

Math 322 Fall 2016  
Number Theory HW 4 Solutions  
Due Friday, September 29

You may *not* discuss the starred problem with classmates, though you should of course feel free to discuss it with me as much as you like. Linguistic precision is important for this problem.

(★) **Starred Problem:** Show that multiplicative inverses  $\pmod m$  are unique up to congruence. That is, if  $a, b, c$  are integers, and  $m$  is a positive integer, and  $ab \equiv 1 \pmod m$  and  $ac \equiv 1 \pmod m$ , then  $b \equiv c \pmod m$ .

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. Prove that an integer is divisible by eleven if and only if the sum of its even-placed base 10 digits minus the sum of its odd-placed digits is divisible by eleven. That is, if  $n = n_0 + n_1 \cdot 10 + n_2 \cdot 10^2 + \cdots + n_k 10^k$ , then  $11|n$  if and only if

$$11 \mid \sum_{i \text{ even}} n_i - \sum_{i \text{ odd}} n_i = n_0 - n_1 + n_2 - n_3 + \dots$$

**Solution:** Notice that  $10 \equiv -1 \pmod{11}$  and thus  $10^\ell \equiv (-1)^\ell \pmod{11}$ , so if  $\ell$  is even then  $10^\ell \equiv 1 \pmod{11}$  and if  $\ell$  is odd then  $10^\ell \equiv -1 \pmod{11}$ . Then

$$\begin{aligned} n &= n_0 + n_1 \cdot 10 + n_2 \cdot 10^2 + \cdots + n_k 10^k \\ &\equiv n_0 - n_1 + n_2 - n_3 + \cdots \pm n_k \pmod{11} \\ &\equiv \sum_{i \text{ even}} n_i - \sum_{i \text{ odd}} n_i \pmod{11} \end{aligned}$$

thus  $11|n$  if and only if 11 divides the right hand side.

2. Fix an integer  $m > 0$ , and suppose that  $m$  has the following property: if  $a$  is an integer and  $m \nmid a$ , then  $a$  has a multiplicative inverse  $\pmod m$ . That is,  $m$  is an integer such that every integer is either divisible by  $m$ , or has a multiplicative inverse  $\pmod m$ . Then prove that  $m$  is prime.

**Solution:** Recall that the linear congruence  $ax \equiv b \pmod m$  has a solution if and only if  $(a, m)$  divides  $b$ . Thus in particular  $ax \equiv 1 \pmod m$  has a solution if and only if

$(a, m)$  divides 1, if and only if  $(a, m) = 1$ . Thus  $a$  has a modular inverse modulo  $m$  if and only if  $(a, m) = 1$ .

So suppose  $m$  has the above property. Then  $m$  is relatively prime to every number it does not divide. We haven't technically proven that this implies that  $m$  is prime, but I've stated it so I'll give you credit.

If we want to prove that this implies  $m$  is prime, suppose  $m = ab$  for some integers  $a, b > 0$ . Suppose  $m \neq a$ . Then  $m \nmid a$  (since e.g.  $a \leq m$  and  $a \neq m$ ). Thus  $(m, a) = 1$ , but  $a|m$ , so this implies that  $a = 1, b = m$ . Thus the only factors of  $m$  are 1 and  $m$ , so  $m$  is prime by definition.

3. Find a solution to each system of congruences:

(a)

$$5x \equiv 3 \pmod{23}$$

**Solution:** Using the Euclidean algorithm, we can write

$$23 = 4 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

so

$$\begin{aligned} 1 &= 3 - 2 = 1 \cdot 3 - (1 \cdot 5 - 1 \cdot 3) \\ &= 1 \cdot (23 - 4 \cdot 5) - (1 \cdot 5 - (23 - 4 \cdot 5)) \\ &= 2 \cdot 23 - 9 \cdot 5 \end{aligned}$$

and thus

$$-9 \cdot 5 \equiv 1 \pmod{23}$$

$$-27 \cdot 5 \equiv 3 \pmod{23}$$

$$-4 \cdot 5 \equiv 3 \pmod{23}$$

$$19 \cdot 5 \equiv 3 \pmod{23}.$$

$-72, -4$ , or  $19$  all make reasonable answers. (and  $-4$  is easy to check by eyeballing).

Notice that this solution is unique up to congruence, since  $(5, 23) = 1$  and thus there is one solution up to congruence.

