Math 322 Fall 2019
Number Theory HW 4 Solutions
Due Friday, September 27

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.

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

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

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

   Solution: Notice that $10 \equiv -1 \mod 11$ and thus $10^\ell \equiv (-1)^\ell \mod 11$, so if ℓ is even then $10^\ell \equiv 1 \mod 11$ and if ℓ is even then $10^\ell \equiv -1 \mod 11$. Then

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

   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 $m \not| a$, then a has a multiplicative inverse $\mod m$. That is, suppose m is an integer such that every integer is either divisible by m, or has a multiplicative inverse $\mod m$. Then prove that m is prime.

   Solution: Recall that the linear congruene $ax \equiv b \mod m$ has a solution if and only if (a, m) divides b. Thus in particular $ax \equiv 1 \mod m$ 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. Suppose $m = ab$ for some integers $a, b > 0$, and $m \neq a$. If $m|a$ then $m = a$ and $b = 1$. If $m \not| a$, then a has a multiplicative inverse mod m, so $(a, m) = 1$. But $a|m$ so $a = 1$ and $b = m$. Thus m is prime by definition.

3. Find a solution to each system of congruences:

(a)

$$5x \equiv 3 \mod 23$$

Solution: Using the Euclidean algorithm, we can write

$$\begin{aligned} 23 &= 4 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

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

$$\begin{aligned} -9 \cdot 5 &\equiv 1 \mod 23 \\ -27 \cdot 5 &\equiv 3 \mod 23 \\ -4 \cdot 5 &\equiv 3 \mod 23 \\ 19 \cdot 5 &\equiv 3 \mod 23. \end{aligned}$$

-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)

$$\begin{aligned} x &\equiv 0 \mod 2 & \qquad x &\equiv 0 \mod 3 \\ x &\equiv 1 \mod 5 & \qquad x &\equiv 6 \mod 7 \end{aligned}$$

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

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

and thus

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

(c)

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

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

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

Then we have

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

4. Find (all) the solutions of

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

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

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

Thus the set of solutions is $\{(6, 0), (1, 1), (3, 2), (5, 3), (0, 4), (2, 5), (4, 6)\}$.

5. Find (all) the solutions of

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

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

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

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

and thus again we see there are no solutions.

6. Find (all) the solutions of

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

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

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

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