Talteori och kryptologi, MA191G, 4,5hp

Föreläsningsmaterial

Yohannes T. Aklilu
Högskolan i Skövde

Mer verktyg från talteori

- Fermats lilla sats
- Eulers funktion
- Det kinesiska restsatsen

- Ett *affint chiffer* är ett chiffer med ett klartextalfabet $\mathcal{M} \subseteq \mathbb{Z}_m$, ett kryptoalfabet $\mathcal{C} \subseteq \mathbb{Z}_m$ och chiffreringsfunktioner som är *affina modulär funktion*

$$e_{(a,b)} : \mathcal{M} \to \mathcal{C},$$

där

$$e_{(a,b)}(x) = ax + b \pmod{m}$$

är bijektiva.

- Paret (a, b) är det hemligt nyckeln.
- Det är ekvivalent med att säga att kongruensen

$$ax + b \equiv c \pmod{m}$$

ska ha en entydig lösning x i $\mathcal{M}$ om $c \in \mathcal{C}$.

- Vad ställer det för krav på nyckeln (a, b)?

Example

- Låt $m = 5$. Betrakta funktionen $e_{(2,1)}(x) = 2x + 1 \pmod 5$.
- Då har vi

x	0	1	2	3	4
$e_{(2,1)}(x)$	1	3	0	2	4

- Det betyder att $e_{(2,1)} : \mathbb{Z}_5 \to \mathbb{Z}_5$ är bijektiv.
- Om vi istället betraktar $m = 6$ och funktionen $e_{(2,1)}(x) = 2x + 1 \pmod 6$, så har vi

x	0	1	2	3	4	5
$e_{(2,1)}(x)$	1	3	5	1	3	5

  $e_{(2,1)} : \mathbb{Z}_6 \to \mathbb{Z}_6$ är alltså varken injektiv eller surjektiv.
- Ser vi funktionen som $e_{(2,1)} : \mathbb{Z}_6 \to \{1, 3, 5\}$ så blir den förstås surjektiv, men inte injektiv, medan $e_{(2,1)} : \{1, 3, 5\} \to \{1, 3, 5\}$ är bijektiv.

Example (exempel fort...)

- Däremot, för $e_{(5,1)}(x) = 5x + 1 \pmod 6$ har vi

x	0	1	2	3	4	5
$e_{(5,1)}(x)$	1	0	5	4	3	2

  alltså bijektivitet.

Vad är skillnaden mellan de olika fallen?

- Observera att

$$ax \equiv b \pmod{m} \tag{1}$$

är ekvivalent med att

$$ax + my = b \tag{2}$$

för något heltal y.

- För att kvation (2) ska ha heltalslösning måste $\gcd(a, m)|b$.
- Omvänt, om $\gcd(a, m)|b$, så har också (2) heltalslösning.
- Om $\gcd(a, m) = 1$ så är $[a]_m$ inverterbart och lösningen är $x = a^{-1}b \pmod{m}$, som är entydig.
- Inversen kan beräknas t.ex. genom Euklides algoritm.
- Om $\gcd(a, m) = d > 1$ men $d|b$ så

$$ax \equiv b \pmod{m} \Leftrightarrow cx \equiv e \pmod{k},$$

där $a = dc$, $b = de$ och $m = dk$. Lösningen är då $x = c^{-1}e \pmod{k}$, som är entydig.

- Observera att lösningen då innefattar d olika kongruensklasser modulo m.

Example

	x	0	1	2	3	4	5
$2x$	mod 6	0	2	4	0	2	4

Definition (Eulers ϕ-funktion)

Eulers funktion $\phi(n)$ av ett positivt heltal n är antalet positiva heltal, mindre än eller lika med n, som är relativt prima till n, eller med andra ord, de tal som inte har några primtalsfaktorer gemensamma med n. Alternativt

$$\phi(n) = |\{m \in \mathbb{Z}_+ : m \leq n \text{ och } \gcd(m, n) = 1\}|,$$

- Euler ϕ-funktion är inte växande

n	1	2	3	4	5	6	7	...
$\phi(n)$	1	1	2	2	4	2	6	...

- $\phi(n)$ är också antalet inverterbara kongruensklasser modulo n.
- Egenskaper hos Eulers ϕ-funktion
  - $\phi(p) = p - 1$ om p är ett primtal;
  - $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n(1 - \frac{1}{p})$ om p är ett primtal;
  - $\phi(ab) = \phi(a)\phi(b)$ om $\gcd(a, b) = 1$.

