Modular Arithmetic
Notes for Wednesday June 18
ACCESS 2003

Jim left us with three questions yesterday:

1) Construct addition and multiplication tables, and then additive inverse and multiplicative inverse tables, for mod 8 arithmetic. What happens?
2) Is 1003 prime?
3) Try to find a multiplicative inverse for 123 mod 1003. (This one is hard!)

What did you figure out for problem 1?

1) continued: Consider the general question of when numbers have multiplicative inverses in modular arithmetic. Use the mod 8 table on the blackboard, and also the two multiplication tables on the next page, to come up with a conjecture about when you can find multiplicative inverses in modular arithmetic; given a residue "m" and a modulus "n", find conditions so that you can solve

$$mx \equiv 1 \mod n$$

for the multiplicative inverse x.

Also on the next page, circle the rows which correspond to numbers which do have multiplicative inverses, and find all the properties you can which distinguish these rows from the "bad" ones. Can you explain your observations?

Mod 15 multiplication table

$$\begin{bmatrix}
X & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\
1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\
2 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 1 & 3 & 5 & 7 & 9 & 11 & 13 \\
3 & 3 & 6 & 9 & 12 & 0 & 3 & 6 & 9 & 12 & 0 & 3 & 6 & 9 & 12 \\
4 & 4 & 8 & 12 & 1 & 5 & 9 & 13 & 2 & 6 & 10 & 14 & 3 & 7 & 11 \\
5 & 5 & 10 & 0 & 5 & 10 & 0 & 5 & 10 & 0 & 5 & 10 & 0 & 5 & 10 \\
6 & 6 & 12 & 3 & 9 & 0 & 6 & 12 & 3 & 9 & 0 & 6 & 12 & 3 & 9 \\
7 & 7 & 14 & 6 & 13 & 5 & 12 & 4 & 11 & 3 & 10 & 2 & 9 & 1 & 8 \\
8 & 8 & 1 & 9 & 2 & 10 & 3 & 11 & 4 & 12 & 5 & 13 & 6 & 14 & 7 \\
9 & 9 & 3 & 12 & 6 & 0 & 9 & 3 & 12 & 6 & 0 & 9 & 3 & 12 & 6 \\
10 & 10 & 5 & 0 & 10 & 5 & 0 & 10 & 5 & 0 & 10 & 5 & 0 & 10 & 5 \\
11 & 11 & 7 & 3 & 14 & 10 & 6 & 2 & 13 & 9 & 5 & 1 & 12 & 8 & 4 \\
12 & 12 & 9 & 6 & 3 & 0 & 12 & 9 & 6 & 3 & 0 & 12 & 9 & 6 & 3 \\
13 & 13 & 11 & 9 & 7 & 5 & 3 & 1 & 14 & 12 & 10 & 8 & 6 & 4 & 2 \\
14 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{bmatrix}$$

Mod 7 multiplication table

$$\begin{bmatrix}
X & 1 & 2 & 3 & 4 & 5 & 6 \\
1 & 1 & 2 & 3 & 4 & 5 & 6 \\
2 & 2 & 4 & 6 & 1 & 3 & 5 \\
3 & 3 & 6 & 2 & 5 & 1 & 4 \\
4 & 4 & 1 & 5 & 2 & 6 & 3 \\
5 & 5 & 3 & 1 & 6 & 4 & 2 \\
6 & 6 & 5 & 4 & 3 & 2 & 1
\end{bmatrix}$$

Terminology:

Prime number:

Composite number:

Prime factorization

“d divides m”, d / m .

Common divisor of m and n

Greatest common divisor of m and n, $\gcd(m,n)$.

We have been led to the following important fact:

Theorem: We can solve the multiplicative inverse equation

$$mx \equiv 1 \mod n$$

if and only if

$$\gcd(m,n) = 1$$

The explanation of this theorem can be broken into two halves:
Part I: If $\gcd(m,n) = d > 1$, then m has no multiplicative inverse mod n. This is because when you create row m of the multiplication table the factor d will divide each term in this row. Thus there will not be a “1” in this row, and m will not have a multiplicative inverse.

Part II: If $\gcd(m,n) = 1$, then m does have a multiplicative inverse mod n. If you like logic arguments you can deduce an explanation of this fact based on the various properties you have discovered for “good” and “bad” rows in the multiplication table. But there is a neat algorithm which will prove this part of the theorem, and at the same time construct the multiplicative inverse, so we’ll get our proof of Part II from there.

