

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

SOLUTIONS FOR HOMEWORK 6: CONGRUENCES II

1. True or False: (You don't have to justify)

(a) $2x \equiv 5 \pmod{m}$ has a solution $x \in \mathbb{Z}$ if and only if m is odd.

TRUE: if m is odd, then 2 is invertible; if m is even, then $m|(2x-5)$ implies that $2|(2x-5)$ but $2x-5$ is odd!

(b) For odd integers k , $2x \equiv k \pmod{m}$ has a solution $x \in \mathbb{Z}$ if and only if m is odd.

TRUE, Same exact reasoning as above.

(c) For integers a, b , the congruence $ax \equiv b \pmod{m}$ has a solution $x \in \mathbb{Z}$ if and only if $\gcd(a, m) = 1$.

NOT QUITE TRUE. In one direction it is true: If $\gcd(a, m) = 1$, then we just multiply by the inverse of $a \pmod{m}$. If $\gcd(a, m) > 1$, then $ax \equiv b \pmod{m}$ *could* have a solution, but it doesn't have to. For example, if $b = 0$, then $ax \equiv b \pmod{m}$ always has the solution $b = 0$, but if $b = 1$, then $ax \equiv b \pmod{m}$ doesn't have a solution.

2. Recall that we are using the notation $\{a\}_m = \{a + km \mid k \in \mathbb{Z}\}$, i.e. $\{a\}_m \in \mathbb{Z}/m\mathbb{Z}$ is the congruence class of a modulo m . For integers a satisfying $\gcd(a, m) = 1$, define

$$\text{order}(\{a\}_m) = \min\{n \geq 1 \mid \{a\}_m^n = \{1\}_m\}.$$

In other words, the order of $\{a\}_m$ is the smallest positive integer n such that $a^n \equiv 1 \pmod{m}$.

(a) Why is $\text{order}(\{a\}_m)$ only defined for a satisfying $\gcd(a, m) = 1$?

If $\gcd(a, m) > 1$, then there does not exist b such that $ab \equiv 1 \pmod{m}$. In particular, for all $k \geq 1$ we have $a^k = aa^{k-1} = ab \not\equiv 1 \pmod{m}$. Thus, no power of a is congruent to 1 so a has "infinite" order or really no order at all.

(b) Prove that when $\gcd(a, m) = 1$, the quantity $\text{order}(\{a\}_m)$ is well-defined by showing that there exists a positive integer n such that $\{a\}_m^n = \{1\}_m$.

Consider the sequence $\{a\}_m, \{a\}_m^2, \{a\}_m^3, \dots$. Can this sequence have infinitely many *distinct* elements? No way, because they are elements of the finite set $\mathbb{Z}/m\mathbb{Z}$. Thus, there must be repetition in the list, i.e. there exist integers $1 \leq i < j$ such that $\{a\}_m^j = \{a\}_m^i$. Let us write $j = i + k$ with $k \geq 1$. Since $\gcd(a, m) = 1$, there exists $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \pmod{m}$. Thus, we multiply both sides of $\{a\}_m^j = \{a\}_m^i$ by $\{a'\}_m^i$ to get $\{a\}_m^k = \{1\}_m$.

(c) Again assuming that $\gcd(a, m) = 1$, prove that for $k \geq 1$, $\{a\}_m^k = \{1\}_m$ if and only if $\text{order}(\{a\}_m) | k$.

One direction is easy. Let $e = \text{order}(\{a\}_m)$. If $k = te$ for some integer t , then $\{a\}_m^k = (\{a\}_m^e)^t = \{1\}_m^t = \{1\}_m$. To prove the other direction, suppose $\{a\}_m^k = \{1\}_m$. We have to show that e divides k , right?! So let's divide $k \div e$ and see what the remainder is! By Euclid, we know there exists an integer r satisfying $0 \leq r < e$ as well as an integer q such that $k = eq + r$. Now $\{a\}_m^k = \{a\}_m^{eq+r} = \{a\}_m^{eq} \{a\}_m^r = \{1\}_m \{a\}_m^r = \{a\}_m^r$, so

$$\{1\}_m = \{a\}_m^k = \{a\}_m^{eq} \{a\}_m^r = \{a\}_m^r.$$

We have just shown that $\{a\}_m^r = \{1\}_m$ which means r cannot be in the range $[1, e - 1]$ by the definition of $e = \text{order}(\{a\}_m)$. Thus, we must have $r = 0$, i.e. $e | k$.

DEFINITION: Recall from HW 5 Problem 8 that if $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$. Therefore the following set (called the set of “units modulo m ”, sometimes denoted $(\mathbb{Z}/m\mathbb{Z})^\times$ and sometimes $U(\mathbb{Z}/m\mathbb{Z})$) is well-defined:

$$U(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^\times = \{\{a\}_m \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}.$$

We can also write

$$U(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^\times = \{\{a\}_m \mid 1 \leq a \leq m \text{ and } \gcd(a, m) = 1\}.$$

3. For each integer $m \geq 1$, define “The Euler φ function” by

$$\varphi(m) = |\{1 \leq a \leq m \mid \gcd(a, m) = 1\}|.$$

(a) Prove that m is a prime number if and only if $\varphi(m) = m - 1$.

