MA2047 Algebra och diskret matematik

Något om restklassaritmetik

Mikael Hindgren

HÖGSKOLAN I HALMSTAD

18 september 2024

Restklassaritmetik

Exempel 1

Klockan är nu 8.00

Vad är klockan om 78 timmar?

Vad var klockan för 53 timmar sedan?

- $8 + 78 = 86 = \underbrace{3}_{kvot} \cdot 24 + \underbrace{14}_{rest} \Rightarrow$ Klockan är 14.00
- $8 - 53 = -45 = \underbrace{-2}_{kvot} \cdot 24 + \underbrace{3}_{rest} \Rightarrow$ Klockan var 03.00
- 86 och 14 har samma rest (14) vid division med 24
- -45 och 3 har samma rest (3) vid division med 24
- Om vi bortser från multiplar av 24 vi kan alltså säga
  - $86 = 14$
  - $-45 = 3$

$\therefore$ Tiden på en klocka är resten vid heltalsdivision med 24

Restklassaritmetik

Exempel 2

58 och 43 har samma rest vid division med 5:

$$\begin{cases} 58 = 11 \cdot 5 + 3 \\ 43 = 8 \cdot 5 + 3 \end{cases} \Rightarrow \quad \begin{aligned} 58 - 43 &= 11 \cdot 5 + 3 - (8 \cdot 5 + 3) \\ &= 11 \cdot 5 - 8 \cdot 5 = (11 - 8) \cdot 5 \end{aligned}$$

$\therefore 5 \mid (58 - 43)$

Vi skriver: $58 \equiv 43 \pmod{5}$ ”58 är kongruent med 43 modulo 5”

Definition 1

$a, b, n \in \mathbb{Z},\ n \geq 1: \quad a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$

Anm: I programmering: $\begin{cases} 58 \text{ mod } 5 = 3 \\ 58 \text{ div } 5 = 11 \end{cases}$

Restklassaritmetik

Definition 2

- Två tal a och b tillhör samma ekvivalensklass om $a \equiv b \pmod{n}$ dvs om de har samma rest vid division med n.
- Mängden av alla dessa ekvivalensklasser kallas heltalen modulo n och betecknas $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$

Exempel 3

- Ekvivalensklass $[1]_3$ kallas restklass 1 modulo 3
  $=$ Mängden av alla tal som vid division med 3 ger resten 1
  $= \{a \in \mathbb{Z} : a = 3k + 1, k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$
- $[1]_3 \in \mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ $\leftarrow$ Heltalen modulo 3

Exempel 4

- $\mathbb{Z}_{24} = \{[0]_{24}, [1]_{24}, [2]_{24}, [3]_{24}, \ldots, [23]_{24}\}$
- $[3]_{24} = \{a \in \mathbb{Z} : a = 24k + 3, k \in \mathbb{Z}\} = \{\ldots, -45, -21, 3, 27, 51, 75, \ldots\}$

Restklassaritmetik

Definition 3

Addition och multiplikation modulo n:
$[a] + [b] = [a + b], \quad [a] \cdot [b] = [a \cdot b]$

Exempel 5

I $\mathbb{Z}_{24}$:

- $[8] + [78] = [8 + 78] = [86] = [14]_{24}$
- $[8] - [53] = [8 - 53] = [-45] = [3]_{24}$

I $\mathbb{Z}_{10}$:

- $[3] \cdot [5] = [3 \cdot 5] = [15] = [5]_{10}$
- $[2] \cdot [5] = [2 \cdot 5] = [10] = [0]_{10}$
- $[3] \cdot [7] = [3 \cdot 7] = [21] = [1]_{10}$
  $[7]_{10}$ är den multiplikativa inversen till $[3]_{10} \Leftrightarrow 3 \cdot 7 \equiv 1 \pmod{10}$

Definition 4

$[b]_n$ är den multiplikativa inversen till $[a]_n$ om $[a]_n \cdot [b]_n = [1]_n$.

