Number Theory and Cryptography

Chapter 4: Part I

© Peter Valovcik 2021

UWO – February 23, 2021

Number Theory and Cryptography

Chapter 4: Part I

© Peter Valovcik 2021

UWO – February 23, 2021

Chapter motivations

1. *Number theory* is the part of mathematics devoted to the study of the integers and their properties.
2. The key ideas in number theory include divisibility and the primality of integers.
3. Representations of integers, including binary and hexadecimal representations, are part of number theory and essential to computer science.
4. Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.
5. We will use many ideas developed in Chapter 1 about proof methods and proof strategies in our exploration of number theory.
6. Mathematicians have long considered number theory to be pure mathematics, but it has important applications to computer science and cryptography studied in the second part of this Chapter

Plan for Part I

1. Divisibility and Modular Arithmetic

1.1 Divisibility

1.2 Division

1.3 Congruence Relation

2. Integer Representations and Algorithms

2.1 Representations of Integers

2.2 Base conversions

2.3 Binary Addition and Multiplication

3. Prime Numbers

3.1 The Fundamental Theorem of Arithmetic

3.2 The Sieve of Erastosthenes

3.3 Infinitude of Primes

4. Greatest Common Divisors

4.1 Definition

4.2 Least common multiple

4.3 The Euclidean Algorithm

Plan for Part I

Divisibility

Definition

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

1. When a divides b we say that a is a *factor* or *a divisor* of b and we say that b is a multiple of a.
2. The notation $a \mid b$ denotes the fact that a divides b.
3. If $a \mid b$, then $\frac{b}{a}$ is an integer.
4. If a does not divide b, then we write $a \nmid b$.

Example

Determine whether $3 \mid 7$ holds and whether $3 \mid 12$ holds.

Solution: $3 \nmid 7$ but $3 \mid 12$

Properties of divisibility

Theorem

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

1. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;* $\frac{b}{a} = x$ $\frac{c}{a} = y$ $\frac{(b+c)}{a} = x + y$.
2. *If $a \mid b$, then $a \mid b\,c$ for all integers c ;* $\frac{b}{a} = x$ $\frac{cb}{a} = cx$.
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$.* $\frac{b}{a} = x$ $\frac{c}{b} = y$ $\frac{c}{a} = xy$.

Proof.

1. We prove the first property. ① Suppose $a \mid b$ and $a \mid c$, ② then it follows that there are integers s and t with $b = as$ and $c = at$. Hence, $b + c = as + at = a(s + t)$. ③ Hence, $a \mid (b + c)$.
2. Parts (2) & (3) can be proven similarly. Try it as an exercise.

$\blacksquare$

Corollary

If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ for any integers m and n. (Proof left as exercise)

Plan for Part I

The division $\quad a = d \cdot (a \ \mathbf{div} \ d) + (a \ \mathbf{mod} \ d)$

Theorem ("Division Algorithm")

If a is an integer and d is a positive integer, then there are unique integers q and r with $0 \le r < d$, *such that* $a = dq + r$ *(proved in the tutorial.*

$r = a \% d$

1. *a is called the dividend.*
2. *d is called the divisor.*
3. *q is called the quotient.*
4. *r is called the remainder.*

Definitions div *and* mod*:*

5. $q = a \text{ div } d$
6. $r = a \text{ mod } d$

We have: $a \text{ div } d = \lfloor \frac{a}{d} \rfloor$.

$a \text{ div } d = \frac{a}{d}$ iff $a = cd$

Example

1. Quotient and remainder when 101 is divided by 11?

   We have $101 \ \mathbf{div} \ 11 = 9$ and $101 \ \mathbf{mod} \ 11 = 2$.

2. Quotient and remainder when 11 is divided by 3?

   We have $11 \ \mathbf{div} \ 3 = 3$ and $11 \ \mathbf{mod} \ 3 = 2$.

3. Quotient and remainder when -11 is divided by 3?

   We have $-11 \ \mathbf{div} \ 3 = -4$ and $-11 \ \mathbf{mod} \ 3 = 1$.

Plan for Part I

Congruence relation

Definition

If a and b are integers and m is a positive integer, then a is *congruent* to b *modulo* m if m divides $a - b$.