Example

$$\begin{aligned}\phi(72) = \phi(2^3 3^2) &= \phi(2^3)\phi(3^2) \\ &= (2^3 - 2^2)(3^2 - 3^1) = (8-4)(9-3) = 4 \cdot 6 = 24\end{aligned}$$

Example

Vi har också

$$\phi(2^3 3^2) = 2^3\left(1-\frac{1}{2}\right)3^2\left(1-\frac{1}{3}\right) = 72\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$$
$$= 72\cdot\frac{1}{2}\cdot\frac{2}{3} = \frac{72}{3} = 24.$$

Generellt

Om n har primtalsdelarna $p_1, \ldots, p_k$, så gäller

$$\phi(n) = n\cdot(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}).$$

Example

Betrakta $n = 40$. Vi har
$\phi(40) = \phi(2^3 \cdot 5) = \phi(2^3)\phi(5) = (2^3 - 2^2)(5 - 1) = 16$. eller
$\phi(40) = 40(1 - \frac{1}{2})(1 - \frac{1}{5}) = \frac{40 \cdot 1 \cdot 4}{10} = 16$.

- Vilka positiva tal under 40 är relativt prima till 40 då?

  $$1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.$$

  De bildar vad vi kallar en reducerad mängd av rester modulo 40.

Definition (Reducerad mängd av rester)

För en *reducerad mängd av rester modulo m* ska gälla:

1. Varje tal i mängden är relativt prima till m;
2. Inga par av element i mängden är kongruenta modulo m;
3. Mängden har maximalt antal element, dvs $\phi(m)$.

Example

$\{1, 3, 5, 7\}$ och $\{9, -5, 85, 167\}$ är båda reducerade mängder av rester modulo 8.

Med andra ord består en reducerad mängd av rester modulo m av en representant för varje inverterbar restklass i $\mathbb{Z}_m$.

Theorem

Om $\{r_1, r_2, \ldots, r_k\}$ är en reducerad mängd av rester, och $\gcd(a, m) = 1$ så är även $\{ar_1, ar_2, \ldots, ar_k\}$ en reducerad mängd av rester.

Med andra ord, om $A \subset \{0, 1, \ldots, n-1\}$ är en reducerad mängd av rester modulo n, och $\gcd(a, n) = 1$ så är funktionen

$$E_a(k) = ak \pmod{n}$$

en bijektion $A \to A$.

Vi kollar vad vi får för rester modulo 10 när vi multiplicerar talen i en reducerad mängd av rester (och övriga rester) modulo 10 upprepade gånger med 3.

r	mod 10	1	3	7	9	2	4	5	6	8	0
$3r$	mod 10	3	9	1	7	6	2	5	8	4	0
3^2r	mod 10	9	7	3	1	8	6	5	4	2	0
3^3r	mod 10	7	1	9	3	4	8	5	2	6	0
3^4r	mod 10	1	3	7	9	2	4	5	6	8	0

Vi ser att $3^4r \mod 10 = r \mod 10$ (dvs $3^4r \equiv r \pmod{10}$) för alla r. Är det en slump?

Theorem

Eulers sats Om $m \in \mathbb{Z}_+$ *och* $\gcd(a, m) = 1$ *så*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Specialfallet av Eulers sats, modulo ett primtal, kallas Fermats lilla sats.

Theorem (Fermats lilla sats.)

Om p är ett primtal, så gäller för alla $a \not\equiv 0 \pmod{p}$ att

$$a^{p-1} \equiv 1 \pmod{p}$$

samt för alla a att

$$a^{p} \equiv a \pmod{p}.$$

Example (Potenser exempel, $\phi(10) = 4$.)

r	mod 10	1	3	7	9	2	4	5	6	8	0
r^2	mod 10	1	9	9	1	4	6	5	6	4	0
r^3	mod 10	1	7	3	9	8	4	5	6	2	0
r^4	mod 10	1	1	1	1	6	6	5	6	6	0
r^5	mod 10	1	3	7	9	2	4	5	6	8	0

Bevis för Fermats lilla sats.

Betrakta de första positiva $p-1$ multipel av a:

$$a, 2a, 3a, \ldots, (p-1)a.$$

Alla de tal ger olika rester då vi delar talen med p, dvs de är kongruent till $1, 2, \ldots, p-1 \pmod{p}$ i någon ordning. Om vi tar produkten då får vi

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv (1 \cdot 2 \cdot 3 \cdots (p-1)) \pmod{p}.$$

Detta ger resultat! □

Example

Exempel.
Talet 97 är ett primtal.
Alltså är $2^{96} \equiv 1 \pmod{97}$.
Faktiskt också $a^{96} \equiv 1 \pmod{97}$ för alla a sådant att $SGD(a, p) = 1$.
Att $a^p \equiv a \pmod{p}$ när $a^{p-1} \equiv 1 \pmod{p}$ är inte konstigt: multiplicera bara båda leden med a.

