Number Theory

Divisibility and Primes

Definition. *If a and b are integers and there is some integer c such that $a = b \cdot c$, then we say that b divides a or is a factor or divisor of a and write $b|a$.*

Definition (Prime Number). *A prime number is an integer greater than 1 whose only positive divisors are itself and* 1*. A non-prime number greater than* 1 *is called a composite number.*

Theorem (The Fundamental Theorem of Arithmetic). *Every positive integer greater than* 1 *may be expressed as a product of primes and this representation is unique up to the order in which the factors are written.*

Theorem. *There are infinitely many prime numbers.*

Proof. Suppose otherwise. Then there would be a finite number n of primes, which we may denote by $p_1, p_2, p_3, \ldots, p_n$. Consider $x = p_1 \cdot p_2 \cdot p_3 \ldots p_n + 1$. There must be some prime number greater than 1 which divides x, but clearly x is not divisible by any of $p_1, p_2, p_3, \ldots, p_n$. This contradicts the assumption that there is are finitely many primes, proving there are infinitely many. $\square$

Sieve of Erastothenes

The Sieve of Erastothenes is a technique which may be used to determine all the prime numbers up to a certain size. One writes down all the integers up to that size. One then crosses out all the multiples of 2 (the even numbers) greater than 2. At each step, one takes the smallest number left whose multiples haven't been crossed out and crosses out all its multiples. One is ultimately left only with the prime numbers.

Test for Primality

One may check every integer less than the number's square root. If none are divisors, then the integer is prime.

This may be seen by recognizing that if an integer n is not prime, there must be integers $p \leq q$ both dividing n. But then $p^2 \leq pq \leq n$, so $p \leq \sqrt{n}$. So every non-prime number must have a divisor no greater than its square root.

There are much more sophisticated tests for primality.

Goldbach's Conjecture

Goldbach's Conjecture is that every even integer greater than 4 may be written as a sum of two odd primes.

Goldbach's Conjecture has been shown to hold for all even integers up to 400 trillion, but has not yet been proven in general. Hence, it remains a *conjecture* rather than a *theorem**.

Theorem (The Division Algorithm). *If a, b are integers with $b > 0$, then there exist unique integers q, r such that $a = q \cdot b + r$ with $0 \leq r < b$. q is called the quotient and r is called the remainder.*

Note: The Division Algorithm is not an algorithm!

Note: Any number which divides both a and b also divides both b and r and visa versa.

Definition (Greatest Common Divisor). *The greatest common divisor of integers a and b is the largest positive integer which divides both a and b. We denote the greatest common divisor by gcd(a, b) or simply (a, b).*

The Euclidean Algorithm gives a method (an algorithm!) for finding the greatest common divisor of any two positive integers:

Given a, b, we apply the Euclidean Algorithm and find $(a, b) = (b, r)$. We then apply the Euclidean Algorithm to the pair b, r. We keep repeating the process, each time getting a new pair of numbers with the same gcd as a, b, until we get two numbers such that one divides the other. That divisor is the gcd we're looking for.

Modular Arithmetic

Definition (mod). *If a is an integer and n is a positive integer, then a mod n is the remainder obtained when we divide a by n using the Euclidean Algorithm.*

Definition (congruence). *If n is a positive integer, two integers a, b are said to be congruent modulo n if they both have the same remainder when divided by n. We write $a \equiv b \mod n$.*

Corollary. *$a \equiv b \mod n$ if and only if $n|(a-b)$.*

Modular arithmetic has many of the same properties as ordinary arithmetic. We may define addition, subtraction and multiplication modulo n because it is easily seen that if $a \equiv b \mod n$ and $c \equiv d \mod n$, then:

1. $a + c \equiv b + d \mod n$

2. $a - c \equiv b - d \mod n$

3. $a \cdot b \equiv b \cdot d \mod n$

Divisibility Tests

Modular arithmetic may be used to show the validity of a number of common divisibility tests.