1. The notations $a \equiv b \pmod{m}$ and $a \equiv b \mod m$ say that a is congruent to b modulo m.
2. We say that $a \equiv b \mod m$ is a *congruence* and that m is its *modulus*.
3. Two integers are congruent mod m if and only if they have the same remainder when divided by m. (to be proved later)
4. If a is not congruent to b modulo m, then we write $a \not\equiv b \mod m$.

$a\%m \neq b\%m$.

Example

1. Determine whether 17 is congruent to 5 modulo 6. $(17-5)\%6 = 0$
   $17 \equiv 5 \mod 6$ because 6 divides $17 - 5 = 12$.
2. Determine whether 24 and 14 are congruent modulo 6. $(24-14)\%6 \neq 0$
   $24 \not\equiv 14 \mod 6$ since $24 - 14 = 10$ is not divisible by 6.

More 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 $a = b + km$.

$a = xm + z$ $\quad$ $a - b = (x - y)m$

$b = ym + z$

Proof.

1. If $a \equiv b \mod m$ holds, then (by the definition of congruence) we have: $m \mid a - b$. $\quad$ $a \equiv b \mod m$ holds $\Rightarrow m \mid a - b \Rightarrow (a-b)\%m = 0$
2. Hence, there is an integer k such that $a - b = km$ holds and equivalently $a = b + km$. $\quad$ $(a-b)/m = k \Rightarrow a = b + km$.
3. Conversely, if there is an integer k such that $a = b + km$, then we have: $km = a - b$.
4. Hence, we have $m \mid a - b$. Thus, $a \equiv b \mod m$ holds.

■

Relationship between the $\bmod m$ and $\mathbf{mod}\ m$ notations

The use of "mod" in $a \equiv b \pmod m$ is different from its use in $a = b \ \mathbf{mod}\ m$.

boolean 1. $a \equiv b \pmod m$ denotes a relation in the Cartesian product $\mathbb{Z} \times \mathbb{Z}$

int. 2. $a = b \ \mathbf{mod}\ m$ denotes a function from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$.

variable.

The relationship between the two notions is stated below:

Theorem

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod m$ if and only if $a \bmod m = b \bmod m$ (See Tutorial.)

Congruences of sums and products

Theorem

Let a, b, c, d be integers. Let m be a positive integer. If $a \equiv b \mod m$ *and* $c \equiv d \mod m$ *both hold, then we have:* $a + c \equiv b + d \mod m$ *and* $ac \equiv bd \mod m$.

Proof.

$(a-b)/m = x$ $\quad a = mx + b$ $\quad a+c = m(x+y) + b + d.$

$(c-d)/m = y.$ $\quad c = my + d.$ $\quad ac = \underbrace{m^2xy + mxd + myb}_{mk.} + bd.$

1. Since we have $a \equiv b \mod m$ and $c \equiv d \mod m$, there exist integers s and t with $b = a + sm$ and $d = c + tm$.
2. Therefore, we have:
   - (a) $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
   - (b) $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.
3. Hence, we have:
   - (a) $a + c \equiv b + d \mod m$, and
   - (b) $ac \equiv bd \mod m$.

■

Because $7 \equiv 2 \mod 5$ and $11 \equiv 1 \mod 5$, it follows that:

$$18 = 7 + 11 \equiv 2 + 1 = 3 \mod 5 \text{ and } 77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \mod 5.$$

Algebraic manipulation of congruences

1. Multiplying both sides of a valid congruence by an integer preserves the congruence.

   If $a \equiv b \mod m$ holds, then $c \cdot a \equiv c \cdot b \mod m$, where c is any integer, holds from the previous slide with $d = c$.

   Subtracting is also valid.

2. Adding an integer to both sides of a valid congruence preserves the congruence.

   If $a \equiv b \mod m$ holds, then $c + a \equiv c + b \mod m$, where c is any integer, holds from the previous slide with $d = c$.

3. NOTE : dividing a congruence by an integer may not produce a valid congruence.
   1. The congruence $14 \equiv 8 \mod 6$ holds.
   2. Dividing both sides by 2 gives an invalid congruence since $\frac{14}{2} = 7$ and $\frac{8}{2} = 4$, but $7 \not\equiv 4 \mod 6$.
   3. Later, we will give conditions for this division to yield a valid congruence.

