Discrete Mathematics, Chapter 4: Number Theory and Cryptography

Richard Mayr

University of Edinburgh, UK

Outline

Division

Definition

If a and b are integers with $a \neq 0$, then a **divides** b if there exists an integer c such that $b = ac$.

- When a divides b we write $a|b$.
- We say that a is a factor or divisor of b and b is a multiple of a.
- If $a|b$ then b/a is an integer (namely the c above).
- If a does not divide b, we write $a \not| b$.

Theorem

Let a, b, c be integers, where $a \neq 0$.

1. *If $a|b$ and $a|c$, then $a|(b + c)$.*
2. *If $a|b$, then $a|bc$ for all integers c.*
3. *If $a|b$ and $b|c$, then $a|c$.*

Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder. This is traditionally called the "Division Algorithm", but it is really a theorem.

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

- a is called the dividend.
- d is called the divisor.
- q is called the quotient. $q = a$ **div** d
- r is called the remainder. $r = a$ **mod** d

Congruence Relation

Definition

If a and b are integers and m is a positive integer, then a is **congruent** to b modulo m iff $m|(a-b)$.

- The notation $a \equiv b(\mod m)$ says that a is congruent to b modulo m.
- We say that $a \equiv b(\mod m)$ is a congruence and that m is its modulus.
- Two integers are congruent mod m if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write $a \not\equiv b(\mod m)$.

Congruence: Examples

Example: Determine

- Whether 17 is congruent to 5 modulo 6, and
- Whether 24 and 14 are congruent modulo 6.

Clicker

1. No and No.
2. No and Yes.
3. Yes and No.
4. Yes and Yes.

Congruence: Examples

Example: Determine

- Whether 17 is congruent to 5 modulo 6, and
- Whether 24 and 14 are congruent modulo 6.

Clicker

1. No and No.
2. No and Yes.
3. Yes and No.
4. Yes and Yes.

Solution: $17 \equiv 5 (\mod 6)$ because 6 divides $17 - 5 = 12$.

Congruence: Examples

Example: Determine

- Whether 17 is congruent to 5 modulo 6, and
- Whether 24 and 14 are congruent modulo 6.

Clicker

1. No and No.
2. No and Yes.
3. Yes and No.
4. Yes and Yes.

Solution: $17 \equiv 5 (\mod 6)$ because 6 divides $17 - 5 = 12$.
$24 \not\equiv 14 (\mod 6)$ since $24 - 14 = 10$ is not divisible by 6.

Terminology

The uses of "mod" in the following expressions are **different**.

- $a \equiv b \pmod{m}$, and
- $a \bmod m = b$

$a \equiv b \pmod{m}$ describes a binary relation on the set of integers.

In $a \bmod m = b$, the notation mod denotes a function (from integers to integers).
The relationship between these notations is made clear in this theorem.

Theorem

Let a and b be integers, and let m be a positive integer.
Then $a \equiv b \pmod{m}$ *if and only if* $a \bmod m = b \bmod m$

A Theorem on Congruences

Theorem

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof.

- If $a \equiv b \pmod{m}$, then (by the definition of congruence) $m|(a-b)$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m|(a-b)$ and $a \equiv b \pmod{m}$.

□

Congruences of Sums and Products

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Proof.

Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by the Theorem above there are integers s and t with $b = a + sm$ and $d = c + tm$. Therefore,

- $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$, and
- $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.

Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$. □

Corollary

Let m be a positive integer and let a and b be integers. Then

- $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.

Arithmetic modulo m

- Let $Z_m = \{0, 1, \ldots, m-1\}$.
- The operation $+_m$ is defined as $a +_m b = (a + b) \mod m$.
  This is addition modulo m.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b) \mod m$.
  This is multiplication modulo m.
- Using these operations is said to be doing arithmetic modulo m.

Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Arithmetic modulo m

- Let $Z_m = \{0, 1, \ldots, m-1\}$.
- The operation $+_m$ is defined as $a +_m b = (a + b) \mod m$.
  This is addition modulo m.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b) \mod m$.
  This is multiplication modulo m.
- Using these operations is said to be doing arithmetic modulo m.

Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.
Solution: Using the definitions above:
$7 +_{11} 9 = (7 + 9) \mod 11 = 16 \mod 11 = 5$
$7 \cdot_{11} 9 = (7 \cdot 9) \mod 11 = 63 \mod 11 = 8$

Arithmetic modulo m

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.

Closure: If $a, b \in Z_m$, then $a +_m b$ and $a \cdot_m b$ belong to Z_m.

Associativity: If $a, b, c \in Z_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

Commutativity: If $a, b \in Z_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

Identity elements: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively. If $a \in Z_m$ then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Additive inverses: If $0 \neq a \in Z_m$, then $m - a$ is the additive inverse of a modulo m. Moreover, 0 is its own additive inverse. $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.

Distributivity: If $a, b, c \in Z_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Base b Representation of Integers

Theorem

Let b be a positive integer greater than 1. Every positive integer n can be expressed uniquely in the form:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where k is a nonnegative integer, $a_0, a_1, \ldots a_k \in \{0, \ldots, b-1\}$ and $a_k \neq 0$. The $a_0, a_1, \ldots a_k$ are called the base-b digits of the representation.

This representation of n is called the base b expansion of n and it is denoted by $(a_k a_{k-1} \ldots a_1 a_0)_b$

$b = 2$ is binary. $b = 8$ is octal. $b = 10$ is decimal. $b = 16$ is hexadecimal, etc.

See Textbook Section 4.2 for algorithms on binary representations.

Primes

Definition

A positive integer $p > 1$ is called **prime** iff the only positive factors of p are 1 and p. Otherwise it is called **composite**.

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 *can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size.*

Example: $765 = 3 \cdot 3 \cdot 5 \cdot 17 = 3^2 \cdot 5 \cdot 17$.

Theorem (Euclid (325-265 BCE))

There are infinitely many primes.

Proof by contradiction. If there were only finitely many primes then multiply them all and add 1. This would be a new prime. Contradiction.

The Sieve of Eratosthenes (276-194 BCE)

How to find all primes between 2 and n?

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$.
2. Remove all strict multiples of i from the list.
3. Let k be the smallest number present in the list s.t. $k > i$. Then let $i := k$.
4. If $i > \sqrt{n}$ then stop else goto step 2.

Trial division: A very inefficient method of determining if a number n is prime, is to try every integer $i \leq \sqrt{n}$ and see if n is divisible by i.

Testing if a number is prime can be done efficiently in polynomial time [Agrawal-Kayal-Saxena 2002], i.e., polynomial in the number of bits used to describe the input number.
Efficient randomized tests had been available previously.

Distribution of Primes

What part of the numbers are primes?
Do primes get scarce among the large numbers?
The prime number theorem gives an asymptotic estimate for the number of primes not exceeding x.

Theorem (Prime Number Theorem)

The ratio of the number of primes not exceeding x and $x/\ln(x)$ approaches 1 as x grows without bound.
($\ln(x)$ is the natural logarithm of x.)

- The theorem tells us that the number of primes not exceeding x, can be approximated by $x/\ln(x)$.
- The odds that a randomly selected positive integer less than x is prime are approximately $(x/\ln(x))/x = 1/\ln(x)$.
- The k-th prime is approximately of size $k \cdot \ln(k)$.

Greatest Common Divisor

Definition

Let $a, b \in Z - \{0\}$. The largest integer d such that $d|a$ and also $d|b$ is called the **greatest common divisor** of a and b. It is denoted by $gcd(a, b)$.

Example: $gcd(24, 36) = 12$.

Definition

The integers a and b are **relatively prime** (**coprime**) iff $gcd(a, b) = 1$.

Example: 17 and 22. (Note that 22 is not a prime.)

Definition

The integers $a_1, a_2, \ldots, a_n$ are **pairwise relatively prime** iff $gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example: 10, 17 and 21 are pairwise relatively prime, since $gcd(10, 17) = gcd(10, 21) = gcd(17, 21) = 1$.

