MAT315 Intro to Number Theory Test 2 Review

Rui Qiu

March 2015

Since this is my very first time writing in "formal" LaTeX, there might be some stupid mistakes there, almost surely.

1 Mersenne Prime

Proposition 14.1. If $a^n - 1$ is prime for some numbers $a \geqslant 2$ and $n \geqslant 2$, then a must equal 2 and n must be a prime.

Definition: Primes of the form $2^p - 1$ are called *Mersenne primes*, where p is a prime.

2 Mersenne Primes and Perfect Numbers

Definition: Sum of proper divisors of n is equal to n itself, such n is called a *perfect number*.

Theorem 15.1 (Euclid's Perfect Number Formula). If $2^p - 1$ is a prime number, then $2^{p-1}(2^p - 1)$ is a *perfect number*.

Theorem 15.2 (Euclid's Perfect Number Theorem). If n is an even perfect number, then n looks like

$$n = 2^{p-1}(2^p - 1)$$

where $2^p - 1$ is a *Mersenne prime*.

Definition:: $\sigma(n)$ = sum of all divisors of n (including 1 and n)

Theorem 15.3 (Sigma Function Formulas)
(a) If p is a prime and $k \geqslant 1$, then

$$\sigma(p^k) = 1 + p + p^2 + ... + p^k = \frac{p^{k+1}-1}{p-1}.$$

(b) If $gcd(m, n) = 1$, then

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Note that a number n is perfect exactly when $\sigma(n) = 2n$.

3 Powers Modulo m and Successive Squaring

Algorithm 16.1 (Successive Squaring to Compute $a^k \pmod{m}$). The following steps compute the value of $a^k \pmod{m}$:

1. Write k as a sum of powers of 2,
$$k = u_0 + u_1 \cdot 2 + u_2 \cdot 4 + u_3 \cdot 8 + ... + u_r \cdot 2^r,$$
where each u_i is either 0 or 1. (This is called the binary expansion of k.)

2. Make a table of powers of a modulo m using successive squaring.
$$\begin{aligned} a^1 &\equiv A_0 \pmod{m} \\ a^2 &\equiv (a^1)^2 \equiv A_0^2 \equiv A_1 \pmod{m} \\ a^4 &\equiv (a^2)^2 \equiv A_1^2 \equiv A_2 \pmod{m} \\ a^8 &\equiv (a^4)^2 \equiv A_2^2 \equiv A_3 \pmod{m} \\ &\cdots \\ a^{2^r} &\equiv (a^{2^{r-1}})^2 \equiv A_{r-1}^2 \equiv A_r \pmod{m} \end{aligned}$$
Note that to compute each line of the table you only need to take the number at the end of the previous line, square it, and then reduce it modulo m. Also note that the table has $r+1$ lines, where r is the highest exponent of 2 appearing in the binary expansion of k in Step 1.

3. The product
$$A_0^{u_0} \cdot A_1^{u_1} \cdot A_2^{u_2} \cdot \ldots \cdot A_r^{u_r} \pmod{m}$$
will be congruent to $a^k \pmod{m}$. Note that all the u_i's are either 0 or 1, so this number is really the product of those A_i's for which u_i equals 1.

4 Computing k^{th} Roots Modulo m

Algorithm 17.1 (How to Compute k^{th} Roots Modulo m). Let b, k, and m given integers that satisfy

$$gcd(b, m) = 1 \text{ and } gcd(k, \phi(m)) = 1$$

The following steps give a solution to the congruence

1. Compute $\phi(m)$. (See Chapter 11. Note that $\phi(m) = \#\{a : 1 \leqslant a \leqslant m \text{ and } gcd(a, m) = 1\}$.)

2. Find positive integers u and v satisfy $ku - \phi(m)v = 1$. [See Chapter 6. Another way to say this is that u is a positive integer satisfying $ku \equiv 1 \pmod{\phi(m)}$, so u is actually the inverse of k modulo $\phi(m)$.]

3. Compute $b^u \pmod{m}$ by successive squaring. (See Chapter 16.) The value obtained gives the solution x.

5 Powers, Roots, and "Unbreakable" Codes

How do we decode the message when we receive it? We have been sent the numbers $b_1, b_2, \ldots, b_r$, and we need to recover the numbers $a_1, a_2, \ldots, a_r$. Each b_i is congruent to $a_i^k \pmod{m}$, so to find a_i we need to solve the congruence $x^k \equiv b_i \pmod{m}$. This is exactly the problem we solved in the last chapter, assuming we were able to calculate $\phi(m)$. But we know the values of p and q with $m = pq$, so we easily compute

$$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1) = pq - p - q + 1 = m - p - q + 1$$

Now we just need to apply the method used in Chapter 17 to solve each of the congruence $x^k \equiv b_i \pmod{m}$. The solutions are the numbers $a_1, a_2, \ldots, a_r$ and then it is easy to take this string of digits and recover the original message.

6 Primality Testing and Carmichael Numbers

Definition: A *Carmichael number* is a composite number n with the property that

$$a^n \equiv a \pmod{n} \text{ for every integer } 1 \leqslant a \leqslant n.$$

In other words, a Carmichael number is a composite number that can masquerade as a prime, because there are no witnesses to its composite nature. The smallest Carmichael number is 561.