Computing the **mod** m function of products and sums

Given integers a, b, c, d and a positive integer m, recall the following properties:

1. $a \equiv b \mod m \iff a \textbf{ mod } m = b \textbf{ mod } m$
2. $(a \equiv b \mod m) \wedge (c \equiv d \mod m) \rightarrow (a + c \equiv b + d \mod m) \wedge (ac \equiv bd \mod m)$

From there, we deduce the following properties:

1. $(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$,
2. $(ab) \textbf{ mod } m = ((a \textbf{ mod } m) \times (b \textbf{ mod } m)) \textbf{ mod } m$.

See the tutorial for a proof.

① $a = xm + \alpha$ $\quad (a+b) \bmod m = [(x+y)m + (\alpha+\beta)] \bmod m . = (\alpha+\beta) \bmod m$

$b = ym + \beta .$ $\quad [(a \bmod m) + (b \bmod m)] \bmod m = (\alpha+\beta) \bmod m .$

②. $\quad (ab) \bmod m = \alpha\beta \bmod m .$

$[\alpha \cdot \beta] \bmod m = \alpha\beta \bmod m .$

Arithmetic modulo m

Definition

Let $\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$ be the set of non-negative integers less than m. Assume $a, b \in \mathbb{Z}_m$.

1. The operation $+_m$ is defined as $a +_m b = a + b \textbf{ mod } m$. This is the *addition modulo m*.
2. The operation $\cdot_m$ is defined as $a \cdot_m b = a \cdot b \textbf{ mod } m$. This is the *multiplication modulo m*.
3. Using these operations is said to be doing *arithmetic modulo m*.

Example

1. Using the definitions above, find $7 +_{11} 9$
2. **Solution**: $7 +_{11} 9 = (7 + 9) \textbf{ mod } 11 = 16 \textbf{ mod } 11 = 5$
3. Using the definitions above, find $7 \cdot_{11} 9$.
4. **Solution**: $7 \cdot_{11} 9 = (7 \cdot 9) \textbf{ mod } 11 = 63 \textbf{ mod } 11 = 8$

Arithmetic modulo m

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

$a < m,\ b < m.$

1. *Closure*: If a and b belong to $\mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbb{Z}_m$.

   $(a+b) \bmod m < m$

   $ab \bmod m < m$

2. *Associativity*: If a, b, and c belong to $\mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
3. *Commutativity*: If a and b belong to $\mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
4. *Identity Elements*: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
   - a. If a belongs to $\mathbb{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

     $(a+0) \bmod m = a$

     $(a \cdot 1) \bmod m = a.$

To be *continued* →

Arithmetic modulo m

5. *Additive inverses*: If $a \neq 0$ belongs to $\mathbb{Z}_m$, then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse. $[a+(m-a)] \bmod m = 0+m0 = 0.$

   $a +_m (m - a) = 0$ and $0 +_m 0 = 0$

6. *Distributivity*: If a, b, and c belong to $\mathbb{Z}_m$, then

   $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and
   $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Multiplicative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6, i.e.

$2 \cdot_m a \neq 1$ for any $a \in \mathbb{Z}_6$

(*optional*) Using the terminology of abstract algebra, $\mathbb{Z}_m$ with $+_m$ is a commutative group and $\mathbb{Z}_m$ with $+_m$ and $\cdot_m$ is a commutative ring.

Plan for Part I

Plan for Part I

Representations of integers

1. In the modern world, we use *decimal*, or *base* 10, to represent integers. For example when we write 965, we mean $9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$.
2. We can represent numbers using any base b, where b is a positive integer greater than 1.
3. The bases $b = 2$ (*binary*), $b = 8$ (*octal*), and $b = 16$ (*hexadecimal*) are important for computing and communications
4. The ancient Mayas used base 20 and the ancient Babylonians used base 60.

Base b representations

1. We can use any positive integer b greater than 1 as a base, because of this theorem:

Theorem

a. *Let b be a positive integer greater than 1.*
b. *Then if n is a positive integer, it 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 non-negative integer, such that $a_0, a_1, \ldots a_k$ *are non-negative integers less than b, and* $a_k \neq 0$.
c. *The* a_j*, for* $j = 0, \ldots, k$ *are called the base-b digits of the representation.*
d. *We will prove this using mathematical induction in Chapter 5.*

2. The representation of n given in the theorem is called the *base b expansion of n* and is denoted by $(a_k a_{k-1} \ldots a_1 a_0)_b$.
3. We usually omit the subscript 10 for base 10 expansions.

