Math 3110: Quiz #3 – Solutions

March 16, 2019

Name:

Question 1

(16 minutes / 16 points) Short answers. Each question is worth 2 points.

1. Give the definition of the Ford circle atop a/b.

   Solution. The Ford circle atop a/b is the circle above the real line, tangent to it at a/b and having radius $1/2b^2$.

2. Circle the values of k for which there are infinitely many fractions a/b such that $|\sqrt{2} - a/b| < 1/b^k$.

   1 2 3 4 5

   Solution. You should circle 1 and 2 only. We know that $\sqrt{2}$ is algebraic, and so the Thue-Siegel-Roth Theorem gauarantees that there are only finitely many such a/b for $k > 2$. On the other hand, $\sqrt{2}$ is irrational, so Dirichlet's theorem guarantees there are infinitely many such, when $k \leq 2$. Note that the correct answer must be all the k's up to some breaking point, since as k increases, satisfying the inequality gets strictly more difficult. (Many people circled just 2 and forgot that this *implies* it is also true for 1.)

3. Compute $3 + 17 \pmod{11}$ (simplify so that the answer is the natural representative).

   Solution. $3 + 17 \equiv 20 \equiv 9 \pmod{11}$.

4. Compute $3^{101} \pmod{4}$ (simplify so that the answer is the natural representative).

   Solution. This can be done quickly by recognizing that $3 \equiv -1 \pmod{4}$, so that $3^{101} \equiv (-1)^{101} \equiv -1 \equiv 3 \pmod{4}$. If you don't notice that, you will still quickly notice that $3^2 \equiv 1 \pmod{4}$ so that $3^{100} \equiv 1^{50} \equiv 1 \pmod{4}$, so that $3^{101} \equiv 1 \cdot 3 \equiv 3 \pmod{4}$.

5. State the definition of a *multiplicative inverse modulo n.*

   Solution. Let $a, n \in \mathbb{Z}$. Let $b \in \mathbb{Z}$. We say that b is the *multiplicative inverse of a modulo n* if $ab \equiv 1 \pmod{n}$.

6. Give an example of $a, b, x, n \in \mathbb{Z}$, $x \not\equiv 0 \pmod{n}$, such that $ax \equiv bx \pmod{n}$ but $a \not\equiv b \mod n$. (Failure of cancellation.)

   Solution. Such an x must not be invertible. For example, take $n = 10$ and an x which is not coprime, say $x = 5$. Then we look for a, b differing by a multiple of 2, so that their difference, multipled by 5, becomes a multiple of 10. For example, $a = 4$, $b = 6$, or $a = 1$, $b = 5$. Then $ax \equiv bx \equiv 0 \pmod{n}$, but $a \not\equiv b \pmod{n}$. (This trick about x and the difference between a and b being proper divisors of n that multiply to a multiple of n is what I used to quickly grade the question.)

7. (True/False) If $a \equiv b \pmod{n}$, then $x^a \equiv x^b \pmod{n}$.

   Solution. False. For example, take $x \equiv 2 \pmod{3}$. Then $x^2 \equiv 1 \pmod{3}$ but $x^5 \equiv 2 \pmod{3}$.

8. (True/False) There are polynomial equations (in several variables) that have solutions modulo n for every integer n, but have no integer solutions.

   Solution. True. The book gives an example on page 135.

Question 2

(10 minutes / 10 points)

Prove the following theorem (i.e. that addition is well-defined modulo n).

Theorem 1. *Let $a, b, x, y, n \in \mathbb{Z}$. Suppose that $a \equiv b \pmod{n}$ and $x \equiv y \pmod{n}$. Then $a + x \equiv b + y \pmod{n}$.*

Solution Your text has a nice proof, as do your course notes. I was picky about introducing variables. If you wrote "Then $a = b + ny$ for $y \in \mathbb{Z}$", you lost a point. This is because the phrase "for $y \in \mathbb{Z}$" is ambiguous. If anything, "for" by itself usually means "for all," but here you want "for some." These are very different meanings. You must be precise. If you didn't introduce the variable at all, you also lost a point.

