6.042J Problem Set - 3

1.(a) Pulverizer

$$\gcd(x,y) = \gcd(y, \text{rem}(x,y))$$

keep track of remainder

$$r = x - q\cdot y$$

$\gcd(135, 59) = 135s + 59t$

x	y	$\text{rem}(x,y) = x - q\cdot y$	
135	59	17	$= 135 - 2\cdot 59$
59	17	8	$= 59 - 3\cdot 17$
			$= 59 - 3\cdot(135 - 2\cdot 59)$
			$= -3\cdot 135 + 7\cdot 59$
17	8	1	$= 17 - 2\cdot 8$
			$= (135 - 2\cdot 59) + -2(-3\cdot 135 + 7\cdot 59)$
			$= 7\cdot 135 - 16\cdot 59$
8	1	0	

$$\Rightarrow \underbrace{7}_{s}\cdot 135 + \underbrace{(-16)}_{t}\cdot 59 = 1 = \gcd(135, 59)$$

(b) Let k be the inverse of 59 modulo 135,

$$59k \equiv 1 \pmod{135} \Rightarrow 135 \mid (1 - 59k)$$

From (a) we know that

$$7\cdot 135 + (-16)\cdot 59 = 1$$

So, $1 \equiv (-16) \cdot 159 \pmod{135}$

but since we need an inverse in the range $\{1, \ldots, 134\}$, we choose another inverse in the range from the set of numbers with remainder = rem$(-16, 135) = 119$

$\because$ 119 lies in the range, It is an inverse of 59

(c) Euler's Thm: If $\gcd(n,k) = 1 \Rightarrow k^{\phi(n)} \equiv 1 \pmod{n}$

$n = 31$, $k = 17$; Since n is prime, $\phi(n) = n-1 = 31 - 1 = 30$

$$\Rightarrow \quad k^{30} \equiv 1 \pmod{n}$$
$$\underbrace{k^{29}}_{\text{inverse}} \cdot k \equiv 1 \pmod{n}$$

To find inverse in range: rem$(17^{29}, 31)$

read about Method of Repeated Squaring

$\rightarrow 17^1 \equiv 17 \pmod{31}$

$\rightarrow 17^2 = 289$
$= 9 \cdot 31 + 10$
$\equiv 10 \pmod{31}$

$\rightarrow 17^4 \equiv 10^2$
$= 100$
$= 3 \cdot 31 + 7$
$\equiv 7 \pmod{31}$

$\rightarrow 17^8 \equiv 7^2$
$= 49$
$= 31 + 18$
$\equiv 18 \pmod{31}$

$\rightarrow 17^{16} \equiv 18^2$
$= 324$
$= 31 \cdot 10 + 14$
$\equiv 14 \pmod{31}$

$16+8+4+1=29$

$$17^{29} = 17^{16} \cdot 17^{8} \cdot 17^{4} \cdot 1 \cdot 17^{1}$$
$$\equiv 14 \cdot 18 \cdot 7 \cdot 17$$
$$= 34 \cdot 49 \cdot 18$$
$$\equiv 3 \cdot 18 \cdot 18 \quad (\text{mod } 31)$$
$$\equiv 54 \cdot 18 \equiv 23 \cdot 18 \equiv 46 \cdot 9 \equiv 15 \cdot 9$$
$$\equiv 45 \cdot 3 \equiv 14 \cdot 3 \equiv 42 \equiv \boxed{11}$$

So inverse of 17 modulo 31 is 11

(d) Let $k=34$, $n=83$.

Since $\gcd(n,k)=1$ and n is prime, $k^{n-1} \equiv 1 \pmod{n}$
(from Euler's Thm)

$$\Rightarrow 34^{82} \equiv 1 \pmod{83}$$

$$82248 = 1003 \cdot 82 + 2$$

$$34^{82248} \equiv 34^{1003 \cdot 82} \cdot 34^{2} \equiv 1^{1003} \cdot 34^{2} \pmod{83}$$
$$= 1159$$
$$\equiv 77 \pmod{83}$$

$\therefore \text{rem}(34^{82248}, 83) = 77$

2(a) If $a | b$, then $\forall c$, $a | bc$

$a | b \Rightarrow b$ can be represented as a multiple of a

$$b = ka \Rightarrow bc = kac = (kc)a$$

$\therefore a | bc$ since bc can be written as a multiple of a

(b) If $a | b$ and $a | c$, then $a | sb + tc$

$a | b \Rightarrow b = k_1 a$, $a | c \Rightarrow c = k_2 a$

$sb + tc = sk_1 a + tk_2 a = (sk_1 + tk_2) a$

$\therefore a | sb + tc$

(c) $\forall c$, $a | b \Leftrightarrow ca | cb$

$a | b \Leftrightarrow b = ka \Leftrightarrow cb = kac = k(ca)$

$\therefore ca | cb$ since sb can be written as a multiple of ca.