Least Common Multiple

Definition

The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b.
It is denoted by $lcm(a, b)$.

Example: $lcm(45, 21) = 7 \cdot 45 = 15 \cdot 21 = 315$.

Gcd and Lcm by Prime Factorizations

Suppose that the prime factorizations of a and b are:

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero). Then

$$gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

This number clearly divides a and b. No larger number can divide both a and b. Proof by contradiction and the prime factorization of a postulated larger divisor.

$$lcm(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$$

This number is clearly a multiple of a and b. No smaller number can be a multiple of both a and b. Proof by contradiction and the prime factorization of a postulated smaller multiple.

Factorization is a very inefficient method to compute *gcd* and *lcm*. The Euclidian algorithm is much better.

Euclidian Algorithm

Lemma

Let $a = bq + r$, where a, b, q, and r are integers.
Then $gcd(a, b) = gcd(b, r)$.

Proof.

Suppose that d divides both a and b. Then d also divides $a - bq = r$. Hence, any common divisor of a and b must also be a common divisor of b and r.
For the opposite direction suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r must also be a common divisor of a and b.
Therefore, $gcd(a, b) = gcd(b, r)$. □

This means that if $a > b$ then $gcd(a, b) = gcd(b, a \mod b)$, which directly yields the algorithm.
(Note that both arguments have gotten smaller.) One can show that its complexity is $O(\log b)$.

Gcd as a Linear Combination

Theorem (Bézout's Theorem)

If a and b are positive integers, then there exist integers s and t such that $gcd(a, b) = sa + tb$

(Proof in exercises of Section 5.2).

The numbers s and t are called Bézout coefficients of a and b.

Example: $2 = gcd(6, 14) = (-2) \cdot 6 + 1 \cdot 14$.

The Bézout coefficients can be computed as follows. First use the Euclidian algorithm to find the *gcd* and then work backwards (by division and substitution) to express the *gcd* as a linear combination of the original two integers.

Linear Congruences

Definition

A congruence of the form

$$ax \equiv b(\mod m)$$

where m is a positive integer, a, b are integers and x is an integer variable is called a **linear congruence**.

The solution of the congruence are all the integers x that satisfy it.

Definition

An integer $\overline{a}$ such that $\overline{a}a \equiv 1(\mod m)$ is called a **multiplicative inverse** of a modulo m.

Multiplicative inverses can be used to solve congruences. If $ax \equiv b(\mod m)$ then $\overline{a}ax \equiv (\overline{a}b)(\mod m)$ and thus $x \equiv (\overline{a}b)(\mod m)$.

Multiplicative Inverses

Example: Let $m = 15$.
Find a multiplicative inverse of 8 modulo 15.
Clicker.

1. 1
2. 2
3. 3
4. 4
5. 5
6. ≥ 6

Multiplicative Inverses

Example: Let $m = 15$.
Find a multiplicative inverse of 8 modulo 15.
Clicker.

1. 1
2. 2
3. 3
4. 4
5. 5
6. ≥ 6

$2 \cdot 8 = 16 \equiv 1 (\mod 15)$.
Thus 2 is a multiplicative inverse of 8 modulo 15.

Multiplicative Inverses

Find a multiplicative inverse of 7 modulo 15.
Clicker.

1. ≤ 3
2. between 4 and 8
3. between 9 and 11
4. between 12 and 14

Multiplicative Inverses

What is the multiplicative inverse of 5 modulo 15?

Multiplicative Inverses

What is the multiplicative inverse of 5 modulo 15?

$$\begin{aligned}
1 \cdot 5 &\equiv 5 \pmod{15} \\
2 \cdot 5 &\equiv 10 \pmod{15} \\
3 \cdot 5 &\equiv 0 \pmod{15} \\
4 \cdot 5 &\equiv 5 \pmod{15} \\
5 \cdot 5 &\equiv 10 \pmod{15} \\
6 \cdot 5 &\equiv 0 \pmod{15} \\
7 \cdot 5 &\equiv 5 \pmod{15} \\
&\ldots
\end{aligned}$$

Where is the inverse??? 5 does not have any inverse modulo 15.

