

## Session 10, July 20

### The Chinese Remainder Theorem

1. Gauss had a certain number of chocolate chip cookies. When he divided his cookies into piles of 2, he had 1 left over. When he divided them into piles of 7, he had 4 left over. How many cookies did he have?
2. Is there more than one solution to Problem 1? If so, find all possible number of cookies that Gauss could have had.
3. Fermat had many oatmeal chocolate chip cookies. When he divided his cookies into piles of 2, he had 1 left over. When divided into piles of 5, there were 3 left over. When divided into piles of 7, there were 4 left over. Find all possible number of cookies that Fermat could have had.
4. Find all integral solutions  $(m, n)$  to the linear Diophantine equation  $2m + 7n = 3$ .

Back to Gauss and his cookies... Let  $x$  be the number of his cookies. Then, we can model the situation in the problem with the following *system of congruences*:

$$x \equiv 1 \pmod{2}$$

$$x \equiv 4 \pmod{7}$$

5. (a) Write an expression that represents all integers equal to 1 mod 2.  
 (b) Write an expression that represents all integers equal to 4 mod 7.  
 (c) Use Problems 4, 5(a), and 5(b) to show that the solution to Gauss' cookie problem is  $x \equiv 11 \pmod{14}$ .
6. Find all integral solutions of the following system of congruences.
 

(a) $x \equiv 14 \pmod{15}$	(b) $y \equiv 7 \pmod{11}$
$x \equiv 25 \pmod{31}$	$y \equiv 12 \pmod{29}$
7. Back to Fermat's cookies...
  - (a) Model his situation with a system of congruences.
  - (b) Solve the system for  $x$ . You may find your work in Problem 5(c) helpful.
8. Consider the following system of congruences.

$$x \equiv 4 \pmod{7}$$

$$x \equiv 8 \pmod{11}$$

$$x \equiv 5 \pmod{13}$$

We will use a *localization* method to solve this system.

Let  $x_1$  be an integer such that    Let  $x_2$  be an integer such that    Let  $x_3$  be an integer such that

$$x_1 \equiv 1 \pmod{7}$$

$$x_2 \equiv 0 \pmod{7}$$

$$x_3 \equiv 0 \pmod{7}$$

$$x_1 \equiv 0 \pmod{11}$$

$$x_2 \equiv 1 \pmod{11}$$

$$x_3 \equiv 0 \pmod{11}$$

$$x_1 \equiv 0 \pmod{13}$$

$$x_2 \equiv 0 \pmod{13}$$

$$x_3 \equiv 1 \pmod{13}$$

- (a) Explain why  $x = 4x_1 + 8x_2 + 5x_3$  solves our original system of congruences.
- (b) It's easy to make  $x_1$  equal to  $0 \pmod{11}$  and  $13$ . Just make it a multiple of  $11 \cdot 13$ . So, we want  $x_1$  to look like  $x_1 = 11 \cdot 13 \cdot k$  for some integer  $k$ . Thus, we have:

$$\begin{aligned} 11 \cdot 13 \cdot k &= 1 \pmod{7} && \text{(Why?)} \\ 143k &= 1 \pmod{7} \\ 3k &= 1 \pmod{7} && \text{(Why?)} \end{aligned}$$

To find  $k$ , we need to multiply both sides by the inverse of 3 in  $\mathbf{Z}_7$ , namely 5. So...

$$\begin{aligned} 5 \cdot 3k &= 5 \cdot 1 \pmod{7} \\ k &= 5 \pmod{7} \\ k &= 5 + 7n && \text{(Why?)} \end{aligned}$$

Therefore,  $x_1 = 11 \cdot 13 \cdot (5 + 7n) = 715 + 1001n$ . In other words,  $x_1 = 715 \pmod{1001}$ .

- (c) Solve for  $x_2$  and  $x_3$ , and then find the value of  $x$  which solves our original system. Check that this solution satisfies all three equations.
9. Solve the following system. Find the smallest positive solution.

$$\begin{aligned} x &= 3 \pmod{12} \\ x &= 17 \pmod{35} \\ x &= 2 \pmod{11} \end{aligned}$$

10. The Chinese Remainder Theorem (CRT) basically states that a system of congruences is guaranteed to have a solution if all the mod's are relatively prime to each other. Write a convincing argument explaining why the CRT is true.
11. But what if the mod's are *not* relatively prime? Consider the following system.

$$\begin{aligned} x &= 2 \pmod{6} \\ x &= 1 \pmod{3} \\ x &= 2 \pmod{11} \end{aligned}$$

- (a) Explain why this system has no solution. (Don't just say "Because the mod's are not relatively prime.")
- (b) What goes wrong when you try to use the localization method on this system? Explain.
12. Consider the following two systems.

$$\begin{array}{ll} x = 3 \pmod{24} & y = 3 \pmod{24} \\ x = 8 \pmod{30} & y = 9 \pmod{30} \end{array}$$

Which system has a solution? When the mod's are *not* relatively prime, how can you tell if a system has a solution or not? Explain.

Here are a couple of real life (well, sort of. . .) problems using the CRT.

13. A band of 17 stock brokers stole a sack of hundred dollar bills. When they were divided equally, there were three left over. So, one associate was sent on vacation. Then, when the sack was divided equally, there were 10 bills left. So, another member of the crew was asked to take a break. Now, the bills could be distributed with none left over. How many bills were in the sack?
14. (This a Problem of the Week question from the Interactive Mathematics Program.)

Shelly (I think that was her name in the problem. . .) was on her way home from grocery shopping. But she tripped and fell off of her bike. Her grocery bags fell on the ground, among them a bunch of eggs. Now, Shelly did not remember how many eggs she had bought, but she did recall the following. When the eggs were divided into groups of two, there was one egg left over. When divided into groups of three, there was one left over. Similarly, when divided into groups of four, five, and six, there was one egg left over. However, when she divided the eggs into groups of seven, there was no egg left over.

How many eggs did Shelly buy? Is there more than one possible solution?

15. (Further exploration) Find a polynomial that satisfies the following table.

$x$	$f(x)$
-1	9
2	-6
5	15

Hint: Use the Chinese Remainder Theorem, and the fact that if  $f(a) = 0$ , then  $(x - a)$  is a factor of  $f(x)$ .

16. (Yikes!) Solve the following system.

$$\begin{aligned}3x &= 5 \pmod{23} \\5x &= 7 \pmod{24} \\7x &= 3 \pmod{25}\end{aligned}$$