MAT315: Intro to Number Theory Final Review

Rui Qiu

The Instructor this semester was Henry Kim. The following material will mostly cover the important definitions, theorems, algorithms and/or (partial) proofs taught in class.

Note: The shaded theorems would be extremenly valuable in the final test.

Chapter 2: Pythagorean Triples

Definition 1. A *primitive Pythagorean triple* (or PPT for short) is a triple of numbers (a,b,c) such that $a,b,$ and c have no common factors and satisfy

$$a^2+b^2=c^2.$$

Theorem 1. *(Pythagorean Triples Theorem). We will get every primitive Pythagorean triple (a, b, c) with a odd and b even by using the formulas*

$$\begin{aligned} a &= st, \\ b &= \frac{s^2-t^2}{2}, \\ c &= \frac{s^2+t^2}{2}, \end{aligned}$$

where $s>t\geqslant 1$ are chosen to be any odd integers with no common factors.

Chapter 3: Pythagorean Triples and the Unit Circle

Theorem 2. *Every point on the circle*

$$x^2 + y^2 = 1$$

whose coordinates are rational numbers can be obtained from the formula

$$(x,y) = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right)$$

by substituting in rational numbers for m [*except for the point* $(-1,0)$ *which is the limiting value as* $m \to \infty$].

Note: The process of getting this formula involves solving a quadratic equation. The trick is to plug in "known" solution term.

If we write the rational number m as a fraction $\frac{v}{u}$, then our formula becomes

$$(x,y) = \left(\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right),$$

and clearing denominators gives the Pythagorean triple

$$(a,b,c) = (u^2 - v^2, 2uv, u^2 + v^2).$$

Note that if we use symbol s,t in Chapter 2, we can set

$$u = \frac{s+t}{2}$$
$$v = \frac{s-t}{2}$$

Chapter 5: Divisibility and the Greatest Common Divisor

Definition 2. The *greatest common divisor* of two numbers a and b (not both zero) is the largest number that divides both of them. It is denoted by $gcd(a,b)$. If $gcd(a,b) = 1$, we say that a and b are *relatively prime*.

Theorem 3. *(Euclidean Algorithm). To compute the greatest common divisor of two number a and b, let* $r_{-1} = a$*, let* $r_0 = b$*, and compute successive quotients and remainders*

$$r_{i-1} = q_{i+1} \times r_i + r_{i+1}$$

for $i = 0, 1, 2, \ldots$ until some remainder r_{n+1} is 0. The last nonzero remainder r_n is then the greatest common divisor of a and b.

Chapter 6: Linear Equations and the Greatest Common Divisor

The smalleste positive value of $ax + by$ is equal to $gcd(a, b)$.

Theorem 4. *(Linear Equation Theorem). Let a and b be nonzero integers, and let $g = gcd(a, b)$. The equation*

$$ax + by = g$$

always has a solution (x_1, y_1) in integers, and this solution can be found by the Euclidean algorithm method described earlier. The every solution to the equation can be obtained by substituting integers k into the formula

$$\left(x_1 + k \cdot \frac{b}{g}, y_1 - k \cdot \frac{a}{g}\right).$$

Chapter 7: Factorization and the Fundamental Theorem of Arithmetic

Definition 3. A *prime number* is a number $p \geqslant 2$ whose only (positive) divisors are 1 and p. Numbers $m \geqslant 2$ that are not primes are called *composite numbers*.

Lemma 1. *Let p be a prime number, and suppose that p divides the product ab. Then either p divides a or p divides b (or p divides both a and b).*

Theorem 5. *(Prime Divisibility Property). Let p be a prime number, and suppose that p divides the product $a_1 a_2 \cdots a_r$. Then p divides at least one of the factors $a_1, a_2, \ldots, a_r$.*

Theorem 6. *(The Fundamental Theorem of Arithmetic). Every integer $n \geqslant 2$ can be factored into a product of primes*

$$n = p_1 p_2 \cdots p_r$$

in exactly one way.

Chapter 8: Congruences

Definition 4. We say that a is *congruent to b modulo m*, and we write $a \equiv b \bmod m$, if m divides $a-b$.

