Tue.,April 20, 2004

Some notes on modular arithmetic.

A prime number is divisible by two positive factors, 1 and itself. We do not consider 1 to be a prime. The primes are infinite (first proved by Euclid). For all of what follows we'll be talking about non-negative integers, though often the same results will hold for negative integers as well.

gcd(m,n) = greatest common divisor of m and n. This is the largest number that is a factor of both m and n.

For example, gcd(12, 22) = 2
gcd(1,10)=1
gcd(–10,10)=10

To find the gcd of two numbers, we can use the **Euclidean algorithm**, a very efficient and ancient algorithm (This algorithm is found in book VII of Euclid's Elements, written around 300 BC, but some historians credit it to Eudoxus). The algorithm is very fast at finding the greatest common factor for two numbers m and n, even when we don't know whether m and n are prime, and if they are not prime, what their factors are! The algorithm uses the "division algorithm", which divides a number n by a smaller number m, leaving a remainder r. Then n is expressed as a multiple of m plus the remainder r. If $m<n$, and $n = km + r$, where $0 \leq r < m$, then it turns out that

gcd(m,n) = gcd(m,r)

Within the Euclidean algorithm, we apply the division algorithm over and over until we get remainder 0; the gcd is the last non-zero remainder in this process. For example,

gcd(18,22) = gcd (4,18), since 22 = 1(18) + 4
gcd(4,18) = gcd(2,4), since 18 = 4(4) + 2
gcd(2,4) = gcd(0,2), since 4 = 2(2) + 0.
gcd(18,22) = 2

This procedure also allows us to express the gcd as a **linear combination** of the two original numbers m and n We work our way “upwards” after applying the Euclidean algorithm, then “collect terms”. For example,

$$\begin{aligned} 2 &= 1(18) - 4(4) \\ &= 1(18) - 4(\ 1(22) - 1(18)) \\ &= -4(22) + 5(18) \end{aligned}$$

HW: Find the gcd(40,65) using the Euclidean Algorithm, then reverse the process to solve gcd(40,65) = x(40) + y(65).

Two numbers m and n are **relatively prime if** gcd(m,n)=1.

For example, 6 and 7 are relatively prime, but 6 and 8 are not.

We define the “Euler phi function” **phi(n)** = the number of numbers from 1 to n that are relatively prime to n.

For example, phi(6) = 2, since of the numbers 1,2,3,4,5,and 6, only 1 and 5 are relatively prime to 6.

HW: Find phi(n) for all numbers 1 through 30, and look for patterns.

In class we observed that

$$\text{phi}(p) = p-1, \text{ for a prime } p,$$

$$\text{phi}(p^2) = p(p-1), \text{ for any prime } p,$$

and

$$\text{phi}(pq) = (p-1)(q-1), \text{ for any primes } p \text{ and } q.$$

HW: Find phi(p^k), for any prime p and integer k > 2.

Fermat’s Little Theorem: If a is not divisible by prime p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Euler's Theorem extends and generalizes Fermat's Little Theorem:
If a is relatively prime to n, then

$$a^{phi(n)} \equiv 1 \ \mathrm{mod}(n)$$

HW: confirm this theorem for several n less than 30, using a = 2.

Another central theorem in modular arithmetic, the **Chinese Remainder Theorem**, allows for fast calculation with very large numbers, accomplished by parallel processors. It was first stated as a special case (see Knuth, vol. 2, pg 287), by Sun Tsu, between A.D. 280 and 473. It was first proved and generalized by Ch'in Chiu-Shao in 1247:

Chinese Remainder Theorem. Let m_1, m_2,... , m_n, be pairwise relatively prime positive integers. The system of "linear congruences"

$$x \equiv a_1 \ (\mathrm{mod}\ m_1)$$

$$x \equiv a_2 \ (\mathrm{mod}\ m_2)$$

.

.

.

$$x \equiv a_n \ (\mathrm{mod}\ m_n)$$

has a unique solution modulo $m= m_1\ m_2\dots\ m_n$ (Unique here means there is one solution from 1 to m.)

The proof is "constructive;" we build the solution by first letting

$$M_k = m/m_k \text{ , for all } k=1,2,\dots,n$$

Then for each k, we find y_k such that

$$M_k\, y_k \equiv 1 \ (\mathrm{mod}\ m_k)$$

(We can do this using the Euclidean algorithm, since M_k and m_k are relatively prime, and so we can find their gcd of 1 as a linear combination of M_k and m_k. We'll do an example in class.)

