Math 110 Homework 2 Solutions

January 22, 2015

1. Let $a, n \in \mathbb{Z}$, $n > 0$.
   (a) Suppose that a is a unit modulo n. Show that the multiplicative inverse of the congruence class $[a]$ is unique. This justifies referring to "the" multiplicative inverse of $[a]$ and using the notation $[a]^{-1}$. *Hint:* Suppose that the congruence classes $[b]$ and $[c]$ are both multiplicative inverses of $[a]$ modulo n; the goal is to show they are equal. Consider the product $[b][a][c]$.
   (b) If $\gcd(a, n) = 1$, show that the equation $ax \equiv d \pmod{n}$ has exactly one solution $[x]$ in $\mathbb{Z}/n\mathbb{Z}$. Conclude that there is a unique integer solution $x = t \in \mathbb{Z}$ with $0 \leq t < n$.

   Solution: (a) Suppose a is a unit modulo n, and let $[b]$ and $[c]$ be multiplicative inverses. This means $[a][b] = [b][a] = [1]$ and $[a][c] = [c][a] = [1]$. But then

$$[b] = [b]\Big([a][c]\Big) = \Big([b][a]\Big)[c] = [c].$$

   Therefore multiplicative inverses are unique.

   (b) If $\gcd(a, n) = 1$, there is a multiplicative inverse for a modulo n. The fact that $x \in \mathbb{Z}$ satisfies $ax \equiv d \pmod{n}$ means that $[a][x] = [d]$. Multiplying by $[a]^{-1}$, we see $[x] = [a]^{-1}[d]$, hence there is a unique congruence class solving the equation. The elements of this congruence class are all possible integer solutions to $ax \equiv d \pmod{n}$. Because elements of the congruence class differ by a multiple of n, there is a unique integer solution in the range $0 \leq x < n$.

2. To receive credit for this question, submit your solution to Problem 3 typeset in Latex, using `template.tex`. Use the "theorem" environment to state the result, and the "proof" environment to type your proof.

   Some useful commands (used in math environments):

`\equiv`	outputs	$\equiv$	
`2 \pmod{3}`	outputs	$2 \pmod{3}$	
`\mathbb{Z}`	outputs	$\mathbb{Z}$	("bb" stands for "blackboard bold")
`a \; \vert \; b`	outputs	$a \mid b$	(The `\;` commands create small spaces)

3. If $a, b \in \mathbb{Z}$ and $3 \mid (a^2 + b^2)$, prove that $3 \mid a$ or $3 \mid b$.
   Hint: Consider the possibilities for the congruence classes of a, b, and $a^2 + b^2 \pmod{3}$.

   Solution:

   Theorem 1.1. *If $a, b \in \mathbb{Z}$ and $3 \mid (a^2 + b^2)$, then $3 \mid a$ or $3 \mid b$.*

   Proof. There are three congruence classes modulo 3: [0], [1], and [2]. In terms of congruence classes, the problem is asking if $[a]^2 + [b]^2 = [0]$ in $\mathbb{Z}/3\mathbb{Z}$, show $[a] = [0]$ or $[b] = 0$.

   Note that $[a]^2 = [0]$ if $[a] = 0$, and $[a]^2 = [1]$ if $[a]$ is [1] or [2]. We need to check that whenever both $[a]$ and $[b]$ are nonzero modulo 3, then $([a]^2 + [b]^2)$ is also nonzero. There are three cases:

- If both $[a]$ and $[b]$ are $[1]$ modulo 3, then $([a]^2 + [b]^2) = ([1] + [1]) = [2]$.
- If both $[a]$ and $[b]$ are $[2]$ modulo 3, then $([a]^2 + [b]^2) = ([1] + [1]) = [2]$.
- If one of $[a]$ and $[b]$ is $[1]$ and the other is $[2]$, then $([a]^2 + [b]^2) = ([1] + [1]) = [2]$.

