Solutions to Homework 5

Tim Smits

February 12, 2022

1.(Computations) Do each of the following computations below. Show your work, don't just write the answer!

(a) Reduce $84526 \cdot 862967^3 - 448184 \cdot 591183^2 \bmod 15$.

(b) Compute $1477^{-1} \bmod 9235$.

(c) Reduce $1769^{234} \bmod 31$.

(d) Reduce $1! + 2! + \ldots + 100! \bmod 25$.

Solution:

(a) First, we just compute everything mod 15. We have $84526 \equiv 1 \bmod 15$, $862967 \equiv 2 \bmod 15$, $448184 \equiv 14 \equiv -1 \bmod 15$, and $591183 \equiv 3 \bmod 15$. Therefore, we want to compute $1 \cdot 2^3 - (-1) \cdot 3^2 \bmod 15 \equiv 8 + 9 \bmod 15 \equiv 2 \bmod 15$.

(b) Note that $\gcd(1477, 9235) = 1$ so that 1477 is indeed invertible mod 9235. Running the Euclidean algorithm and performing back substitution says $1477 \cdot 4308 + 9235 \cdot (-689) = 1$, so taking this mod 9235 says $1477 \cdot 4308 \equiv 1 \bmod 9235$, so $1477^{-1} \equiv 4308 \bmod 9235$.

(c) First, note that $1769 \equiv 2 \bmod 31$, so we want to compute $2^{234} \bmod 31$. We have $2^5 \equiv 1 \bmod 31$, and $234 = 5 \cdot 46 + 4$, so $2^{234} \equiv 2^{5 \cdot 46 + 4} \bmod 31 \equiv (1)^{46} \cdot 2^4 \bmod 31 \equiv 16 \bmod 31$.

(d) Note that 10! is divisible by 25 because both 5 and 10 appear as terms in the product. For $n > 10$, 5 and 10 still appear as terms in the product, so $n!$ remains divisible by 25. This says $1! + 2! + \ldots + 100! \equiv 1! + 2! + \ldots + 9! \bmod 25 \equiv 409113 \bmod 25 \equiv 13 \bmod 25$.

2. Prove that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer for all $n \in \mathbb{Z}$.

Solution: Putting everything over a common denominator, we wish to show that $\frac{3n^5+5n^3+7n}{15}$ is an integer, or equivalently, that $15 \mid 3n^5 + 5n^3 + 7n$. This is the same thing as checking that $3n^5 + 5n^3 + 7n \equiv 0 \bmod 15$. Note that divisibility by 15 is equivalent to divisibility by both 3 and 5, because $15 = 3 \cdot 5$ and 3 and 5 are relatively prime. Mod 3, we have $3n^5 + 5n^3 + 7n \equiv 2n^3 + n \bmod 3$. Plugging in $n = 0, 1, 2$ shows that $2n^3 + n \equiv 0 \bmod 3$ always holds, so $3n^5 + 5n^3 + 7n$ is always divisible by 3. Similarly, mod 5 we have $3n^5 + 5n^3 + 7n \equiv 3n^5 + 2n \bmod 5$ and plugging in $n = 0, 1, 2, 3, 4$ shows that $3n^5 + 2n \equiv 0 \bmod 5$ always holds, so we're done.

3. This problem deals with divisibility tests for integers. Let $n = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0$ be the decimal expansion of n. For example, $123 = 1 \cdot 100 + 2 \cdot 10 + 3$.

(a) Prove that n is divisible by 3 if and only if $a_0 + a_1 + \ldots + a_n$ is divisible by 3. Show that a similar condition holds for divisibility by 9, but does not work for divisibility by 27.

(b) Prove that n is divisible by 11 if and only if $a_0 - a_1 + a_2 + \ldots + (-1)^n a_n$ is divisible by 11.

(c) For $k \geq 1$, prove that n is divisible by 2^k if and only if the last k digits of n are divisible by 2^k. Show that a similar condition holds for powers of 5 as well.

