Problem 1. [16 points] **Warmup Exercises**

For the following parts, a correct numerical answer will only earn credit if accompanied by it's derivation. Show your work.

(a) [4 pts] Use the Pulverizer to find integers s and t such that $135s + 59t = \gcd(135, 59)$.

(b) [4 pts] Use the previous part to find the inverse of 59 modulo 135 in the range $\{1, \ldots, 134\}$.

(c) [4 pts] Use Euler's theorem to find the inverse of 17 modulo 31 in the range $\{1, \ldots, 30\}$.

(d) [4 pts] Find the remainder of 34^{82248} divided by 83. (*Hint: Euler's theorem.*)

a) $\gcd(135,59) = \gcd(59, \text{rem}(135,59))$
$= \gcd(17, \text{rem}(59,17))$
$\gcd(8, \text{rem}(17,8))$
$\gcd(8,1) = 1$..

$135 - 2\cdot 59 = 17$
$59 - 17\cdot 3 = 59 - (135 - 2\cdot 59)\cdot 3$
$= 59 - 135\cdot 3 - 2\cdot 59$
$= -135\cdot 3 + 59\cdot 7 = 8.$

$1 = \text{rem}(17,8) = 17 - 2\cdot 8$
$= 135 - 2\cdot 59$
$-2(59\cdot 7 - 135\cdot 3)$
$= 135 - 2\cdot 59 - 14\cdot 59 + 6\cdot 135$
$= 7\cdot 135 - 16\cdot 59 = 1$

$\Rightarrow \gcd(135,59) = 135\cdot 7 - 59\cdot 16$ //

b) $59\cdot k \equiv 1 \bmod 135$
$\Rightarrow 135 \mid 59\cdot k - 1$

Since $\gcd(135,59) = 1$, and $135\cdot 7 - 59\cdot 16 = 1$.
$135\cdot 7 = 1 + 59\cdot 16$
$\Rightarrow 59\cdot(-16) - 1 \mid 135$
$\Rightarrow 59\cdot(-16) \equiv 1 \bmod 135$
$\Rightarrow -16$ is an inverse of 59.

$59\cdot k - (135\cdot 7 - 59\cdot 16)$
$59\cdot k + 59\cdot 16 - 135\cdot 7$
$59(16 + k) - 135\cdot 7$
$\Rightarrow 135 \mid 16 + k.$
$\Rightarrow k = 135 - 16 = 119$ //

Ans: 119.

c) $17\cdot k \equiv 1 \bmod 31$
Euler's theorem states that $17^{\phi(31)} \equiv 1 \bmod 31$
$\Rightarrow 17\cdot 17^{\phi(31)-1} \equiv 1 \bmod 31$
$\phi(31) = 30$ since 31 is prime.
$\Rightarrow 17^{29}$ is an inverse of 17 mod 31.
Inverse of 17 mod 31 $\Rightarrow 17\cdot k \equiv 1 \bmod 31$
$\Rightarrow 31 \mid 17\cdot k - 1$

$17^{29}\cdot 17 \equiv 1 \bmod 31$
$17^{29} \equiv \text{rem}(17^{29}, 31) \bmod 31$
$\Rightarrow 17\cdot \text{rem}(17^{29}, 31) \equiv 1 \bmod 31$

$rem(17^{29}, 31)$

$a \equiv rem(a,n) \bmod n$
since $n | a - (a - kn)$
$n | a + ka - n$
$n | a(1+k) - n$
$\Rightarrow n | a(1+k)$

$17^2 = 289$
$= 31 \times 9 + 10$
$17^4 = (31 \times 9 + 10)^2$
$= 31^2 \times 81 + 20 \cdot 31 \times 9 + 100$
$= 31^2 \times 81 + 180 \times 31 + 100$
$= 31(31 \times 81 + 180) + 100$
$= 31(31 \times 81 + 180) + 31 \times 3 + 7$
$= 31(31 \times 81 + 183) + 7.$