(d) $\gcd(ka, kb) = k \gcd(a, b)$

$\gcd(x, y) \Rightarrow$ small linear combination (+) of x and y

$\gcd(ka, kb) = s(ka) + t(kb) \leftarrow$ smallest
$= k(sa + tb)$
$\hookrightarrow$ need to prove $sa + tb = \gcd(a, b)$

Pf (by contradiction)

Assume $sa + tb$ is not the $\gcd(a,b)$, then $\exists_{s',t'}$ s.t. $s'a + t'b = \gcd(a,b)$

But $\therefore$ $s'a + t'b < sa + tb \Rightarrow$
$s'(ka) + t'(kb) < s(ka) + t(kb)$

But $s(ka) + t(kb)$ is the smallest linear combination of (ka) and (kb) $[\gcd(ka, kb)]$. $\times$

So, $sa + tb = \gcd(a,b)$

$\therefore$ ~~gcd(ka~~ $\gcd(ka, kb) = k\gcd(a,b)$

3.(a) $x^2 \equiv y^2 \pmod p \Leftrightarrow x \equiv y \pmod p$ or $x \equiv -y \pmod p$

$x^2 \equiv y^2 \pmod p \Leftrightarrow p \mid (x^2 - y^2)$

$p \mid (x-y)(x+y) \Leftrightarrow p \mid (x+y)$ OR $p \mid (x-y)$

$\Leftrightarrow$ ~~or~~ $x \equiv -y \pmod p$ OR $x \equiv y \pmod p$

(b) If n is a square modulo p then $n^{\frac{p-1}{2}} \equiv 1 \pmod p$

$n \equiv x^2 \pmod p$

Consider $x \in \{0, 1, 2, \dots, p-1\}$,

Since p is prime, $\phi(p) = p-1$

By Fermat's theorem,

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

$$\Rightarrow \quad (x^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$$

$$\Rightarrow \quad n^{\frac{p-1}{2}} \equiv 1 \pmod p$$

(c) $p \equiv 3 \pmod 4$

By defn; $p-3 = 4k \Rightarrow p = 4k-3$

$\rightarrow \quad \frac{p-3}{4} = k$

By Euler's criterion,

$$n^{\frac{p-1}{2}} \equiv 1 \pmod p$$

$$\Rightarrow n^{\frac{4k+2}{2}} \equiv 1 \pmod p \Rightarrow n^{2k+1} \equiv 1 \pmod p$$

Multiply both sides by n,

$$n^{2k+2} \equiv n \pmod p \Rightarrow (n^{k+1})^2 \equiv n \pmod p$$

So, a possible value for x is,

$$x = n^{k+1} = n^{\frac{p-3}{4}+1} = \boxed{n^{\frac{p+1}{4}}}$$

4. $\phi(p^k) = p^k - p^{k-1}$

$\phi(n) \rightarrow$ ~~All no~~ Count of all numbers $\in \{1, \dots, n-1\}$ that are relatively prime to n, $\gcd(x, n) = 1$

Since, p is prime, $\phi(p) = p - 1$

$\phi(p^k) = (p^k - 1) - [\text{all no. that divide } p^k]$

$\because$ p is prime, only the multiples of p divide p^k. Prime factors of p^k are $(1, p)$

$\overbrace{1p \quad 2p}^{p} \cdots p^k = (p^{k-1})p$ Largest Multiple in the interval $= p^{k-1} - 1$

$\therefore$ There are $p^{k-1} - 1$ multiples of p in the range $(1, p^k - 1)$.