Casting Out Nines

A test for divisibility is called *Casting Out Nines*:

Theorem. *A positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.*

Proof. Since $10 \equiv 1 \mod 9$, it follows that $10^n \equiv 1 \mod 9$ for any positive integer n. Given any integer N, we may write $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + a_{m-2} \cdot 10^{m-2} + \ldots a_0 \cdot 10^0$, where $a_0, a_1, a_2, \ldots a_m$ are the digits in N. But then $N \equiv a_m \cdot 1 + a_{m-1} \cdot 1 + \cdots + a_0 \mod 9$. □

Essentially the same reasoning shows:

Theorem. *A positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3.*

A variation gives a method called *Casting out Elevens* for testing divisibility by 11. It's based on the fact that $10 \equiv -1 \mod 11$, so $10^n \equiv (-1)^n \mod 11$.
Theorem (Casting Out Elevens). *A positive integer is divisible by* 11 *if and only if the alternating sum of its digits is divisible by* 11*.*

Proof. Since $10 \equiv -1 \mod 9$, it follows that $10^n \equiv (-1)^n \mod 11$ for any positive integer n. Given any integer N, we may write $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + a_{m-2} \cdot 10^{m-2} + \ldots a_0 \cdot 10^0$, where $a_0, a_1, a_2, \ldots a_m$ are the digits in N. But then $N \equiv a_m \cdot (-1)^m + a_{m-1} \cdot (-1)^{m-1} + \cdots + a_0 \mod 11 \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m \mod 11$. □

Other Tests

- Divisibility By 2 – The units digit must be even.

- Divisibility By 4 – The number formed by its last two digits must be divisible by 4.

- Divisibility By 5 – The units digit must be 0 or 5.

- Divisibility By 6 – It must be even and divisible by 3.

- Divisibility By 7 – When the units digit is doubled and subtracted from the number formed by the remaining digits, the resulting number must be divisible by 7. (To verify, write the original number in the form

$10a + b \equiv 3a + b \mod 7$, so the resulting number is $a - 2b$, and check the possible ways for $3a + b$ to be divisible by 7.)

- Divisibility By 8 – The number formed by its last three digits must be divisible by 8.

- Divisibility By 10 – Its last digit must be 0.

Check Digits

Definition (Check Digit). *A check digit is an extra digit tacked onto a number which is mathematically related in some way to the other digits.*

Example: Airline Tickets – The check digit is the main part $\pmod 7$.

Example: U.S. Postal Service Money Orders – The check digit is the main part $\pmod 9$.

These do not catch all *single-digit errors* nor do they catch *transposition errors*.

Bank Identification Number Check Digit Formula: Every bank has a nine digit identification number of the form $a_8a_7a_6a_5a_4a_3a_2a_1a_0$ where $a_0 = (7a_8 + 3a_7 + 9a_6 + 7a_5 + 3a_4 + 9a_3 + 7a_2 + 3a_1) \mod 10$.

UPC Number Check Digit Formula: a_0 is chosen so $(3a_{11}+a_{10}+3a_9+a_8+3a_7+a_6+3a_5+a_4+3a_3+a_2+3a_1) \equiv 0 \mod 10$.

ISBN Check Digit Formula: $a_0 \equiv (a_9+2a_8+3a_7+4a_6+5a_5+6a_4+7a_3+8a_2+9a_1) \mod 11$.

There is a check digit method that detects all single-digit and transposition errors and only generates 0 through 9 as a check digit.

Tournament Scheduling

Problem: How do we schedule the teams playing in a round-robin tournament?

Solution:

Let N be the number of teams in the tournament and number the teams $1, 2, 3, \ldots, N$.

Let $T_{m,r}$ be the team which Team m plays in Round r.

If there is an odd number of teams, we let $T_{m,r}$ be the unique integer between 1 and N such that

$$T_{m,r} \equiv r - m \mod N.$$

If $T_{m,r} = m$, then Team m gets a bye.

If there is an even number of teams, we schedule the teams as if there was one fewer team and let the team that would otherwise get a bye play the last team.

Cryptology

Definition (Cryptology). *Cryptology is the discipline of encoding and decoding messages.*

Cryptology is critical in everyday life today. Our banking system, including the ability to use ATM's and to do online banking, would collapse without the ability to securely transmit financial information over public networks.

Cryptology has played a crucial role in history. Many believe that World War II was shortened by several years because the Allies were able to *crack* the secret codes used by the Axis powers.