17^8: $rem(17^8, 31) = 7^2 - 31 = 18.$
17^{16}: $rem(17^{16}, 31) = 18^2 - 310 = 14$

$17^2 = 289 \equiv 10 \bmod 31$
$17^4 = 17^2 \cdot 17^2 \equiv 10 \cdot 10 \bmod 31$
$17^4 \equiv 100 \bmod 31$
$\equiv 7 \bmod 31$
$\Rightarrow 17^4 \equiv 7 \bmod 31$

$17^8 = 17^4 \cdot 17^4 \equiv 7 \cdot 7 \bmod 31$
$= 49 \bmod 31$
$\equiv 18 \bmod 31$
$\Rightarrow 17^8 \equiv 18 \bmod 31$

$17^{16} = 17^8 \cdot 17^8 \equiv 18 \cdot 18 = 324 \bmod 31$
$\equiv 14 \bmod 31$

$17^{29} = 17^{16} \cdot 17^8 \cdot 17^4 \cdot 17$
$\equiv 252 \cdot 17^4 \cdot 17 \bmod 31$
$\equiv 4 \cdot 17 \cdot 17^4 \bmod 31$
$\equiv 4 \cdot 7 \cdot 17 \bmod 31$
$\equiv 4 \cdot 26 \bmod 31$
$\equiv 11 \bmod 31$

$\Rightarrow 17^{29} \equiv 11 \bmod 31$

Since $17^{29} \cdot 17 \equiv 1 \bmod 31$ and $17^{29} \equiv 11$
$11 \cdot 17 \equiv 1 \bmod 31$

$\Rightarrow$ 11 is an inverse of 17.

d) $\text{rem}(34^{82248}, 83) \Rightarrow 34^{82248} \equiv k \mod 83$

83 is prime $\Rightarrow 34^{82} \equiv 1 \mod 83.$

$\Rightarrow 34^{82000} \equiv 1 \mod 83$

$\Rightarrow 34^{82246} \equiv 1 \mod 83$

$34^{82247} \equiv 34 \mod 83$

$34^{82248} \equiv 34 \cdot 34 \mod 83$

$\equiv 77 \mod 83$

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

Problem 2. [**16 points**]

Prove the following statements, assuming all numbers are positive integers.

(a) [4 pts] If $a \mid b$, then $\forall c$, $a \mid bc$

(b) [4 pts] If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$.

(c) [4 pts] $\forall c$, $a \mid b \Leftrightarrow ca \mid cb$

(d) [4 pts] $\gcd(ka, kb) = k \gcd(a, b)$

a) If $a \mid b$, then $b = ka$.

$bc = kac$

$= a(kc)$

$\Rightarrow a$ is a factor of bc

$\Rightarrow a \mid bc.$

$\square.$

b) $a \mid b$ and $a \mid c$

Let $b = ka$, $c = ma$

$sb + tc = ska + tma = a(sk + tm)$

$\Rightarrow a \mid sb + tc$

$\square.$

Problem 3. [**20 points**] In this problem, we will investigate numbers which are squares modulo a prime number p.

(a) [5 pts] An integer n is a square modulo p if there exists another integer x such that $n \equiv x^2 \pmod p$. Prove that $x^2 \equiv y^2 \pmod p$ if and only if $x \equiv y \pmod p$ or $x \equiv -y \pmod p$. (*Hint:* $x^2 - y^2 = (x + y)(x - y)$)

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

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

$\Leftrightarrow x \equiv y \mod p \vee x \equiv -y \mod p.$

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

<u>Pf:</u> If n is square modulo p, then $n \equiv x^2 \mod p$

$$\Rightarrow n^{\frac{1}{2}} \equiv \pm x \mod p$$

$$\Rightarrow n^{\frac{1}{2}} \equiv x \mod p \quad \text{or} \quad n^{\frac{1}{2}} \equiv -x \mod p$$

For case where $p \mid n$, $p \mid n - x^2$

$$p \mid pk - x^2$$

$$\Rightarrow p \mid x$$

$\Rightarrow$ Euler's theorem does not apply to x.

