REU 2006 Apprentice

Instructor: László Babai
Scribe: Matthew Booth
NOT PROOF-READ

July 7, 2006. Last updated July 8, 2006

Recall that Euler's ϕ function is defined so that $\phi(n)$ is the number of integers between 1 and n that are relatively prime to n. Note that if p is prime then $\phi(p) = p - 1$ because all integers from 1 to $p - 1$ are relatively prime to p.

So for example, what would be $\phi(p^7)$? A number is not relatively prime to p^7 if and only if it is a multiple of p. So the numbers at most p^7 which are not relatively prime to p^7 are $p, 2p, 3p, \ldots, p \cdot p^6$. So there are p^6 such numbers. Hence, $\phi(p^7) = p^7 - p^6 = p^7(1 - \frac{1}{p})$. Another way of looking at this is that one out of every p numbers is divisible by p, and so out of the first p^7 integers, the probability that an element is relatively prime to p^7 is $(1 - \frac{1}{p})$.

Now let's consider

$$\sum_{d|p^7} \phi(d) = \phi(p) + \phi(p^2) + \ldots \phi(p^7) = 1 + (p-1) + (p^2 - p) + \ldots + (p^7 - p^6)$$

Note that this is a telescoping sum, and so the result is p^7. This leads us to wonder if we get a similar result for all numbers.

Conjecture 1.0.1. $\sum_{d|n} \phi(n) = n$

Now, consider pq where p and q are primes. There are q multiples of p that are at most pq and there are p multiples of q that are at most pq. The only number $\leq pq$ that is a multiple of both is pq itself. So we get that $\phi(pq) = pq - p - q + 1$ where adding the 1 back is because pq is both a multiple of p and a multiple of q and so was counted twice. Note that we can factor this as $\phi(pq) = (p-1) \cdot (q-1)$. So $\frac{\phi(pq)}{pq} = \frac{p-1}{p} \cdot \frac{q-1}{q} = (1 - \frac{1}{p}) \cdot (1 - \frac{1}{q})$.

Exercise 1.0.2 (The Chinese Remainder Theorem). If we have integers $m_1, \ldots, m_n$ such that each m_i is relatively prime to m_j for $i \neq j$ then system of congruences

$$x \equiv a_1 (mod m_1) \quad (1.0.1)$$
$$x \equiv a_2 (mod m_2) \quad (1.0.2)$$
$$\vdots \quad (1.0.3)$$
$$x \equiv a_k (mod m_k) \quad (1.0.4)$$

has a solution which is unique mod $\prod_{1 \leq i \leq k} m_i$

Now note that

$$\sum_{d|pq} \phi(d) = \phi(1) + \phi(p) + \phi(q) + \phi(pq) = 1 + (p-1) + (q-1) + (pq - p - q + 1) = pq.$$

So that's more evidence for our conjecture.

It would be good to get an explicit formula for $\phi(n)$.

Theorem 1.0.3. *If $n = p_1^{a_1} \cdots p_k^{a_k}$, where p_i are distinct primes, then $\phi(n) = n(1-\frac{1}{p_1}) \cdots (1-\frac{1}{p_k})$.*

Proof. Let $\Omega = \{1, \ldots, n\}$ and j be a random number in Ω. Let A_i be the subset of Ω of numbers which are not divisible by p_i. The events $j \in A_i$ are independent of each other (which can be seen from the Chinese Remainder Theorem).

Note that the probability that a random number in Ω is relatively prime to n is just $\frac{\phi(n)}{n}$. But also note that a number in Ω is relatively prime to n if and only if it is not divisible by any of the p_i (and that the probability of not being divisible by a particular p_i is $(1 - \frac{1}{p_i})$). Since these events are independent, we get the desired formula

$$\frac{\phi(n)}{n} = \prod_{1 \le i \le k} (1 - p_i).$$

□

Let G be a group and $a \in G$.

Definition 1.0.4. The *order* of a, $ord(a)$, is the smallest $k \ge 1$ such that $a^k = 1$.

Exercise 1.0.5. $a^l = 1$ if and only if $ord(a)|l$.