Binary expansions

Most computers represent integers and do arithmetic with binary (base 2) expansions of integers. In these expansions, the only digits used are 0 and 1.

Example

1. What is the decimal expansion of the integer that has $(1\,0101\,1111)_2$ as its binary expansion?

   Solution: $(1\,0101\,1111)_2 =$
   $1\cdot 2^8+0\cdot 2^7+1\cdot 2^6+0\cdot 2^5+1\cdot 2^4+1\cdot 2^3+1\cdot 2^2+1\cdot 2^1+1\cdot 2^0 = 351.$

2. What is the decimal expansion of the integer that has $(1\,1011)_2$ as its binary expansion?

   Solution: $(1\,1011)_2 = 1\cdot 2^4+1\cdot 2^3+0\cdot 2^2+1\cdot 2^1+1\cdot 2^0 = 27.$

Octal expansions

The octal expansion (base 8) uses the digits $\{0, 1, 2, 3, 4, 5, 6, 7\}$.

Example

1. What is the decimal expansion of the number with octal expansion $(7016)_8$?

   Solution: $7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$
2. What is the decimal expansion of the number with octal expansion $(111)_8$?

   Solution: $1 \cdot 8^2 + 1 \cdot 8^1 + 1 \cdot 8^0 = 64 + 8 + 1 = 73$

Hexadecimal expansions

The hexadecimal expansion needs 16 digits, but our decimal system provides only 10. So letters are used for the additional symbols. The hexadecimal system uses the digits $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$. The letters A through F represent the decimal numbers 10 through 15.

Example

1. What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

   Solution: $2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627$

2. What is the decimal expansion of the number with hexadecimal expansion $(1E5)_{16}$?

   Solution: $1 \cdot 16^2 + 14 \cdot 16^1 + 5 \cdot 16^0 = 256 + 224 + 5 = 485$

Plan for Part I

Base conversion

To construct the base b expansion of an integer n (given in base 10):

1. Divide n by b to obtain the quotient q_0 and remainder a_0:
$$n = bq_0 + a_0, \quad 0 \leq a_0 < b$$
2. The remainder, a_0, is the rightmost digit in the base b expansion of n.
3. If $q_0 = 0$, then $n = (a_0)_b$.
4. If $0 < q_0 < b$, then $n = (q_0 a_0)_b$.
5. If $b \leq q_0$, then divide q_0 by b to obtain the quotient q_1 and remainder a_1:
$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b$$
6. The remainder, a_1, is the second digit from the right in the base b expansion of n.
7. Continuing in this manner (by successively dividing the quotients by b) we obtain the additional base b digits as remainders. The process terminates when a quotient is 0.

continued →

Algorithm: constructing base b expansions

Algorithm 1 base_b_expansion(n, b)

Require: $n, b \in \mathbb{Z}^+, \; b > 1$
Ensure: base b expansion of n: $(a_{k-1} \cdots a_1 a_0)_b$.

$q \leftarrow n$
$k \leftarrow 0$
while $q \neq 0$ **do**
  $a_k \leftarrow q \mod b$
  $q \leftarrow q$ **div** b
  $k \leftarrow k + 1$
end while
return $(a_{k-1} \cdots a_1 a_0)$

1. q represents the quotient obtained by successive divisions by b, starting with $q = n$.
2. The digits in the base b expansion are the remainders of the division given by q **mod** b.
3. The algorithm terminates when $q = 0$ is reached.

Base conversion

Example

Find the octal expansion of $(12345)_{10}$

Solution: Successively dividing by 8 gives:

1. $12345 = 8 \cdot 1543 + 1$
2. $1543 = 8 \cdot 192 + 7$
3. $192 = 8 \cdot 24 + 0$
4. $24 = 8 \cdot 3 + 0$
5. $3 = 8 \cdot 0 + 3$

The remainders are the digits from right to left yielding $(30071)_8$.

Comparison of the hexadecimal, octal, and binary representations

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Initial 0s are not shown

1. Each octal digit corresponds to a block of 3 binary digits.
2. Each hexadecimal digit corresponds to a block of 4 binary digits.
3. So, conversion between binary, octal, and hexadecimal is easy.