Restklassaritmetik

Definition 5

Talet b är multiplikativ invers till a modulo n om $ab \equiv 1 \pmod{n}$

Exempel 6

Finns det något tal x sådant att $6x \equiv 1 \pmod{10}$?

- Om $6x$ divideras med 10 skulle vi i så fall få en kvot k och resten 1:

$$6x = 10k + 1 \Leftrightarrow 6x - 10k = 1 \qquad \leftarrow \text{Diofantisk ekvation}$$

- Ekvationen har heltalslösning omm $\text{SGD}(6, 10) = 1$
- Men $\text{SGD}(6, 10) = 2 \Rightarrow$ heltalslösning saknas!

$\therefore$ 6 saknar multiplikativ invers modulo 10.

Sats 1

Ett tal a har multiplikativ invers modulo n omm $\text{SGD}(a, n) = 1$.

Restklassaritmetik

Anm: Vi har att

$$ab \equiv 1 \pmod{n} \Leftrightarrow ab = kn + 1 \tag{1}$$

- Om $\mathrm{SGD}(a, n) = 1$ har den Diofantiska ekvationen (1) oändligt många lösningar (b, k)
- Om (b_0, k_0) är en lösning ges den allmänna lösningen av

$$(b, k) = (b_0 \pm nm, k_0 \pm am) \qquad (m \text{ godtyckligt heltal})$$

- Om $0 < b_0 < n$ är multiplikativ invers till a modulo n ges alla multiplikativa inverser av talen $b = b_0 + nm$, där m är ett godtyckligt heltal.
- Dessa tal bildar ekvivalensklass $[b_0]_n$ i $\mathbb{Z}_n$.

Exempel 7

7 är multiplikativ invers till 3 modulo 10 eftersom $3 \cdot 7 = 21 \equiv 1 \pmod{10}$
$\Rightarrow$ alla tal $7 + 10k$ i $[7]_{10}$ är multiplikativa inverser.

Restklassaritmetik

Exempel 8

Bestäm alla element i $\mathbb{Z}_5$ som har multplikativ invers.

Vi gör en multiplikationstabell i $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Identifiera ”ettorna” i tabellen:

- Elementen i $\mathbb{Z}_5$ som har multiplikativ invers: $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$
- Ex: $[2]_5 \cdot [3]_5 = [1]_5$ dvs $[2]_5$ är multiplikativ invers till $[3]_5$ och tvärt om

Restklassaritmetik

Exempel 9

$5 \mid (58-43) \Rightarrow 5 \mid 6(58-43) = 6\cdot 58 - 6\cdot 43 \Rightarrow 6\cdot 58 \equiv 6\cdot 43 \pmod 5$

Exempel 10

$$58 \equiv 43 \pmod 5 \qquad \begin{cases} 24 = 4\cdot 5+4 \\ 14 = 2\cdot 5+4 \end{cases} \Rightarrow 24 \equiv 14 \pmod 5$$

1. $5 \mid (58-43)$ och $5 \mid (24-14)$
   $\Leftrightarrow 5 \mid (58-43+24-14) \Leftrightarrow 5 \mid ((58+24)-(43+14))$
   $\Leftrightarrow 58+24 \equiv 43+14 \pmod 5$
2. $58\cdot 24 = (11\cdot 5+3)(4\cdot 5+4) = (\ldots)\cdot 5+3\cdot 4 = (\ldots)\cdot 5+12 = (\ldots+2)\cdot 5+2$
   $43\cdot 14 = (8\cdot 5+3)(2\cdot 5+4) = (\ldots)\cdot 5+3\cdot 4 = (\ldots)\cdot 5+12 = (\ldots+2)\cdot 5+2$
   $\Leftrightarrow 58\cdot 24 \equiv 43\cdot 14 \pmod 5$

Restklassaritmetik

Sats 2

Om $n \in \mathbb{Z}_+$ så gäller:

1. $x \equiv y \pmod{n}$ *och* $c \in \mathbb{Z} \Rightarrow cx \equiv cy \pmod{n}$
2. $x_1 \equiv y_1 \pmod{n}$ *och* $x_2 \equiv y_2 \pmod{n} \Rightarrow$
   - a $x_1 + x_2 \equiv y_1 + y_2 \pmod{n}$
   - b $x_1 x_2 \equiv y_1 y_2 \pmod{n}$

Anm: Upprepad användning av Sats 2.2b ger $x^n \equiv y^n \pmod{n}$

Exempel 11

Vilken rest erhålles då $627 \cdot 423 + 355$ divideras med 7?

$627 = 89 \cdot 7 + 4, \quad 423 = 60 \cdot 7 + 3, \quad 355 = 50 \cdot 7 + 5$

$\Rightarrow 627 \equiv 4 \pmod{7}, \quad 423 \equiv 3 \pmod{7}, \quad 355 \equiv 5 \pmod{7}$

Sats 2.2 ger nu:

$627 \cdot 423 + 355 \equiv 4 \cdot 3 + 5 = 12 + 5 = 17 = 2 \cdot 7 + 3 \equiv 3 \pmod{7}$

$\therefore$ Resten blir 3

Restklassaritmetik

Exempel 12

Vilken rest erhålles då 68^{45} divideras med 23?

- $68 = 3 \cdot 23 - 1 \Leftrightarrow 68 \equiv -1 \pmod{23}$
- Sats 2.2b $\Rightarrow 68^{45} \equiv (-1)^{45} = -1 \equiv 22 \pmod{23}$

$\therefore$ Resten blir 22

Restklassaritmetik

Exempel 13

Vilken rest erhålles då $17^{23} + 12^{14}$ divideras med 5?

- $17 = 3 \cdot 5 + 2, \quad 12 = 2 \cdot 5 + 2$
- Sats 2.2 ger:

$$\begin{aligned}
17^{23} &\equiv 2^{23} \pmod 5, \quad 12^{14} \equiv 2^{14} \pmod 5 \\
\Rightarrow 17^{23} + 12^{14} &\equiv 2^{23} + 2^{14} = 4^{11} \cdot 2 + 4^{7} = (5-1)^{11} \cdot 2 + (5-1)^{7} \\
&= 2 \cdot 5(\ldots) + (-1)^{11} \cdot 2 + 5(\ldots) + (-1)^{7} \\
&= 5(\ldots) - 3 = 5(\ldots) - 5 + 2 \\
&= 5(\ldots) + 2 \equiv 2 \pmod 5
\end{aligned}$$

$\therefore$ Resten blir 2

Restklassaritmetik

Exempel 14

$$
\begin{aligned}
10 \equiv 1 \pmod 9 \quad &\underset{\text{Sats 2.2b}}{\Rightarrow} \quad 10^k \equiv 1^k = 1 \pmod 9 \\
&\Rightarrow \quad 64548 = 6 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 8 \\
&\equiv \quad 6 + 4 + 5 + 4 + 8 = 27 \equiv 0 \pmod 9.
\end{aligned}
$$

$\therefore$ Ett heltal är delbart med 9 om summan av alla siffrorna är delbar med 9.

Restklassaritmetik

HÖGSKOLAN I HALMSTAD

Exempel 15

Visa att om $\text{SGD}(a, n) = 1$ och $a \equiv b \pmod{n}$ så är $\text{SGD}(b, n) = 1$.