Consider the complex n^{th} roots of unity (i.e. the complex numbers z such that $z^n = 1$). They are evenly spaced on the unit circle in the complex plane. Call them $z_0, \ldots z_{n-1}$ where we have $z_k = cos(\frac{2k\pi}{n}) + isin(\frac{2k\pi}{n})$.

Observation 1.0.6. z is an n^{th} root of unity if and only if $ord(z)|n$.

Definition 1.0.7. If $ord(z) = n$, then z is a *primitive* n^{th} root of unity.

Exercise 1.0.8. Show z_k is a primitive n^{th} root of unity if and only if $gcd(k, n) = 1$.

Therefore the number of primitive n^{th} roots of unity is $\phi(n)$.

Let $U_n = \{z_0, \ldots, z_{n-1}\}$. How many of the z_i have order d where $d|n$ (i.e. the number of primitive d^{th} roots of unity)? Let P_d be the set of primitive d^{th} roots of unity. Then $U_n = \bigcup_{d|n} P_d$ and the P_d are disjoint. So

$$n = |U_n| = \sum_{d|n} |P_d| = \sum_{d|n} \phi(n)$$

and we have proven the conjecture given earlier in the class.

For another proof, take the numbers $\frac{1}{n}, \frac{2}{n}, \ldots \frac{n}{n}$. Put each of these fractions in their lowest terms and look at the denominators d that you get (which are exactly the numbers which divide n).

Exercise 1.0.9. Show that the number of occurences of the denominator d in this list is $\phi(d)$ and finish the proof.

As a reminder, we restate

Theorem 1.0.10 (Fermat's Little Theorem). *If p is prime and $gcd(a, p) = 1$, then $a^{p-1} \equiv 1$ (mod p).*

Definition 1.0.11. The *order of a mod p*, $ord_p(a)$, is the smallest $k \geq 1$ such that $a^k \equiv 1$ (mod p).

So Fermat's Little Theorem can be restated as $ord_p(a)|(p-1)$.

Definition 1.0.12. If p is prime then we say a is a *primitive root mod p* if $ord_p(a) = p - 1$.

Theorem 1.0.13. *For all primes p there is a primitive root mod p.*

Before preparing for the proof, here's a nice exercise.

Exercise 1.0.14. Find infinitely many 2x2 matrices A such that $A^2 = I$ where I is the identity matrix.

Let $\mathbb{F}$ be a field (for example it could be $\mathbb{C}$, $\mathbb{R}, \mathbb{F}_p, \mathbb{Q}$, or $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$).

Definition 1.0.15. A *multiplicative inverse of a mod m* is a number x such that $ax \equiv 1$ mod m.

For example, since $3 \cdot 5 = 15 \equiv 1$ (mod 7), we have that $5 = 3^{-1}$ (mod 7)

Exercise 1.0.16. Show that a has a multiplicative inverse mod m if and only if $gcd(a, m) = 1$.

Definition 1.0.17. Let $f(x) = a_0 + a_1 x + \dots a_n x^n$ where $a_i \in \mathbb{F}$ and $a_n \neq 0$. Then we say that the *degree* of f, $deg(f)$, is n. A *root* of f is an element $z \in \mathbb{F}$ such that $f(z) = 0$.

Exercise 1.0.18. Find a quadratic polynomial with coefficients in $\mathbb{F}_2$ which does not have a root in $\mathbb{F}_2$.

Theorem 1.0.19. *For f as above, f has at most n roots in $\mathbb{F}$.*

Lemma 1.0.20. *If $f(a) = 0$, then $f(x) = (x - a) \cdot g(x)$ for some polynomial $g(x)$ over $\mathbb{F}$.*

This is a special case of the following lemma.

Lemma 1.0.21. *$f(x) - f(a) = (x - a) \cdot g(x)$ for some polynomial $g(x)$ over $\mathbb{F}$.*

Example 1.0.22. *Let $f(x) = x^n$. Then $f(x) - f(a) = x^n - a^n = (x - a) \cdot (x^{n-1} + ax^{n-2} + a^2x^{n-3} + \cdots + a^{n-2}x + a^{n-1})$. One can see this by expanding out the right hand side and noticing that it is a telescoping sum.*

For the general case, it is not that much different from the example.

