \in R, s \in S \}$
- ▶ Komponentvis addition and multiplikation
- ▶ $R \simeq S$ omm existerar bijektion $F : R \rightarrow S$ som bevarar multiplikation och addition:
 1. $F(a + b) = F(a) + F(b)$
 2. $F(ab) = F(a)F(b)$

Vi behöver maskineriet för följande:

Teorem

Om R, S kommutativa, unitära ringar, så

$$(R \times S)^* \simeq R^* \times S^*.$$

Det ger:

Teorem

- ▶ $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ om $\gcd(m, n) = 1$
- ▶ Om $\gcd(m, n) = 1$ så $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

Exempel

- ▶ $m = 3, n = 4$
- ▶ $\gcd(m, n) = 1$
- ▶ $\mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_{12}$ as rings
- ▶ $\mathbb{Z}_3^* \simeq C_2, \mathbb{Z}_4^* \simeq C_2$
- ▶ $\mathbb{Z}_{12}^* \simeq C_2 \times C_2 \not\simeq C_4$
- ▶ Multiplikationstabeller:

$\mathbb{Z}_3^*$		
*	1	2
1	1	2
2	2	1

$\mathbb{Z}_4^*$		
*	1	3
1	1	3
3	3	1

$\mathbb{Z}_{12}^*$				
*	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1