The solution is then

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n$$

Example: Solve

$x \equiv 2 \pmod{3}$
$x \equiv 4 \pmod{5}$
$x \equiv 5 \pmod{7}$

We let m = (3)(5)(7) = 105, M_1 = 105/3 = 35, M_2 = 105/5 = 21, M_3 = 107/7 = 15.
Also,

$y_1 \equiv 2$, $y_2 \equiv 1$, and $y_3 \equiv 1$,

since

$35(2) \equiv 1 \pmod{3}$,
$21(1) \equiv 1 \pmod{5}$,
$15(1) \equiv 1 \pmod{7}$

The solution is then

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2(35)(2) + 4(21)(1) + 5(15)(1) = 299 \equiv 89$ (mod 105)

Notice that 89 leaves remainders of 2 when divided by 3, 4 when divided by 5, and 5 when divided by 7.

Added on Friday, Apr. 23, 2004:

Here's another example of how we use Euclid's algorithm to find the gcd of two numbers, then express the gcd as the linear combination of the two numbers, then use that to solve a "linear congruence." First, I'll define some of the terminology and show how it all ties together.

A **linear congruence** is one of the form

$$ax \equiv b \pmod{m}$$

(Actually, to be completely general, we'd want to consider all congruences of the form $ax + b \equiv c \pmod{m}$, but this is easily reduced by subtracting b from both sides.) Not all of these "congruences" (they're NOT equations!) can be solved, in the same way that the equation

$$4x = 5$$

has no solution among the integers.

For example, if we try to find a solution to

$$4x \equiv 5 \pmod{6}$$

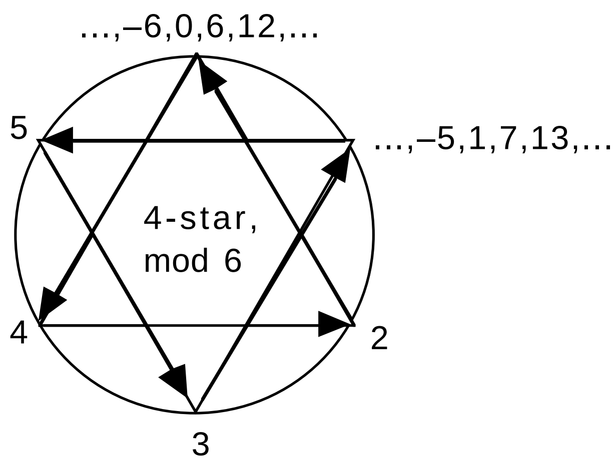
we can see that all possible substitutions for x don't work:

$$4(0) \equiv 0 \pmod{6}$$
$$4(1) \equiv 4 \pmod{6}$$
$$4(2) \equiv 2 \pmod{6}$$
$$4(3) \equiv 0 \pmod{6}$$
$$4(4) \equiv 4 \pmod{6}$$
$$4(5) \equiv 2 \pmod{6}$$

We can visualize what's going on with these multiples of 4 by looking at what are called "Poinsot stars". This geometric depiction is also a great way to study any linear congruence $ax + b \equiv c \pmod{m}$. They are named for the French mathematician who introduced them in the 1800's. An easy-to-use java applet for making and investigating them can be found at
http://www.geocities.com/SoHo/Exhibit/8033/room/poinsot/poinsot.ht

ml (For more help with how to use them see http://nebula.deanza.fhda.edu/math/karl/apdffiles/Poinsot.stars.pdf)

Here is the Poinsot 4-star, mod 6:



Notice that we have labeled the six points on this mod 6 clock with the numbers 0,1,2,3,4, and 5. For 0 and 1 I've added in a few more so you can see that each number actually represents the entire equivalence class, as in our text (in congruence arithmetic these are sometimes called "residues", a term that reminds you that they're what are left over after you divide a number by the modulus, in this case 6.) We tend to use 0 through 5, the "least non-negative" residues, mod 6, in place of any other numbers, just to simplify things.

Notice also that when we start at 0 we go next to 4 because the 4-star is what you get when you add 4 to every number and draw an arrow to the point on the circle that represents the result. This process gives us two disjoint triangles. That's an indication that no matter how many 4's we add together, we'll never end up at 5. So $4x \equiv 5 \pmod 6$ indeed has no solution.

