17/12/19

הרצאה אומיטרית

רקע תשבון מודולרי

פעולת מודולו פותרת לנו כמה דברים בחשבון ביטוי מתמטי (למעט חזקה)

דוגמה:

* מודולו 9 למספר שווה לסכום הספרות של המספר

$$\underset{\text{mod } 9}{abcde} = \underset{\text{mod } 9}{a\cdot 10^4} + \underset{\text{mod } 9}{b\cdot 10^3} + \underset{\text{mod } 9}{c\cdot 10^2} + \underset{\text{mod } 9}{d\cdot 10^1} + \underset{\text{mod } 9}{e\cdot 10^0}$$

$$abcde \bmod 9 = a+b+c+d+e$$

$$\left(10^4 \bmod 9 = 1 \quad , \quad 10^i \bmod 9 = 1 \quad \forall i \in \mathbb{R}\right)$$

דוגמה: מודולו 11

H=abcd

d+b ~~a+b~~=x =sum digits at even locations

a+c ~~b+c~~=y = sum digits at odd locations

H mod 11=(x-y) mod 11

* $\left(10 \bmod 11 = (-1) \bmod 11\right)$

* **המשפט הקטן של פרמה**

$$a^{p-1} = 1 \ / \bmod p$$

p - מספר ראשוני

$a \neq 0$ ואינו כפולה של p

למשל $a^{12} = 1 \ / \bmod 13$

מסקנה:

אנו מעוניינים לחזור אותם a, p : $a^b = a^{b \bmod (p-1)} \ / \bmod p$ (*)

את הקשה לתשב מודולו $a^b \bmod p = a^{b \bmod (p-1)} \bmod p$

לחזרה חזקה b גדולה. מתילה לקיטין אותה נוכל לתשב מודולו.

הוכחה בעמוד הבא

* **הופכי כפלי מודולרי**

שבה שלוחה סגור תחת כפל, חיבור = חיסור.

איך מחלקים? $a\cdot b = c \implies a = c\cdot \underbrace{b^{-1}}_{\text{נרצה לחשב}}$

* **משפט**: כל מספר שונה מאפס ושאינו כפולה **של** מספר ראשוני p, קיים לו הופכי כפלי מודולו p.

כלומר, לחזור a שמקיים את השוויון קיים b כך ש: $a\cdot b = 1 \ / \bmod p$

הוכחה למשוואה (*)

לכל b שהוא, נוכל להתאר r, s כך ש:

$$(**)\quad b = \underbrace{r(p-1)}_{\text{מכפלה אמיתית של } p-1} + \underbrace{s}_{\text{שארית שנקבל לאחר חילוק ב-}p-1 \text{ ב-}b}, \quad s = b \bmod (p-1)$$

לכן:

$$a^b \underset{(**)}{=} a^{r(p-1)+b \bmod (p-1)} = a^{r(p-1)} \cdot a^{b \bmod (p-1)}$$

$$\underset{\text{פרמה}}{=} \underbrace{\left(\left(a^{p-1}\right)^r \bmod p\right)}_{\underbrace{(a^{p-1} \bmod p)\cdots(a^{p-1} \bmod p)}_{r \text{ פעמים}} \bmod p} \cdot \left(a^{b \bmod (p-1)} \bmod p\right) \bmod p$$

$$\underset{\text{נקבל את השוויון}}{=} 1 \cdots 1 = 1$$

$$\underset{\text{כי}}{=} a^{b \bmod (p-1)} \bmod p$$

$$\underset{\text{מכפלה}}{=} x \bmod p$$

$$(a^b) \bmod p = (a \bmod p)(b \bmod p) \bmod p$$

$$x \bmod p = x \bmod p$$

אלגוריתם אוקלידס לחישוב הופכי כפלי מודולרי

* נתבונן בדוגמה פשוטה: $2^{-1} \bmod 9$

נשאל את עצמנו $2 \cdot x = 1 \ / \bmod 9$

בדוגמה זו קל לראות $x = 5 = 2^{-1}$

איך נפתור בצורה אלגוריתמית?