Assertion:
(A) Every Carmichael number is odd.
(B) Every Carmichael number is a product of distinct primes.

7 Squares Modulo p

Definition: A nonzero number that is congruent to a square modulo p is called a *quadratic residue modulo p*. (QR)

Definition: A nonzero number that is not congruent to a square modulo p is called a *(quadratic) nonresidue modulo p*. (NR)

Theorem 20.1 Let p be an odd prime. Then there are exactly $\frac{p-1}{2}$ quadratic residues modulo p and exactly $\frac{p-1}{2}$ nonresidues modulo p.

Theorem 20.2 (Quadratic Residue Multiplication Rule). (Version 1) Let p be an odd prime. Then:

1. The product of two quadratic residues modulo p is a quadratic residue.
2. The product of a quadratic residue and a nonresidue is a nonresidue.

3. The product of two nonresidues is a quadratic residue.

These three rules can be summarized symbolically by the formulas

$$QR \times QR = QR, QR \times NR = NR, NR \times NR = QR.$$

Definition: The *Legendre symbol* of a mod p is

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

Theorem 20.3 (Quadratic Residue Multiplication Rule). (Version 2) Let p be an odd prime. Then

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

8 Is -1 a Sqaure Modulo p? Is 2?

Theorem 21.1 (Euler's Criterion). Let p be an odd prime. Then

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

Theorem 21.2 (Quadratic Reciprocity). (Part I) Let p be an odd prime. Then -1 is a quadratic residue modulo p if $p \equiv 1 \pmod 4$, and -1 is a nonresidue modulo p if $p \equiv 3 \pmod 4$.
In other words, using the Legendre symbol,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Theorem 21.3 (Primes 1 (Mod 4) Theorem). There are infinitely many primes that are congruent to 1 modulo 4.

Theorem 21.4 (Quadratic Reciprocity). (Part II) Let p be an odd prime. Then 2 is a quadratic residue modulo p if p is congruent to 1 or 7 modulo 8, and 2 is a nonresidue modulo p if p is congruent to 3 or 5 modulo 8. In terms of the *Legendre symbol*,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

9 Quadratic Reciprocity

Theorem 22.1 (Law of Quadratic Reciprocity). Let p and q be distinct odd primes.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

Theorem 22.2 (Generalized Law of Quadratic Reciprocity). Let a and b be odd positive integers.

$$\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \pmod 4, \\ -1 & \text{if } b \equiv 3 \pmod 4. \end{cases}$$

$$\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } b \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{if } a \equiv 1 \pmod 4 \text{ or } b \equiv 1 \pmod 4, \\ -\left(\frac{b}{a}\right) & \text{if } a \equiv b \equiv 3 \pmod 4. \end{cases}$$

10 Which Primes Are Sums of Two Squares?

Theorem 24.1 (Sum of Two Squares Theorem for Primes). Let p be a prime. Then p is a sum of two squares exactly when

$$p \equiv 1 \pmod 4 \quad (\text{or } p = 2).$$

The Sum of Two Squares Theorem really consists of two statements.

Statement 1. If p is a sum of two squares, then $p \equiv 1 \pmod 4$.

Statement 2. If $p \equiv 1 \pmod 4$, then p is a sum of two squares.

Algorithm: Descent Procedure

1. p any prime $\equiv 1 \pmod 4$

2. Write $A^2 + B^2 = Mp$ with $M < p$
3. Choose numbers u and v with $u \equiv A \pmod{M})$, $v \equiv B \pmod{M}$, $\frac{1}{2}M \leqslant u, v \leqslant \frac{1}{2}M$
4. Observe that $u^2 + v^2 \equiv A^2 + B^2 \equiv 0 \pmod{M}$
5. So we can write $u^2 + v^2 = Mr, A^2 + B^2 = Mp$ (for some $1 \leqslant r < M$)
6. Multiply to get $(u^2 + v^2)(A^2 + B^2) = M^2 rp$.
7. Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$.
8. $(uA + vB)^2 + (vA - uB)^2 = M^2 rp$.
9. Divide by M^2. $\left(\frac{uA+vB}{M}\right)^2 + \left(\frac{vA-uB}{M}\right)^2 = rp$ This gives a smaller multiple of p written as a sum of two squares.
10. Repeat the process until p itself is written as a sum of two squares.

11 Which Numbers Are Sums of Two Squares?

Divide: Factor m into a product of primes $p_1 p_2 \ldots p_r$.

Conquer: Write each prime p_i as a sum of two squares.
Unify: Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$ repeatedly to write m as a sum of two squares.

Theorem 25.1 (Sum of Two Squares Theorem). Let m be a positive integer.

(a) Factor m as

$$m = p_1 p_2 \ldots p_r M^2$$

with distinct prime factors $p_1, p_2, \ldots, p_r$. Then m can be written as a sum of two squares exactly when every p_i is either 2 or is congruent to 1 modulo 4.

(b) The number m can be written as a sum of two squares $m = a^2 + b^2$ with $gcd(a, b) = 1$ if and only if it satisfies one of the following two conditions:

1. m is odd and every prime divisor of m is congruent to 1 modulo 4.
2. m is even, $\frac{m}{2}$ is odd, and every prime divisor of $\frac{m}{2}$ is congruent to 1 modulo 4.