11/6/ Discrete: Quiz 15

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

(a) $\underline{a_n = 7a_{n-1} - 12a_{n-2}}$

$a_2 = 7a_1 - 12a_0$

$= 7(1) - 12(0) = 7 - 0 = 7$

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

$= 49 - 12 = 37$

(b) $P(n)$: $\boxed{a_n = 4^n - 3^n}$ $n \geq 0$

<u>base</u>

$a_0 = 0$
$\shortparallel$
$4^0 - 3^0$ ✓

$a_1 = 1$
$\shortparallel$
$4^1 - 3^1 = 4 - 3 = 1$ ✓

Induction step:

Induction hypothesis: $P(k)$ $0 \le k \le n$

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

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

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

Then defn

Ind hypoth

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

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

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

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

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

$$(7-3)4^n \qquad (-7+4)3^n$$
$$4 \cdot 4^n \qquad -3(3^n)$$
$$\| \qquad\qquad \| $$
$$4^{n+1} \qquad \cancel{} \; 3^{n+1}$$

Last time

Thm 1 $\forall a, b \in \mathbb{Z}, b > 0,$
There are unique $\underline{\underline{q}}, \underline{\underline{r}} \in \mathbb{Z}$ so that

① $\underline{a = bq + r}$

② $0 \leq r < b$

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

r = remainder $=$ a $\boxed{\text{mod}}$ b

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

$a \equiv b \ (\boxed{\text{mod}} \ m)$ iff $\underline{\underline{m \mid b - a}}$

Easy tests: $d = a_n a_{n-1} \ldots a_0$ decimal expansion

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) $11 \mid d \iff 11 \mid \sum (-1)^i a_i$

Ex1: (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) $100 \equiv 1 \pmod 9$ T

$9 \mid 99$ ✓

Ex2 for a, b, m find

(a) a div m

(b) a mod m

(c) b div m

(d) b mod m

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

1 $a = 25, \quad b = 15, \quad m = 7$

$$25 = 7(\underbrace{3}_{q}) + (\underbrace{4}_{r})$$

25 div $7 = 3$

25 mod $7 = 4$

$15 = 7(2) + 1$

$15 \text{ div } 7 = 2$

$15 \text{ mod } 7 = 1$

e) $25 \not\equiv 15 \pmod 7$??

NO

② $a = 103,\ b = 48,\ m = 5$

$103 = 5(\underline{20}) + \underline{3}$ $103 \text{ div } 5 = 20$

$103 \text{ mod} = 3$

$48 = 5(9) + 3$ $48 \text{ div } 5 = 9$

$48 \text{ mod } 5 = 3$

$103 \equiv 48 \pmod 5$ ✓

$5 \mid 103 - 48 = 55$

T

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

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

$2024 \text{ div } 10 = 202$

$2024 \bmod 10 = 4$

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

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

$-36 \bmod 10 = 4$

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

$2024 - (-36) = 2060$

<u>Connection</u>:

<u>Proposition</u>: For $a, b, m \in \mathbb{Z}$, $m > 0$

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

Proof HW ($\Leftarrow$) Easy

($\Rightarrow$) more involved

Special: $m = 2$

$$a \bmod 2 = 0 \quad \text{or} \quad 1$$

$$\begin{array}{ccc} 0 & & 1 \\ \Updownarrow & & \Updownarrow \\ 2 \mid a & & a = 2x+1 \\ \Updownarrow & & \Updownarrow \\ a \text{ even} & & a \text{ odd} \end{array}$$

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

a even or a odd $\boxed{\text{not both}}$

$(r=0)$ $(r=1)$

§3.6 **GCD**

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

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

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

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

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

Ex1 $a = 24$, $b = 36$

find $\gcd(24, 36)$

<u>divisors of 24</u> $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$

<u>divisors of 36</u> $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36$

$$\gcd(24, 36) = 12$$

<u>Inefficient</u> :

<u>Better way</u> : Use prime factors

$$24 = 2^{3} \cdot 3^{1}$$

$$36 = 2^{2} \cdot 3^{2}$$

$\rightarrow \gcd(24, 36)$

$\parallel$

$2^2 \cdot 3^1 = 12$ ✓

21

<u>Ex2</u> $a = 2317 = 7 \cdot 331$

$b = 175 = 5 \cdot \underbrace{35} =$

$5 \cdot 5 \cdot 7 = 5^2 \cdot 7^1$

$\gcd(2317, 175) = 7^1$

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

$175 \quad 5^2 \cdot 7^1 \cdot 331^0$

So 9.

<u>Ex 3</u> $a = 111{,}111$

$b = 1{,}287 \qquad 429$

143

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

1001

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

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

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

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

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

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

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

$$\underset{a}{2317} = \underset{b}{175}(13) + 42$$ ← Gen

$\gcd(175, 42)$

$$175 = 42(4) + 7$$

$\gcd(42, 7) = 7$

Ex 2 $\gcd(221, 45)$

$$221 = 45(4) + 41$$

$$\gcd(45, 41)$$

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

$$\gcd(41, 4)$$

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

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

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