Another way to see this, an algebraic method, is to remember that $4x \equiv 5$ (mod 6) means that there must be an integer k such that

$$4x = 5 + 6k$$

Then we can rewrite this

$$4x - 6k = 5$$

or

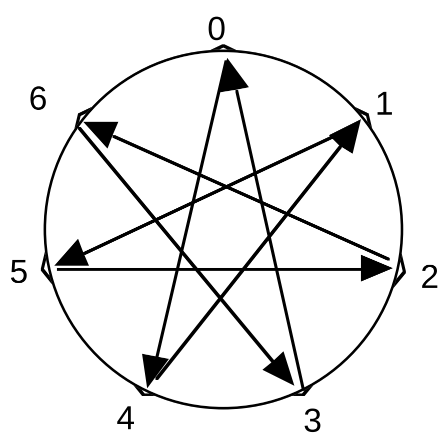
$$2(2x - 3k) = 5$$

Now 2 is a factor of the left side, but it is not a factor of the right side, so we have reached a contradiction, and our assumption, that $4x = 5 + 6k$, must be false (no matter what k is!)

Other examples of congruences, mod 6, that don't have solutions are

$$3x \equiv 4 \pmod{6}$$
$$6x \equiv 3 \pmod{6}$$
$$3x \equiv 5 \pmod{6}$$

Here is the 4 star, mod 7:



4-star,
mod 7

You don't have to draw the arrows (that will simplify drawing these!) Then you'll notice, for example, that the 3-star, mod 7, looks exactly like the 4-star, mod 7. Why?

HW: Investigate Poinsot stars for other moduli besides 6. How can you predict whether a star will "go to all the points"? Your answer should be of the form, "If it is an n-star, mod m, and ……… (a statement about m and n) then ………….. How can you predict how many disjoint sections the n-star will occur in? (For example in the 4-star, mod 6, there are two disjoint sections.) Again, your answer should be stated in terms of the relationship between n and m.

Your investigation of the previous HW problem should lead you to believe that the congruence

$$ax \equiv b \pmod{m}$$

has solutions if and only if gcd(a,m) is a divisor of b. (In most of the examples we'll look at, this gcd will be 1, and the steps will be simpler than the following.) In fact this is a standard theorem of number theory at this level:

Theorem 1: $ax \equiv b \pmod{m}$ has solutions if and only if gcd(a,m) is a divisor of b.

I'm not going to give a proof at this point, just want to convince you that it is true and outline how we might go about proving it:

Remember that we can find the gcd of a and m using the Euclidean algorithm, and then express it as a linear combination of a and m by "reversing" the Euclidean algorithm. (We haven't seen a proof that this always works, either, since such proofs are usually accomplished by the process of "induction", and that is a topic we have not quite gotten to yet.) But suppose we have used the Euclidean algorithm to find d=gcd(a,m), and we've expressed d as a linear combination of a and m:

$$d = \gcd(a,m) = Xa + Ym, \text{ for some integers } X \text{ and } Y$$

Then let $b/d = B$, so that $Bd = b$. Then

$$b = Bd = B(Xa + Ym) = (BX)a + (BY)m$$

Now if we reduce this equation, mod m, we'll find that

$$b = (BX)a + (BY)m \equiv (BX)a \pmod{m}$$

since (BY)m can be replaced with 0, mod m. So the solution is $x \equiv (BX) \pmod{m}$. This is essentially the method of the proof, as usually given in textbooks, but we want to be able to show that it works for all cases, and that is where we'll need induction.

Let's try to apply this. For example, if we were trying to solve

$$6x \equiv 4 \pmod{16},$$

We can create the following steps. First find gcd(6,16):

$$16 = 2(6) + 4$$
$$6 = 1(4) + 2$$
$$4 = 2(2) + 0$$

So 2 = gcd(6,16). Now reverse the process:

$$2 = 1(6) - 1(4)$$
$$2 = 1(6) - 1(16 - 2(6)) = -1(16) + 3(6)$$

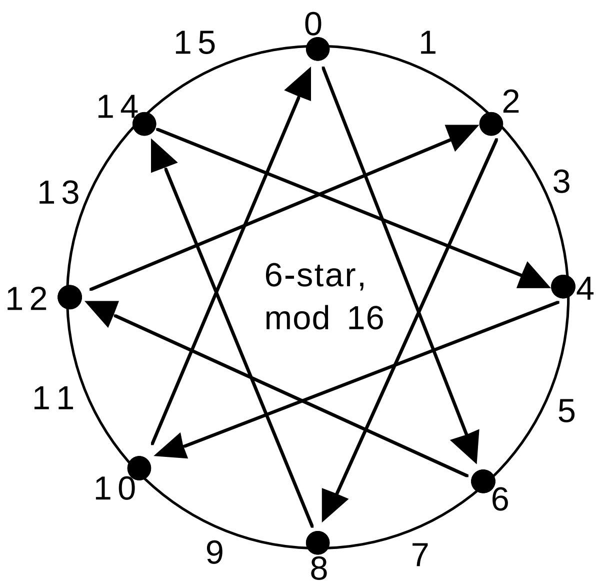
So our $d = Xa + Ym$ is $2 = 3(6) + (-1)(16)$, and $B = b/d = 4/2 = 2$. We should have

$$b \equiv (BX)a \equiv (2)(3)(6) = 36 \equiv 4 \pmod{16}$$

and therefore the solution to $ax \equiv b \pmod{m}$ (in our case it is $6x \equiv 4 \pmod{16}$), is $x \equiv (2)(3) \equiv 6 \pmod{16}$. Sure enough, $6(6) \equiv 4 \pmod{16}$.

HW: Unfortunately, in cases where the gcd is not 1, we might not find all the solutions! For example, find another solution to $6x \equiv 4 \pmod{16}$ besides $x \equiv 6 \pmod{16}$. Hint: there are only 16 numbers to try, mod 16, so if nothing else you can try them all! Can you explain what happened?

Here’s a visual explanation of this last issue:



I've left out "half" of the 6-star, the part that "goes" to the odd numbers, since it is not necessary for what we'll be looking at. Notice that if we map out the multiples of 6, mod 16, we'll see that they trace out this portion of the 6-star, and return to the 0 after 8 arrows. (Also, we'll arrive at 4 at the end of the 6^{th} arrow, showing that indeed $6(6) \equiv 4 \pmod{16}$!) That is,

$$8(6) \equiv 0 \pmod{16}$$

So the next eight multiples of 6 will again take us over this 8 pointed star, and we'll arrive at 4 again, this time after 8 + 6 = 14 arrows. Thus 14 is another solution to our congruence, and this kind of thing will happen whenever b is divisible by the gcd(a,m).

Theorem 2. Suppose that $d = \gcd(a,m)$ and that $d \mid b$. Then $ax \equiv b \pmod{m}$ has exactly d incongruent solutions modulo m.

In the example above, there were d = 2 incongruent solutions modulo 16. We find these d solutions by first finding one solution x, and then adding the d multiples of m/d:

$$\begin{array}{l} 0(m/d)+x \\ (m/d) + x \\ 2(m/d) + x \\ , \ldots , \\ (d-1)(m/d) + x \quad \pmod{m} \end{array}$$

The following proof will be a little long-winded, partly because we have not proceeded in a rigorous fashion up to this point. Mainly you need to try to understand how these things work, read the proof for more background.

Proof: From theorem 1 we know that the congruence has at least one solution x. The above will all be solutions as well, since for each k = 0,1,2,…d-1,

$$a[k(m/d) + x] = a(k)(m/d) + ax \equiv (a/d)km + b \equiv 0 + b \equiv b \pmod{m}$$

since a is divisible by d, and thus (a/d)km will be a multiple of m. Suppose two of these solutions k(m/d) + x and k'(m/d) + x are congruent to each other:

$$k(m/d) + x \equiv k'(m/d) + x \pmod{m}$$

Then

$$k(m/d) + x - [k'(m/d) + x] \equiv (k-k')(m/d) \equiv 0 \pmod{m}$$

This can only be true if (k-k')(m/d) is a multiple of m

$$(k-k')(m/d) = Lm = L(d(m/d))$$

expressing m as the product of d and m/d. Then

$$(k-k') = Ld$$
$$k = k' + Ld$$

This is only possible if L = 0, since k and k' are both assumed to be in the sequence 0,1,2,…,d–1.

One more step of the proof is to show that there cannot be more than these d solutions. Suppose y is another solution, so that

$$ax \equiv ay \equiv b \pmod{m}$$

Then ax – ay ≡ a(x – y) ≡ 0 (mod m). This can only be true if a (x – y) is a multiple of m:

$$a(x - y) = km$$

$a/d\ (x - y) = k\ m/d$

Since m/d and a/d cannot share any more factors in common, we must have that x – y is a multiple of m/d:

$x - y = L(\ m/d)$
$x + (-L)(M/d) = y$

However we've already "used up" all the numbers of this form, so we must have met y already!