We conclude that $([a]^2 + [b]^2)$ can be zero only when at least one of a and b is divisible by 3. □

4. In this question we will verify the textbook's procedure for finding solutions for $ax \equiv b \pmod{n}$ when $\gcd(a, n) = d$ (page 74).
   (a) As a warm-up, verify what happens to the 12 congruence classes modulo 12 when they are reduced modulo 4. Verify that each class modulo 4 (considered as a set of integers) is a union of congruence classes modulo 12.
   (b) Suppose that n is a positive integer with divisor k. Show that if a congruence class modulo n reduces to the class $[c]$ modulo k, it must have been one of the $\frac{n}{k}$ classes

$$[c], \quad [c+k], \quad [c+2k], \quad \ldots, \quad [c+\left(\frac{n}{k}-1\right)k] \qquad \text{modulo } n.$$

   (c) Suppose that $ax \equiv b \pmod{n}$ with $\gcd(a, n) = d$. Show that if $[x_0]$ modulo $\frac{n}{d}$ is a solution to

$$\left(\frac{a}{d}\right)x \equiv \left(\frac{b}{d}\right) \pmod{\frac{n}{d}},$$

   then the solutions to $ax \equiv b \pmod{n}$ are exactly the congruence classes

$$[x_0], \quad [x_0 + \frac{n}{d}], \quad [x_0 + 2\left(\frac{n}{d}\right)], \quad \ldots, \quad [x_0 + (d-1)\left(\frac{n}{d}\right)] \qquad \text{modulo } n.$$

Solution: (a) Since we need to use congruence classes modulo two different numbers, here is an alternate notation that makes it easy to express the dependence on n: $a + n\mathbb{Z} = \{a + tn : t \in \mathbb{Z}\}$. Then

$$0 + 4\mathbb{Z} = 0 + 12\mathbb{Z} \bigcup 4 + 12\mathbb{Z} \bigcup 8 + 12\mathbb{Z}$$
$$1 + 4\mathbb{Z} = 1 + 12\mathbb{Z} \bigcup 5 + 12\mathbb{Z} \bigcup 9 + 12\mathbb{Z}$$
$$2 + 4\mathbb{Z} = 2 + 12\mathbb{Z} \bigcup 6 + 12\mathbb{Z} \bigcup 10 + 12\mathbb{Z}$$
$$3 + 4\mathbb{Z} = 3 + 12\mathbb{Z} \bigcup 7 + 12\mathbb{Z} \bigcup 11 + 12\mathbb{Z}$$

(b) We have to check two things: that every congruence class modulo n of the form $[c + tk]$, with $0 \leq t < \frac{n}{k}$ does reduce to $[c]$ modulo k, and conversely that every class that reduces to c modulo k must be among this set.

The first claim follows since $c + tk \equiv c \pmod{k}$ for any $t \in \mathbb{Z}$, so all of these congruence classes do reduce to $[c]$ modulo k.

Conversely, suppose that $a \equiv c \pmod{k}$. Then by definition $a = c + kt$ for some $t \in \mathbb{Z}$. Finally, note that changing t by a multiple of $\frac{n}{k}$ does not change $a + n\mathbb{Z}$:

$$c + k(t + \frac{n}{k}s) = c + +kt + nts \equiv c + kt \pmod{n},$$

so $[a]$ depends only on the conjugacy class of t modulo $\frac{n}{k}$. Thus $[a]$ is one of the $\frac{n}{k}$ congruence classes

$$[c], \quad [c+k], \quad [c+2k], \quad \ldots, \quad [c+\left(\frac{n}{k}-1\right)k] \qquad \text{modulo } n.$$

(c) Now suppose x is a solution to

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

This means there is a $t \in \mathbb{Z}$ such that $nt = ax - b$. Dividing by d (as a, n, and b are all multiples of d, we see that $\frac{a}{d}x - \frac{b}{d} = \frac{n}{d}t$, hence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

As $(\frac{n}{d}, \frac{a}{d}) = 1$, there is a unique solution to this modulo $\frac{n}{d}$, so x reduces to x_0 modulo $\frac{n}{d}$. Let $k = \frac{n}{d}$. By the previous part, $x + n\mathbb{Z}$ must be one of the congruence classes

$$x_0 + n\mathbb{Z}, x_0 + \frac{n}{d} + n\mathbb{Z}, \ldots c + \frac{n}{d}(d-1) + n\mathbb{Z}.$$

5. Find all solutions to each of the following equations. Show your work.
   (a) $5x + 3 \equiv 7 \pmod{8}$
   (b) $4x \equiv 12 \pmod{20}$
   (c) $10x \equiv 8 \pmod{25}$

Solution: (a) For the first, rearrange so $5x \equiv 4 \bmod 8$. Note 5 and 8 are relatively prime. By inspection, a multiplicative inverse to 5 is 5, so multiplying by 5 we see $25x \equiv x \equiv 20 \equiv 4 \pmod{8}$. Thus all solutions are $x \equiv 4 \pmod{8}$ or equivalently the elements of $[4] = \{\ldots, -4, 4, 12, \ldots\}$.

