Problem Set 3 Solutions

Due: Monday, September 26

Reading Assignment: Sections 4.0-4.3, 4.5, 4.6

Problem 1. [18 points]

(a) [4 pts] Use the Pulverizer to find integer values of x, y that satisfy $71x + 50y = 1$. What is the inverse of 71 modulo 50 (Write the inverse as a number in the set $\{1, 2, \ldots, 49\}$?

Solution.

$$
\begin{array}{cc r c l}
x & y & \text{rem}(x,y) & = & x - q \cdot y \\
\hline
71 & 50 & 21 & = & 71 - 1 \cdot 50 \\
50 & 21 & 8 & = & 50 - 2 \cdot 21 \\
 & & & = & 50 - 2 \cdot (71 - 1 \cdot 50) \\
 & & & = & -2 \cdot 71 + 3 \cdot 50 \\
21 & 8 & 5 & = & 21 - 2 \cdot 8 \\
 & & & = & (71 - 1 \cdot 50) - 2 \cdot (-2 \cdot 71 + 3 \cdot 50) \\
 & & & = & 5 \cdot 71 - 7 \cdot 50 \\
8 & 5 & 3 & = & 8 - 5 \\
 & & & = & (-2 \cdot 71 + 3 \cdot 50) - (5 \cdot 71 - 7 \cdot 50) \\
 & & & = & -7 \cdot 71 + 10 \cdot 50 \\
5 & 3 & 2 & = & 5 - 3 \\
 & & & = & (5 \cdot 71 - 7 \cdot 50) - (-7 \cdot 71 + 10 \cdot 50) \\
 & & & = & 12 \cdot 71 - 17 \cdot 50 \\
3 & 2 & 1 & = & 3 - 2 \\
 & & & = & (-7 \cdot 71 + 10 \cdot 50) - (12 \cdot 71 - 17 \cdot 50) \\
 & & & = & \boxed{-19 \cdot 71 + 27 \cdot 50} \\
2 & 1 & 0 & &
\end{array}
$$

Hence we have $x = -19, y = 27$. Considering the equation modulo 50, we have that $-19 \cdot 71 \equiv 1 \pmod{50}$. Thus the inverse of 71 mod 50 is 31, as $31 \equiv -19 \pmod{50}$. ■

(b) [4 pts] Use the Pulverizer to find integer values of x, y that satisfy $43x + 64y = 1$. What is the inverse of 64 modulo 43 (Write the inverse as a number in the set $\{1, 2, \ldots, 42\}$?

Solution.

x	y	$\text{rem}(x,y)$	$=$	$x - q \cdot y$
64	43	21	$=$	$64 - 1 \cdot 43$
43	21	1	$=$	$43 - 2 \cdot 21$
			$=$	$43 - 2 \cdot (64 - 43)$
			$=$	$\boxed{-2 \cdot 64 + 3 \cdot 43}$
21	1	0		

Hence we have $x = -2, y = 3$. Considering the equation modulo 43, we have that $-2 \cdot 64 \equiv 1 \pmod{43}$. Thus the inverse of 64 mod 43 is 41, as $41 \equiv -2 \pmod{43}$. ■

(c) [4 pts] Prove that $2 \mid (n)(n+1)$ for all integers n.

Solution. We may solve this problem in cases on whether n is even or odd.

1. If n is even, then $2|n$ so $2|(n)(n+1)$.
2. If n is odd, then let $n = 2k - 1$ for some $k \in \mathbb{Z}$. Then $n + 1 = 2k$, so $2|(n+1)$. Thus, $2|(n)(n+1)$.

■

(d) [6 pts] Prove that $3! \mid (n)(n+1)(n+2)$ for all integers n.

Solution. From part c, we know that $2|(n)(n+1)\ \forall n \in \mathbb{Z}$. Thus, we only need to show that $3|(n)(n+1)(n+2)$. We again solve this problem in cases.