Proof of Lemma. Let $f(x) = \sum c_i x^i$. Then

$$f(x) - f(a) = \sum c_i(x^i - a^i) = \sum c_i(x-a) \cdot g_i(x) = (x-a) \cdot \sum g_i(x)$$

where the g_i are polynomials.

□

Exercise 1.0.23. If $\mathbb{F}$ is a field and $a, b \in \mathbb{F}$, then $a \cdot b = 0$ if and only if either a or b is 0.

Proof of the previous theorem. Let $a_1, \ldots, a_n$ be the distinct roots of f. So since $f(a_1) = 0$, we have that $f(x) = (x - a_1)f_1(x)$. But we also have that $f(a_2) = 0$, so we have that $(a_2 - a_1)f_1(a_2) = 0$. Since $a_1 \neq a_2$, we have that $a_1 - a_2 \neq 0$ and hence $f_1(a_2) = 0$. So we have that $f(x) = (x - a_1)(x - a_2)f_2(x)$. Continuing this argument we get $f(x) = (x - a_1) \cdots (x - a_l)f_l(x)$. By looking at the degree of f, we see that l can be no greater than the degree of f, as desired.

□

Now, in $\mathbb{F}_p$, Fermat's little theorem tells us that all $a \neq 0$ are roots of $f(x) = x^{p-1} - 1$. So we get that $f(x) = (\prod_{a \in \mathbb{F}_p - \{0\}}(x - a)) \cdot g(x)$. Looking at degrees, we see that $g(x)$ is a constant polynomial, and looking at the coefficient of x^{p-1} on the left and right gives us that $g(x) = 1$. So we have just proven

Theorem 1.0.24. *In* $\mathbb{F}_p$,

$$x^{p-1} - 1 = (\prod_{a \in \mathbb{F}_p - \{0\}} (x - a)).$$

Now, Fermat's Little Theorem tells us that the order of every nonzero element in $\mathbb{F}_p$ is a divisor of $p - 1$.

Question 1.0.25. How many elements of $\mathbb{F}_p - \{0\}$ have order that divides d (where $d|p-1$)?

In other words, how many $a \in \mathbb{F}_p - \{0\}$ are such that $a^d = 1$? Call this number k_d. Now we know that $k_d \leq d$ because these are the roots of $x^d - 1$ in $\mathbb{F}_p$.

Lemma 1.0.26. $k_d = d$.

Proof. We need only show that $k_d \geq d$ by the above. Consider the map $g(x) = x^{\frac{p-1}{d}}$. How many elements can have the same $(\frac{p-1}{d})^{th}$ power? No more than the number of solutions to the polynomial $x^{\frac{p-1}{d}} - a$ where a is their common power. So no more than $\frac{p-1}{d}$. Hence, if we group the $p-1$ elements of $\mathbb{F}_p - \{0\}$ by their $(\frac{p-1}{d})^{th}$ power, we are grouping $p-1$ elements into groups of no more than $\frac{p-1}{d}$. Hence, we have at least d groups. So there are at least d different $(\frac{p-1}{d})^{th}$ powers.

And if $b = a^{\frac{p-1}{d}}$, $b^d = a^{p-1} = 1$ by Fermat's Little Theorem. So since there are at least d different $(\frac{p-1}{d})^{th}$ powers, there are at least d distinct d^{th} roots of unity. Hence $k_d \geq d$ and we are done. □

Theorem 1.0.27. *Let $d|p-1$. Then the number of primitive d^{th} roots of unity in $\mathbb{F}_p - \{0\}$ is $\phi(d)$.*

Corollary 1.0.28. There exists a primitive root mod p.

The corollary follows by noting tht a primitive root mod p is just a primitive $(p-1)^{st}$ root of unity and $\phi(p-1) \geq 1$.

Proof of theorem by induction on d. For the base case, we take $d = 1$ and note that $a^1 = 1$ has the unique solution of $a = 1$ and $\phi(1) = 1$.