(b) For the second, we use the technique of the previous problem to divide through by 4. We are solving $x \equiv 3 \pmod{5}$ which is easy. Then the solutions are $x \equiv 3, 8, 13, 18 \pmod{20}$.

(c) The third has no solutions because $5 \mid 25$ and $5 \mid 10$, but $5 \nmid 8$. More formally, a solution would satisfy $25 \mid (10x - 8)$. If $25 \mid 10x - 8$, then there is a $t \in \mathbb{Z}$ such that $25t = 10x - 8$. But rearranging gives $8 = 5(2x - 5t)$. But 5 does not divide 8.

6. In this question, we will let the letters of the alphabet represent congruence classes modulo 26 as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

To facilitate encoding and decoding, you may wish to use an online program such as: `http://rumkin.com/tools/cipher/affine.php`. They denote α by a and β by b.

   (a) Read Chapter 2 of the textbook up to the end of Section 2.2 (ie, pages 12-16). State the definition of an *affine cipher*.
   (b) Show that the affine function

$$x \longmapsto \alpha x + \beta \pmod{26}$$

   is invertible if and only if $\gcd(\alpha, 26) = 1$. In the case that it is invertible, write down its inverse (in terms of α^{-1}).
   (c) The following text was encoded using an invertible affine function $x \longmapsto \alpha x + \beta \pmod{26}$.

   G CGRVWCGRMOMGT MA G FWZMOW NKJ RIJTMTE OKNNWW MTRK RVWKJWCA
   - GLNJWF JWTYM KT BGIL WJFKA

   Suppose that you correctly guess that "MA G" encodes the words " is a". Find the affine function used to encode this message. Show your work.

(d) Find the inverse of the affine function in part (c). Show your work.

(e) Decode the message from part (c).

Solution: (a) For the definition, look in the textbook.

(b) Let $f(x) = \alpha x + \beta \pmod{26}$ be the affine function. Suppose $\gcd(\alpha, 26) = 1$. Then α is invertible modulo 26, and we claim that $g(x) = \alpha^{-1}x - \alpha^{-1}\beta$ is an inverse. To verify this claim, we must check that $f(g(x)) \equiv x \pmod{26}$ and $g(f(x)) \equiv x \pmod{26}$ for every congruence class x modulo 26.

$$f(g(x)) \equiv f(\alpha^{-1}x - \alpha^{-1}\beta) \equiv \alpha(\alpha^{-1}x - \alpha^{-1}\beta) + \beta \equiv x - \beta + \beta \equiv x \pmod{26}$$

and similarly

$$g(f(x)) \equiv g(\alpha x + \beta) \equiv \alpha^{-1}(\alpha x + \beta) - \alpha^{-1}\beta \equiv x \pmod{26} \qquad \text{as desired.}$$

Conversely, suppose $\gcd(\alpha, 26) \neq 1$. Then there is a common divisor $d > 1$, and $\alpha\frac{26}{d} \equiv 0 \pmod{26}$. Then $f(0) = f(\frac{26}{d}) = \beta$ and $\frac{26}{d} \not\equiv 0 \pmod{26}$, so the function is not injective and hence not invertible.

(c) The guess that "MA G" encodes " is a" means that $f(8) = 12$, $f(18) = 0$ and $f(0) = 6$. The last says that $\beta = 6$. Then the first says

$$f(8) = 8\alpha + 6 \equiv 12 \pmod{26}.$$

Solving, $8\alpha \equiv 6 \pmod{26}$, or $4\alpha \equiv 3 \pmod{13}$. A multiplicative inverse for 4 is $10 \pmod{13}$, so $\alpha \equiv 4 \pmod{13}$. Thus we have two solutions for α modulo 26, $\alpha \equiv 4, 17 \pmod{26}$. But the affine function must be invertible, so by (b) α must be coprime to 26. We conclude that $\alpha \equiv 17 \pmod{26}$, and the encryption function is

$$f(x) = 17x + 6 \pmod{26}.$$

(d) Using the formula for the inverse, an inverse is given by $g(x) = \alpha^{-1}x - \alpha^{-1}\beta$. Now $\beta = 6$ and an inverse for $\alpha = 17$ is $23 \pmod{26}$. Thus the inverse function is

$$g(x) = 23x + 18 \pmod{26}.$$

(e) Using the website listed to do the actual calculation, we read

> a mathematician is a device for turning coffee into theorems
> – alfred renyi on paul erdos

7. (a) State the general form of the Chinese Remainder Theorem.