$$9 = 2 \cdot (4) + 1$$

$$\underset{=0}{9} + 2\underset{=5}{(-4)} = 1 \ / \bmod 9$$

$$9 \bmod 9 + 2 \bmod 9 \times \underbrace{(-4) \bmod 9}_{5 \bmod 9} = 1 \bmod 9$$

$$2 \cdot 5 = 1 \ / \bmod 9 \implies x = 5 = 2^{-1}$$

* דוגמה יותר מורכבת: $14^{-1} \bmod 25$

$\boxed{\text{נרשום משוואות}}$

(I) $25 = 14(1) + 11$

(II) $14 = 11(1) + 3$

(III) $11 = 3(3) + 2$

(IV) $3 = 2(1) + 1$

$\boxed{\text{נסדר משוואות}}$

(I) $3 + 2(-1) = 1$

(II) $11 + 3(-3) = 2$

(III) $14 + 11(-1) = 3$

(IV) $25 + 14(-1) = 11$

$\boxed{\text{נדיק}}$

(II) → (I) $3 + [11 + 3(-3)](-1) = 1$

$3(4) + 11(-1) = 1$

(III) → (I) $[14 + 11(-1)](4) + 11(-1) = 1$

$14(4) + 11(-5) = 1$

(IV) → (I) $14(4) + [25 + 14(-1)](-5) = 1$

$14(9) + \underbrace{25(-5)}_{0} = 1 \ / \bmod 25$

$14 \cdot 9 = 1 \ / \bmod 25$

מצאנו: $9 = 14^{-1} \ / \bmod 25$

17/12/19

* העלאה מהירה בחזקה (מודולו)

$$a^b \bmod c = \underbrace{a \cdot a \cdot a \cdot a \cdot a}_{b \text{ פעמים}} \bmod c$$

נלמד את אלגוריתם Square and multiply

נתון a, b, c $\quad d = a^b \bmod c$

נסמן $b(i)$ הביט במקום ה-i בייצוג הבינארי של b.

נניח b באורך n ביטים בייצוג בינארי

נרשום אלגוריתם:

```
k = 1
for i = 1 to n
    k ⇐ k^2 mod c
    if b(i) = 1 then k ⇐ (k·a) mod c
    i++
d ⇐ k
```

הינו $O(\log_2 b)$ פעולות.

לעומת b מכפלות בפעולה בחזקה ישירה.

* נראה איך זה עובד:

#(n-1)

(I) $b = 1 \underbrace{0 \cdots 0}_{\#(n-1)} = 2^{n-1}$ **נניח למשל:**

שלב ראשון באלגוריתם

$a^{(2^0)} \; a^{(2^1)} \; a^{(2^2)} \; a^{(2^{n-1})} = a^b$

(II) $b = 1 \; 0 \; 0 \cdots 0 \; 1 = 2^{n-1} + 1$ **כעת נניח:**

multiply by a

$a^{(2^0)} \; a^{(2^1)} \; a^{(2^{n-1}+1)} = a^{(2^{n-1}+1)} = a^b$

(III) $b = 1 \; 0 \; 0 \; 1 \; 0 \cdots 0 = 2^{n-1} + 2^{n-4}$ **כעת נניח:**

$a^{(2^0)} \; a^{(2^1)} \; a^{(2^2)} \; a^{(2^3+1)} \quad a^{(2^3+1)2^{n-4}} = a^{(2^{n-1}+2^{n-4})} = a^b$

העלאה בריבוע זו הזזה בחזקה
הכפלה ב a זו תוספת 1 בחזקה

$a=9, b=13, c=15 \Leftarrow$ $9^{13} \bmod 15$ - לחזקה מודולו

$b = 1101$ - $n=4$ המספר הבינארי

$b(1)$

$i = 1$

$k = 1^2 \bmod 15 = 1$

$b(1) = 1 \rightarrow k = 1 \cdot 9 \bmod 15 = 9$

$k = 9$

$i = 2$

$k = 9^2 \bmod 15 = 6$

$b(2) = 1 \rightarrow k = 6 \cdot 9 \bmod 15 = 9$

$k = 9$

$i = 3$

$k = 9^2 \bmod 15 = 6$

$b(3) \neq 1$

$k = 6$

$i = 4$

$6^2 \bmod 15 = 6$

$b(4) = 1$ $k = 6 \cdot 9 \bmod 15 = 9$

$k = 9$

$2 \cdot 2$

2^{i-1}

$9^{13} \bmod 15 = 9$ סיום