1. Suppose $3|n$. Then $3|(n)(n+1)(n+2)$.
2. Suppose n leaves a remainder 1 when divided by 3, then let $n = 3k+1$ for some $k \in \mathbb{Z}$. Now $n + 2 = 3k + 1 + 2 = 3(k+1)$ and so $3|n+2$. Thus $3|(n)(n+1)(n+2)$.
3. Suppose n leaves a remainder 2 when divided by 3, then let $n = 3k+2$ for some $k \in \mathbb{Z}$. Now $n + 1 = 3k + 2 + 1 = 3(k+1)$ and so $3|n+1$. Thus $3|(n)(n+1)(n+2)$.

■

Although we won't ask you to prove it, this formula from parts c, d actually generalizes to $k! \mid (n)(n+1) \cdot \ldots \cdot (n+k-1)$. As an extra challenge, see if you can prove it yourself.

Problem 2. [20 points] Prove the following statements about divisibility.

(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 $cb = c(ak) = ca(k)$, from which it follows that cb is a multiple of ca. So the implication is true. Conversely, if $ca \mid cb$ then there is some positive integer k such that $cb = cak$. We can cancel c from both sides to conclude that $a \mid b$. ■

(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 $\gcd(ka, kb) = k\gcd(a, b)$. ■

(e) [4 pts] Prove that for integers a, b, c, d and $n \geq 1$, $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$ implies $ac \equiv bd \pmod{n}$.

Solution. We want to show that $n \mid (ac - bd)$ and we know that $n \mid (a - b)$ and $n \mid (c - d)$. Thus we consider $(ac - bd) = (ac - bc) + (bc - bd) = c(a - b) + b(c - d)$. We have that $n \mid c(a - b) + b(c - d)$, and so the claim follows. ■

Problem 3. [22 points] In this problem, we are going to walk through a proof of Wilson's theorem, which states the following:

Theorem 1 (Wilson's Theorem)**.** *If p is a prime number, then $(p - 1)! \equiv -1 \pmod{p}$.*

(a) [2 pts] Verify that Wilson's theorem holds for $p = 2, 3$.

Solution. For $p = 2$, we have that $(2 - 1)! = 1 \equiv -1 \pmod{2}$. For $p = 3$, we have that $(3 - 1)! = 2 \equiv -1 \pmod{3}$. ■

(b) [6 pts] Prove the following theorem about the existence and uniqueness of modular inverses for prime modulos.

Theorem 2. *If p is a prime, show that for all a, if $\gcd(a,\ p) = 1$, then there exists some unique b such that $ab \equiv 1 \pmod{p}$ and $b \in \{1, 2, \ldots p - 1\}$.*

There are two components to this proof (1) to show that such a b exists and (2) that there is a unique b.

Hint: To show that b exists, consider that since $\gcd(a, p) = 1$, there exist integers b, c such that $ab + pc = 1$. What happens if you consider this equation modulo p?

Solution. Since, $\gcd(a, p) = 1$, we know that there exist integers b, c such that $ab + pc = 1$ (The Pulverizer helps us find these integers for given values of a, p). Now if we consider the equation modulo p. That is

$$1 = ab + pc \equiv ab \pmod{p}$$

Now we find b' such that $b' \equiv b \pmod{p}$ and $b' \in \{1, 2, \ldots p - 1\}$. Therefore, we can conclude that b' is the inverse of a modulo p. So such an inverse exists. Now we show that such an inverse is unique.

Suppose that there are two integers b, b' such that $ab \equiv ab' \equiv 1 \pmod{p}$ with $b, b' \in \{1, 2, \ldots p - 1\}$. Then we have that $p \mid ab - ab'$, and so $p \mid (b - b')$ since $p \nmid a$. However, since $b, b' \in \{1, 2, \ldots p - 1\}$, this is only possible if $b = b'$, and hence the inverse is unique.

■

(c) [6 pts] Let p be a prime number. Prove that for integer a, $a^2 \equiv 1 \pmod{p}$ if and only if $a \equiv \pm 1 \pmod{p}$.

