Problem Set 3 Solutions

Due: Monday, September 27 at 7:00 PM

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

Solution.

$$\begin{array}{llrcl}
x & y & \text{rem}(x, y) & = & x - q \cdot y \\
\hline
135 & 59 & 17 & = & 135 - 2 \cdot 59 \\
59 & 17 & 8 & = & 59 - 3 \cdot 17 \\
 & & & = & 59 - 3 \cdot (135 - 2 \cdot 59) \\
 & & & = & -3 \cdot 135 + 7 \cdot 59 \\
17 & 8 & 1 & = & 17 - 2 \cdot 18 \\
 & & & = & (135 - 2 \cdot 59) - 2 \cdot (-3 \cdot 135 + 7 \cdot 59) \\
 & & & = & \boxed{7 \cdot 135 - 16 \cdot 59} \\
2 & 1 & 0 & &
\end{array}$$

Exam tip: *Each time rem(x, y) is calculated, substitutions are immediately made to then express it as a linear combination of 135 and 59 (using the remainders calculated on previous lines). Simplifying at each step leads to a much faster computation of s and t.* ■

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

Solution. 119

From part (a), $1 = 7 \cdot 135 - 16 \cdot 59$ and so $1 \equiv -16 \cdot 59 \pmod{135}$. Therefore -16 is *an* inverse of 59. However, it is not the *unique* inverse of 59 in the range $\{1, \ldots, 134\}$, which is given by $\text{rem}(-16, 135) = 119$. One can easily check this by multiplication. ■

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

Solution. 16

Since 31 is prime, Euler's theorem implies $17^{31-2} \cdot 17 \equiv 1 \pmod{31}$ and so $\operatorname{rem}(17^{31-2}, 31)$ is the inverse of 17 in the range $\{1, \ldots, 30\}$. Using the method of repeated squaring,

$$\begin{aligned}
17^2 &= 289 \\
&= 9 \cdot 31 + 10 \\
&\equiv 10 \\
\\
17^4 &\equiv 10^2 \\
&= 100 \\
&= 3 \cdot 31 + 7 \\
&\equiv 7 \\
\\
17^8 &\equiv 7^2 \\
&= 49 \\
&= 31 + 18 \\
&\equiv 18 \\
\\
17^{16} &\equiv 18^2 \\
&= 324 \\
&\equiv 14 \\
\\
17^{29} &= 17^{16} \cdot 17^8 \cdot 17^4 \cdot 17^1 \\
&\equiv 14 \cdot 18 \cdot 7 \cdot 17 \\
&= (2 \cdot 7) \cdot (3 \cdot 6) \cdot 7 \cdot 17 \\
&= (2 \cdot 17) \cdot (7 \cdot 6) \cdot (3 \cdot 7) \\
&\equiv 3 \cdot 11 \cdot 21 \\
&\equiv 2 \cdot 21 \\
&= 42 \\
&\equiv \boxed{11}
\end{aligned}$$

where the modulus for each of the congruences is 31. ■

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

Solution. 77

Since $34 = 2 \cdot 17$ and 83 are relatively prime, Euler's theroem implies that $34^{\phi(83)} \equiv 1 \pmod{83}$ where

$$\phi(83) = 82$$

Now, notice that $82248 = 82 \cdot 1003 + 2$. But then, this implies that

$$\begin{aligned} 34^{82248} &= 34^2 \cdot 34^{1003 \cdot 82} \\ &\equiv 34^2 \cdot 1^{1003} \pmod{83} && \text{(by Euler's Theorem)} \\ &= 1156 \\ &\equiv 77 \pmod{83} \end{aligned}$$

■

Problem 2. [16 points]

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

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

Solution. If $a \mid b$, then there is some positive integer k such that $b = ak$. But then, $bc = akc = a(kc)$, which is a multiple of a. ■

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

Solution. If $a \mid b$, then there is some positive integer j such that $b = aj$. Similarly, there is some positive integer k such that $c = ak$. But then, we can rewrite the right side as $s(aj) + t(ak)$. But we can rewrite this as $a(js) + a(kt) = a(js + kt)$, which is a multiple of a. ■