Theorem 7. *(Linear Congruence Theorem). Let a, c and m be integers with $m \geqslant 1$, and let $g = gcd(a, m)$.*

(a) If $g \nmid c$, then the congruence $ax \equiv c \bmod m$ has no solutions.
(b) If $g \mid c$, then the congruence $ax \equiv c \bmod m$ has exactly g incongruent solutions. To find the solutions, first find a solution (u_0, v_0) to the linear equation

$$au + mv = g.$$

(A method for solving this equation is described in Chapter 6.) Then $x_0 = \frac{cu_0}{g}$ is a solution to $ax \equiv c \bmod m$, and a complete set of incongruent solutions is given by

$$x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m} \text{ for } k = 0, 1, 2, \ldots, g-1.$$

Theorem 8. *(Polynomial Roots Mod p Theorem). Let p be a prime number and let*

$$f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d$$

be a polynomial of degree $d \geqslant 1$ with integer coefficients and with $p \nmid a_0$. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most d incongruent solutions.

Chapter 9: Congruences, Powers, and Fermat's Little Theorem

Theorem 9. *(Fermat's Little Theorem). Let p be a prime number, and let a be any number with $a \not\equiv 0 \pmod{p}$. Then*

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

Lemma 2. *Let p be a prime number and let a be a number with $a \not\equiv 0 \pmod{p}$. Then the numbers*

$$a, 2a, 3a, \ldots, (p-1)a \pmod{p}$$

are the same as the numbers

$$1, 2, 3, \ldots, (p-1) \pmod{p},$$

although they may be in a different order.

Chapter 10: Congruences, Powers, and Euler's Formula

Definition 5. The number of integers between 1 and m that are relatively prime to m is an important quantity, so we give this quantity a name:

$$\phi(m) = \#\{a : 1 \leqslant a \leqslant m \text{ and } gcd(a,m) = 1\}.$$

The function ϕ is called *Euler's phi function*.

Theorem 10. *(Euler's Formula). If $gcd(a,m) = 1$, then*

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

Lemma 3. *If $gcd(a,m) = 1$, then the numbers*

$$b_1 a, b_2 a, b_3 a, \ldots, b_{\phi(m)} a \pmod{m}$$

is congruent to one number in the list

$$b_1, b_2, b_3, \ldots, b_{\phi(m)} \pmod{m}.$$

Chapter 11: Euler's Phi Function and the Chinese Remainder Theorem

Theorem 11. *(Phi Function Formulas).*

(a) If p is a prime and $k \geqslant 1$, then

$$\phi(p^k) = p^k - p^{k-1}.$$

(b) If $gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Theorem 12. *(Chinese Remainder Theorem). Let m and n be integers satisfying $gcd(m,n) = 1$, and let b and c be any integers. Then the simultaneous congruences*

$$x \equiv b \pmod m \text{ and } x \equiv c \pmod n.$$

have exactly one solution with $0 \leqslant x < mn$.

Note: There's always a general solution for CRT. How to solve? Substitution + Euclidean Algorithm.

Chapter 12: Prime Numbers

Theorem 13. *(Infinitely Many Prime Theorem). There are infinitely many prime numbers.*

Euclid's Proof. Suppose we have some list of primes $p_1, p_2, \ldots, p_r$. we multiply them together and add 1, which gives the number

$$A = p_1 p_2 \cdots p_r + 1.$$

If A itself a prime, we're done, since A is too large to be in the original list. But even if A is not prime, it will certainly be divisible by some prime, since every number can be written as a product of primes. Let q be some prime dividing A, for example, the smallest one. I claim that q is not in the original list, so it will be the desired new prime.

Why isn't q in the original list? We know q divides A, so

$$q \text{ divides } p_1 p_2 \ldots p_r + 1.$$

If q were to equal one of the p_i's, then it would have to divide 1, which is not possible. This means q is a new prime that may be added to our list. Repeating this process, we can create a list of primes that is as long as we want. This shows that there must be infinitely many prime numbers.