Conversion between the binary, octal, and hexadecimal expansions

Example

1. Find the octal expansion of $(11111010111100)_2$.

   Solution: To convert to octal, we group the digits into blocks of three $(011\ 111\ 010\ 111\ 100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,7,2,7, and 4. Hence, the solution is $(37274)_8$.

2. Find the hexadecimal expansions of $(11111010111100)_2$.

   Solution: To convert to hexadecimal, we group the digits into blocks of four $(0011\ 1110\ 1011\ 1100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,E,B, and C. Hence, the solution is $(3EBC)_{16}$.

Plan for Part I

Binary addition of integers

Algorithms for performing operations with integers using their binary expansions are important as computer chips work with binary numbers. Each digit is called a *bit*.

Algorithm 2 add (a, b)

Require: $a, b \in \mathbb{Z}^+$, {the binary expansions of a and b are $(a_{n-1}, a_{n-2}, \ldots, a_0)_2$ and $(b_{n-1}, b_{n-2}, \ldots, b_0)_2$, respectively}

Ensure: $(s_n, \ldots, s_1, s_0)$, the addition of a and b. {the binary expansion of the sum is $(s_n, s_{n-1}, \ldots, s_0)_2$ }

$c_{prev} \leftarrow 0$ ▷ represents *carry* from the previous bit addition

for $j \leftarrow 0, n-1$ **do**

  $c \leftarrow \lfloor \frac{(a_j + b_j + c_{prev})}{2} \rfloor$ ▷ quotient (*carry* for the next digit of the sum)

  $s_j \leftarrow a_j + b_j + c_{prev} - 2c$ ▷ remainder (j-th digit of the sum)

  $c_{prev} \leftarrow c$

end for

$s_n \leftarrow c$

return $(s_n, \ldots, s_1, s_0)$

$$\begin{aligned} a_0 + b_0 &= c_0 \cdot 2 + s_0 \\ a_1 + b_1 + c_0 &= c_1 \cdot 2 + s_1 \\ &\vdots \\ a_j + b_j + c_{j-1} &= c_j \cdot 2 + s_j \end{aligned}$$

The number of additions of bits used by the algorithm to add two n-bit integers is $\mathcal{O}(n)$.

Binary multiplication of integers

Algorithm for computing the product of two n bit integers.

$$
\begin{array}{llllll}
a \cdot b = a \cdot (& b_k 2^k & + b_{k-1} 2^{k-1} & + \dots & + b_1 2 & + b_0 \\
 & = ab_k 2^k & + ab_{k-1} 2^{k-1} & + \dots & + ab_1 2 & + ab_0) \\
 & \text{shift by } k & \text{shift by } k-1 & & \text{shift by } 1 & \text{no shift}
\end{array}
$$

Algorithm 3 multiply (a, b)

Require: $a, b \in \mathbb{Z}^+$, {the binary expansions of a and b are $(a_{n-1}, a_{n-2}, \dots, a_0)_2$ and $(b_{n-1}, b_{n-2}, \dots, b_0)_2$, respectively}
Ensure: p, the value of ab.

```
for j ← 0, n − 1 do
    if b_j = 1 then
        c_j ← a                         ▷ shifted j places
    else
        c_j ← 0                         ▷ { c_0, c_1, ..., c_{n−1} are the partial products}
    end if
end for
p ← 0
for j ← 0, n − 1 do
    p ← p + c_j
end for
return p {p is the value of ab}
```

$$
\begin{array}{rl}
110 & a \\
\times\, 101 & b \\
\hline
110 & ab_0 \\
000 & ab_1 \\
110 & ab_2
\end{array}
$$

The number of additions of bits used by the algorithm to multiply two n-bit integers is $\mathcal{O}(n^2)$.

Plan for Part I

Plan for Part I

Primes

Definition

1. A positive integer p greater than 1 is said *prime* if the only positive factors of p are 1 and p.
2. A positive integer that is greater than 1 and is not prime is called *composite* .