Solution:

(a) n is divisible by 3 if and only if $n \equiv 0 \bmod 3$. Writing $n = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0$, we have $n \equiv a_n + \ldots + a_0 \bmod 3$ because $10 \equiv 1 \bmod 3$. Therefore, $n \equiv 0 \bmod 3$ if and only if $a_0 + \ldots + a_n$ is divisible by 3. The same condition holds mod 9 because $10 \equiv 1 \bmod 9$, so we get the same test for divisibility by 9. It doesn't work for 27, because $2 + 7 = 9$ is not divisible by 27.

(b) Similarly to the above, $10 \equiv -1 \bmod 11$ So n is divisible by 11 if and only if $n \equiv 0 \bmod 11$, which holds if and only if $a_n \cdot (-1)^n + \ldots + a_1 \cdot (-1) + a_0 \equiv 0 \bmod 11$, i.e. if $a_0 - a_1 + \ldots + (-1)^n a_n$ is divisible by 11.

(c) We have n is divisible by 2^k if and only if $n \equiv 0 \bmod 2^k$. For $n \geq k$, we have $10^n \equiv 0 \bmod 2^k$, so $n \equiv 0 \bmod 2^k$ if and only if $a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv 0 \bmod 2^k$. The number $a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$ is simply the last k digits of n. The exact same proof holds for powers of 5, just replacing the 2's everywhere with a 5.

4. This problem deals with solving linear equations in $\mathbb{Z}/n\mathbb{Z}$, which we know is the same as solving linear congruences mod n. Assume $n > 1$ is an integer, and that a, b are integers.

(a) Show that the congruence $ax \equiv b \bmod n$ is solvable if and only if $\gcd(a, n) \mid b$.

(b) If x_0 is a solution to $ax \equiv b \bmod n$, prove that all the solutions to $[a]x = [b]$ in $\mathbb{Z}/n\mathbb{Z}$ are $[x_0 + \frac{n}{\gcd(a,n)}k]$ for $k = 0, 1, \ldots, (a, n) - 1$. *(Remember: $[x]$ denotes the congruence class of x mod n, and that the elements of $\mathbb{Z}/n\mathbb{Z}$ are congruence classes, not numbers!)*

(c) Solve the congruences $1723x \equiv 3574 \bmod 4914$ and $126x \equiv 91 \bmod 217$. Your answer should be a single congruence class in each case: $x \equiv \_ \bmod \_$.

(d) Write down the solutions to $[1723]x = [3574]$ in $\mathbb{Z}/4914\mathbb{Z}$ and $[126]x = [91]$ in $\mathbb{Z}/217\mathbb{Z}$.

In particular, this problems shows that it's possible for a linear equation in $\mathbb{Z}/n\mathbb{Z}$ to have more than one solution in $\mathbb{Z}/n\mathbb{Z}$, which is very different from how things work in $\mathbb{Z}$!

Solution:

(a) Suppose that there is a solution x_0 to $ax \equiv b \bmod n$. This means $ax_0 \equiv b \bmod n$, so $ax_0 = b + nk$ for some integer k. This says $ax_0 - nk = b$, and since $\gcd(a, n)$ divides both a and n, it therefore divides b because it's a linear combination of a and n. Conversely, suppose that $\gcd(a, n) \mid b$. Then we can write $b = \gcd(a, n)k$ for some integer k. By Bezout's lemma, we can find integers x, y such that $ax + ny = \gcd(a, n)$. Multiplying by k says $a(xk) + n(yk) = b$, so taking this mod n says $a(xk) \equiv b \bmod n$. Therefore, xk is a solution to $ax \equiv b \bmod n$.

(b) First, we point out that solutions to $ax \equiv b \bmod n$ correspond to solutions to $ax + ny = b$. Indeed, if $ax \equiv b \bmod n$ then there exists an integer y such that $ax = b + ny$, so $ax + n(-y) = b$ produces the solution $(x, -y)$ to the equation $ax + ny = b$. On the other hand, suppose that $ax + ny = b$ for some integers x, y. Then taking this mod n says $ax \equiv b \bmod n$, so we've solved the congruence.