Theorem 14. *(Prime 3 (Mod 4) Theorem). There are infinitely many primes that are congruent to 3 modulo 4.*

Proof: We suppose that we have already compiled a (finite) list of primes, all of which are congruent to 3 modulo 4. Our goal is to make the list longer by finding a new 3 modulo 4 prime. Repeating this process gives a list of any desired length, thereby proving that there are infinitely many primes congruent to 3 modulo 4.

Suppose that our initial list of primes congruent to 3 modulo 4 is

$$3, p_1, p_2, \ldots, p_r.$$

Consider the number

$$A = 4p_1p_2\cdots p_r + 3.$$

(Notice that we don't include the prime 3 in the product.) We know that A can be factored into a product of primes, say

$$A = q_1q_2\cdots q_s.$$

I claim that among the primes $q_1, q_2, \ldots, q_s$ at least one of them must be congruent to 3 modulo 4. This is the key step in the proof. Why is it true? If not, then $q_1, q_2, \ldots, q_s$ would all be congruent to 1 modulo 4, in which case their product A would be congruent to 1 modulo 4. But you can see from its definition that A is clearly congruent to 3 modulo 4. Hence, at least one of $q_1, q_2, \ldots, q_s$ must be congruent to 3 modulo 4, say $q_i \equiv 3 \bmod 4$.

My second claim is that q_i is not in the original list. Why not? We know that q_i divides A, while it is clear from the definition of A that none of $3, p_1, p_2, \ldots, p_r$ divides A. Thus, q_i is not in our original list, so we may add it to the list and repeat process. In this way we can create as long a list as we want, which shows that there must be infinitely many primes congruent to 3 modulo 4.

Theorem 15. *(Dirichlet's Theorem on Primes in Arithmetic Progressions). Let a and m be integers with* $\gcd(a,m) = 1$*. Then there are infinitely many primes that are congruent a modulo m. That is, there are infinitely many prime numbers p satisfying*

$$p \equiv a \bmod m.$$

Chapter 14: Mersenne Primes

Definition 6. Primes of the form $2^p - 1$ are called *Mersenne primes*

Note: Not every $2^p - 1$ is prime.

Chapter 15: Mersenne Primes and Perfect Numbers

Definition 7. A *perfect number* is a number that is equal to the sum of its proper divisors. The proper divisors of a number are the divisors other than itself.

Theorem 16. *(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 17. *(Euler'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 8. A *sigma function* is equal to $\sigma(n) =$ sum of all divisors of n (including 1 and n).

Theorem 18. *(Sigma Function Formulas).*

(a) If p is a prime and $k \geqslant 1$, then

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

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

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

A number n is perfect if the sum of its divisors, other than n itself, is equal to n. The sigma function $\sigma(n)$ is the sum of the divisors of n, including n, so it has an extra n. Therefore,

$$n \text{ is perfect exactly when } \sigma(n) = 2n.$$

Chapter 16: Powers Modulo m and Successive Squaring

Algorithm (Successive Squaring to Compute a^k mod m). The following steps compute the value of a^k mod m:

1. Write k as a sum of powers of 2,

$$k = u_0 + u_1 \cdot 2 + u_2 \cdot 4 + u_3 \cdot 8 + \cdots + u_r \cdot 2^r,$$

   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.

$$\begin{aligned} a^1 &\equiv A_0 \bmod m \\ a^2 \equiv (a^1)^2 \equiv A_0^2 &\equiv A_1 \bmod m \\ a^4 \equiv (a^2)^2 \equiv A_1^2 &\equiv A_2 \bmod m \\ a^8 \equiv (a^4)^2 \equiv A_2^2 &\equiv A_3 \bmod m \\ &\cdots \\ a^{2r} \equiv \left(a^{2^{r-1}}\right)^2 \equiv A_{r-1}^2 &\equiv A_r \bmod m \end{aligned}$$

   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

$$A_0^{u_0} \cdot A_1^{u_1} \cdot A_2^{u_2} \cdots A_r^{u_r} \bmod m$$

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.

Using successive squaring and Fermat's Little Theorem, we can show that a number m is composite without finding any factors. Take any number a less than m. First compute $gcd(a,m)$. If it is greater than 1, then it's a factor of m, we are done. If not, if $gcd(a,m) = 1$, use successive squaring to compute

$$a^{m-1} \bmod m.$$

Fermat's Little Theorem says that if m is prime then the answer will be 1.