- $n = dm$ där $d > 1$ och $m \geq 1$ är två heltal.

$$a \equiv b \pmod{n} \Rightarrow \begin{cases} a = k_1 n + r \\ b = k_2 n + r \end{cases} \quad k_1, k_2 \in \mathbb{Z},\ 0 \leq r < n.$$

Varje tal $d > 1$ som delar n delar inte a eftersom $\text{SGD}(a, n) = 1$:

$$d \mid n \Rightarrow d \nmid (a = k_1 \cdot n + r) \Rightarrow d \nmid r \Rightarrow d \nmid (b = k_2 n + r) \Rightarrow \text{SGD}(b, n) = 1.$$

Anm: Här utnyttjade vi den kontrapositiva formen $(X \Rightarrow Y) \Leftrightarrow (\neg Y \Rightarrow \neg X)$ och att $\neg(X \wedge Y) \Leftrightarrow \neg X \vee \neg Y$ (De Morgans lag). Utsagorna

$$a|b \wedge a|c \Rightarrow a|(b + c) \quad \text{och} \quad a \nmid (b + c) \Rightarrow a \nmid b \vee a \nmid c$$

är tautologiskt ekvivalenta dvs de har samma sanningsvärdestabell.

Restklassaritmetik

ISBN = International Standard Book Number (ISBN10)

- $a_1, a_2, a_3, ..., a_{10}$ siffrorna i ISBN
- a_{10} väljs så att

$$a_1 + 2a_2 + 3a_3 + \cdots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}$$

  Om $a_{10} = 10$ skrivs X

- Ex: ISBN $= 093603103a_{10}$
  a_{10} välj så att

$$1 \cdot 0 + 2 \cdot 9 + 3 \cdot 3 + \cdots + 9 \cdot 3 + 10 \cdot a_{10} = 103 + 10a_{10} \equiv 0 \pmod{11}$$

$$\Rightarrow a_{10} = 4 \text{ eftersom } 11 \mid 103 + 40 = 143$$

Restklassaritmetik

Test av ISBN detekterar fel om en enskild siffra är fel:

- Korrekt ISBN: $a = a_1 + 2a_2 + 3a_3 + \cdots + ia_i + \cdots + 10a_{10}$
- Fel ISBN: $b = a_1 + 2a_2 + 3a_3 + \cdots + ib_i + \cdots + 10a_{10}, \quad b_i \neq a_i$
- $\Rightarrow b - a = b_i - a_i \neq 0$
- $0 \leq a_i,\, b_i \leq 9 \Rightarrow b_i - a_i \not\equiv 0 \pmod{11}$
- $\Rightarrow b \not\equiv a \pmod{11} \Rightarrow b \not\equiv 0 \pmod{11}$

Collatz problem (Lothar Collatz 1937)

1. Utgå från ett positivt heltal n.
2. Om n är jämnt, dividera det med 2. Om det är udda, multiplicera det med 3 och addera därefter 1.
3. Upprepa steg 2 tills du når talet ett.

Matematisk formulering: Sätt

$$f(n) = \begin{cases} \dfrac{n}{2}, & \text{om } n \equiv 0 \pmod 2 \\ 3n+1, & \text{om } n \equiv 1 \pmod 2 \end{cases}$$

Talföljden $\{a_k\} = \{a_0, a_1, a_2, a_3, ...\}$ definieras nu rekursivt av

$$a_k = \begin{cases} n, & \text{om } k = 0 \\ f(a_{k-1}), & \text{om } k > 0 \end{cases}$$

Exempel 16

$n = 6$: $\{a_0, a_1, a_2, ..\} = \{6, 3, 10, 5, 16, 8, 4, 2, 1\}$
$n = 17$: $\{a_0, a_1, a_2, ..\} = \{17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1\}$

Problem: Är det oavsett val av n alltid möjligt att nå talet 1?
Man tror det men ingen har lyckats bevisa det. Problemet är alltså olöst.

RSA-kryptot

- Ronald L. Rivest, Adi Shamir och Leonard M. Adleman (1977)
- Assymetriskt krypto:
  - Publik nyckel för kryptering
  - Hemlig nyckel för avkryptering
- Säkerheten bygger på svårigheten att primtalsfaktorisera stora heltal
- Används av de flesta stora IT-företagen, myndigheter, banker,...
- Anses vara säkert
- Nackdel: Säkrare men långsammare än symmetriska krypto
- Kan användas i kombination med symmetriska krypto för snabb kryptering och säker nyckelöverföring:
  - Meddelandet (stort) krypteras med symmetriskt krypto
  - Nycklarna (små) krypteras med RSA
- Används ofta för signering av meddelanden

RSA-kryptot

Definition 6 (Eulers ϕ-funktion)

$\phi(n) =$ antalet positiva heltal mindre än $n \in \mathbb{Z}_+$ som är relativt prima med n.