(b) Find the unique solution $[x]$ modulo $(4)(3)(5) = 60$ to the system of simultaneous congruences

$$x \equiv 2 \pmod{4} \qquad x \equiv 1 \pmod{3} \qquad x \equiv 3 \pmod{5}.$$

(c) Find an example of integers m, n, a, b where $\gcd(m, n) \neq 1$ so that

$$x \equiv a \pmod{m} \qquad x \equiv b \pmod{n}$$

has no solutions, and an example of m, n, a, b as above where the system has more than one solution.

Solution: (a) The Chinese Remainder Thereom says : let $m_1, m_2, \ldots, m_n$ be pairwise coprime integers. Then a system of congruences

$$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_n \pmod{m_n}$$

has an integer solution that is unique modulo $m_1 m_2 \ldots m_n$.

(b) To solve the three equations, do them pairwise using the extended Euclidean algorithm (or by inspection, as these numbers are small). If $x \equiv 2 \pmod 4$ and $x \equiv 1 \pmod 3$, inspection shows the solution is $x \equiv 10 \pmod{12}$. Now solve this and $x \equiv 3 \pmod 5$. We'll do this by the general algorithm.

We must have $x = 10 + 12s$ and $x = 3 + 5t$. Thus

$$7 = -12s + 5t$$

Running the Euclidean algorithm on 12 and 5 gives that $-12 \cdot 2 + 5 \cdot 5 = 1$, so $s = 14$ and $t = 35$ is a solution. In other words, $x = 3 + 5 \cdot 35 = 178 \equiv -2 \pmod{60}$.

Note that there are other ways to approach this: one method involves finding a number which is a multiple of two of the primes and is $\equiv 1$ modulo the third prime, and then forming a linear combination. This will be illustrated in the next problem.

(c) The system $x \equiv 2 \pmod 4$ and $x \equiv 1 \pmod 2$ has no solutions, as we see by reducing the first equation modulo 2.

The system $x \equiv 2 \pmod 4$ and $x \equiv 2 \pmod 6$ has two solutions modulo 24: 2 and 14.

8. Find all solutions x to the equation $x^2 \equiv 1 \pmod{77}$, using a method other than simply squaring all 77 congruence classes. (Note that $77 = (7)(11)$ is a product of distinct primes). Explain how you know that your answer includes every solution.

Solution: By the Chinese remainder theorem, solutions to this equation modulo 77 are in bijection with solutions to

$$x^2 \equiv 1 \pmod 7 \quad \text{and} \quad x^2 \equiv 1 \pmod{11}.$$

We proved in class that when p is prime, the equation $x^2 \equiv 1 \pmod p$ has precisely two solutions: 1 and -1 modulo p. Thus the solutions are exactly those integers x congruent to 1 or 6 modulo 7 and to 1 or 10 modulo 11. There are four solutions, one for each of the following possible systems of simultaneous congruences:

$$\begin{array}{cccc} x \equiv 1 \pmod 7 & x \equiv 1 \pmod 7 & x \equiv -1 \pmod 7 & x \equiv -1 \pmod 7 \\ x \equiv 1 \pmod{11} & x \equiv -1 \pmod{11} & x \equiv 1 \pmod{11} & x \equiv -1 \pmod{11} \end{array}$$

Now we combine them using the Chinese remainder theorem to get solutions modulo 77 using the technique alluded to in the previous solution.

Using the Euclidean algorithm (or by inspection) we can find numbers $w_1 = 22$ such that

$$w_1 \equiv 1 \pmod 7 \qquad \text{and} \qquad w_1 \equiv 0 \pmod{11},$$

and $w_2 = 56$ such that

$$w_2 \equiv 0 \pmod 7 \qquad \text{and} \qquad w_2 \equiv 1 \pmod{11}.$$

This means that

$$aw_1 + bw_2 \equiv a \pmod 7 \quad \text{and} \quad aw_1 + bw_2 \equiv b \pmod{11}$$

It is now arithmetic to find the four solutions:

$$\begin{aligned} (1)w_1 + (1)w_2 &\equiv 78 \equiv 1 \pmod{77} \\ (1)w_1 + (-1)w_2 &\equiv -34 \equiv 43 \pmod{77} \\ (-1)w_1 + (1)w_2 &\equiv 34 \pmod{77} \\ (-1)w_1 + (-1)w_2 &\equiv 76 \pmod{77} \end{aligned}$$