But numbers like *Carmichael numbers* do exist, and those composite numbers m do satisfy the equation $a^{m-1} \equiv 1 \bmod m$ for all a's with $gcd(a,m) = 1$. The smallest *Carmichael number* is 561.

Chapter 17: Computing k^{th} Roots Modulo m

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

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

The following steps give a solution to the congruence

$$x^k \equiv b \bmod m.$$

1. Compute $\phi(m)$.
2. Find positive integers u and v that satisfy $ku - \phi(m)v = 1$.
3. Compute $b^u \bmod m$ by successive squaring. The value obtained gives the solution x.

Chapter 20: Squares Modulo p

Definition 9. A nonzero number that is congruent to a square module p is called a *quadratic residue modulo p (QR)*. A number that is not congruent to a square modulo p is called a *(quadratic) nonresidue modulo p (NR)*.

Theorem 19. *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. *(Quadratic Residue Multiplication Rule). (Version 1) Let p be an odd prime. Then:*

(i) QR × QR = QR,
(ii) QR × NR = NR,
(iii) NR × NR = QR.

QR behaves like +1 and NR behaves like -1.

Definition 10. The *Legendre symbol* of a modulo 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 21. *(Quadratic Residue Multiplication Rule). (Version 2) Let p be an odd prime. Then*

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

Chapter 21: Is -1 a Square Modulo p? Is 2?

Theorem 22. *(Euler's Criterion). Let p be an odd prime. Then*

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

Theorem 23. *(Quadratic Reciprocity). (Part I) Let p be an odd prime. Then*

$$-1 \textit{ is a quadratic residue modulo } p \textit{ if } p \equiv 1 \bmod 4, \textit{ and}$$
$$-1 \textit{ is a nonresidue modulo } p \textit{ if } p \equiv 3 \bmod 4.$$

In other words, using the Legendre symbol,

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

Theorem 24. *(Primes 1 (Mod 4) Theorem). There are infinitely many primes that are congruent to 1 modulo 4.*

Proof. Suppose given a list of primes $p_1, p_2, \ldots, p_r$, all of which are congruent to 1 modulo 4. Consider the number

$$A = (2p_1 p_2 \cdots p_r)^2 + 1.$$

We know that A can be factored into a product of primes, say

$$A = q_1 q_2 \cdots q_s.$$

It's clear that $q_1, q_2, \ldots, q_s$ are not in our original list, since none of the p_i's divide A. So all we need to do is show that one of the q_i's is congruent to 1 modulo 4. In fact, we'll see all of them are.

First note that A is odd, so all the q_i's are odd. Next, each q_i divides A, so

$$(2p_1 p_2 \cdots p_r)^2 + 1 = A \equiv 0 \bmod q_i.$$

This means that $x = 2p_1 p_2 \cdots p_r$ is a solution to the congruence

$$x^2 \equiv -1 \bmod q_i,$$

so -1 is a quadratic residue modulo q_i. Now Quadratic Reciprocity tells us that $q_i \equiv 1 \bmod 4$.

Theorem 25. *(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,*

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

Chapter 22: Quadratic Reciprocity

Theorem 26. *(Law of Quadratic Reciprocity). Let p and q be distinct odd primes.*

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

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

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

Theorem 27. *(Generalized Law of Quadratic Reciprocity). Let a and b be odd positive integers.*

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

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

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

Chapter 23: Proof of Quadratic Reciprocity

Definition 11. Consider a list of numbers $a, 2a, 3a, \ldots, Pa$, and we reduce them modulo p into the range from $-P$ to P. some of the reduced values will be positive and some of them will be negative.

Let $\mu(a,p) =$ number of integers in the list that become negative when the integers in the list are reduced to modulo p into the interval from $-P$ to P.