Exempel 17

- $\phi(15) = ?$
  Positiva heltal mindre än 15 som är relativt prima med 15:
  $1, 2, 4, 7, 8, 11, 13, 14 \Rightarrow \phi(15) = 8$
- Om p är ett primtal är alla positiva heltal $< p$ relativt prima med p
  $\Rightarrow \phi(p) = p - 1$

Sats 3

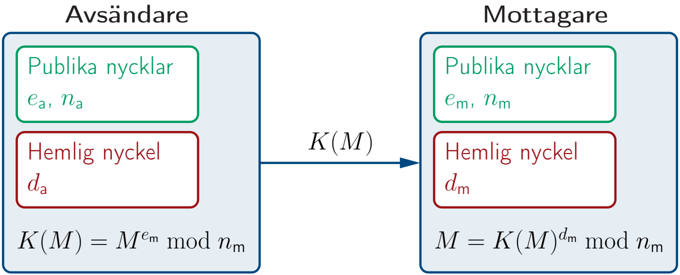
Om $n = pq$, p, q primtal, $p \neq q$, så är $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$.

Exempel 18

- $p = 7$ och $q = 3 \Rightarrow n = pq = 21 \Rightarrow \phi(21) = (7-1)(3-1) = 6 \cdot 2 = 12$
- 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20 är relativt prima med 21 (12 tal)

RSA-algoritmen

- Publika nycklar n och e:
  - $n = pq$, p och q stora hemliga primtal
  - e väljs så att $1 < e < \phi(n)$ och $\operatorname{sgd}(e, \phi(n)) = 1$
- Hemlig nyckel d: Väljs så att $ed \equiv 1 \pmod{\phi(n)}$
- Meddelandet översätts till ett tal $M < n$
- Kryptering: $K(M) = M^e \mod n$
- Avkryptering: $A(K(M)) = K(M)^d \mod n$
- Säkerheten: Hitta p och $q \to \phi(n) = (p-1)(q-1) \to d$



RSA-algoritmen

Exempel 19

Vi krypterar det korta meddelandet ”H” som är bokstav nr 8 dvs $M = 8$

- Välj $p = 3$ och $q = 11 \Rightarrow n = pq = 33 \Rightarrow \phi(n) = (p-1)(q-1) = 20$
- Bestäm publika nyckeln e så att e och $\phi(n)$ är relativt prima: Vi väljer $e = 7$
- Bestämning av hemliga nyckeln d: $\quad ed \equiv 1 \pmod{\phi(n)}$

$$\begin{aligned} \text{Divisionsalgoritmen} \quad &\Rightarrow \quad ed = k\phi(n) + 1 \Leftrightarrow ed - k\phi(n) = 1 \\ &\Leftrightarrow \quad 7d - 20k = 1 \leftarrow \text{Diofantisk ekvation} \end{aligned}$$

Euklides algoritm ger en lösning:

$$\begin{aligned} 20 &= 2 \cdot 7 + 6 \\ 7 &= 1 \cdot 6 + 1 \end{aligned} \Rightarrow \begin{aligned} 1 &= 7 - 1 \cdot 6 = 7 - (20 - 2 \cdot 7) \\ &= 7\underbrace{(3)}_{d} - 20 \cdot \underbrace{(1)}_{k} \end{aligned} \Rightarrow d = 3$$

- Kryptering: $K(M) = M^e \mod n = 8^7 \mod 33 = 2$ motsvarar ”B”
- Avkryptering: $A(K(M)) = K(M)^d \mod n = 2^3 \mod 33 = 8 = M \quad$ OK!