Example

The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

The fundamental theorem of arithmetic (prime factorization)

Theorem

1. *Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.*
2. *More formally, for every positive integer a greater than 1, there exists a positive integer n such that there exist prime numbers $p_1, \ldots, p_n$ and positive integers $a_1, \ldots, a_n$ such that:*

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \quad \text{and} \quad p_1 < p_2 < \cdots < p_n.$$

Example

1. $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
2. $641 = 641$
3. $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
4. $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Plan for Part I

The sieve of Erastosthenes

Erastothenes (276-194 B.C)

The *Sieve of Erastosthenes* can be used to find all primes not exceeding a specified positive integer.

Example

1. Consider the list of integers between 1 and 100:
   a. Delete all the integers, other than 2, divisible by 2.
   b. Delete all the integers, other than 3, divisible by 3.
   c. Next, delete all the integers, other than 5, divisible by 5.
   d. Next, delete all the integers, other than 7, divisible by 7.

all remaining numbers between 1 and 100 are prime:
$\{2, 3, 7, 11, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$

Why does this work?

continued →

The sieve of Erastosthenes

TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

1. If an integer n is a composite integer, then it must have a prime divisor less than or equal to $\sqrt{n}$.
2. To see this, note that if $n = ab$, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$.
3. For n $= 100$, $\sqrt{n} = 10$, thus any composite integer ≤ 100 must have prime factors less than 10, that is 2,3,5,7. The remaining integers ≤ 100 are prime.
4. *Trial division*, a very inefficient method of determining if a number n is prime, is to try every integer $i \le \sqrt{n}$ and see if n is divisible by i.

Plan for Part I

Infinitude of primes

Euclid (325 - 265 B.C)

Theorem

There are infinitely many primes.

PROOF.

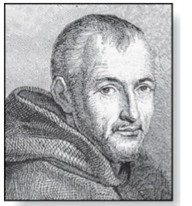
1. Assume finitely many primes: $p_1, p_2, \ldots, p_n$.
2. Let $q = p_1 p_2 \cdots p_n + 1$
3. Either q is prime or by the fundamental theorem of arithmetic it is a product of primes.
   - a. If a prime p_j divides q, and since $p_j \mid p_1 p_2 \cdots p_n$ holds as well, then p_j divides $q - p_1 p_2 \cdots p_n = 1$.
   - b. Thus, if a prime p_j divides q, then $p_j = 1$, which is a contradiction with $p_j > 1$.
4. Hence, there is no prime on the list $p_1, p_2, \ldots, p_n$ dividing q, that is, q is a prime.
5. This contradicts the assumption that $p_1, p_2, \ldots, p_n$ are all the primes.
6. Consequently, there are infinitely many primes.

This proof was given by Euclid in *The Elements* .

Generating primes

1. The problem of generating large primes is of both theoretical and practical interest.
2. Finding large primes with hundreds of digits is important in cryptography.
3. So far, no useful closed formula that always produces primes has been found. There is no simple function $f(n)$ such that $f(n)$ is prime for all positive integers n.
4. $f(n) = n^2 - n + 41$ is prime for all integers $1, 2, \ldots, 40$. Because of this, we might conjecture that $f(n)$ is prime for all positive integers n. But $f(41) = 41^2$ is not prime.
5. More generally, there is no polynomial with integer coefficients such that $f(n)$ is prime for all positive integers n.
6. Fortunately, we can generate large integers which are almost certainly primes.

Mersenne primes



Marin Mersenne

(1588 - 1648)

Definition

Prime numbers of the form $2^p - 1$, where p is prime, are called *Mersenne primes*.

1. $2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 37$, and $2^7 - 1 = 127$ are Mersenne primes.
2. $2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \cdot 89$.
3. There is an efficient test for determining if $2^p - 1$ is prime.
4. The largest known prime numbers are Mersenne primes .
5. On December 26 2017, the 50-th Mersenne primes was found, it is $2^{77,232,917} - 1$, which is the largest Marsenne prime known. It has more than 23 million decimal digits.
6. The *Great Internet Mersenne Prime Search* (*GIMPS*) is a distributed computing project to search for new Mersenne Primes.

http://www.mersenne.org/

Conjectures about primes

Even though primes have been studied extensively for centuries, many conjectures about them are unresolved, including:

1. **Goldbach's conjecture** : Every even integer n, $n > 2$, is the sum of two primes. It has been verified by computer for all positive even integers up to $1.\ 6 \cdot 10^{18}$. The conjecture is believed to be true by most mathematicians.
2. **Landau's conjecture** : There are infinitely many primes of the form $n^2 + 1$, where n is a positive integer . But it has been shown that there are infinitely many numbers of the form $n^2 + 1$ which are the product of at most two primes.
3. **The Twin Prime Conjecture**: there are infinitely many pairs of twin primes. Twin primes are pairs of primes that differ by 2. Examples are 3 and 5, 5 and 7, 11 and 13, etc. The current world's record for twin primes (as of mid 2011) consists of numbers $65,516,468,355 \cdot 23^{33,333} \pm 1$, which have 100,355 decimal digits.