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

Solution. If $a \mid b$, then there is some positive integer k such that $b = ak$. But then, we can rewrite $cb = c(ak) = ca(k)$, which is a multiple of ca. So the implication is true. ■

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

Solution. Let s, t be coefficients so that $s(ka) + t(kb) = \gcd(ka, kb)$. We can factor out the k so that $\gcd(ka, kb) = k(sa + tb)$. We now argue that $sa + tb = \gcd(a, b)$. Suppose it were not. Then, there is some smaller positive linear combination of a, b with coefficients s' and t' so that $s'a + t'b = \gcd(a, b)$. But then, if we multiply this by k, we find that $0 < ks'a + kt'b = s'(ka) + t'(kb) < s(ka) + t(kb) = \gcd(ka, kb)$. This is a contradiction with the definition of the gcd, so $sa + tb = \gcd(a, b)$, and we can conclude that $\gcd(ka, kb) = k \gcd(a, b)$. ■

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:* $x^2 - y^2 = (x + y)(x - y)$)

Solution. $x^2 \equiv y^2 \pmod{p}$ iff $p \mid x^2 - y^2$. But $x^2 - y^2 = (x-y)(x+y)$, and since p is a prime, this happens iff either $p \mid x - y$ or $p \mid x + y$, which is iff $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$. ■

(b) [5 pts] There is a simple test we can perform to see if a number n is a square modulo p. It states that

Theorem 1 (Euler's Criterion)**.** *:*

1. *If n is a square modulo p then $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*
2. *If n is not a square modulo p then $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

Prove the first part of Euler's Criterion. (*Hint: Use Fermat's theorem.*)

Solution. If n is a square modulo p, then there exists an x such that $x^2 \equiv n(modp)$. Consequently,

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

by Fermat's theorem. ■

(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.*)

Solution. From Euler's Criterion:

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

We can write $p = 4k+3$, so $\frac{p-1}{2} = \frac{4k+3-1}{2} = k+1$. As a result, $n^{2k+1} \equiv 1 \pmod{p}$, so $n^{2k+2} \equiv n \pmod{p}$. This can be rewritten as $\left(n^{k+1}\right)^2 \equiv n \pmod{p}$, so

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

is one possible value of 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?*)

Solution. The numbers in the interval from 0 to $p^k - 1$ that are divisible by p are all those of the form mp. For mp to be in the interval, m can take any value from 0 to $p^{k-1} - 1$ and no others, so there are exactly p^{k-1} numbers in the interval that are divisible by p. Now $\phi(p^k)$ equals the number of remaining elements in the interval, namely, $p^k - p^{k-1}$. ■

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 $\gcd(x, y)$.

Solution. We use induction. Let $g = \gcd(x, y)$. Let our inductive hypothesis be $P(n) =$ "After n moves, every number on the board is either x, y, or a positive divisor of g." For $n = 0$, only x and y are on the board, so $P(0)$ holds. For the inductive case, after $n + 1$ moves the numbers on the board are the same as the numbers after n moves plus an additional positive integer m which is a divisor of two numbers a and b which were already on the board. We must show that m is either x, y, or a positive divisor of g. We know m cannot be equal x or y because it must be a new number, and we know m is positive, so we have to show that $m|g$. We will consider two cases:

1. $a = x$ and $b = y$
   In this case, $m|a$ and $m|b$, so $a = km$ and $b = lm$ for some integers k and l. We know we can write g as a linear combination of a and b:
   $$sa + tb = g.$$
   Substituting the expressions for for a and b, we obtain
   $$skm + tlm = g,$$
   which means $m(sk + tl) = g$, so $m|g$ and $P(n + 1)$ holds.
2. $a \neq x$ or $b \neq y$
   In this case, by inductive assumption $a|g$ or $b|g$. Assume that $a|g$. Then $m|a$ and $a|g$, so $m|g$. If on the other hand $a \not| g$ then $b|g$ and $m|b$, so $m|g$. Again, $P(n + 1)$ holds.

By induction, 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.