The multiplicative group Z_m^*

Theorem

If a and m are relatively prime integers and $m > 1$, then a multiplicative inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.

Proof. Since $gcd(a, m) = 1$, by Bézout's Theorem there are integers s and t such that $sa + tm = 1$.
Hence, $sa + tm \equiv 1 (\mod m)$.
Since $tm \equiv 0 (\mod m)$, it follows that $sa \equiv 1 (\mod m)$.
Consequently, s is a multiplicative inverse of a modulo m.
Uniqueness: Exercise.

Definition

Let $Z_m^* = \{x \mid 1 \leq x < m \text{ and } gcd(x, m) = 1\}$. Together with multiplication modulo m, this is called the multiplicative group modulo m. It is closed, associative, has a neutral element (namely 1) and every element has an inverse.

The Chinese Remainder Theorem

Let

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

What is x ? (Or rather, what is the smallest x that satisfies these?)

Theorem (Chinese Remainder Theorem)

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$. (I.e., there is a solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution.)

The Chinese Remainder Theorem: Proof

We will construct a solution x.
First, let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$ and $m = m_1 m_2 \ldots m_n$.
Since $gcd(m_k, M_k) = 1$, the number M_k has a multiplicative inverse y_k modulo m_k. I.e.,

$$M_k y_k \equiv 1 (\mod m_k)$$

Now we let

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

Why does this x satisfy all the congruences?
If $j \neq k$ then $M_j \equiv 0 (\mod m_k)$, since M_j contains m_k as a factor.
Thus

$$\begin{aligned} x \mod m_k &= 0 + a_k M_k y_k \mod m_k \\ &= (a_k \mod m_k)(M_k y_k \mod m_k) \\ &= (a_k \mod m_k) \cdot 1 \\ &= a_k \mod m_k \end{aligned}$$

Fermat's Little Theorem (Pierre de Fermat (1601-65))

Theorem

If p is prime and $p \not| a$, then $a^{p-1} \equiv 1 (\mod p)$.
Furthermore, for every integer a we have $a^p \equiv a (\mod p)$.

Proof sketch: $a^x \mod p = (a \mod p)^x \mod p$. Also $p \not| a$.
So without restriction we consider only $0 < a < p$.
Consider the powers of $a^1, a^2, a^3, \ldots$ modulo p.
These form a subgroup of Z_p^* which has some size k and we have $a^k \equiv 1 \mod p$.
By Lagrange's theorem, k divides the size of Z_p^* which is $p-1$, so $p-1 = km$ for some positive integer m. Thus

$$a^{p-1} \equiv a^{km} \equiv (a^k)^m \equiv 1^m \equiv 1 \mod p$$

This directly implies $a^p \equiv a (\mod p)$.
In the other case where $p|a$ we trivially have $a^p \equiv a \equiv 0 (\mod p)$.

Fermat's Little Theorem

Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

Example: Find $7^{222} \mod 11$.

By Fermat's little theorem, we know that $7^{10} \equiv 1 \mod 11$, and so $(7^{10})^k \equiv 1 (\mod 11)$ for every positive integer k.
Therefore, $7^{222} = 7^{22 \cdot 10+2} = (7^{10})^{22} 7^2 \equiv 1^{22} \cdot 49 \equiv 5 (\mod 11)$.
Hence, $7^{222} \mod 11 = 5$.

Number Theory in Cryptography

Terminology: Two parties **Alice** and **Bob** want to communicate securely s.t. a third party **Eve** who intercepts messages cannot learn the content of the messages.

Symmetric Cryptosystems: Alice and Bob share a secret. Only they know a secret key K that is used to encrypt and decrypt messages. Given a message M, Alice encodes it (possibly with padding) into m, and then sends the ciphertext $encrypt(m, K)$ to Bob. Then Bob uses K to decrypt it and obtains $decrypt(encrypt(m, K), K) = m$.

