Math 116 Number Theory with Travis Kelm | **Homework #5 Congruences** | **Spring 2007 CSU - Fresno** | **Due 1 March 2007 Solutions**

In your solutions you must explain what you are doing using complete sentences.

Section 4.3 - The Chinese Remainder Theorem

Exercise 4abc: Find all of the solutions to each system of linear congruences

$$(a)\quad \begin{aligned} x &\equiv 4 \pmod{11} \\ x &\equiv 3 \pmod{17} \end{aligned} \qquad (b)\quad \begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned} \qquad (c)\quad \begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 6 \pmod{7} \end{aligned}$$

Solution:

(a) Note that -3 is an inverse of 11 mod 17 and that 2 is an inverse of 17 mod 11. So using the construction outlined in class, we get

$$\begin{aligned} &x \equiv (4)(17)(2) + (3)(11)(-3) \pmod{11 \cdot 17} \qquad \text{so} \\ &x = 37 + 187t \end{aligned}$$

(b) First observe that

- $3 \cdot 5 \equiv 1 \pmod{2}$
- $2 \cdot 5 \equiv 1 \pmod{3}$
- $2 \cdot 3 \equiv 1 \pmod{5}$

Thus using the construction outlined in class

$$\begin{aligned} &x \equiv (1)(15)(1) + (2)(10)(1) + (3)(6)(1) \pmod{2 \cdot 3 \cdot 5} \qquad \text{so} \\ &x = 53 + 30t \end{aligned}$$

(c) The first two congruences imply that x is a multiple of 6. My favorite multiple of 6 is 6 itself. Lucky Day! The number 6 satisfies the other two congruences as well. Thus the set of all solutions is

$$x = 6 + 240t \text{ (since } 2 \cdot 3 \cdot 5 \cdot 7 = 240)$$

□

Exercise 12: If eggs are removed from a basket 2,3,4,5,6, and 7 at a time, there remain, respectively, 1,2,3,4,5, and 0 eggs. What is the least number of eggs that could have been in the basket?

Solution: We can use the Chinese remainder theorem to solve the congruences

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 0 \pmod{7} \end{aligned}$$

This gives that

$$x \equiv 1 \times 105 \times 1 + 2 \times 70 \times 1 + 4 \times 42 \times (-2) + 0 \times 30 \times (-3) \pmod{2 \times 3 \times 5 \times 7}$$

So $x \equiv -91 \pmod{210}$. Naturally, there can't be a negative number of eggs in the basket. But the CRT says that our solution is only unique up to multiples of 210, so let's look at the congruence class of -91 modulo 210:

$$\{\ldots, -91, 119, 329, 539, \ldots\}$$

Note that 119 is the least positive residue. It can be verified than 119 satisfies all of the congruences demanded. □

Exercise 18: Does the system

$$\begin{aligned} x &\equiv 1 \pmod 8 \\ x &\equiv 3 \pmod 9 \\ x &\equiv 2 \pmod{12} \end{aligned}$$

have a solution? Be sure to explain why or why not.

Solution: Since 8 and 9 are relatively prime, we can use the Chinese remainder theorem to solve the congruences

$$\begin{aligned} x &\equiv 1 \pmod 8 \\ x &\equiv 3 \pmod 9 \end{aligned}$$

One comes up with $x \equiv 57 \pmod{72}$. Thus since 12 divides 72, we must also have $x \equiv 57 \pmod{12}$. But $57 \not\equiv 2 \pmod{12}$ thus there can be no solutions to this system of congruences. □

Section 5.1 - Divisibility Tests

Exercise *: Invent your own divisibility tests for 37, 101, and 33. I will give extra points for tests that I find especially inventive or useful.

Solution: Here are the ones that I thought of. They are all basically the same. (It was late and I was not feeling especially creative when I was typing these solutions.)

(37) Since $1000 \equiv 1 \pmod{37}$, given a number n, starting from the ones digit, break n into chunks of three digits. Then add all these three digit numbers together. The 3-chunk sum is divisible by 37 if and only if n is divisible by 37.

