MATH 115, SUMMER 2012
LECTURE 5

JAMES MCIVOR

Last time:

- defined congruence - listed a bunch of properties, similar to "=", except that we can't always "cancel"
- defined complete residue system mod m - one representative per residue class
- forgot to mention: if $a \equiv b \mod m$, then $(a, m) = (b, m)$.

1. Reduced Residue Systems and the ϕ-function

Since we can't cancel numbers that aren't prime to the modulus, we sometimes want to omit these numbers from our complete residue system, and consider only representatives from the various congruence classes that are relatively prime to m. This is called a **reduced residue system** mod m.

Example 1.1. mod 10, $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is a complete residue system mod 10. $\{1, 3, 5, 7\}$ is a *reduced* residue system. Notice that 0 (or any multiple of m) will almost[1] never be in a reduced residue system mod m - since everything divides 0, we always have $(0, m) = m$.

Fix some m. Although there are many different complete residue systems mod m, they all have the same size, namely m. Similarly, all reduced residue systems mod m all have the same size.

Definition 1. The size of a reduced residue system mod m is denoted by $\phi(m)$. This defines a function of m, called Euler's phi-function, or the totient function.

2. Euler's Theorem and Fermat's Little Theorem

Today we put the notion of congruence to good use by obtaining some neat theorems. Here are some motivating questions, the types of questions number theorists love. Compare them to the questions we mentioned at the beginning of lecture 1.

(1) How can we tell if a to some power is congruent to 1 mod m?
(2) For which x is $x \equiv \pm 1 \mod m$?
(3) Which integers can be written as a sum of two squares?

The following two theorems are very useful; the second follows from the first.

To motivate these two results, recall an important **caution**: you cannot substitute congruent numbers as exponents! For example, even though $1 \equiv 5 \mod 4$, it is not true that $2^1 \equiv 2^5 \mod 4$. So when can we use congruence to simplify large exponents? Fermat had the answer, but Euler did it better.

[1]The only exception is if $m = 1$, which is allowed in the definition, but we never work with this case, since it collapses the integers all down to one point: everything is congruent mod 1.

Theorem 1 (Euler's Theorem)**.** *If a and m are relatively prime, then*

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

Theorem 2 (Fermat's Little Theorem)**.** *If p is a prime that doesn't divide a, then*

$$a^{p-1} \equiv 1 \mod p.$$

Even if p does divide a, we still have $a^p \equiv a \mod p$.

To get this from Euler's Theorem, just take $m = p$ and note that for p prime $\phi(p) = p - 1$. In the case that p divides a both sides are zero!

Proof of Euler. Take a reduced residue system mod m. Multiply it through by a - this gives you another reduced residue system since $(a, m) = 1$. Then for each residue system, multiply all the elements together. This gives two integers, but they're congruent mod m, since each number of the first system is congruent to exactly one number of the second system. In each product, the elements of the original residue system appear, but one side they all got multiplied by a. Cancel all those and you have the answer. □

Example 2.1 (Typical Exam Problem!)**.** —— Maybe do this in section —— You can use these theorems to compute incredibly large exponentiations modulo m. For example say we want to find the value of 21^{296} modulo 14. 21^{296} is an incredibly large number, so we've no chance of just computing and then reducing mod 14. So we use congruences. First of all, we may as well reduce 21 mod 14 to get 7 mod 14. This was one of our properties - notice we can make this substitution (replace 21 by 7) in the base but *not* in the exponent. So we must compute $7^{296} \mod 14$. This is still too large for direct computation. Since the modulus is not prime, we must use Euler's Thm instead of Fermat's Little Thm. We compute $\phi(14)$: just list all the numbers prime to 14 in order: 1,3,5,9,11,13. Hence $\phi(14) = 6$. So Euler's theorem tells us $7^6 \equiv 1 \mod 14$. To see how this helps us, we need to extract as many copies as we can of 7^6 from the big number 7^{296}. We use long division: $296 = 49 \cdot 6 + 2$, so putting it all together:

$$21^{296} \equiv 7^{296} = 7^{49 \cdot 6 + 2} = (7^6)^{49} \cdot 7^2 \equiv (1)^{21} \cdot 7^2 \equiv 7 \mod 14.$$

3. Wilson's Theorem

We're mostly interested in the question of when an integer n can be expressed as a sum of squares, i.e., when can we find integers a, b such that $n = a^2 + b^2$? To get there, we'll need a few preliminary results, including Wilson's Theorem.