Question 3

(10 minutes / 10 points)

Solve the linear congruence $28x \equiv 6 \pmod{62}$. Show your work. Give the full set of solutions modulo 62.

Solution.

First I will give the full general solution, then give some variations and speedups.

Full version. This is equivalent to solving the linear Diophantine equation

$$28x + 62y = 6,$$

or, equivalently,

$$14x + 31y = 3.$$

We perform the Extended Euclidean algorithm on the coefficients 31 and 14:

$(1,0)$ gives 31	$= 2 \cdot$	$(0,1)$ gives 14	$+$	$(1,-2)$ gives 3
$(0,1)$ gives 14	$= 4 \cdot$	$(1,-2)$ gives 3	$+$	$(-4,9)$ gives 2
$(1,-2)$ gives 3	$= 1 \cdot$	$(-4,9)$ gives 2	$+$	$(5,-11)$ gives 1
$(-4,9)$ gives 2	$= 2 \cdot$	$(5,-11)$ gives 1	$+$	$(-14,31)$ gives 0

This informs us that $(5,-11)$ is a solution to $31y + 14x = 1$.

Therefore, multiplying by 3, $(15,-33)$ is a solution to $31y + 14x = 3$.

The homogeneous solution family to $31y + 14x = 0$ is

$$\{(14k, -31k) : k \in \mathbb{Z}\}.$$

Therefore, the general solution to our equation $31y + 14x = 3$ is

$$\{(15 + 14k, -33 - 31k) : k \in \mathbb{Z}\}.$$

Translating this back to the congruence situation, we have

$$x \equiv -33 \pmod{31},$$

which is the same as

$$x \equiv 29 \pmod{31},$$

or, since the question asked for all solutions modulo 62, this is

$$x \equiv 29, 60 \pmod{62}.$$

Variations and speedups and comments.

1. Examining the table, you may notice that by chance, the 3 we wanted actually appears in the first row! So we don't need the other three rows, strickly speaking.
2. I asked for the set of solutions $\pmod{62}$, so if you left off at one of the equations above besides the last, you lost a point. Translating back into the modular world is important.
3. It's also OK to do the Euclidean algorithm on 62 and 28, without dividing by 2 first. After all, you might not so easily notice a common factor. It will work out just fine that way too (the Euclidean algorithm finds that common factor along the way).

Question 4

(10 minutes / 10 points)

Recall that we use the notation $\mathbb{Z}/n\mathbb{Z}$ to represent the set of n different equivalence classes of integers modulo n.

Prove the following theorem.

Theorem 2. *Suppose that* $\gcd(a, n) = 1$. *Show that the function*

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

defined by

$$f(x) = ax \pmod{n}$$

is a bijection.

Solution.

Proof by finding the inverse function.

Since $\gcd(a, n) = 1$, we know that a has a multiplicative inverse, a^{-1}. Therefore there is a well-defined function

$$g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

defined by

$$g(x) = a^{-1}x \pmod{n}.$$

These two functions have the property

$$g \circ f(x) \equiv g(f(x)) \equiv a^{-1}ax \equiv x \pmod{n},$$

and

$$f \circ g(x) \equiv f(g(x)) \equiv aa^{-1}x \equiv x \pmod{n}.$$

Therefore

$$g \circ f(x) = f \circ g(x) = x,$$

and therefore g is the inverse of f.

Direct proof of injectivity and surjectivity.

First, we show that f is injective. Suppose that

$$f(x) \equiv f(y) \pmod{n}.$$

Then,

$$ax \equiv ay \pmod{n}.$$

But since $\gcd(a, n) = 1$, a is invertible and can be cancelled, so

$$x \equiv y \pmod{n}.$$

Next, we show that f is surjective. Let x be an integer. We wish to find an integer y so that $f(y) = x$. Recall that a is invertible. Let a^{-1} be its multiplicative inverse. Let $y = a^{-1}x$. Then

$$f(y) = f(a^{-1}x) = aa^{-1}x = x.$$

Note: In fact, as this is a map from a set onto itself, the domain and codomain have the same size. This means it suffices to show just injectivity or just surjectivity, and then call on this general result.