Hint: Consider $a^2 - 1 = (a + 1)(a - 1)$.

Solution. This follows almost directly from the hint. If we have $a^2 \equiv 1 \pmod{p}$, then we must have that $p \mid (a^2 - 1)$. So $p \mid (a + 1)(a - 1)$. However, since p is prime, we can conclude $p \mid (a + 1)$ or $p \mid (a - 1)$. Hence $a \equiv \pm 1 \pmod{p}$.

The other direction follows since if $a \equiv \pm 1 \pmod{p}$, then we have that $p \mid (a + 1)$ or $p \mid (a - 1)$ and so $p \mid (a^2 - 1)$ as desired. ■

(d) [8 pts] Prove Wilson's theorem using the above parts.

Hint: Use theorem 2 to pair up the integers in the expansion of $(p - 1)!$ with their inverses. Based on part c, which integers don't get paired?

Solution. Consider the integers in the expansion of $(p - 1)!$. Each of these integers is in the set $\{1, 2, \ldots p - 1\}$, and so we can pair each integer with its unique inverse modulo p as we proved in theorem 2. Thus we will have pairs of integers $a, b \in \{1, 2, \ldots p - 1\}$ such that $ab \equiv 1 \pmod{p}$. However, we must account for the case where $a = b$. This implies that $a^2 \equiv 1 \pmod{p}$. However, by part c, we know that there are only two such numbers in the set $\{1, 2, \ldots p - 1\}$ for which $a^2 \equiv 1 \pmod{p}$. Namely $a = 1, (p - 1)$. Hence we have that $(p - 1)! \equiv 1 \cdot (p - 1) \pmod{p}$. This means that $(p - 1)! \equiv -1 \pmod{p}$ as desired. ■

Problem 4. [20 points] The following parts can be solved using Fermat's little theorem, which states that for integers a, p such that $\gcd(a, p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$.

(a) [2 pts] Find $3^{31} \pmod 7$.

Solution. By a direct application of Fermat's little theorem, $3^6 \equiv 1 \pmod 7$. Therefore, $3^{30} \equiv 1 \pmod 7$. Thus $3^{31} \equiv 3^{30} \cdot 3 \equiv 1 \pmod 7$. ■

(b) [4 pts] Prove that $7 \mid n^6 - 1$ for all integers n such that $\gcd(n, 7) = 1$.

Solution. As $\gcd(n, 7) = 1$, we have that $n^6 \equiv 1 \pmod 7$ by Fermat's little theorem. By definition, this means that $7 \mid n^6 - 1$. ■

(c) [6 pts] Prove that $42 \mid n^7 - n$ for all integers n.

Solution. We have that

$$n^7 - n = n(n^6 - 1) = n(n^3 + 1)(n^3 - 1) = n(n + 1)(n - 1)(n^2 + n + 1)(n^2 - n + 1)$$

We can use part d of problem 1 on this problem set to conclude that $3! \mid n(n + 1)(n - 1)$. So we have that $6 \mid n^7 - n$ for all integers n. Now we need to show that $7 \mid n^7 - n$ for all integers n. Suppose that $7 \mid n$, then we are done. Now if we assume that $7 \nmid n$, then $\gcd(7, n) = 1$. Then we can use the previous part of this problem to conclude that $7 \mid n^6 - 1$ and so $7 \mid n^7 - n$. ■

(d) [8 pts] Prove that $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ is an integer $\forall n \in \mathbb{Z}$.

Solution. We first take a common denominator.

$$\begin{aligned} \frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} &= \frac{3n^5 + 5n^3 + 7n}{15} \\ &= \frac{n(3n^4 + 5n^2 + 7)}{15} \end{aligned}$$

Now all we need to show is that $15 \mid n(3n^4 + 5n^2 + 7)$ for all integers n. We first show that $3 \mid n(3n^4 + 5n^2 + 7)$. If $3 \mid n$, then we are done. Otherwise, $\gcd(n, 3) = 1$. In this case, by Fermat's little theorem we have that $n^2 \equiv 1 \pmod 3$. Thus we have that

$$3n^4 + 5n^2 + 7 \equiv 2 + 1 \equiv 0 \pmod 3$$

Thus we have that $3 \mid n(3n^4 + 5n^2 + 7)$ for all integers n.