Now assume the $d > 1$. Our inductive hypothesis is that our theorem is true for all $d' < d$ where $d'|d$. So we need to count the elements which have order d. So let P_d be the set of such elements and let U_d be the set of solutions of $x^d - 1$. Now $U_d = \bigcup_{d'|d} P_{d'}$ where the $P_{d'}$ are disjoint. So we have

$$d = k_d = |U_d| = \sum_{d'|d} |P'_d| = |P_d| + \sum_{d'|d, d' \neq d} \phi(d')$$

The last equality comes from our inductive hypothesis that for the $d' < d$, $|P_d| = \phi(d)$. By our earlier theorem the summation on the right is equal to $d - \phi(d)$. So we have that $d = |P_d| + d - \phi(d)$ and hence $|P_d| = \phi(d)$ as desired. □

Definition 1.0.29. An element $a \in \mathbb{F}_p$ is a *quadratic residue* mod p if $a \neq 0$ and there is a b such that $a = b^2$.

Example 1.0.30. *2 is a quadratic residue mod 7 because $2 = 3^2$ in $\mathbb{F}_7$.*

Definition 1.0.31. An element $a \in \mathbb{F}_p$ is a *quadratic nondesidue mod p* if there is no $b \in \mathbb{F}_p$ such that $a = b^2$.

Definition 1.0.32 (The Legendre Symbol).

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \\ -1 & \text{if } a \text{ is a quadratic nonresidue} \\ 0 & \text{if } a = 0 \end{cases}$$

Theorem 1.0.33 (Euler). *For odd primes p, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ (mod p).*

Proof. Let $b = a^{\frac{p-1}{2}}$. If $a = 0$, then $b = 0$ and the theorem holds. If $a \neq 0$, then $b^2 = a^{p-1} = 1$. So $0 = b^2 - 1 = (b+1)(b-1)$ which implies that $b - 1 = 0$ or $b + 1 = 0$ and hence $b = \pm 1$.

If a is a quadratic residue mod p, then there is a c such that $c^2 = a$ and hence $a^{\frac{p-1}{2}} = c^{p-1} = 1$ by Fermat's Little Theorem and the desired result holds.

Now consider the case where a is a quadratic nonresidue mod p. Now by the corollary above, there is a primitive root mod p. Call it g. So $ord_p(g) = p-1$ which implies that there is an l such that $g^l = a$. We call l the discrete log of a in $\mathbb{F}_p$ with base g.

Lemma 1.0.34. *$a = g^l$ is a quadratic residue mod p if and only if l is even.*

If we can show the lemma, then we would know that for a a quadratic nonresidue, l would be odd. So $a^{\frac{p-1}{2}} = g^{\frac{l\cdot(p-1)}{2}}$. Since l is odd, it cannot cancel the 2 in the denominator and hence $\frac{l\cdot(p-1)}{2}$ would not be divisible by $p-1$. Hence since the order of g is $p-1$, this means that $a^{\frac{p-1}{2}} = g^{\frac{l\cdot(p-1)}{2}} \neq 1$. By the above, this means that $a^{\frac{p-1}{2}} = -1$ as desired.

Proof of Lemma. If l is even, then $a = g^l = (g^{\frac{l}{2}})^2$ and hence a is a quadratic residue.

Now assume that a is a quadratic residue. Then $a = b^2$ for some $b \neq 0$. But then $b = g^s$ for some s and hence $g^l = a = b^2 = g^{2s}$ and so $g^{2s-l} = 1$. But g has order $p-1$. Hence $(p-1)|(2s-l)$. Since p is odd, $p-1$ is even and hence $2|(p-1)$. So $2|(2s-l)$. Since $2|2s$, this means that $2|l$ whence l is even. □

□

Corollary 1.0.35. -1 is a quadratic residue mod p if and only if $p \equiv 1 \pmod 4$ or $p = 2$.

Proof. For $p = 2$, $1 = -1$ and so $1^2 = 1 = -1$. So let $p \geq 3$. So

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } 4|p-1 \\ -1 & \text{if } 4 \not| p-1 \end{cases}$$

□

Corollary 1.0.36. If $p \equiv 1 \pmod 4$ then there is an a such that $p|(a^2+1)$ (i.e. $a^2 \equiv -1$ (mod p)).

Experiment 1.0.37. *Evaluate $\left(\frac{2}{p}\right)$ experimentally.*