Theorem 28. *(Gauss's Criterion). Let p be an odd prime, let a be an integer that is not divisible by p, and let $\mu(a,p)$ be the number defined previously. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}.$$

Lemma 4. *When the numbers $a, 2a, 3a, \ldots, Pa$ are reduced modulo p into the range from $-P$ to P, the reduced values are $\pm 1, \ldots, \pm P$ in some order, with each number appearing once with either a plus sign or a minus sign.*

Lemma 5. *Let p be an odd prime, let $P = \frac{p-1}{2}$, let a be an odd integer that is not divisible by p, and let $\mu(a,p)$ be the quantity defined previously that appears in Gauss's criterion. Then*

$$\sum_{k=1}^{P} \lfloor \frac{ka}{p} \rfloor \equiv \mu(a,p) \bmod 2.$$

Definition 12. *Jacobi symbol*: n odd positive integer, $gcd(a,n) = 1$, $n = p_1 \cdots p_r$ product of prime, p_i's are not necessarily distinct. Define

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

With following properties:

1. If $a \equiv a' \bmod n$, $\left(\frac{a}{n}\right) = \left(\frac{a'}{n}\right)$.
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
3. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
4. If $x^2 \equiv a \bmod n$ has a solution, then $\left(\frac{a}{n}\right) = 1$.

Chapter 24: Which Primes Are Sums of Two Squares?

Theorem 29. *(Sum of Two Squares Theorem for Primes). Let p be a prime. Then p is a sum of two squares exactly when*

$$p \equiv 1 \bmod 4 \textit{ or } p = 2.$$

Know that $A^2 + B^2 = Mp$ for some integers A, B, and M. What to find integers a, b, and m with $a^2 + b^2 = mp$ and $m \leqslant M - 1$.

Denote the identity that $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$.

Descent Procedure

1. p any prime $\equiv 1 \bmod 4$
2. Write $A^2 + B^2 = Mp$ with $M < p$
3. Choose numbers u and v with $u \equiv A \bmod M, v \equiv B \bmod M, -\frac{1}{2}M \leqslant u, v \leqslant \frac{1}{2}M$
4. Observe that $u^2 + v^2 \equiv A^2 + B^2 \equiv 0 \bmod M$
5. So we can write $u^2 + v^2 = Mr, A^2 + B^2 \equiv Mp$ (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 above.
8. $(uA + vB)^2 + (vA - uB)^2 = M^2 rp$
9. Divide by M^2. $\left(\frac{uA+vB}{M}\right)^2 + \left(\frac{vA-uB}{M}\right)^2 = rp$
10. Repeat this process until p itself is written as a sum of two squares

Chapter 25: Which Numbers Are Sums of Two Squares?

Divide and Conquer: Divide: Factor m into a product of primes $p_1 p_2 \cdots p_r$. 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 30. *(Sum of Two Squares Theorem). Let m be a positive integer.*

(a) Factor m as

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

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:

(i) m is odd and every prime divisor of m is congruent to 1 modulo 4.

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

Theorem 31. *(Pythagorean Hypotenuse Proposition). A number c appears as the hypotenuse of a primitive Pythagorean triple (a,b,c) if and only if c is a product of primes each of which is congruent to 1 modulo 4.*

Chapter 27: Euler's Phi Function and Sums of Divisors

Recall Euler's phi functions for primes: $\phi(p^k) = p^k - p^{k-1}$. Define a function $F(n)$ by the formula: $F(n) = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_r)$, where $d_1, d_2, \ldots, d_r$ are the divisors of n.

Lemma 6. *If $gcd(m,n) = 1$, then $F(mn) = F(m)F(n)$.*

Theorem 32. *(Euler's Phi Function Summation Formula). Let $d_1, d_2, \ldots, d_r$ be the divisors of n. Then*

$$\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r) = n$$

Chapter 28: Powers Modulo p and Primitive Roots

Definition 13. The *order of a modulo p* is $e_p(a) =$ the smallest exponent $e \geqslant 1$ such that $a^e \equiv 1 \bmod p$).

Theorem 33. *(Order Divisibility Property). Let a be an integer not divisible by the prime p, and suppose that $a^n \equiv 1 \bmod p$. Then the order $e_p(a)$ divides n. In particular, the order $e_p(a)$ always divides $p-1$.*

Definition 14. A number g with maximum order $e_p(g) = p-1$ is called a *primitive root modulo p*.