Plan for Part I

Plan for Part I

Greatest common divisor (GCD)

Definition

Let a and b be integers, not both zero.

1. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of a and b.
2. The *greatest common divisor* (GCD) of a and b is denoted by $\gcd(a, b)$.

One can find GCDs of small numbers by inspection.

Example

1. What is the greatest common divisor of 24 and 36?

   Solution: $\gcd(24, 26) = 12$
2. What is the greatest common divisor of 17 and 22?

   Solution: $\gcd(17, 22) = 1$

Greatest common divisor (GCD)

Definition

The integers a and b are *relatively prime* if their greatest common divisor is $\gcd(a, b) = 1$.

Example

17 and 22

Definition

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

Example

1. Determine whether the integers 10, 17 and 21 are pairwise relatively prime.
   Solution: Because $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, and $\gcd(17, 21) = 1$, 10, 17, and 21 are pairwise relatively prime.
2. Determine whether the integers 10, 19, and 24 are pairwise relatively prime.
   Solution: No, since $\gcd(10, 24) = 2$.

Finding GCDs using prime factorizations

1. Suppose that the prime factorizations of a and b are:

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

   where each exponent is non-negative, and where all primes occurring in either prime factorization are included in both.

2. Then:

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

3. This formula is valid since
   a. the integer on the right-hand side divides both a and b,
   b. No larger integer can divide both a and b.

Example

Since $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, we have:

$$\gcd(120, 500) = 2^{min(3,2)} \cdot 3^{min(1,0)} \cdot 5^{min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

Remark: finding the GCD of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Plan for Part I

Least common multiple (LCM)

Definition

1. The least common multiple (LCM) of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\mathrm{lcm}(a, b)$.
2. The least common multiple can also be computed from the prime factorizations.
$$\mathrm{lcm}(a, b) = p_1^{max(a_1, b_1)} p_2^{max(a_2, b_2)} \cdots p_n^{max(a_n, b_n)}$$
3. This number is divided by both a and b and no smaller number is divided by a and b.

Example

$\mathrm{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{max(3,4)} 3^{max(5,3)} 7^{max(2,0)} = 2^4 3^5 7^2$

Theorem

Let a and b be positive integers. Then, we have:

$$a \cdot b = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$$

Plan for Part I

The Euclidean Algorithm

1. The Euclidean Algorithm is an efficient method for computing the GCD of two integers.
2. It is based on the idea that

$$\gcd(a, b) = \gcd(b, r)$$

   when $a > b$ and r is the remainder when a is divided by b.
3. Indeed, since $a = bq + r$, then $r = a - bq$. Thus, if $d \mid a$ and $d \mid b$ then $d \mid r$.

Example

1. Find $\gcd(287, 91)$:
   a. $287 = 91 \cdot 3 + 14$ – Divide 287 by 91
   b. $91 = 14 \cdot 6 + 7$ – Divide 91 by 14
   c. $14 = 7 \cdot 2 + 0$ – Divide 14 by 7

   Zero remainder is our stopping condition.

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = \gcd(7, 0) = 7$$

continued →

The Euclidean Algorithm

The Euclidean algorithm expressed in pseudo-code is:

Algorithm 4 gcd(a, b)

Require: $a, b \in \mathbb{Z}^+,\ a > b$

Ensure: x, the GCD of a and b.

$x \leftarrow a$
$y \leftarrow b$
while $y \neq 0$ **do**
    $r \leftarrow x$ **mod** y
    $x \leftarrow y$
    $y \leftarrow r$
end while
return x

Note: the time complexity of the algorithm is $\mathcal{O}(\log^2 a)$, where $a > b$.