If $p \nmid n$, then $p \nmid x \Rightarrow x^{p-1} \equiv 1 \mod p$

$$\Rightarrow n^{\frac{1}{2}(p-1)} \equiv x^{p-1} \mod p \quad \text{for} \quad n^{\frac{1}{2}} \equiv x \mod p$$

$$\Rightarrow n^{\frac{1}{2}(p-1)} \equiv 1 \mod p.$$

For $n^{\frac{1}{2}} \equiv -x \mod p$

$$n^{\frac{1}{2}(p-1)} \equiv (-x)^{p-1} \mod p$$
$$= (-1)^{p-1} x^{p-1}$$

$$n^{\frac{1}{2}(p-1)} \equiv (-1)^{p-1} x^{p-1}$$
$$\equiv (-1)^{p-1} \cdot 1$$
$$\equiv (-1)^{p-1}$$
$$\equiv 1$$ since p cannot be even except for 2.

Thus, if $n \equiv x^2 \mod p$,

$n^{\frac{1}{2}} \equiv x$ or $n^{\frac{1}{2}} \equiv -x \mod p$

$\Rightarrow n^{\frac{1}{2}(p-1)} \equiv 1 \mod p$ for both cases.

Therefore, $n \equiv x^2 \mod p \Leftrightarrow n^{\frac{1}{2}(p-1)} \equiv 1 \mod p$.

(c) [10 pts] Assume that $p \equiv 3 \pmod 4$ and $n \equiv x^2 \pmod p$. Given n and p, find one possible value of x. (*Hint: Write p as $p = 4k+3$ and use Euler's Criterion. You might have to multiply two sides of an equation by n at one point.*)

$p = 4k+3.$

$n \equiv x^2 \pmod p$

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

$n^{\frac{4k+3-1}{2}} = n^{\frac{4k+2}{2}} = n^{2k+1} \equiv 1 \bmod p$

$n \cdot n^{2k} \equiv 1 \bmod p$

$\Rightarrow x^2 \cdot n^{2k} \equiv 1$

$(xn^k)^2 \equiv 1 \bmod p$

$xn^k \equiv 1 \bmod p$ or $xn^k \equiv -1 \bmod p$

$x \cdot x^{2k} \equiv 1$

$x^{2k+1} \equiv 1$

$\Rightarrow x = 1.$

$n \equiv x^2 \Rightarrow n^k \equiv x^{2k}$

$n^{2k+2} \equiv n \bmod p$

$\Rightarrow n^{2k+2} \equiv x^2 \bmod p$

$\Rightarrow n^{k+1} \equiv x \bmod p$

$\Rightarrow x = n^{k+1}$

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

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

$= n^{\frac{p-3+4}{4}}$

$= n^{\frac{p+1}{4}}$

$(n^{k+1})^{2k+1}$

$= n^{(k+1)(2k+1)}$

$\equiv x$

Problem 4. [**10 points**] Prove that for any prime, p, and integer, $k \geq 1$,

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

where ϕ is Euler's function. (*Hint: Which numbers between 0 and* $p^k - 1$ are *divisible by* p*? How many are there?*)

$\phi(p^k)$. Between 1 to $p^k - 1$, there are

$$p, 2p, 3p, \ldots p^2, 2p^2, \ldots p^3, \ldots p^k$$

$$\Rightarrow \quad (1, 2, 3 \ldots, (p-1)) = \frac{(p-1+1)p}{2}$$

$$= \frac{p^2}{2}.$$

$$\frac{p^2}{2}k.$$

$p^k -$

$$p^2 \quad (p+1)p \quad (p+2)p \cdot \ldots \; 2p \cdot p \quad (2p+1)p \quad \ldots$$
$$(p^2-1)p \quad p^3 \ldots (p^2+1)p \ldots (p^3-1)p + \ldots$$
$$(p^{k-2}+1)p \quad \ldots \quad (p^{k-1}-1)p$$

$$p^k - 1 - (p^{k-1} - 1) = p^k - 1 - p^{k-1} + 1$$
$$= p^k - p^{k-1} \quad //$$

Problem 5. [**18 points**] Here is a *very, very fun* game. We start with two distinct, positive integers written on a blackboard. Call them x and y. You and I now take turns. (I'll let you decide who goes first.) On each player's turn, he or she must write a new positive integer on the board that is a common divisor of two numbers that are already there. If a player can not play, then he or she loses.