Now we show that $5 \mid n(3n^4 + 5n^2 + 7)$ for all integers n. Again if $5 \mid n$, then we are done. Otherwise, $\gcd(n, 5) = 1$. In this case, by Fermat's little theorem we have that $n^4 \equiv 1 \pmod 5$. Thus we have that

$$3n^4 + 5n^2 + 7 \equiv 3 + 2 \equiv 0 \pmod 5$$

Thus we have that $5 \mid n(3n^4 + 5n^2 + 7)$ for all integers n.

Hence we have that $15 \mid n(3n^4 + 5n^2 + 7)$ for all integers n. ■

Problem 5. [20 points]

Prove that the greatest common divisor of three integers a, b, and c is equal to their smallest positive linear combination; that is, the smallest positive value of $sa + tb + uc$, where s, t, and u are integers.

Solution. Let m be the smallest positive linear combination of a, b, and c. We'll prove that $m = \gcd(a, b, c)$ by showing both $\gcd(a, b, c) \leq m$ and $m \leq \gcd(a, b, c)$.

First, we show that $\gcd(a, b, c) \leq m$. By the definition of common divisor, $\gcd(a, b, c)$ divides a, b, and c. Therefore, for every triple of integers s, t, and u:

$$\gcd(a, b, c) \mid sa + tb + uc$$

Thus, in particular, $\gcd(a, b, c)$ divides m, and so $\gcd(a, b, c) \leq m$.

Now we show that $m \leq \gcd(a, b, c)$. We do this by showing that $m \mid a$. Symmetric arguments show that $m \mid b$ and $m \mid c$, which means that m is a common divisor of a, b, and c. Thus, m must be less than or equal to the *greatest* common divisor of a, b, and c.

All that remains is to show that $m \mid a$. By the division algorithm, there exists a quotient q and remainder r such

$$a = q \cdot m + r \qquad\qquad \text{(where } 0 \leq r < m\text{)}$$

Now $m = sa + tb + uc$ for some integers s and t. Subtituting in for m and rearranging terms gives:

$$\begin{aligned} a &= q \cdot (sa + tb + uc) + r \\ r &= (1 - qs)a + (-qt)b + (-qu)c \end{aligned}$$

We've just expressed r as a linear combination of a, b, and c. However, m is the *smallest positive* linear combination and $0 \leq r < m$. The only possibility is that the remainder r is not positive; that is, $r = 0$. This implies $m \mid a$.

■

Problem 6. [20 points] In this problem, we will investigate numbers which are squares modulo a prime number p. These numbers are referred to quadratic residues of p.

(a) [5 pts] An integer n is a quadratic residue of 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: This is similar to problem 3c*)

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] The following is a simple test we can perform to see if a number $n \not\equiv 0 \pmod{p}$ is a quadratic residue of p for odd primes p.

Theorem 3 (Euler's Criterion)**.** *:*

1. *n is a quadratic residue of p if and only if $n^{\frac{p-1}{2}} \equiv 1 \pmod p$.*
2. *n is quadratic non-residue p if and only if $n^{\frac{p-1}{2}} \equiv -1 \pmod p$.*

This can be proved completely using Wilson's theorem and part a of this problem. However for this part prove the following: If n is a quadratic residue of p, then $n^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Solution. If n is a quadratic residue p, then there exists an a such that $a^2 \equiv n \pmod p$. Consequently,

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

by Fermat's theorem. ■

(c) [10 pts] Assume that $p \equiv 3 \pmod 4$ and $n \equiv x^2 \pmod p$. Find one possible value for x, expressed as a function of n and p. (*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. ■