$\phi(p^k) = (p^k - 1) - (p^{k-1} - 1) = \underline{\underline{p^k - p^{k-1}}}$

5 (a) (by induction)

$P(n)$:= Every no. on the board after n steps is either x, y, ~~or~~ a positive divisor of $\gcd(x, y)$

Base Case : $P(0)$, The only nos on the boards are x and y itself ✓

Inductive Step: Assume $P(n)$, prove $P(n+1)$

Let the new no. added be m, and a, b are the numbers from which m is derived. There are two cases:

$\hookrightarrow m | a$ and $m | b$

(i) $a = x$ and $b = y$

~~Since~~ $m | a \Rightarrow \underset{x}{\underset{\shortparallel}{a}} = mk$, $m | b \Rightarrow \underset{y}{\underset{\shortparallel}{b}} = ml$

$g = \gcd(x, y) = sx + ty$

$g = s(mk) + t(ml) = m(sk + tl)$

$\therefore m | g$

(ii) $a \neq x$ or $b \neq y$

$m | a$ and $a | g \Rightarrow m | g$

$\hookrightarrow$ from $P(n)$ OR

$m | b$ and $b | g \Rightarrow m | g$

$\therefore P(n+1)$ is true $\square$

(b) (by contradiction)

Suppose a divisor d of $\gcd(x, y)$ ~~doe~~ is not on the board at the end of the game.

But ~~d~~ since $\gcd(x, y) | x$ and $\gcd(x, y) | y$, $d | x$ and $d | y$, so, the game is not yet over since another term can be added. $\times$.

(c) Let D be the no. of divisors of $\gcd(x,y)$

NOTE - boundary condition,
if $\gcd(x,y) = x$, or $\gcd(x,y) = y \Rightarrow D-1$
divisors in total

Choose your turn based on the parity of the no. of divisors.
If even, then you go second, $\because \div w$
If odd, then you go first $\because \div w$

6. (a) (by contradiction)

Assume set of all prime nos. $F = \{p_1, \dots, p_k\}$ is finite

Consider $n = p_1 p_2 \dots p_k + 1$

$$\forall p \in F, \quad n \equiv 1 \pmod p$$

So n is not divisible by any ps in F. So no prime factors of n exist. That means the only factors of n are $\{1, n\}$ itself. $\Rightarrow$ n is prime

But since $n \notin F$, the assumption is wrong X.

$\therefore$ There are an infinite no. of prime nos.

(b) if p is an odd prime, then $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$

By division thm,

$p = 4q + r, \quad 0 \leq r \leq 3$

if $r \mid 2$, then $p \mid 2$, but p is odd so $r \nmid 2$.

$\therefore p = 4q + \{1, 3\} \Rightarrow p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$

(c) (by contradiction)

if $n \equiv 3 \pmod 4$, assume $p \not\equiv 3 \pmod 4$ for all prime factors p

Then $p = 2$ or $p \equiv 1 \pmod 4$ (from (b))

$p \neq 2$, since $n \equiv 3 \pmod 4 \Rightarrow n$ is odd

So $\forall p, \; p \equiv 1 \pmod 4$

$$\left.\begin{array}{l} p_1 \equiv 1 \\ p_2 \equiv 1 \\ \vdots \equiv 1 \\ p_k \equiv 1 \end{array}\right\} \times \Rightarrow p_1 \cdot p_2 \cdot p_3 \cdots p_k \equiv 1 \Rightarrow n \equiv 1 \pmod 4$$

But $n \equiv 3 \pmod 4$ $\times$

Thus, $\exists p$ (prime factor of n) st. $p \equiv 3 \pmod 4$.

(d) (by contradiction)

Assume F is finite i.e. $F = \{p_1, p_2, \dots p_k\}$

Consider $n = 4p_1p_2 \cdots p_k - 1$

$n \equiv -1 \pmod 4$

and $-1 \equiv 3 \pmod 4$

$\Rightarrow n \equiv 3 \pmod 4$

From (c), n has a prime factor $p_i \in F$

So $\forall p$, $p \mid n \Rightarrow n \equiv 0 \pmod p$

But since $n = 4(p_1 \cdots p_k) - 1$

$n \equiv -1 \pmod p \longrightarrow \times$

$\therefore$ Set F in infinite, i.e. There are infinite no. of primes p s.t. $p \equiv 3 \pmod 4$ $\square$

$\times$