Since we start with a solution x_0 to $ax \equiv b \bmod n$, this means there is some y_0 such that $ax_0 + ny_0 = b$. Recall from homework 3 that all solutions to the equation $ax + ny = b$ are given by $x = x_0 + n'k$ and $y = y_0 - a'k$ for $k \in \mathbb{Z}$, where $n' = \frac{n}{\gcd(a,n)}$, and $a' = \frac{a}{\gcd(a,n)}$. Taking this mod n says all solutions to $ax \equiv b \bmod n$ are given by $x \equiv x_0 + n'k \bmod n$ for $k \in \mathbb{Z}$. Therefore, the solutions to $[a]x = [b]$ in $\mathbb{Z}/n\mathbb{Z}$ are given by the different congruence classes $[x_0 + n'k]$ for $k \in \mathbb{Z}$. We just need to see what these different classes are. Set $x_k = x_0 + n'k$, so we wish to know when does $[x_k] = [x_\ell]$ for integers k, ℓ. This happens precisely when $x_k \equiv x_\ell \bmod n$, and we see that $x_k \equiv x_\ell \bmod n$ if and only if we have $n'k \equiv n'\ell \bmod n$. This says $n'(k - \ell) \equiv 0 \bmod n$, which is the same as saying $n \mid n'(k - \ell)$. Equivalently, dividing out by n' says this happens precisely when $d \mid k - \ell$, i.e. $k \equiv \ell \bmod d$ where $d = \gcd(a, n)$. What we've shown is that $[x_k]$ depends on the congruence class of k mod d, and so running through $k = 0, 1, \ldots, d - 1$ gives us all possible congruence classes for $[x_k]$, and therefore all solutions to the equation.

(c) Running the Euclidean algorithm says $\gcd(1723, 4914) = 1$, so $x \equiv 1723^{-1} \cdot 3574 \bmod 4914$. Performing back substitution says $1723 \cdot (-713 \cdot 3574) + 4914 \cdot (250 \cdot 3574) = 3574$, so taking this mod 4914 says $1723^{-1} \equiv -713 \cdot 3574 \bmod 4914 \equiv 2104 \bmod 4914$. Therefore, the solution is $x \equiv 2104 \bmod 4914$. For the other congruence, since $\gcd(126, 217) = 7$ and $7 \mid 91$, we can divide out by 7 to get the congruence $18x \equiv 13 \bmod 31$, so $x \equiv 18^{-1} \cdot 13 \bmod 31$. Running the Euclidean algorithm and performing back substitution says $31 \cdot 7 + 18 \cdot (-12) = 1$, so $18^{-1} \equiv -12 \bmod 31 \equiv 19 \bmod 31$. This says $x \equiv 19 \cdot 13 \bmod 31 \equiv 30 \bmod 31$.

(d) By part (b), there is a unique solution to $[1723]x = [3574]$ in $\mathbb{Z}/4914\mathbb{Z}$, and it's given by $[2104]$ by the previous part. There are 7 solutions to $[126]x = [91]$ in $\mathbb{Z}/217\mathbb{Z}$ given by $[30 + 31k]$ for $k = 0, 1, \ldots, 6$. These are $[30], [61], [92], [123], [154], [185], [216]$.

5. The goal of this problem is to demonstrate how working in $\mathbb{Z}/n\mathbb{Z}$ can detect obstruction to equations having integer solutions.

(a) Write down the perfect squares in $\mathbb{Z}/8\mathbb{Z}$ and perfect cubes in $\mathbb{Z}/9\mathbb{Z}$.

(b) Prove that $x^3 + y^3 + z^3 = 4$ has no integer solutions. For what other integers can you replace 4 with and have your same argument work?

(c) Prove that there are no integers m, n such that $3^m + 3^n + 1$ is a perfect square.