Example

Visa att $2^{340} \equiv 1 \pmod{31}$.

Example

Ange vad klockan är i en 24 timmarsklocka om 5^{10} timmar om vi antar att klockan är 12:00 just nu.

Beräkning av multiplikativ invers

Eulers sats ger ett sätt att beräkna multiplikativ invers i $\mathbb{Z}_m$.
Eftersom $a^{\phi(m)} \equiv 1 \pmod{m}$ så är $a^{\phi(m)-1}$ en multiplikativ invers till a, modulo m.
Antag att $\gcd(a, m) = 1$ och att man vill bestämma $[x]_m$ där $ax \equiv b \pmod{m}$. Vi har då

$$x \equiv a^{\phi(m)}x = a^{\phi(m)-1}ax \equiv a^{\phi(m)-1}b,$$

och problemet har delats upp i att bestämma $\phi(m)$, beräkna potensen $a^{(\phi(m)-1)}$ och multiplicera med b.

Example

Låt oss lösa kongruensen $8x + 3 \equiv 14 \pmod{15}$,
eller ekvivalent, $8x \equiv 11 \pmod{15}$. Det går att göra med Euklides algoritm, men vi gör det med metoden ovan.

Lösning.

Vi noterar att $\gcd(8, 15) = 1$, så det finns lösning.

$$\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8.$$

Alltså är $x \equiv 8^{8-1} \cdot 11$. Då $7 = 111_2 = 4 + 2 + 1$, så har vi

$$8^7 = 8^4 \cdot 8^2 \cdot 8^1 \pmod{15},$$

och då

$$8^2 = 64 = 64 - 4 \cdot 15 = 4 \pmod{15}, \quad 8^4 = 4^2 = 16 = 1 \pmod{15}.$$

så är

$$x = 1 \cdot 4 \cdot 8 \cdot 11 = 32 \cdot 11 = 2 \cdot 11 = 22 = 7 \pmod{15}.$$

□

För knappt 2000 år sedan Kineskt matematiken Sun-Tsu frågade:

Example

Det finns några tal i vilken när dividerade med 3 blir resten 2, när dividerade med 5 blir resten 3, och när deviderade med 7 blir resten 2. Vilka kan talen vara?

Rent matematiskt kan vi kan skapa (och lösa) **system av kongruenser**.

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Hur många lösningar finns det? Vilka är lösningarna?

System av kongruenser

Säg att vi t.ex. vill bestämma alla heltal x sådana att

$$\begin{cases} x \equiv 5 \pmod{14} \\ x \equiv 2 \pmod{15} \\ x \equiv 9 \pmod{49} \end{cases}$$

Kan vi veta *om* det finns några sådana tal x, och i så fall vilka? Notera att 7 delar både 14 och 49.

$$\begin{aligned} x \equiv 5 \pmod{14} &\implies x \equiv 5 \pmod{7} \\ x \equiv 9 \pmod{49} &\implies x \equiv 2 \pmod{7} \end{aligned}$$

Finns inget heltal x som uppfyller båda dessa villkor.

Theorem (Kinesiska resttalssatsen)

Låt $m_1, \ldots, m_n$ vara parvist relativt prima positiva heltal. Kongruenssystemet

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ x & \equiv a_2 \pmod{m_2} \\ & \vdots \\ x & \equiv a_n \pmod{m_n} \end{cases}$$

har en **unik** *lösning modulo $m = m_1 \cdot m_2 \cdots m_n$.*

Två lösningar x och x' uppfyller alltså $x \equiv x' \pmod{m}$.

Hur hittar vi lösningarna till ett system av kongruenser som uppfyller den Kinesiska resttalssatsen?

1. Sätt $m = m_1 \cdots m_n$.
2. Sätt $M_k = \frac{m}{m_k}$ för $k = 1, \ldots, n$
3. Så gäller det att $GCD(M_k, m_k) = 1$.
4. Beräkna inversen y_k av $M_k \pmod{m_k}$.
5. Sätt $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$ och det är en gemensam lösning till ekvationssystemet.

Ekvationssystemet har lösningen

$$a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \equiv \quad (\text{mod } m).$$

Example

Lös ekvationssystemet i Sun-Tsus fråga.