Math 116 Number Theory with Travis Kelm	**Homework #4 Congruences**	**Spring 2007 CSU - Fresno**	**Solutions**

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

Section 3.7 - Linear Diophantine Equations

Exercise 2bc: For each of the following Diophantine equations either find all the solutions or explain why there are no integral solution.

b) $12x + 18y = 50$ c) $30x + 47y = -11$

Solution: (b) $\gcd(12, 18) = 6$ and 6 does **not** divide 50, thus there are no solutions

(c) $\gcd(30, 47) = 1$ so there is a solution. Using the Euclidean algorithm we get $30(11) + 47(-5) = 1$ hence

$$x_0 = -121 \qquad \text{and} \qquad y_0 = 55$$

is one solution to $30x + 47y = -11$. By the Fundamental Theorem of Linear Diophantine equations we then get all solutions have the form

$$x = -121 + 47t \qquad \text{and} \qquad y = 55 - 30t$$

□

Exercise 4: A student returning home from Europe changes his euros and Swiss francs into U.S. dollars. The exchange rates are \$1.11 for each euro and \$0.83 for each franc. If the student receives a total of \$46.26 how much of each type of currency was exchanged?

Solution: This question is asking us to solve the linear diophantine equation

$$111e + 83f = 4626$$

Note that the $\gcd(111, 83) = 1$ thus we know that there is a solution. Using the Euclidean algorithm, we get that □

Exercise 10: At a clambake the cost of a lobster dinner is \$11 and the cost of chicken dinner is \$8. What can you conclude if the total bill is is each of the following amounts:

\$777 \$96 \$69

Exercise 13: Which combinations of pennies, dimes and quarters have a total value of \$0.99?

Not quite in book: Is it possible to have 50 coins, a mix of pennies, dimes and quarters, with a total value of \$3.00? What about \$2.00?

Solution: For the \$3.00 problem we have two equations going for us:

$$\begin{aligned} p + 10d + 25q &= 300 \\ p + d + q &= 50 \end{aligned}$$

By subtracting the second equation from the first we get:

$$9d + 24q = 250$$

Since the $\gcd(9, 24) = 3 \nmid 250$ we can conclude that there is no solution for the \$3.00 problem.

For the \$2.00 problem we have two equations going for us:

$$\begin{aligned} p + 10d + 25q &= 200 \\ p + d + q &= 50 \end{aligned}$$

By subtracting the second equation from the first we get:

$$9d + 24q = 150$$

This is a Diophantine equation that has solutions. Using the Euclidean algorithm, guess-and-check, or whatever, one sees that

$$d_0 = -2 \qquad \text{and} \qquad q_0 = 7$$

is an initial solution. Thus by the theory of Diophantine equations, all solutions have the form:

$$d = -2 + 8t \qquad \text{and} \qquad q = 7 - 3t$$

Note also that the number of pennies is $p = 50 - d - q$ so the set of solutions for all three variables is:

$$d = -2 + 8t \qquad \text{and} \qquad q = 7 - 3t \qquad \text{and} \qquad p = 45 - 5t$$

Finally, we note that the only solutions that make sense in this case are the positive solutions. There are two such solutions, namely when $t = 1$ or $t = 2$. So our two sets of solutions are:

$$\begin{array}{ll} p = 40 & p = 35 \\ d = 6 & d = 14 \\ q = 4 & q = 1 \end{array}$$

□

Section 4.1 - Intro to Congruences

Exercise 2: Determine whether each of the following pairs are congruent modulo 7:

$$\begin{array}{ccc} 1, 15 & 2, 99 & -9, 5 \\ 0, 42 & -1, 8 & -1, 699 \end{array}$$

Solution:

- $7 | (15 - 1)$ so $15 \equiv 1 \pmod 7$.
- 42 is divisible by 7 so $42 \equiv 0 \pmod 7$.
- $7 | (99 - 2) = 97$ so $99 \equiv 2 \pmod 7$.
- $-1 - 8 = -9$ is not a multiple of 7 so $-1 \not\equiv 8$.
- $7 | (-9 - 5) = -14$ so $-9 \equiv 5 \pmod 7$.
- $7 | (-1 - 699) = -700$ so $-1 \equiv 699 \pmod 7$.