(101) Since $100 \equiv -1 \pmod{101}$, given a number n, starting from the ones digit, break n into chunks consisting of two digits. Then find the *alternating* sum of these two digit numbers. This alternating sum is divisible by 101 if and only if n is divisible by 101.

(33) Since $100 \equiv 1 \pmod{33}$, given a number n, starting from the ones digit, break n into chunks consisting of two digits. Then find the sum of these two digit numbers. This sum is divisible by 33 if and only if n is divisible by 33.

□

Section 6.1 - Wilson's Theorem and Fermat's Little Theorem

Exercise 4: Find the remainder when 5!25! is divided by 31.

Solution: Suppose that $x \equiv 5!\,25! \pmod{31}$. Multiply both sides by $(26)(27)(28)(29)(30)$ to get

$$(26)(27)(28)(29)(30)x \equiv 5!\,30! \pmod{31}$$

Using Wilson's theorem we then get $(26)(27)(28)(29)(30)x \equiv -(5!) \pmod{31}$. Note then that $26 \equiv -5, 27 \equiv -4, \ldots, 30 \equiv -1 \pmod{31}$ so we actually have

$$\begin{aligned} (-5)(-4)(-3)(-2)(-1)x &\equiv -(5!) \pmod{31} \qquad \text{or} \\ -120x &\equiv -120 \\ -4x &\equiv -4 \qquad \text{multiply both sides by } -8 \\ 32x &\equiv 32 \\ x &\equiv 1 \end{aligned}$$

Thus the remainder is 1 when 5! 25! is divided by 31.

□

Exercise 6: Find the remainder when $7 \times 8 \times 9 \times 15 \times 16 \times 17 \times 23 \times 24 \times 25 \times 43$ is divided by 11.

Solution: When we put on our mod 11 goggles we have

$$15 \equiv 4 \qquad 16 \equiv 5 \qquad 17 \equiv 6 \qquad 23 \equiv 1$$
$$24 \equiv 2 \qquad 25 \equiv 3 \qquad 43 \equiv 10$$

Thus

$$\begin{aligned} 7 \times 8 \times 9 \times 15 \times 16 \times 17 \times 23 \times 24 \times 25 \times 43 &\equiv 10! \\ &\equiv -1 \pmod{11} \qquad \text{using Wilson's theorem} \end{aligned}$$

Thus the remainder is 10 when $7 \times 8 \times 9 \times 15 \times 16 \times 17 \times 23 \times 24 \times 25 \times 43$ is divided by 11. □

Exercise 12: Use Fermat's Little Theorem to find the least positive residue of 2^{10^6} modulo 7.

Solution: Note that $10^6 = 6(166{,}666) + 4$. By Fermat's little theorem we have that $2^6 \equiv 1 \pmod 7$. This gives

$$2^{10^6} = (2^6)^{166{,}666}\, 2^4 \equiv 2^4 \equiv 2 \pmod 7$$

So 2 is the least positive residue of 2^{10^6} modulo 7. □

Exercise 16: Show that if n is composite integer other than 4, then $(n-1)! \equiv 0 \pmod n$.

Solution: Before we begin we should take note of the easy fact that if $a|n$ then $a \leq (n-1)$. Hence if $a|n$ then $a|(n-1)!$.

Also note that to show $(n-1)! \equiv 0 \pmod n$ it suffices to demonstrate that n divides $(n-1)!$. This is what we will do.

Let p be a prime factor of n. Since n is composite $n = pc$ where $c \neq 1$. If $c \neq p$ then we are done as p and c are two distinct divisors of n, and hence two distinct divisors of $(n-1)!$. Thus $n = pc$ divides $(n-1)!$ as desired.

If $c = p$ then we have that $n = p^2$. Since we are assuming that $n \neq 4$ we must have that $p \neq 2$. Thus observe that p and $2p$ are both less than $p^2 = n$ and hence p and $2p$ are distinct factors of $(n-1)!$. Thus $p(2p) = 2p^2 = 2n$ divides $(n-1)!$. It follows that n divides $(n-1)!$ as desired.

□