If m is a prime number, then for $1 \leq a \leq m - 1$, $1 \leq \gcd(a, m) \leq a < m$ and $\gcd(a, m) | m$ imply that $\gcd(a, m) = 1$ because the only positive divisor of m less than m is 1. Thus, all $m - 1$ positive integers less than m are coprime to m so $\varphi(m) = m - 1$. Conversely, if $\varphi(m) = m - 1$, then all $m - 1$ positive integers less than m are coprime to m ; if $d | m$ and $1 \leq d < m$, then $d | \gcd(d, m) = 1$ so $d = 1$; in other words, m has no divisors in $(1, m)$ which means m is prime.

(b) Compute $\varphi(m)$ for $1 \leq m \leq 25$.

I'll let you do this yourself.

(c) Find integers m, n such that $\varphi(mn) \neq \varphi(m)\varphi(n)$.

Say $\varphi(4) = 2$ and $\varphi(2) = 1$ but $\varphi(8) = 4$. Basically every time $\gcd(m, n) > 1$, we get this.

(d) Use your table to make a guess as to whether the following is true or false:

$$\text{If } \gcd(m, n) = 1, \text{ then } \varphi(mn) = \varphi(m)\varphi(n).$$

Should seem true from your table

4. Suppose $a, b, c, m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$.

(a) Prove that $mn|c$ if and only if $m|c$ and $n|c$.

Hint: I have three words for you: Bézout, Bézout, Bézout!

Just for the record:

BEZOUT'S THEOREM: GIVEN INTEGERS m, n , WITH $d = \gcd(m, n)$, THERE EXIST INTEGERS x, y SUCH THAT $mx + ny = d$.

One direction is very easy and does not need $\gcd(m, n) = 1$.

Recall that $a|b$ means $a/b \in \mathbb{Z}$. If $mn|c$, then $x = c/(mn) \in \mathbb{Z}$, thus $nx = c/m \in \mathbb{Z}$ and $mx = c/n \in \mathbb{Z}$ so $m|c$ and $n|c$.

In the other direction, we will use Bézout.

Suppose $m|c$ and $n|c$. We find $x, y \in \mathbb{Z}$ such that $mx + ny = 1$ since $\gcd(m, n) = 1$. We multiply by c to get $mx + ny = c$. Now $c/(mn) = x(c/n) + y(c/m)$. Since c/n and c/m are integers, we get $c/(mn)$ is an integer, so $mn|c$.

(b) Use (a) to prove that $a \equiv b \pmod{mn}$ if and only if $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.

Easy, let $c = b - a$. Then $mn|c$ if and only if $m|c$ and $n|c$, i.e. $b - a \equiv 0 \pmod{mn}$ if and only if $b - a \equiv 0 \pmod{m}$ and $b - a \equiv 0 \pmod{n}$. Now we just add a to both sides of the congruences.

5. We continue to assume that $m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$. Consider the map $f : \mathbb{Z}/mn\mathbb{Z} \rightarrow (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ defined by $f(\{a\}_{mn}) = (\{a\}_m, \{a\}_n)$. [Recall that if X and Y are sets, then the Cartesian product $X \times Y$ is defined to be the set $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$.

(a) Show that f is well-defined, i.e. show that if $a, a' \in \mathbb{Z}$ and $a \equiv a' \pmod{mn}$, then $(\{a\}_m, \{a\}_n) = (\{a'\}_m, \{a'\}_n)$.

If $a \equiv a' \pmod{mn}$, then $a \equiv a' \pmod{m}$, and $a \equiv a' \pmod{n}$, by the previous problem, so $\{a\}_m = \{a'\}_m$ and $\{a\}_n = \{a'\}_n$ as desired.

(b) Given integers $r, s \in \mathbb{Z}$, show that there exists $x \in \mathbb{Z}$ that simultaneously solves both congruences

$$x \equiv r \pmod{m}, \quad x \equiv s \pmod{n}.$$

We use Bézout to write $mu + nv = 1$ with $u, v \in \mathbb{Z}$, then make the *unbelievably* clever choice $x = mus + nvr$. We have $x - r = mus + nvr - r = mus + r(nv - 1) = mus + r(-mu) = m(us - ru)$ so $m|(x - r)$ i.e. $x \equiv r \pmod{m}$. Similarly, $x - s = mus + nvr - s = s(mu - 1) + nvr = s(-nv) + nvr = n(-sv + rv)$ so $n|(x - s)$ i.e. $x \equiv s \pmod{n}$.

(c) Use (b) to show that f is surjective.

If we choose any pair $(\{r\}_m, \{s\}_n)$, then we take x as in (b) and find that $f(x) = (\{r\}_m, \{s\}_n)$, so f is surjective.

