Number Theory

Review

Given integers $a, b \in \mathbb{Z}$ with $a \neq 0$, a **divides** b (notated $a|b$) if $b = c \cdot a$ for some integer $c \in \mathbb{Z}$. The divisibility relation forms a partial order on the positive integers.

The **division algorithm** states that for any integer $a \in \mathbb{Z}$ and any positive integer $d \in \mathbb{Z}^+$, there are unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < d$ for which $a = q \cdot d + r$. We call q the **quotient** and r the **remainder** when a is divided by d.

The **modulo** operator (notated $\mod$) returns the remainder of its left argument when divided by its right argument. For example, $75 \mod 12 = 3$ since $75 = 6 \cdot 12 + 3$.

Given a particular $m \in \mathbb{Z}^+$, the **modulus**, we can define the equivalence relation **congruence modulo** m such that $a \equiv b \pmod{m}$ when $a \mod m = b \mod m$, or equivalently when $m|(a - b)$.

The properties $(a + b) \mod m = ((a \mod m) + (b \mod m)) \mod m$ and $(ab \mod m) = (a \mod m)(b \mod m) \mod m$ allow us to perform calculations in **modular arithmetic** without the need to work with large numbers (greater than m^2).

To represent a number n in **base** b, use the following procedure: Represent $n = q_1 \cdot b + r_1$. r_1 is the rightmost digit of the base b representation. To find the remaining digits, recurse on q_1.

The **fast exponentiation** procedure allows us to quickly compute $m^e \pmod{n}$. To perform this procedure:

1. Compute the binary representation of exponent $e = (1\, b_2 \ldots b_k)_2$.
2. Start with $m_1 = m \mod n$.
3. Working from left to right in the binary representation of e, starting with b_2:
   (a) If $b_i = 0$, compute $m_i = (m_{i-1})^2 \mod n$.
   (b) If $b_i = 1$, compute $m_i = (m_{i-1})^2 \cdot m \mod n$.
4. Then, $m_k = m^e \pmod{n}$.

A positive integer n is **prime** if its only positive integer divisors are 1 and n. Otherwise, if $n > 1$, then n is **composite**.

The **Fundamental Theorem of Arithmetic** states that each positive integer can be represented uniquely as a product of non-decreasing primes.

Given two integers a and b, their **greatest common divisor** (notated $\gcd(a, b)$) is the largest integer d such that $d|a$ and $d|b$. If $\gcd(a, b) = 1$, we say that a and b are **relatively prime**.

The **Euclidean Algorithm** gives us an efficient way to calculate the gcd of two positive integers. The main idea of the algorithm is that if $a > b$, then $\gcd(a, b) = \gcd(b, a \mod b)$. We can repeatedly apply this fact until the second argument is 0, at which point the first argument is $\gcd(a, b)$.

The **Extended Euclidean Algorithm** allows us to represent $\gcd(a, b)$ as an integer linear combination of a and b. That is, $\gcd(a, b) = m \cdot a + n \cdot b$ for some integers m and n. To run this algorithm, we work backward through our calculations in the Euclidean algorithm:

Suppose we currently have $\gcd(b, a \mod b) = m \cdot b + n \cdot (a \mod b)$. Further, suppose that $a = q \cdot b + (a \mod b)$. Then,

$$\gcd(a, b) = \gcd(b, a \mod b) = m \cdot b + n \cdot (a \mod b) = m \cdot b + n \cdot (a - q \cdot b) = n \cdot a + (m - qn) \cdot b.$$

Fermat's Little Theorem says that for any integer n and any prime p, $n^p \equiv n \pmod p$. In particular, when $\gcd(n, p) = 1$, then $n^{p-1} \equiv 1 \pmod p$.

In a **public key cryptosystem**, such as RSA, an agent publishes a procedure, a **public key**, whereby anyone can encrypt a message. However, a **private key**, known only to the agent is necessary to decrypt these messages. The security of these schemes relies on the fact that it is computationally difficult to determine the private key given only the information in the public key.

The **RSA Cryptosystem** works as follows:

1. The receiver chooses two large prime numbers p and q, and computes $N = pq$ and $\phi = (p-1)(q-1)$.
2. The receiver selects some e with $\gcd(e, \phi) = 1$ and computes d such that $ed \mod \phi = 1$. (To do this, they want $d \cdot e - c \cdot \phi = 1$ for some $c \in \mathbb{Z}$. c and d can be computed using the Extended Euclidean Algorithm since $\gcd(e, \phi) = 1$.)
3. The receiver distributed the public key (N, e). In order to encrypt a message M, a sender computes $C = M^e \mod N$ (via fast exponentiation).
4. To decrypt the message, the receiver computes $M = C^d \mod N$ (again with fast exponentiation).

1. For each of the given values of $a, d \in \mathbb{Z}$, find the quotient q and remainder r such that

$$a = qd + r, \qquad 0 \leq r < d.$$

(a) $a = 96, \quad d = 6$:

(b) $a = 83, \quad d = 7$:

(c) $a = 189, \quad d = 13$:

(d) $a = -74, \quad d = 8$:

2. In this question, we'll explore some properties of integer division.

(a) Suppose that $a|b$ and $c|d$. Argue that $ac|bd$.

(b) Now, suppose that $a|b$ and $ac|bd$. Is it necessarily true that $c|d$? Explain your answer.

3. In this question, we'll practice converting numbers into different bases. We use the notation $(n)_b$ to signify that the n is the representation of a number in base b. For example, $(1101)_2 = (13)_{10}$.

(a) Find the binary representation of $(77)_{10}$.

(b) Find the decimal (base-10) representation of $(1110100101)_2$.

(c) Find the decimal representation of $(ABC)_{16}$.

(d) Find the ternary (base-3) representation of $(65)_{10}$.

4. Complete the following addition and multiplication tables for $\mathbb{Z}_6$.

$+$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

$\times$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

5. Compute the following congruences.

(a) 314 mod 7

(b) $(7^{183} + 5^{40} + 4^7 + 3) \bmod 2$

(c) $7^{57} \bmod 13$ (**Hint:** Use fast exponentiation)

6. Argue that if there is an integer x for which $ax \equiv b \pmod{n}$, then $\gcd(a, n) | b$.

Note that the converse of this statement also holds (try showing this), giving us a characteristic for when a 1-variable linear congruence is solvable.

7. For each of the following pairs of numbers (x, y),

- Use the Euclidean Algorithm to compute $\gcd(x, y)$.
- Use the Extended Euclidean Algorithm to find $a, b \in \mathbb{Z}$ such that $ax + by = \gcd(x, y)$.

(a) $x = 84, \quad y = 30.$

(b) $x = 325, \quad y = 234.$

8. In this question, we consider an instantiation of the RSA cryptosystem. Suppose that Bob sets up the cryptosystem with primes $p = 53$ and $q = 37$.

(a) Compute the values of N and ϕ.

(b) Argue that $e = 55$ is a valid choice of the public key exponent.

(c) Compute the private key d by solving the linear congruence $55d \equiv 1 \pmod{1872}$.

(d) Alice wishes to send the message "Sup Bob" to Bob. She, ignoring capitalization and spacing, represents this message numerically as

$$\text{su pb ob} = 1921\ 1602\ 1502,$$

which she will send to Bob in blocks of 4 digits at a time. Given Bob's public key (N, e), what would the encrypted version of Alice's message be? You can use a calculator to solve any concurrences, but please write out the computations you are performing.

(e) Verify that Bob can correctly decode this encrypted message using his private key d.