

1/6/Discrete : Quiz 15

a_n $a_0 = 0, \quad a_1 = 1$

(a)

$a_n = 7a_{n-1} - 12a_{n-2}$ ✓

$a_2 = 7a_1 - 12a_0$

$= 7(1) - 12(0) = 7 - 0 = 7$ ✓

$a_3 = 7a_2 - 12a_1 = 7(7) - 12(1)$

$= 49 - 12 = 37$

(b)

$P(n) :$

$a_n = 4^n - 3^n$

$n \geq 0$

base

$a_0 = 0$ ✓

$4^0 - 3^0$

$a_1 = 1$ ✓

✓

$4^1 - 3^1 = 4 - 3 = 1$

Induction step:

Induction hypothesis: $P(k) \quad 0 \leq k \leq n$

i.e. $a_k = 4^k - 3^k \quad \text{for } 0 \leq k \leq n$

NTS: $\Rightarrow P(n+1)$

$$a_{n+1} = 4^{n+1} - 3^{n+1}$$

Then defn

$$a_{n+1} = 7a_n - 12a_{n-1}$$

ind hyp

$$7(4^n - 3^n) - 12(4^{n-1} - 3^{n-1})$$

$$7 \cdot 4^n - 7 \cdot 3^n - 12 \cdot 4^{n-1} + 12 \cdot 3^{n-1}$$

$$7 \cdot 4^n - \frac{12 \cdot 4^{n-1}}{3 \cdot 4^{n-1}} \cdot 4^n$$

$$= 7 \cdot 4^n - 3 \cdot 4^n$$

$$-7 \cdot 3^n + 4 \cdot 3 \cdot 3^{n-1}$$

$$= -7 \cdot 3^n + 4 \cdot 3^n$$

$$\begin{aligned}
 & (-7-3)4^n \\
 & 4 \cdot 4^n \\
 & 4^{n+1}
 \end{aligned}$$

$$\begin{aligned}
 & (-7+4)3^n \\
 & -3(3^n) \\
 & \del{3^{n+1}} \quad 3^{n+1}
 \end{aligned}$$

Lact time

Thm 1 $\forall a, b \in \mathbb{Z}, b > 0,$

There are unique $q, r \in \mathbb{Z}$

so that

$$(1) \quad \underline{a = bq + r}$$

$$(2) \quad 0 \leq r < b$$

Defns $q = \text{quotient} = \left\lfloor \frac{a}{b} \right\rfloor$

$a \text{ div } b$

$r = \text{remainder} = a \bmod b$

Defn $a, b, m \in \mathbb{Z}, m > 0$

$\rightarrow a \equiv b \pmod{m}$ iff $\underline{\underline{m \mid b-a}}$

Easy tests:

$d = a_n a_{n-1} \dots a_0$
decimal ~~repres~~ repres

- a) $2 \mid d \iff 2 \mid a_0$
- b) $5 \mid d \iff 5 \mid a_0$
- c) $3 \mid d \iff 3 \mid \sum a_i$
- d) $9 \mid d \iff 9 \mid \sum a_i$
- e) $11 \mid d \iff 11 \mid \sum (-1)^i a_i$

Ex 1: (a) $23 \equiv 8 \pmod{3}$ T

(b) $10 \equiv -10 \pmod{9}$ F

$10 \not\equiv -10 \pmod{9}$

(c) $23 \equiv 8 \pmod{5}$ T

$$d) 100 \equiv 1 \pmod{9} \quad \uparrow$$

$$9 \mid 99 \quad \checkmark$$

Ex 2 für a, b, m find

(a) $a \text{ div } m$

(b) $a \text{ mod } m$

(c) $b \text{ div } m$

(d) $b \text{ mod } m$

(e) determine if $a \equiv b \pmod{m}$

① $a = 25, \quad b = 15, \quad m = 7$

$$25 = 7 \underbrace{(3)}_9 + \underbrace{(4)}_r$$

$$25 \text{ div } 7 = 3$$

$$25 \text{ mod } 7 = 4$$

$$15 = 7(2) + 1$$

$$\begin{aligned} 15 \text{ div } 7 &= 2 \\ 15 \text{ mod } 7 &= 1 \end{aligned}$$

e) $25 \not\equiv 15 \pmod{7} \text{ ??}$

25

② $a = 103, b = 48, m = 5$

$$103 = 5 \left(\frac{20}{9} \right) + \frac{3}{9}$$

$$\begin{aligned} 103 \text{ div } 5 &= 20 \\ 103 \text{ mod } 5 &= 3 \end{aligned}$$