(d) Suppose X, Y are finite sets of the same size, i.e. $|X| = |Y|$ and that $F : X \rightarrow Y$ is a **surjective** map from X to Y . Show that F is injective also, i.e. show that if $x_1, x_2 \in X$ and $x_1 \neq x_2$, then $F(x_1) \neq F(x_2)$.

Let us write $n = |X| = |Y|$. Let y_1, y_2, \dots, y_n be the n distinct elements of Y in some order. Since F is surjective, we can find elements $x_1, \dots, x_n \in X$ such that $f(x_i) = y_i$ for $i = 1, 2, \dots, n$. Now we claim that for $i \neq j$, $x_i \neq x_j$. We prove this by contradiction. Suppose $x_i = x_j$ for some $1 \leq i < j \leq n$; then $f(x_i) = f(x_j)$ or $y_i = y_j$ but we know that $y_i \neq y_j$ for $i \neq j$. So we have n distinct elements x_1, \dots, x_n in X . Since X has size n , there are no other elements in X , thus we have shown that for each $y_i \in Y$, the pre-image of y_i is $\{x \in X \mid F(x) = y_i\} = \{x_i\}$. Thus, F is injective.

(e) Use (c) and (d) to show that f is injective, hence bijective.

We know that if X, Y are finite sets, then $X \times Y$ has size $|X \times Y| = |X| \times |Y|$, so $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has size mn , which is the same as the size of $\mathbb{Z}/mn\mathbb{Z}$. Applying (c) and (d) we find that f is injective, hence bijective.

6. We continue to assume that $m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$. Let f^* be the “restriction” of the map f from the previous problem to the classes which are co-prime to mn . In other words, consider the map $f^* : (\mathbb{Z}/mn\mathbb{Z})^\times \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ defined by $f^*({a}_{mn}) = ({a}_m, {a}_n)$.

(a) Show that f^* is well-defined.

This is not hard. We just have to check that if $\gcd(a, mn) = 1$, then $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$ so that $f^*({a}_{mn})$ really DOES live in $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ as claimed. But it's clear that $\gcd(a, m) \leq \gcd(a, mn) = 1$ implies $\gcd(a, m) = 1$ and similarly for $\gcd(a, n)$ we get 1. So, f^* is well-defined.

(b) Show that f^* is surjective and injective.

If f^* were not injective, then f would not be injective because f^* is just a restriction of f . But f is injective, so f^* must be injective too. Now, given $(\{r\}_m, \{s\}_n)$ with $\gcd(r, m) = 1$ and $\gcd(r, n) = 1$, we know from the previous problem that there exists $x \in \mathbb{Z}$ such that $x \equiv r \pmod{m}$ and $x \equiv s \pmod{n}$. It remains only to show that $\gcd(x, mn) = 1$. Recalling from the last problem of HW5, we have $\gcd(x, m) = \gcd(r, m) = 1$ and $\gcd(x, n) = \gcd(s, n) = 1$. Suppose p is a prime such that $p \mid \gcd(x, mn)$, i.e. $p \mid x$ and $p \mid mn$. Then $p \mid m$ or $p \mid n$; if $p \mid m$, then p is a common divisor of x and m , which is not possible, and similarly since x and n have no common divisor, we find that $\gcd(x, mn)$ is not divisible by any prime. Thus, $\gcd(x, mn) = 1$, i.e. $\{x\}_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^\times$.

(c) Use (b) to show that $\varphi(mn) = \varphi(m)\varphi(n)$.

In (b), we have shown that there is a bijection between a set of size $\varphi(mn)$ and one of size $\varphi(m)\varphi(n)$, so these quantities must be equal.

7. Solve the congruences

(a) $7x \equiv 155 \pmod{181}$

We want to multiply by $7^{-1} \pmod{181}$. How do find that? Bézout of course: we apply Euclid to solve $181a + 7b = 1$, which is easy in this case, because $-181 + 7 \cdot 26 = 1$. Thus, $7^{-1} \equiv 26 \pmod{181}$. Multiplying by 26 we get $x \equiv 48 \pmod{181}$.

(b) $7y^3 \equiv 155 \pmod{181}$.

We must solve $y^3 \equiv 48 \pmod{181}$. We check that 2 has order 180 modulo 181, so there are 180 distinct powers of 2 modulo 181, i.e. every non-zero congruence class mod 181 is a power of 2. In particular, $2^k \equiv 48 \pmod{181}$ for some integer k . To find k , we note that $48^3 \equiv 1 \pmod{181}$ so 48 has order 3. Thus, $(2^k)^3 = 2^{3k} \equiv 1 \pmod{181}$, so $3k$ is a multiple of 180 by problem 2, so $k = 60, 120, 180, \dots$ we find easily that $k = 60$ is correct. So $48 \equiv 2^{60}$ giving $y_1 \equiv 2^{20} \pmod{181}$ as one solution. Two more solutions are gotten by $y_2 = 48y_1$ and $y_3 = 48^2y_1$.