□

Exercise 4: Show that if a is an even integer, then $a^2 \equiv 0 \pmod 4$ and if a is an odd integer, then $a^2 \equiv 1 \pmod 4$.

Solution: Since the gcd is the smallest possible positive linear combination of a and $a + 2$, we must have that $\gcd(a, a + 2) \le 2$ since $2 = 1(a + 2) - 1(a)$. If a is even, then so is $a + 2$, thus 2 does divide both a and $a + 2$ so we must have that $\gcd(a, a + 2) = 2$. But if a is odd then 2 cannot be a divisor of a thus we must have that $\gcd(a, a + 2) = 1$. □

Exercise 6: Find the least non-negative residue modulo 13 of each of the following integers:

$$\begin{array}{ccc} 22 & 1001 & -100 \\ 100 & -1 & -1000 \end{array}$$

Solution:

1. $22 \equiv 9 \pmod{13}$
2. $100 \equiv 9 \pmod{13}$
3. $1001 \equiv 0 \pmod{13}$
4. $-1 \equiv 12 \pmod{13}$
5. $-100 \equiv 4 \pmod{13}$
6. $-1000 \equiv 1 \pmod{13}$

□

Exercise 8: Show that if a, b, m and n are integers such that $m > 0$, $n > 0$, $n|m$, and $a \equiv b \pmod{m}$ then $a \equiv b \pmod{n}$.

Solution: $a \equiv b \pmod{m} \Longrightarrow a = b + km$ for some integer m. Since $n|m$ we have that $m = tn$ for some integer t. Thus we can make a substitution to get $a = b + (kt)n$. This final equaiton implies that $a \equiv b \pmod{n}$. □

Exercise 14: Construct a multiplication table modulo 6.

Solution:

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

□

Exercise 24: Give a complete system of residues modulo 13 using only odd numbers.

Solution: The least non-negative residue system is

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

So to answer the question we simply replace each even number with a congruent odd number. The simplest thing is to simply add 13 to each even number. This gives

$$\{13, 1, 15, 3, 17, 5, 19, 7, 21, 9, 23, 11, 25\}$$

Note, however that there are many other possible solutions to thei problem. □

Exercise 33: Find the least positive residue of each of the following:

- 3^{10} modulo 11
- 2^{12} modulo 13
- 5^{16} modulo 17
- 3^{22} modulo 23
- Propose a theorem based upon the above congruences.

Solution: They are all congruent to 1. These are all examples of Fermat's Little Theorem. □

Exercise 34: Find the least positive residue of each of the following:

- 6! modulo 7
- 10! modulo 11
- 12! modulo 13
- 16! modulo 17
- Propose a theorem based upon the above congruences.

Solution: They are all congruent to -1. These are all examples of Wilson's Theorem. □

Section 4.2 - Linear Congruences

Exercise 2: Find all solutions to each of the following:

$$3x \equiv 2 \pmod{7} \qquad 17x \equiv 14 \pmod{21} \qquad 128x \equiv 833 \pmod{1001}$$
$$6x \equiv 3 \pmod{9} \qquad 15x \equiv 9 \pmod{25} \qquad 987x \equiv 610 \pmod{1597}$$

Exercise 6: For which integers c with $0 \leq c < 30$ does the congruence $12x \equiv c \pmod{30}$ have solutions? When there are solutions, how many incongruent solutions are there?

Exercise 10:

1. Determine the integers from 1 to 14 that have an inverse modulo 14.
2. Find the inverses of each of the integers from the previous part that have inverses.

Solution:

1. As is shown in a later homework, the integers that have an inverse are precisely those integers that are relatively prime to 14. They are $\{1, 3, 5, 9, 11, 13\}$.
2. (a) 1 is its own inverse.
   (b) 3 and 5 are inverses.
   (c) 9 and 11 are inverses.
   (d) 13 is its own inverse.

□