Correctness of the Euclidean Algorithm

Lemma

Let $r = a \mathbf{~mod~} b$ *, where* $a \geq b > r$ *are integers. Then, we have:*

$$\gcd(a, b) = \gcd(b, r).$$

Proof.

1. Any divisor of a and b must also be a divisor of b and r since $r = a - bq$ (with $q = a\,\mathbf{d}iv\,b$.)
2. Similarly, any divisor of b and r is also a divisor of a and b.
3. Therefore, the set of common divisors of a and b is equal to the set of common divisors of b and r.
4. Therefore, $\gcd(a, b) = \gcd(b, r)$.

■

Correctness of the Euclidean Algorithm

1. Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. Successive applications of the division algorithm yields:

$$
\begin{aligned}
r_0 &= q_1 r_1 + r_2 && 0 \leq r_2 < r_1 \leq r_0 \\
r_1 &= q_2 r_2 + r_3 && 0 \leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_n \qquad \text{(gcd)}
\end{aligned}
$$

2. Eventually, a remainder of zero occurs in the sequence of terms: $a = r_0 \geq r_1 > r_2 > \cdots \geq 0$. The sequence can not contain more than $(a + 1)$ terms.
3. Then, the Lemma implies: $\gcd(a, b) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$.
4. Hence the GCD is the last nonzero remainder in the sequence of divisions . ■

GCD(s) as linear combinations

Étienne Bézout

(1730 - 1783)

Theorem (Bézout's Theorem)

If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

Definition

1. If a and b are positive integers, then integers s and t such that $\gcd(a, b) = sa + tb$ are called *Bézout coefficients* of a and b.
2. The equation $\gcd(a, b) = sa + tb$ is called *Bézout's identity.*
3. The expression $sa + tb$ is also called a *linear combination* of a and b with coefficients of s and t.

Example

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

Finding GCD(s) as linear combinations

Example

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show $\gcd(252, 198) = 18$

- a. $252 = 1 \cdot 198 + 54$
- b. $198 = 3 \cdot 54 + 36$
- c. $54 = 1 \cdot 36 + 18$
- d. $36 = 2 \cdot 18$

1. Working backwards , from c and b above

$$18 = 54 - 1 \cdot 36$$
$$36 = 198 - 3 \cdot 54$$

2. Substituting the 2^{nd} equation into the 1^{st} yields:

$$18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$$

3. Substituting $54 = 252 - 1 \cdot 198$ (from a above) yields:

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$$

This method illustrated above is a two pass method. It first uses the Euclidean algorithm to find the GCD and then works backwards to express the GCD as a linear combination of the original two integers. There is a one pass method, called the *extended Euclidean algorithm.*

Consequences of Bézout's Theorem

Lemma

If a, b, c are positive integers such that a and b are relatively prime (that is, $\gcd(a, b) = 1$) and $a \mid bc$, then we have $a \mid c$.

PROOF:

1. Assume $\gcd(a, b) = 1$ and $a \mid bc$ both hold.
2. Since $\gcd(a, b) = 1$, by Bézout's Theorem there are integers s and t such that $sa + tb = 1$ holds.
3. Multiplying both sides of the equation by c, yields $sac + tbc = c$.
4. Since $a \mid bc$, we have $a \mid tbc$, that is, there exists q so that we have $tbc = qa$.
5. With $sac + tbc = c$, it follows that $a(sc + q) = c$, that is, $a \mid c$ holds.

A generalization of the above lemma is important in practice:

Lemma

If p is prime and $p \mid a_1 a_2 \ldots a_n$ where a_i are integers then $p \mid a_i$ for some i.

Dividing congruences by an integer

1. Dividing both sides of a valid congruence by an integer does not always produce a valid congruence, as illustrated earlier.
2. But dividing by an integer relatively prime to the modulus does produce a valid congruence.

Theorem

Let m be a positive integer and let a, b, and c be integers. If $\gcd(c, m) = 1$ and $ac \equiv bc \mod m$, then $a \equiv b \mod m$.

Proof.

1. Since $ac \equiv bc \mod m$ holds, we have
$$m \mid ac - bc = c(a - b).$$
2. With the previous lemma and since $\gcd(c, m) = 1$ holds, it follows that $m \mid a - b$..
3. Hence, $a \equiv b \mod m$.

∎