Modular Arithmetic
Notes for Wednesday June 15
ACCESS 2005

Yesterday, Jim introduced us to the idea of using modular (clock) arithmetic for encryption, after we first converted letters to numbers. Do you remember how to describe the encryption and decryption functions for a Caesar shift? Using multiplication to make an encryption cipher led us to the question of whether we can find multiplicative inverses in modular arithmetic, in order to find the decryption function. Surprisingly, the answer to the multiplicative inverse problem goes all the way back to the ancient Greeks, and to the Euclidean algorithm for finding the greatest common divisor for a pair of numbers.

As Jim will explain today (and as you've been reading), RSA cryptography, a key element in secure internet transactions, is based on encryption functions which raise (huge) numbers to (huge) powers, with respect to (huge) moduli. The amazing and amazingly important feature of this sort of "public key cryptography" is that you can tell everyone how to encrypt messages sent to you without giving away the secret of how you will decrypt them. When you create your encryption algorithm (which you will make public), and your decryption algorithm (which you will keep secret), you'll need to do some modular arithmetic computations. In particular, you'll need to solve a certain multiplicative inverse problem. (Actually, you'll get MAPLE to do the grunge work.) That's why we'll review multiplicative inverses and the Euclidean algorithm this morning – because of their role in RSA cryptography.

1) Consider the general question of when numbers have multiplicative inverses in modular arithmetic. NOT ALL NUMBERS DO!

1a) Use the two multiplication tables on the next page to construct multiplicative inverse tables, when the modulus is n=7 and when it is n=15. (You could squeeze these tables in next to the multiplication tables.)

1b) Call a clock number "good" if it has a multiplicative inverse mod n. What properties do good numbers have relative to n, and what properties do the corresponding rows in the multiplication table have? Call a clock number "bad" if it does not have a multiplicative inverse, mod n. List all the properties of bad numbers and bad rows. Explain the "why" behind each of your observations, if you can!

Mod 15 multiplication table

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

Mod 7 multiplication table

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

2) **Terminology:** These words and phrases pop up in our discussion:

Prime number:

Composite number:

Prime factorization:

"d divides n", d / n.

Common divisor of b and n

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

"b and n are relatively prime":

residue (or clock number) of b, mod n.

3) From our work in (1) we have been led to the following important fact:

Theorem: We can solve the multiplicative inverse equation for b,

$$bx \equiv 1 \mod n$$

if and only if

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

The explanation of this theorem can be broken into two halves:
Part I: If $\gcd(b, n) = d > 1$, then b has no multiplicative inverse mod n. This is because when you create row b 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 b will not have a multiplicative inverse.

Part II: If $\gcd(b, n) = 1$, then b 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 the Euclidean algorithm 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.

4) Euclid in action. Can we find the multiplicative inverse for 68, mod 1003? Well, we can use the Euclidean algorithm to find out whether or not $\gcd(68,1003) = 1$: Fill in the table:

a (numerator)	b (denominator)	r (remainder	q (quotient)
1003	68		

Answer:

By the way, now would be a good time to carefully verify that Euclid's algorithm really does construct the greatest common divisor. Here's why:

Focus on the numerator (a) and denominator (b) entries in each successive row. We can show that gcd(a,b) stays the same as we move down successive rows, and so by the time we get to the row with zero remainder, the last b-entry will be the gcd of the bottom row (since it divides the bottom row's a value). Thus this last b-entry is also the gcd of the top row!

If we look at the numerators and denominators for two successive rows they have the form

numerator	denominator
a	b
b	r

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

$$\frac{a}{b} = q + \frac{r}{b}$$
$$a = qb + r$$
$$r = a - qb$$

From the third equation we see that if d / a and d / b, then d / r, so any divisor of a and b is also a divisor of b and r. From the second equation we see that if d / b and d / r then also d / a, so any divisor of b and r is also a divisor of b and a. Since the common divisors of a and b are exactly the common divisors of b and r, deduce

$$\gcd(a,b) = \gcd(b,r)$$

Thus

$$\gcd(1003,68) = \gcd(68,51) = \gcd(51,17) = 17$$

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

5a) Can we find a multiplicative inverse to 123, mod 1003? Here's the filled-in Euclidean algorithm table, from which you can see that gcd(1003,123)=1.

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

Thus we should be able to solve the inverse equation, using the hocus-pocus Jim showed us at the end of his presentation yesterday. We should practice this!

Here's how it goes: In case $\gcd(a,b)=1$, you can use the table from the bottom up in order to find the multiplicative inverse for b mod a. Actually, start on the second to last row and express the remainder 1 in terms of the current a and b:

$$r = a - q*b$$

$$1 = 19 - 2*9$$

Notice at this stage we have expressed 1 as a linear combination of the "a" and "b" values in the third row of our table. We use the next higher row to express the remainder 9 in terms of that row's a and b:

$$9 = 123 - 6*19$$

Substitute this expression for 9 into the previous equation, and we get:

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

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

At this stage we have expressed the number 1 as a linear combination of the "a" and "b" values from row 2! Now use the top row to substitute the 19's, in terms of that row's a and b, 1003 and 123:

$$19 = 1003 - 8*123$$

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

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

So,

$$-106*123 \equiv 1 \mod 1003$$

$$897*123 \equiv 1 \mod 1003$$

This needs practice!!!!

5b) Find $(8)^{-1} \mod 15$ with the Euclidean algorithm, and compare to the table on page 2.

5c) Find $(26)^{-1} \mod 53$

5d) Use 5c) to solve the following equation for x, and check your answer:

$$26x \equiv 15 \mod 53$$

5e) Find $(38)^{-1} \mod 123$

5f) Solve $12345*x \equiv 6 \mod 54321$. Hint: Start by using the Euclidean algorithm to find $\gcd(54321,12345)$, which is NOT 1.

For future reference:

A table of powers, mod 15

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