Solution. Proof by contradiction. Assume there is a number d such that $d|gcd(x, y)$ and d is not on the board at the end of the game. Since $d|gcd(x, y)$ and $gcd(x, y)|x$ and $gcd(x, y)|y$, therefore $d|x$ and $d|y$. But x and y are on the board, so it is possible to add d to the board. This means the game is not over yet! We have reached a contradiction, so d must be on the board. This is true for all positive divisors of $gcd(x, y)$, so all of them must be on the board. ■

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

Solution. We showed that x, y, and all positive divisors of $gcd(x, y)$ and only those numbers will be on the board at the end of the game. Let D be the number of positive divisors of $gcd(x, y)$. If $x = gcd(x, y)$ or $y = gcd(x, y)$, then $D - 1$ values will be added to the board before the game ends. Otherwise, D values will be added. You can calculate the number of values to be placed and if this number is odd, decide to go first. Otherwise, decide to go second.

■

Problem 6. [20 points] In one of the previous problems, you calculated square roots of numbers modulo primes equivalent to 3 modulo 4. In this problem you will prove that there are an infinite number of such primes!

(a) [6 pts] As a warm-up, prove that there are an infinite number of prime numbers. (*Hint: Suppose that the set F of all prime numbers is finite, that is $F = \{p_1, p_2, \ldots, p_k\}$ and define $n = p_1 p_2 \ldots p_k + 1$.*)

Solution. By contradiction. Suppose that F is finite. Let it be $F = \{p_1, p_2, \ldots, p_k\}$ and define $n = p_1 p_2 \ldots p_k + 1$. For every $p \in F$,

$$n \equiv 1 \pmod{p}.$$

Consequently, $\forall p \in F$, $p \not| n$. But the numbers in F are all the prime numbers, so it must be that for all primes p, $p \not| n$. As a result, n does not have a prime factor smaller than itself, so n is a prime number! But n is definitely larger than any number in F, so $n \notin F$. This is a contradiction. The initial assumption that F is finite is false. ■

(b) [2 pts] Prove that if p is an odd prime, then $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$.

Solution. By the division theorem, there exist integers x and r with $0 \leq r \leq 3$ such that $p = 4x + r$. If $2|r$, then $2|p$. Since p is odd, $2 \not| r$. So, $r = 1$ or $r = 3$. ■

(c) [6 pts] Prove that if $n \equiv 3 \pmod{4}$, then n has a prime factor $p \equiv 3 \pmod{4}$.

Solution. By contradiction. Suppose the contrary that $n \equiv 3 \pmod{4}$ and that, for all primes $p|n$, $p \not\equiv 3 \pmod{4}$. By part b, if prime $p \not\equiv 3 \pmod{4}$, then $p = 2$ or $p \equiv 1 \pmod{4}$. Since $n \equiv 3 \pmod{4}$, n is odd and $2 \not| n$. So, by the fundamental theorem in arithmetic, n is a product of primes p with $p \equiv 1 \pmod{4}$. This means that $n \equiv 1 \pmod{4}$. This contradicts the original assumption that $n \equiv 3 \pmod{4}$. ■

(d) [6 pts] Let F be the set of all primes p such that $p \equiv 3 \pmod{4}$. Prove by contradiction that F has an infinte number of primes.

(*Hint: Suppose that F is finite, that is $F = \{p_1, p_2, \ldots, p_k\}$ and define $n = 4p_1 p_2 \ldots p_k - 1$. Prove that there exists a prime $p_i \in F$ such that $p_i | n$.*)

Solution. By contradiction. Suppose that F is finite. Let it be $F = \{p_1, p_2, \dots, p_k\}$ and define $n = 4p_1p_2 \dots p_k - 1$. Notice that F is not empty since $3 \in F$. This shows that n is at least 0. By part c, $n = 4x - 1$ has a prime factor $p_i \in F$ such that $p_i | n$. So, $n \equiv 0 \pmod{p_i}$. Also, $n = 4p_1p_2 \dots p_k - 1 = yp_i - 1$. This means $n \equiv -1 \pmod{p_i}$. This is a contradiction. The initial assumption that F is finite is false. ■