For example, $p = 7, 1^1 \equiv 1 \bmod 7, 2^3 \equiv 1 \bmod 7, 3^6 \equiv 1 \bmod 7, 4^3 \equiv 1 \bmod 7, 5^6 \equiv 1 \bmod 7, 6^2 \equiv 1 \bmod 7$. So the primitive roots modulo 7 are 3 and 5.

Theorem 34. *(Primitive Root Theorem). Every prime p has a primitive root. More precisely, there are exactly $\phi(p-1)$ primitive roots modulo p.*

Chapter 29: Primitive Roots and Indices

Definition 15. For any number $1 \leqslant a < p$, we can pick out exactly one of the powers $g, g^2, g^3, \ldots, g^{p-3}, g^{p-2}, g^{p-1}$ as being congruent to a modulo p. The exponent is called the *index of a modulo p for the base g*. Write $I(a)$ for the index.

If we use the primitive root 2 as base for the prime 13, then $I(3) = 4$, since $2^4 = 16 \equiv 3 \bmod 13$.

Theorem 35. *(Rules for Indices). Indices satisfy the following rules:*

(a) $I(ab) \equiv I(a) + I(b) \bmod (p-1)$ *[Product Rule]*
(b) $I(a^k) \equiv kI(a) \bmod (p-1)$ *[Power Rule]*

Chapter 31: Square-Triangular Numbers Revisited

Theorem 36. *(Square-Triangular Number Theorem).*

(a) Every solution in positive integers to the equation

$$x^2 - 2y^2 = 1$$

is obtained by raising $3+2\sqrt{2}$ *to powers. That is, the solutions* (x_k, y_k) *can all be found by multiplying out*

$$x_k + y_k\sqrt{2} = (3+2\sqrt{2})^k \text{ for } k = 1,2,3,\ldots$$

(b) Every square-triangular number $n^2 = \frac{1}{2}m(m+1)$ *is given by*

$$m = \frac{x_k - 1}{2}, n = \frac{y_k}{2} \text{ for } k = 1,2,3,\ldots,$$

where the (x_k, y_k)*'s are the solutions from (a).*

Chapter 32: Pell's Equation

Definition 16. A *Pell's equation* is an equation of the form $x^{-}Dy^2 = 1$ where D is a fixed positive integer that is not a perfect square.

Theorem 37. *(Pell's Equation Theorem). Let D be a positive integer that is not a perfect square. Then Pell's equation*

$$x^2 - Dy^2 = 1$$

always has solutions in positive integers. If (x_1, y_1) *is the solution with smallest* x_1*, then every solution* (x_k, y_k) *can be obtained by taking powers*

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k \text{ for } k = 1,2,3,\ldots.$$

There is no known pattern as to when the smallest solution is actually small and when it is large.

Chapter 35: Number Theory and Imaginary Numbers

Theorem 38. *(The Fundamental Theorem of Algebra). If* $a_0, a_1, a_2, \ldots, a_d$ *are complex numbers with* $a_0 \neq 0$ *and* $d \geqslant 1$*, then the equation*

$$a_0x^d + a_1x^{d-1} + a_2x^{d-2} + \cdots + a_{d-1}x + a_d = 0$$

has a solution in complex numbers.

Definition 17. The *Gaussian integers* are the complex numbers of the form $a + bi$ with a and b both integers.

The sum and product of two Gaussian integers are also Gaussian integers, but the quotient need not be a Gaussian integer.

Theorem 39. *(Gaussian Unit Theorem). The only units in the Gaussian integers are* $1, -1, i$, *and* $-i$. *That is, these are the only Gaussian integers that have Gaussian integer multiplicative inverses.*

Definition 18. The *norm* of $x+yi$ is $N(x+yi) = x^2+y^2$.

Theorem 40. *(Norm Multiplication Property). Let* α *and* β *be any complex numbers. Then*

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

A Gaussian integer α is a unit if and only if $N(\alpha) = 1$.