Solution:

(a) By literally just squaring every element in $\mathbb{Z}/8\mathbb{Z}$ we see that the perfect squares are $[0], [1], [4]$, and similarly the perfect cubes in $\mathbb{Z}/9\mathbb{Z}$ are $[0], [1], [8]$.

(b) Suppose that $x^3 + y^3 + z^3 = 4$ has integer solutions. Then the same equation would have to hold mod 9 as well, so $[x]^3 + [y]^3 + [z]^3 = [4]$ in $\mathbb{Z}/9\mathbb{Z}$. By (a), the only perfect cubes in $\mathbb{Z}/9\mathbb{Z}$ are $[0], [1], [8]$ which we can write as $[0], [1], [-1]$. It's then quite clear there's no way to take three elements from the set $\{[0], [1], [-1]\}$ and add them to get $[4]$, so there is no solution mod 9. This is a contradiction, so we couldn't have had any integer solutions to begin with. The easiest generalization is that we can replace 4 with any integer congruent to 4 mod 9 and the same argument will work. Slightly less obvious is that any integer congruent to 5 mod 9 also works as well ($[5]$ is the only other element in $\mathbb{Z}/9\mathbb{Z}$ that you can't get from a sum of three elements in the set $\{[0], [1], [-1]\}$).

(c) Suppose there were integers m, n such that $3^m + 3^n + 1$ is a perfect square. Then it would have to be a perfect square in $\mathbb{Z}/8\mathbb{Z}$ as well. By (a), the perfect squares in $\mathbb{Z}/8\mathbb{Z}$ are

$[0], [1], [4]$, so let's show that $[3]^m + [3]^n + [1]$ is never any of these. Note that if k is even, then $[3]^k = [1]$ and if k is odd, then $[3]^k = [3]$. Therefore, there are four possibilities for the value of this sum: it's either $[1]+[1]+[1] = [3], [1]+[3]+[1] = [5], [3]+[1]+[1] = [5]$, or $[3] + [3] + [1] = [7]$. In all cases, it's never $[0], [1]$ or $[4]$, so we get a contradiction. Therefore, $3^m + 3^n + 1$ is never a perfect square.

6.

(a) Prove that if p is prime, then $(p-1)! \equiv -1 \bmod p$ *(Hint: try pairing up integers in the product in a useful way)*.

(b) Prove that if $n > 4$ is composite, then $(n-1)! \equiv 0 \bmod n$.

Combining these two parts says than an integer is prime if and only if $n \nmid (n-1)!$. Of course, this is a very *bad* way of checking that an integer is prime, because $(n-1)!$ gets very large, very fast!

Solution:

(a) Since p is prime, every integer a between 1 and $p-1$ is invertible mod p. Therefore in the product $(p-1)!$, for each a we pair it up with its inverse mod p and then the product reduces to 1 mod p. The only question we have to ask is when is an integer it's own inverse mod p? This is when we don't have a different element to pair with. Saying a is it's own inverse mod p means $a^2 \equiv 1 \bmod p$, which we have proven before only has solutions $a \equiv \pm 1 \bmod p$. This says the only elements in the product that *don't* have something to pair up with are 1 and $p-1$. Therefore, $(p-1)! \equiv 1 \cdot (p-1) \bmod p \equiv p-1 \bmod p \equiv -1 \bmod p$.

(b) Since n is composite, we can write $n = ab$ with $1 \leq a, b \leq n-1$. If a and b are *distinct*, then they both appear as terms in $(n-1)!$ so we have $(n-1)! \equiv 0 \bmod n$. Otherwise, if $a = b$ then $n = a^2$ for some a. We obviously have a appearing as a term in $(n-1)!$, so we need to find another multiple of a in order to be divisible by a^2. Well, we have $2a < a^2$ as long as $a > 2$, which is true because $n > 4$. Therefore, $2a$ appears as a term in the product, so $(n-1)! \equiv 0 \bmod n$ and we're done.