Back to Jim's questions:

2) Is 1003 prime? (answer: no)

3) Can we find a multiplicative inverse to 123, mod 1003?
Well, let's check whether gcd(1003,123)=1. You can do this with prime factorization, but you can also use the **Euclidean Algorithm**: We create a table of successive quotients and remainders, starting with the division problem 1003/123 in the first row. In the second row we take the "m" and"r" terms in columns 2 and 3, slide them over to columns 1 and 2, and repeat the division process, this time for 123/19. Then continue:

n (numerator)	m (denominator)	r (remainder	q (quotient)
1003	123	19	8
123	19	9	6
19	9	1	2
9	1	0	9

What good is this table? Answer1: gcd(m,n) is the same on each row. Here's why. If we look at the numerators and denominators for two successive rows they have the form

numerator	denominator
n	m
m	r

where r was the remainder from the first row. But the first row represents the equivalent equations

$$\frac{n}{m} = q + \frac{r}{m}$$
$$n = qm + r$$
$$r = n - qm$$

From the third equation we see that if d / n and d / m, then d / r, so any divisor of m and n is also a divisor of m and r. From the second equation we see that if d / m and d / r then also d / n, so any divisor of m and r is also a divisor of m and n.

Thus

$$\gcd(1003,123) = \gcd(123,19) = \gcd(19,9) = \gcd(9,1) = 1$$

In general, the Euclidean algorithm will terminate after a finite number of steps with a remainder of zero (why?), and then the preceding denominator will be the greatest common denominator of the original m and n!

What good is this table? Answer 2: In case $\gcd(m,n) = 1$, you can use the table from the bottom up in order to find the multiplicative inverse for m mod n. Actually, start on the second to last row and express the remainder 1 in terms of the current n and m:

$$r = n - qm$$

$$1 = 19 - 2 * 9$$

Use the row above to express the remainder 9 in terms of that row's m and n:

$$9 = 123 - 6 * 19$$

and substitute this expression into the previous equation:

$$1 = 19 - 2 * (123 - 6 * 19)$$

$$1 = -2 * 123 + 13 * 19$$

Now use the top row to get rid of the 19's:

$$19 = 1003 - 8 * 123$$

$$1 = -2 * 123 + 13 * (1003 - 8 * 123)$$

$$1 = 1 = -106 * 123 + 13 * 1003$$

So,

$$-106 * 123 \equiv 1 \quad \text{mod } 1003$$

$$897 * 123 \equiv 1 \quad \text{mod } 1003$$

This needs practice:

4) Find $(26)^{-1} \quad \text{mod } 53$

5) Solve the following equation for x

$$26x \equiv 15 \quad \text{mod } 53$$

6) Find $(38)^{-1} \quad \text{mod } 123$

A table of powers, mod 15

$$\left[\begin{array}{ccccccccccccccc}
P & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
2 & 2 & 4 & 8 & 1 & 2 & 4 & 8 & 1 & 2 & 4 & 8 & 1 & 2 & 4 \\
3 & 3 & 9 & 12 & 6 & 3 & 9 & 12 & 6 & 3 & 9 & 12 & 6 & 3 & 9 \\
4 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 \\
5 & 5 & 10 & 5 & 10 & 5 & 10 & 5 & 10 & 5 & 10 & 5 & 10 & 5 & 10 \\
6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\
7 & 7 & 4 & 13 & 1 & 7 & 4 & 13 & 1 & 7 & 4 & 13 & 1 & 7 & 4 \\
8 & 8 & 4 & 2 & 1 & 8 & 4 & 2 & 1 & 8 & 4 & 2 & 1 & 8 & 4 \\
9 & 9 & 6 & 9 & 6 & 9 & 6 & 9 & 6 & 9 & 6 & 9 & 6 & 9 & 6 \\
10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\
11 & 11 & 1 & 11 & 1 & 11 & 1 & 11 & 1 & 11 & 1 & 11 & 1 & 11 & 1 \\
12 & 12 & 9 & 3 & 6 & 12 & 9 & 3 & 6 & 12 & 9 & 3 & 6 & 12 & 9 \\
13 & 13 & 4 & 7 & 1 & 13 & 4 & 7 & 1 & 13 & 4 & 7 & 1 & 13 & 4 \\
14 & 14 & 1 & 14 & 1 & 14 & 1 & 14 & 1 & 14 & 1 & 14 & 1 & 14 & 1
\end{array}\right]$$