X. Number Theory (Tech-Level 2)

Po-Shen Loh*

July 2, 2003

1 Warm-Ups

1. Factor a large (200+ digit) number.
2. (Uses Taylor Series). Find all integer polynomials $f(n)$ for which the sequence $\{f(1), f(2), f(3), f(4), \ldots\}$ eventually takes only prime values.

   Solution: Apply Taylor's formula for $f(1 + kf(1))$.

2 Theorems

1. (Lucas's Theorem). Let p be prime, and suppose we are trying to compute $\binom{n}{r}$ modulo p. Start by expressing n and r in base-p notation:

$$\begin{aligned} n &= \{n_k n_{k-1} n_{k-2} \ldots n_0\} = n_0 + n_1 p + n_2 p^2 + \cdots + n_k p^k, \\ r &= \{r_k r_{k-1} r_{k-2} \ldots r_0\} = r_0 + r_1 p + r_2 p^2 + \cdots + r_k p^k, \end{aligned}$$

   (where the braces denote digit strings, and all of the digits are between 0 and $p-1$ inclusive). Then:

$$\binom{n}{r} \equiv \binom{n_k}{r_k}\binom{n_{k-1}}{r_{k-1}} \cdots \binom{n_0}{r_0} \pmod{p}.$$

2. (Wilson's Theorem). If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.
3. (Multiplicativity of Euler-ϕ). If $(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$.

   Solution: Write out the numbers from 0 to $ab - 1$ as a table, with a columns and b rows. Then the numbers that are not relatively-prime to a or b are entire rows/columns.
4. (Formula for Euler-ϕ). We have a complete formula:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

   Solution: For each prime power p^e with $e > 0$, $\phi(p^e) = p^{e-1}(p-1)$: just count the number of multiples of p. Then use the multiplicative property.
5. (Existence of Primitive Roots). The only numbers having primitive roots are 2, 4, p^n, and $2p^n$, where n is a positive integer and p is an **odd** prime.

*Much of this lecture was drawn from LeVeque's *Fundamentals of Number Theory*

6. (Criterion for Primitive Roots). If $p \not| a$ and for every prime divisor q of $p-1$,

$$a^{(p-1)/q} \not\equiv 1 \pmod{p}$$

then a is a primitive root of p.

Solution: Assume not. From last lecture, the order (call it k) divides $\phi(p) = p-1$; therefore, if $a^k \equiv 1 \pmod{p}$, some more powering-up will get you to some $(p-1)/q$, and this should still give residue 1, contradiction.

7. (Pythagorean Substitution). If x, y, z are pairwise relatively prime integers that satisfy $x^2+y^2=z^2$, then there exist integers r and s such that:

$$\begin{aligned} x &= r^2 - s^2 \\ y &= 2rs \\ z &= r^2 + s^2 \end{aligned}$$

(Here we assumed that y was even and x was odd. Note that by going modulo 4, we see that we can't have both x and y odd, and if they are both even, then they aren't pairwise relatively prime.)

Solution: This comes from the y-axis parameterization of the rational points of the unit circle.

8. Prove that there are no integral solutions to $x^4 + y^4 = z^4$.

Solution: Use Pythagorean substitution. Suffices to consider the problem $x^4 + y^4 = z^2$. Suppose we are reduced. Then (WLOG y is even):

$$\begin{aligned} x^2 &= r^2 - s^2 \\ y^2 &= 2rs \\ z &= r^2 + s^2, \end{aligned}$$

and r, s relatively prime. From the first equation, we have $x^2 + s^2 = r^2$ with x odd, so s will be the $2pq$ term and it's also reduced. Hence:

$$\begin{aligned} x &= p^2 - q^2 \\ s &= 2pq \\ r &= p^2 + q^2, \end{aligned}$$

with p and q relatively prime. Since we have $y^2 = 2rs$, we can split (we know s is even) into $s = 2a^2$ and $r = b^2$. Now we have $2a^2 = s = 2pq$, so $pq = a^2$. So p and q are perfect squares. But then from $r = p^2 + q^2$, since each of r, p, q are squares, we got a smaller one. Smaller by comparing r and z: $z = r^2 + s^2$.

3 Quadratic Residues

Definition 1 *We say that x is a **quadratic residue** modulo m if there exists integral a for which $x \equiv a^2 \pmod{m}$.*

1. Show that if p is prime, n is positive, and $a \equiv b \pmod{p^n}$, then $a^{p^k} \equiv b^{p^k} \pmod{p^{n+k}}$.

Solution: Induct on k. Then for each inductive step, just write $b = a + p^n\alpha$ and use Binomial expansion to get b^p, and see that it differs from a^p by a multiple of p^{n+1}.