Theorem 41. *(Gaussian Prime Theorem). The Gaussian primes can be described as follows:*

(i) $1+i$ *is a Gaussian prime.*
(ii) Let p be an ordinary prime with $p \equiv 3 \bmod 4$. *Then p is a Gaussian prime.*
(iii) Let p be an ordinary prime with $p \equiv 1 \bmod 4$ *and write p as a sum of two squares* $p = u^2+v^2$. *Then* $u+vi$ *is a Gaussian prime.*

Every Gaussian prime is equal to a unit (± 1 *or* $\pm i$*) multiplied by a Gaussian prime of the form (i),(ii) or (iii).*

Lemma 7. *(Gaussian Divisibility Lemma). Let* $\alpha = a+bi$ *be a Gaussian integer.*

(a) If 2 divides $N(\alpha)$, *then* $1+i$ *divides* α.
(b) Let pi = p be a category (ii) prime, and suppose that p divides $N(\alpha)$ *as ordinary integers. Then pi divides* α *as Gaussian integers.*
(c) Let pi = $u+vi$ *be a Gaussian prime in category (iii), and let* $\overline{\pi} = u - vi$. *(This is a natural notation, since* $\overline{\pi}$ *is indeed the complex conjugate of the complex number* π.*) Suppose that* $N(\pi) = p$ *divides* $N(\alpha)$ *as ordinary integers. Then at least one of* π *and* $\overline{\pi}$ *divides* α *as Gaussian integerse.*

Chapter 36: The Gaussian Integers and Unique Factorization

Definition 19. We say that $x+yi$ is *normalized* if $x > 0$ and $y \geqslant 0$.

Theorem 42. *(Unique Factorization of Gaussian Integers). Every Gaussian integer* $\alpha \neq 0$ *can be factored into a unit u multiplied by a product of normalized Gaussian primes*

$$\alpha = u\pi_1\pi_2\cdots\pi_r$$

in exactly one way.

Theorem 43. *(Gaussian Integer Division with Remainder). Let α and β be Gaussian integers with $\beta \neq 0$. Then there are Gaussian integers γ and ρ such that*

$$\alpha = \beta\gamma + \rho \text{ and } N(\rho) < N(\beta).$$

Theorem 44. *(Gaussian Integer Common Divisor Property). Let α and β be Gaussian integers, and let S be the collection of Gaussian integers*

$$A\alpha + B\beta, \text{ where } A \text{ and } B \text{ are any Gaussian integers.}$$

Among all Gaussian integers in S, choose an element

$$g = a\alpha + b\beta$$

having the smallest nonzero norm. In other words,

$$0 < N(g) \leqslant N(A\alpha + B\beta) \text{ for any Gaussian integers } A \text{ and } B \text{ with } A\alpha + B\beta \neq 0.$$

Then g divides both α and β.

Theorem 45. *(Gaussian Prime Divisibility Property). Let π be a Gaussian prime, letα and β be Gaussian integers, and suppose that pi divides the product $\alpha\beta$. Then either pi divides α or pi divides β (or both). More generally, if pi divides a product $\alpha_1\alpha_2\cdots\alpha_n$ of Gaussian integers, then it divides at least one of the factors $\alpha_1, \alpha_2, \ldots, \alpha_n$.*

Theorem 46. *(Sum of Two Squares Theorem (Legendre)). For a given positive integer N, let*
$D_1 =$ (the number of positive integers d dividing N that satisfying $d \equiv 1 \bmod 4$),
$D_3 =$ (the number of positive integers d dividing N that satisfying $d \equiv 3 \bmod 4$).
Then N can be written as a sum of two squares in exactly $R(N) = 4(D_1 - D_3)$ ways.

Theorem 47. *(Difference of $D_1 - D_3$ Theorem). Factor the integer N into a product of ordinary primes as*

$$N = 2^t p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \cdot q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}.$$

where p_i's are 1 mod 4 primes, q_j's are 3 mod 4 primes. Let
$D_1 =$ (the number of positive integers d dividing N that satisfying $d \equiv 1 \bmod 4$),
$D_3 =$ (the number of positive integers d dividing N that satisfying $d \equiv 3 \bmod 4$).
Then the difference $D_1 - D_3$ is given by the rule

$$D_1 - D_3 = \begin{cases} (e_1+1)(e_2+1)\cdots(e_r+1) & \text{if } f_1, \ldots, f_s \text{ are all even,} \\ 0 & \text{if any of } f_1, \ldots, f_s \text{ is odd.} \end{cases}$$