Example: Solve $9x \equiv 6 \pmod{15}$. (Using Euclidean algorithm, etc.)

$15 = 1(9) + 6$
$9 = 1(6) + 3$
$6 = 2(3) + 0$
$3 = 9 - 6$
$3 = 9 - (15 - 9) = (-1)\ 15 + 2(9)$
$3 \equiv 2(9) \pmod{15}$

As above (following theorem 1), B = b/d = 6/3 = 2, and the first solution is

$x \equiv BX \equiv 2(2) \pmod{15}$, since $6(2)(2) \equiv 36 \equiv 6 \pmod{15}$

The 3 solutions are thus

$x \equiv 4,\ 4 + 15/3 \equiv 9,\ 4 + 2(15/3) \equiv 14 \quad \pmod{15}$

Another approach, which I mentioned in class, is to use

Theorem 3. If a, b, c, and m are integers with m>0, d = gcd(c,m) and ac ≡ bc (mod m), then a ≡ b (mod m/d).

Proof: We must have that

$ac - bc \equiv 0 \pmod{m}$
$c(b-c) = km$, for some k
$c/d(b-c) = k(m/d)$, since we can divide out the gcd(c,m) =d
$b-c = k'(m/d)$, since m/d and c/d can share no more factors
$b \equiv c \pmod{m/d}$

Example: $9x \equiv 6 \pmod{15}$. Gcd(9,15) = 3, so $3x \equiv 2 \pmod{5}$. We solve this for x, finding $x \equiv 4 \pmod{5}$, which actually takes in all the possibilities we found above, mod 15: $x \equiv 4,\ 4 + 5,\ 4 + 2(5) \pmod{15}$.

RSA Encryption code. Invented by Rivest, Shirer, and Addleman in 1976, this code scheme uses the modular arithmetic that we've been investigating. Let M be the message that we want to encrypt (put into code) – we make up M by changing the letters of what we want to encrypt into numbers, for example letting the letter a=0, b = 1, etc. We choose two very large primes, p and q, letting n=pq, and choose d so that gcd(phi(n),d) = 1. Remember that phi(pq) = (p-1)(q-1).

To put M into code, let

$$C \equiv M^{d} \pmod{n}$$

(We use the fast exponentiation algorithm I showed in class).
To decipher C we first have to find the solution e to

$$de \equiv 1 \pmod{\text{phi}(n)}$$

using the Euclidean algorithm (this is also a very efficient algorithm). (We know e exists because we chose d so that it would be relatively prime to phi(n).)
Then we raise C to the e power. Since de ≡ 1 (mod phi (n)), we must have that there is an integer k with de = 1 + k(phi(n)):

$$C^{e} \equiv M^{de} \equiv M^{1+k(\text{phi}(n))} \equiv (M)\ M^{k(\text{phi}(n))} \equiv (M)\ (M^{\text{phi}(n)})^{k}$$

$$\equiv (M)\ (1)^{k} \equiv M \pmod{n}$$

Again, this exponentiation is accomplished efficiently using the method we used in class.

The numbers n and d are announced publicly, so anyone can put a message into the code simply by raising their M to the power d modulo n. The numbers p,q, and e are kept secret, allowing only the person knowing them to decode messages. This is the unusual example of a public key code, in which knowing how to encode messages does not give enough information for someone to break the code!

Example:
Suppose we want to encode the message YO. We'll use the primes p=43, q=59, so n = pq=2537, and phi(n) = (p-1)(q-1)=(42)(58) = 2436. We

choose d $\equiv$ 13 (mod 2436), and find that e $\equiv$ 937 (mod 2436) has the property that de $\equiv$ 1 (mod 2436). Then we make YO into the 4 digit block 2414, since Y is the 24th letter and O is the 14th, assuming A is 0.

$$C \equiv 2414^{13} \equiv 1683$$

To decode:

$$1683^{937} \equiv 2414 \pmod{2537}$$

HW: Solve the following or explain why they can't be solved. Also use the Poinsot star approach to visually explain how to solve these.

$12x \equiv 10 \pmod{18}$
$8x \equiv 10 \pmod{18}$
$8x \equiv 12 \pmod{18}$

HW: Suppose someone using the RSA code has been careless and allowed you to find out both n=pq=14647 and phi(n)=14400. Use this information to find p and q.

HW: If p=23, q= 47, and d=21, find e.