2. Let p be an odd prime and let n be a positive integer. Prove that x is a quadratic residue modulo p^n if and only if x is a quadratic residue modulo p.

   Solution: Since p is odd, we must have $a^{(p-1)/2} \equiv 1 \pmod p$ by Fermat's Little Theorem. Using the previous result, we can power both sides by p^{e-1} to get

$$a^{p^{e-1}(p-1)/2} \equiv 1 \pmod{p^e}$$

   Now since we have a prime power (p^e), there exists a primitive root; call it r. The order of r is $\phi(p^e) = p^{e-1}(p-1)$. Suppose that $a \equiv r^k$. Now this means that $r^{kp^{e-1}(p-1)/2} \equiv 1 \pmod{p^e}$. In other words, $\phi(p^e)$ divides the exponent. Hence $k/2$ is an integer which implies that $a \equiv (r^{(k/2)})^2$, and we are done.

3. A number a is a quadratic residue modulo m if and only if it is a quadratic residue of all odd prime divisors of m and is a quadratic residue modulo the power-of-two component of m. Here, the "power-of-two-component" is defined as the largest factor that is a power of two.

   Solution: Let $m = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Chinese remainder theorem: the congruence $x^2 \equiv a \pmod m$ is equivalent to the system:

$$\begin{array}{rcll} x^2 & \equiv & a & \pmod{2^e} \\ x^2 & \equiv & a & \pmod{p_1^{e_1}} \\ x^2 & \equiv & a & \pmod{p_2^{e_2}} \\ & \vdots & & \\ x^2 & \equiv & a & \pmod{p_r^{e_r}}, \end{array}$$

   since all of the modulo-thingies are coprime. Then use the previous result.

4. The quadratic residues modulo 2^e are:

   If e is 1: everything

   If e is 2: anything congruent to 0 or 1 modulo 4

   If e is at least 3: anything congruent to 0 or 1 modulo 8

5. The **Legendre symbol** is defined as follows: (let p be an odd prime)

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } a \text{ is a quadratic residue of } p \\ -1, & \text{if } a \text{ is not a quadratic residue of } p \end{cases}$$

   Prove the following properties:

   (a) (Euler) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$.

   Solution: Use primitive root; suppose that $a \equiv r^k$. Then we get QR iff k is even, which does the trick.

   (b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

   Solution: Immediately from previous.

   (c) If $a \equiv b \pmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

   (d) $\left(\frac{a^2}{p}\right) = 1$ if $p \nmid a$.

(e) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Actually, this just means that -1 is a quadratic residue of p exactly when $p \equiv 1 \pmod 4$.

6. 2 is a quadratic residue of p exactly when $p \equiv \pm 1 \pmod 8$.

7. (More Primitive Roots).

   (a) 2 is a primitive root of the prime $p = 4q+1$ if q is an odd prime.

   (b) 2 is a primitive root of $p = 2q+1$ if q is a prime congruent to 1 modulo 4.

   (c) -2 is a primitive root of $p = 2q+1$ if q is a prime congruent to -1 modulo 4.

8. (Quadratic Reciprocity). Let p and q be distinct odd primes. Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless both p and q are congruent to -1 modulo 4, in which case they are negatives of each other. More briefly:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

9. (Taiwan97/4). Let $k = 2^{2^n} + 1$ for some positive integer n. Show that k is a prime if and only if k is a factor of $3^{(k-1)/2} + 1$.

   Solution: Suppose k is a factor of $3^{(k-1)/2} + 1$. Then $3^{(k-1)/2} \equiv -1 \pmod k$. Yet $3^{k-1} \equiv 1 \pmod k$. This means that the order of 3 modulo k is $k-1$. But this divides $\phi(k) \le k-1$, and we get that k is prime.

   Conversely, assume that k is prime; we need to show that $3^{(k-1)/2} \equiv -1 \pmod k$. This is Euler's Criterion for a quadratic residue, so we just need to compute $\left(\frac{3}{k}\right)$. By the Law of QR, this is $\left(\frac{k}{3}\right)$, and k is one more than a square of a non-multiple of 3; hence, $k \equiv 2 \pmod 3$, and we are down to $\left(\frac{2}{3}\right)$, which is -1 since 2 is not a QR modulo 3.

Well, thanks for making this MOP so wonderful, guys; I really liked your (Red Group) class. If any of you happen to pass by Caltech next year, feel free to drop me a line—my phone extension is the golden ratio (x1618). Also, since this is probably my last MOP, good luck to all of you in your future endeavors! I'm sure I will read about many of you in the years to come.

Signing off,

$\square$