$$48 = 5(9) + 3$$

$$\begin{aligned} 48 \text{ div } 5 &= 9 \\ 48 \text{ mod } 5 &= 3 \end{aligned}$$

$$103 \equiv 48 \pmod{5}$$

$$5 \mid 103 - 48 = 55 \quad \checkmark$$

T

③ $a = \underline{\underline{2024}}, b = -36, m = 10$

$$2024 = 10(202) + \underline{4}$$

$$2024 \text{ div } 10 = 202$$

$$2024 \text{ mod } 10 = 4$$

$$-36 = 10(-4) + \underline{4}$$

$$-36 \text{ div } 10 = -4$$

$$-36 \text{ mod } 10 = 4$$

$$2024 \equiv -36 \pmod{10}$$

yes

$$2024 - (-36) = 2060$$

Connection:

Proposition 1 For $a, b, m \in \mathbb{Z}$,

$$m > 0$$

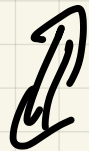
$$a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$$

Proof HW (\Leftarrow) Easy

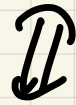
(\Rightarrow) were involved

Special: $m=2$

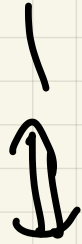
$$a \bmod 2 = 0 \quad \text{or}$$



$$2|a$$



a even



$$a = 2x + 1$$



a odd

Corollary: $\forall a \in \mathbb{Z}$,

a even or a odd

$$(r=0)$$

$$(r=1)$$

not both

§ 36

GCD

Defn Let $a, b \in \mathbb{Z}$, $d \in \mathbb{Z}$

(1) d is a common divisor of a and b if $d|a$ and $d|b$

(2) d is the greatest common divisor of a & b

if (a) d common divisor of a, b

(b) If $e|a$ & $e|b$ then $e \leq d$

Notation : $d = \text{gcd}(a, b)$

Ex | $a = 24$, $b = 36$

$$\text{Find } \text{gcd}(24, 36)$$

divisors of 24 $\pm 1, \pm 2, \pm 3, \pm 4,$
 $\pm 6, \pm 8, \pm 12, \pm 24$

divisors of 36 $\pm 1, \pm 2, \pm 3, \pm 4,$
 $\pm 6, \pm 9, \pm 12, \pm 18, \pm 36$

$$\text{gcd}(24, 36) = 12$$

Inefficient:

Better way: Use prime factors

$$\begin{array}{l} 24 = 2^{\textcircled{3}} \cdot 3^{\textcircled{1}} \\ 36 = 2^{\textcircled{2}} \cdot 3^{\textcircled{2}} \end{array} \Rightarrow \text{gcd}(24, 36) = 2^2 \cdot 3^1 = 12 \checkmark$$

Ex 2 $a = 2^3 \cdot 17 = 7 \cdot 3 \cdot 31$

$$b = 175 = 5 \cdot 35 = 5 \cdot 5 \cdot 7 = 5^2 \cdot 7$$

$$\text{gcd}(2317, 175) = 7$$

$$2317 = 5^0 \cdot 7^1 \cdot 331^1$$

$$175 = 5^2 \cdot 7^1 \cdot 31^0$$

$$\text{so } 9^0$$

Ex 3

$$a = 111,111$$

$$b = 1,287$$

$$429$$

$$143$$

$$a = 111111 = 3 \cdot 37 \cdot 7 \cdot 11 \cdot 13$$

$$1001$$

$$b = 3 \cdot 3 \cdot 11 \cdot 13$$

$$a = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$$

$$b = 3^2 \cdot 11 \cdot 13$$

$$\gcd(a, b) = 3^1 \cdot 11 \cdot 13 = \boxed{429}$$

Prop 1 If $0 < a, b \in \mathbb{Z}$ and
 $r = a \bmod b$. Then

$$\gcd(a, b) = \gcd(b, r)$$

Ex 1: $\gcd(2317, 175)$

$$\left(\begin{array}{l} 2317 = 175(13) + 42 \leftarrow r \\ \begin{array}{cc} a & b \end{array} \end{array} \right)$$

$$\gcd(175, 42)$$

$$\left(\begin{array}{l} 175 = 42(4) + 7 \\ \gcd(42, 7) = 7 \end{array} \right)$$

Ex² $\gcd(221, 45)$

$$221 = 45(\underline{4}) + 41$$

$$\gcd(45, 41)$$

$$45 = 41(1) + 4$$

$$\gcd(41, 4)$$

$$41 = 4 \cdot (10) + 1$$

$$\gcd(4, 1) = 1 \quad \checkmark$$

Defn: a, b are relatively prime
iff $\gcd(a, b) = 1$