(b)

$$x \equiv 0 \pmod{2}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 0 \pmod{3}$$

$$x \equiv 6 \pmod{7}$$

**Solution:** We have  $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ . Then the algorithm from the Chinese Remainder Theorem gives

$$\begin{aligned} M_1 &= 3 \cdot 5 \cdot 7 = 105 \equiv 1 \pmod{2} & y_1 &= 1 \\ M_2 &= 2 \cdot 5 \cdot 7 = 70 \equiv 1 \pmod{3} & y_2 &= 1 \\ M_3 &= 2 \cdot 3 \cdot 7 = 42 \equiv 2 \pmod{5} & y_3 &= 3 \\ M_4 &= 2 \cdot 3 \cdot 5 = 30 \equiv 2 \pmod{7} & y_4 &= 4 \end{aligned}$$

and thus

$$x = 0 \cdot 105 \cdot 1 + 0 \cdot 70 \cdot 1 + 1 \cdot 42 \cdot 3 + 6 \cdot 30 \cdot 4 = 126 + 720 = 846 \equiv 6 \pmod{210}.$$

(c)

$$\begin{aligned} x &\equiv 2 \pmod{11} & x &\equiv 3 \pmod{12} \\ x &\equiv 4 \pmod{13} & x &\equiv 5 \pmod{17} \\ x &\equiv 6 \pmod{19} \end{aligned}$$

**Solution:** We have  $M = 11 \cdot 12 \cdot 13 \cdot 17 \cdot 19 = 554268$ . We should check that these are pairwise relatively prime—they are not all prime, but they have no primes in common, so they are pairwise relatively prime. Then

$$\begin{aligned} M_1 &= 12 \cdot 13 \cdot 17 \cdot 19 = 50388 \equiv 8 \pmod{11} & y_1 &= 7 \\ M_2 &= 11 \cdot 13 \cdot 17 \cdot 19 = 46189 \equiv 1 \pmod{12} & y_2 &= 1 \\ M_3 &= 11 \cdot 12 \cdot 17 \cdot 19 = 42636 \equiv 9 \pmod{13} & y_3 &= 3 \\ M_4 &= 11 \cdot 12 \cdot 13 \cdot 19 = 32604 \equiv 15 \pmod{17} & y_4 &= 8 \\ M_5 &= 11 \cdot 12 \cdot 13 \cdot 17 = 29172 \equiv 7 \pmod{19} & y_5 &= 11 \end{aligned}$$

Then we have

$$\begin{aligned} x &= 2 \cdot 50388 \cdot 7 + 3 \cdot 46189 \cdot 1 + 4 \cdot 42636 \cdot 3 + 5 \cdot 32604 \cdot 8 + 6 \cdot 29172 \cdot 11 \\ &\equiv 4585143 \equiv 150999 \pmod{554268}. \end{aligned}$$

4. Find (all) the solutions of

$$\begin{aligned} 2x + 3y &\equiv 5 \pmod{7} \\ x + 5y &\equiv 6 \pmod{7}. \end{aligned}$$

**Solution:** Notice that  $x + 5y \equiv 6 \pmod{7}$  if and only if  $2x + 10y \equiv 12 \pmod{7}$  (since  $(2, 7) = 1$ ) if and only if  $2x + 3y \equiv 5 \pmod{7}$ . Thus any solution to one congruence is a solution to both. Thus the set of solutions is the set of  $(x, y)$  where  $x \equiv 6 - 5y \pmod{7}$ .

We can check this (or solve it alternatively) by noting that  $x + 5y \equiv 6 \pmod{7}$  if and only if  $x \equiv 6 - 5y \pmod{7}$ . Substituting this into the first equation, we have  $2(6 - 5y) + 3y = 12 - 10y + 3y \equiv 5 \pmod{7}$  so if the second congruence is satisfied, so is the first.

5. Find (all) the solutions of

$$\begin{aligned}4x + y &\equiv 5 \pmod{7} \\ x + 2y &\equiv 4 \pmod{7}.\end{aligned}$$

**Solution:** The first congruence is satisfied if and only if  $8x + 2y \equiv 10 \pmod{7}$  if and only if  $x + 2y \equiv 3 \pmod{7}$ . Thus the system of congruences is satisfied if and only if  $x + 2y \equiv 3 \pmod{7}$  and  $x + 2y \equiv 4 \pmod{7}$ . Since both statements cannot be true, there are no solutions to this congruence.

Alternatively, we can observe the second congruence is equivalent to  $x \equiv 4 - 2y \pmod{7}$ , and substituting that into the first congruence gives

$$4(4 - 2y) + y = 16 - 8y + y = 16 - 7y \equiv 2 \not\equiv 5 \pmod{7}$$

and thus again we see there are no solutions.

6. Find (all) the solutions of

$$\begin{aligned}x + y &\equiv 2 \pmod{7} \\ 3x + 2y &\equiv 3 \pmod{7}.\end{aligned}$$

**Solution:** We compute  $\Delta = 2 - 3 = -1 \equiv 6 \pmod{7}$ .  $(6, 7) = 1$ , so we can use our theorem. We have  $\Delta^{-1} \equiv -1$ . Thus we get

$$\begin{aligned}x &\equiv \Delta^{-1}(de - bf) \equiv (-1)(2 \cdot 2 - 1 \cdot 3) \equiv (-1)(1) \equiv 6 \pmod{7} \\ y &\equiv \Delta^{-1}(af - ce) \equiv (-1)(1 \cdot 3 - 3 \cdot 2) \equiv 3 \pmod{7}.\end{aligned}$$

Plugging these in to the original system confirms that they are solutions to the system of congruences.