Definition (Cipher). *A cipher is a method for encoding messages.*

Definition (Plaintext). *Plaintext refers to the original text that is being encoded.*

Definition (Ciphertext). *Ciphertext refers to the encoded message.*

Definition (Enciphering, Encryption). *The process of encoding a message is sometimes referred to as enciphering or encryption.*

Definition (Deciphering, Decryption). *The process of Decoding a message is sometimes referred to as deciphering or decryption.*

The Caesar Cipher

The Caesar Cipher is one of the earliest known ciphers and was used by Julius Casar. Each letter in a message is simply replaced by the letter coming three letters after it in the alphabet.

Obvious problem: What about x, y and z?

Obvious solution: Replace them with a, b and c.

We may make this somewhat quantitative by assigning a numerical value to each letter: 0 to A, 1 to B, 2 to C, . . . , 25 to Z. If we let P represent the numerical value of a given letter in plaintext and C represent the number it is replaced by in ciphertext, we have

$$C \equiv (P + 3) \mod 26.$$

To decode, we have

$$P \equiv (C - 3) \mod 26.$$

More generally, we might use a shift other than 3 and let $C \equiv (P + b) \mod 26$ for some other integer b.

We might mix things up a little more and let

$$C \equiv (aP + b) \mod 26 \qquad (1)$$

for some choice of integers a and b. Such a cipher would be called an *affine cipher*.

To decode, we could try to *solve* the congruence (1) for P in terms of C. We might proceed as follows:

$C \equiv aP + b \mod 26$,

$aP \equiv C - b \mod 26$,

$P \equiv a^{-1}(C - b) \mod 26$.

Question: What is a^{-1}, the multiplicative inverse of a?

It would have to be a number such that $a \cdot a^{-1} \equiv 1 \mod 26$.

It turns out that not all integers have such an inverse. For example, no even numbers could have inverses $\mod 26$ since any multiple of an even number would be even and could only be congruent to another even integer and thus could not possibly be congruent to 1.

Theorem 1. *An integer a has a multiplicative inverse* $\mod n$ *if and only if a and n have no factors in common other than* 1*, in other words, if $(a, n) = 1$.*

The Hill Cipher

With the *Hill Cipher*, blocks of letters are encoded simultaneously rather than encoding letters separately in a method similar to an affine cipher. For a block of two letters, P_1, P_2, the corresponding encoded letters C_1, C_2 would be determined by the formulas

$$\begin{aligned} C_1 &\equiv (aP_1 + bP_2) \quad \text{mod } 26 \\ C_2 &\equiv (cP_1 + dP_2) \quad \text{mod } 26, \end{aligned}$$

where a, b, c, d are integers. It turns out we will need $(ad - bc, 26) = 1$ in order to be able to decipher the encoded message. To see this, we may try to solve for P_1 and P_2 in terms of C_1 and C_2 the same way we would if we were dealing with ordinary equations–by matching coefficients and using elimination.

We might match the coefficients of P_2 by multiplying the first equation by d and the second by b to get

$$\begin{aligned} dC_1 &\equiv (adP_1 + bdP_2) \mod 26 \\ bC_2 &\equiv (bcP_1 + bdP_2) \mod 26, \end{aligned}$$

.

Subtracting, we get

$$dC_1 - bC_2 \equiv (ad - bc)P_1 \mod 26.$$

We need $ad - bc$ to have an inverse mod 26 in order to solve:

$$P_1 \equiv (ad - bc)^{-1}(dC_1 - bC_2) \mod 26.$$

Similarly, we may find

$$P_2 \equiv (ad - bc)^{-1}(aC_2 - cC_1) \quad \text{mod } 26.$$

Variations may be used for larger blocks of letters.

The RSA Public Key System

In *public key systems*, the encoding method is made public, so that anyone may send an encoded message, but the decoding method is known only to the recipient. This depends on the difficulty of determining the decoding method even if the encoding method is known.

The RSA Public Key System was created by Ron Rivest, Adi Shamir and Len Adelman in 1975. It is probably the most widely used system today.

The Method

Two large primes, p, q, are determined along with their product $n = pq$ and a positive integer r relatively prime to both $p - 1$ and $q - 1$. The values of n and r are *published*. A block of letters is then encoded by letting

$$C \equiv P^r \mod n.$$

To decode the message, the recipient determines the multiplicative inverse $k = r^{-1} \mod (p-1)(q-1)$ and calculates

$$P \equiv C^k \mod n.$$