For example, suppose that 12 and 15 are on the board initially. Your first play can be 3 or 1. Then I play 3 or 1, whichever one you did not play. Then you can not play, so you lose.

(a) [6 pts] Show that every number on the board at the end of the game is either x, y, or a positive divisor of $\gcd(x, y)$.

(b) [6 pts] Show that every positive divisor of $\gcd(x, y)$ is on the board at the end of the game.

(c) [6 pts] Describe a strategy that lets you win this game every time.

Let $P(n) ::=$ For turn n, the number played is a divisor of $\gcd(x, y)$.

By induction,
Base case: $P(1)$. For turn 1, the numbers x, y are on the board, hence the number played must divide both x, y. Let all divisors of both x, y be $d_i \in D$, where D is the set of all common divisors.

We now show that $\forall d_i \in D$, $d_i \mid \gcd(x, y)$.

Let $\gcd(x, y) = sx + ty$, where $s, t \in \mathbb{Z}$.
Since $d_i \mid x$ and $d_i \mid y$, $\frac{sx+ty}{d_i} = s\frac{x}{d_i} + t\frac{y}{d_i} \Rightarrow d_i \mid sx+ty$

$$\Rightarrow d_i \mid \gcd(x, y).$$

$\therefore \forall d_i \in D$ are divisors of $\gcd(x, y)$.

Hence, the number played, $d_i \in D$, is a divisor of $\gcd(x,y)$

Assume $p(n)$ is true for n,
Let $1 \le k \le n$,
Inductive step: $p(k+1)$: At turn k, all numbers on the board are x, y and divisors of $\gcd(x,y)$
By cases on the 2 numbers chosen to divide,
$x, y \Rightarrow$ players pick $d_i \in D \Rightarrow$ divisor of $\gcd(x,y)$
x, d_i or $y, d_i \Rightarrow$ By symmetry, we analyse x, d_i WLOG with y, d_i.

Let $k \in \mathbb{N}$, since $k | d_i$, k also can divide x.
$\Rightarrow k | \gcd(x,y)$ since $\gcd(x,y) = d_1 d_2, \ldots d_i, \ldots d_m$

$\Rightarrow k$ must be a divisor of $\gcd(x,y)$.

Between d_i, d_j we can use the same argument as before for x, d_i.

Hence, for turn $k+1$, the number added must also be a common divisor of $\gcd(x,y)$.

$\therefore$ Since $p(n)$ is true for 1 and $k+1$, $p(n)$ is true for $\forall n \in \mathbb{N}$.

Therefore, all numbers on the board are x, y and divisors of $\gcd(x,y)$.
$\square$.

b) From above, we showed that for each turn, we must play a divisor of $\gcd(x,y)$.
D, the set of common divisors is finite. Hence, the turn ends when no divisor of $\gcd(x,y)$ can be placed.

For this to happen, all elements in D must be placed on the board.
Hence, all positive divisors of $\gcd(x,y)$ must be on the board.
$\square$.

c) To win the game, break down the $\gcd(x,y)$ into a product of primes. Sum up all its powers. e.g $2^3 \cdot 5^4 \cdot 7^7 \cdot a^1 \Rightarrow 3+4+7+1$.
Let this value be n.
Calculate the total combinations $\sum_{k=0}^{n} \binom{n}{k} = 2^n \Rightarrow$ there are 2^n divisors

Since the number of divisors of $\gcd(x,y)$ is 2^n

Hence, to win, the player must always choose to start 2nd, unless x and y are relatively prime, in which case the player must start first.
$\square$.