Example: AES.

Public Key Cryptosystems: Alice and Bob do a-priori **not** share a secret. How can they establish a shared secret when others are listening to their messages?

Idea: Have a two-part key, i.e., a key pair. A public key that is used to encrypt messages, and a secret key to decrypt them. Alice uses Bob's public key to encrypt a message (everyone can do that). Only Bob can decrypt the message with his secret key.

RSA: an example of a Public Key Cryptosystem

- Named after Rivest, Shamir, Adelman (1976 at MIT). Discovered earlier by Clifford Cocks, working secretly for the UK government.
- Still widely used, e.g., in PGP and ssh.
- Described here because it is easy to explain with elementary number theory.

Cryptography: Caveats

- There do **not exist** any cryptosystems that are proven to be secure for complexity theoretic reasons (i.e., easy to encrypt, hard to decrypt).
- The only systems proven secure are so for information theoretic reasons. Random one-time pad: secret key longer than message and used only once (Vernam scheme). Message: $m_n \ldots m_0$ bits. Secret key: $k_n \ldots k_0$ bits. Ciphertext: $c_i = m_i \; xor \; k_i$. Decryption: $m_i = c_i \; xor \; k_i$.

Cryptography: More Caveats

- RSA could be broken with an efficient algorithm to factorize numbers, but possibly also by other means. It is an open question if an efficient method to break RSA would imply an efficient factorization method.
- A 768 bit RSA key has been broken, and experts believe 1024 bit could be broken with sufficient resources.
- Many experts increasingly doubt the security of RSA in general, and recommend to use Elliptic curve cryptography systems instead. (Also based on number theory, but harder to explain.)
- Key generation relies on strong random number generation. Vulnerabilities have been deliberately inserted by the NSA into some systems (e.g., Dual_EC_DRBG).
- Closed source implementations of cryptographic software are likely to contain more such backdoors, and can not be considered secure.

Description of RSA: Key generation

- Choose two distinct prime numbers p and q. Numbers p and q should be chosen at random, and be of similar bit-length. Prime integers can be efficiently found using a primality test.
- Let $n = pq$ and $k = (p-1)(q-1)$. (In particular, $k = |Z_n^*|$).
- Choose an integer e such that $1 < e < k$ and $gcd(e, k) = 1$; i.e., e and k are coprime.
  e (for encryption) is released as the public key exponent.
  (e must not be very small.)
- Let d be the multiplicative inverse of e modulo k, i.e., $de \equiv 1 (\mod k)$. (Computed using the extended Euclidean algorithm.) d (for decryption) is the private key and kept secret.

The public key is (n, e) and the private key is (n, d).

RSA: Encryption and Decryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret.

Encryption: Bob then wishes to send message M to Alice. He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c \equiv m^e \mod n$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

Decryption: Alice can recover m from c by using her private key exponent d via computing

$$m \equiv c^d \mod n$$

Given m, she can recover the original message M by reversing the padding scheme.

RSA: Correctness of decryption

Given that $c \equiv m^e \pmod{n}$, why is $c^d \equiv m \pmod{n}$?

$c^d \equiv (m^e)^d \equiv m^{ed} (\mod n)$.
By construction, d and e are each others multiplicative inverses modulo k, i.e., $ed \equiv 1 (\mod k)$. Also $k = (p-1)(q-1)$.
Thus $ed - 1 = h(p-1)(q-1)$ for some integer h.
We consider m^{ed} modulo p. If $p \not| m$ then

$$m^{ed} = m^{h(p-1)(q-1)} m = (m^{p-1})^{h(q-1)} m \equiv 1^{h(q-1)} m \equiv m (\mod p)$$

by Fermat's little theorem. Otherwise $m^{ed} \equiv 0 \equiv m (\mod p)$.
Symmetrically, $m^{ed} \equiv m (\mod q)$.
Since p, q are distinct primes, we have $m^{ed} \equiv m (\mod pq)$.
Since $n = pq$, we have $c^d \equiv m^{ed} \equiv m (\mod n)$.