First, note that when $ab \equiv 1 \mod m$, we can think of a and b as multiplicative inverses to each other, just as when working with rational numbers, 2 and $\frac{1}{2}$ are inverses. This is a little strange at first: in the "usual" integers, no numbers have inverses except ± 1 - that's the whole point of using fractions! But when we work modulo m all of a sudden some integers have inverses under multiplication.

Which numbers have inverses mod m? - those in a reduced residue system.:

Proposition 1. *The integer a has a multiplicative inverse mod m if and only if it's relatively prime to m. The inverse is unique up to congruence.*

- For example, let's work mod 6. We have a complete residue system $\{0, 1, 2, 3, 4, 5\}$, and reduced residue system $\{1, 5\}$ (so $\phi(6) = 2$). Clearly 1 has an inverse, namely 1 itself - this is always true, for any modulus.

- What is the inverse of 5? Well, it's inverse must also be in our reduced residue system, so it can only be 1 or 5. But 1 is already the inverse to 1, so 5 must be its own inverse, too. And we can check: $5 \cdot 5 = 25 \equiv 1 \mod 6$.

- But why doesn't, say, 3 have an inverse? Well, suppose it did, call the inverse x. So we have $3x \equiv 1 \mod 6$. But now multiply both sides by 2, to get $2 \cdot 3 \cdot x \equiv 2 \mod 6$, which means $0 \equiv 2 \mod 6$, a contradiction.

This leads us to another natural question to ask: when is an element its own inverse? For prime modulus, this is easy:

Proposition 2. *$x^2 \equiv 1 \mod p$ if and only if $x \equiv \pm 1 \mod p$*

Proof. Factor $x^2 - 1 \bmod p$. Check $x - 1$ and $x + 1$ are prime to p. □

Now here's a neat theorem:

Theorem 3 (Wilson's Theorem)**.** *Let p be prime. Then $(p-1)! \equiv -1 \mod p$.*

Let's see if this is believable. If $p = 2$, then $(p-1)! = 1! = 1$, which is congruent to -1 mod 2. If $p = 3$, then $(p-1)! = 2 \equiv -1 \mod 3$. How about $p = 11$? Already this gets dificult: $(p-1)! = 10! = 3,628,800$. We ask whether this is congruent to -1 mod 11. That's the same as adding 1, and asking whether 3,628,801 is congruent to 0 mod 11, i.e., whether 11 divides 3,628,801. From last time, you know how to do this: to test for divisibility by 11, take the difference of the alternating digits: $(3+2+8+1) - (6+8+0) = 14 - 14 = 0$, which is divisible by 11. Since factorial grows so quickly, you can see that this is a very useful result.

Here's a proof that's slightly different from the one in the text, but I'll omit a few details that we cover in a few days.

Proof. We'll take two different reduced residue systems and multiply them out, similar to the proof of Euler's Thm. One reduced residue system is the usual $\{1, 2, \ldots, p-1\}$. Its product is clearly $(p-1)!$. Now pick an a with $1 < a < p$ with the property that $\{a, a^2, \ldots, a^{p-1}\}$ is a reduced residue system. We'll see that this is possible in a few days[2]. By the argument in the proof of Euler's Thm, we have

$$(p-1)! \equiv a \cdot a^2 \cdots a^{p-1} \mod p,$$

so we now just need to show that $a \cdot a^2 \cdots a^{p-1}$ is congruent to -1. Firstly,

$$a \cdot a^2 \cdots a^{p-1} = a^{1+2+\ldots+p-1} = a^{\frac{1}{2}(p-1)p},$$

by standard counting tricks. Let's show this last thing is congruent to -1.

First, we checked the theorem for $p = 2$ above, so we can assume p is odd. By Fermat's Little Thm, using $\phi(p) = p - 1$, we have $a^{p-1} - 1 \equiv 0 \mod p$, and we factor this to get

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \mod p,$$

and since p is prime, it must therefore divide one of the two factors. Now we know by Fermat that $a^{p-1} \equiv 1 \mod p$, and in fact, there is no positive integer smaller than $p - 1$ which does this (we will prove this in a few days). This means that in particular, $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$, since $\frac{p-1}{2}$ is smaller than $p - 1$. In other words, p cannot divide $(a^{\frac{p-1}{2}} - 1)$, so it must divide $(a^{\frac{p-1}{2}} + 1)$. Thus

$$a^{\frac{p-1}{2}} \equiv -1 \mod p.$$

[2]This a is called a **primitive root mod** p.

Now we're basically done:

$$a^{\frac{1}{2}(p-1)p} = (a^{\frac{p-1}{2}})^p \equiv (-1)^p \equiv (-1) \mod p,$$

where we used in the last congruence the fact that p was odd.

□