Algebraic Foundations of Computer Science.

Computational Introduction to Number Theory (I)

Ferucio Laurenţiu Ţiplea

Department of Computer Science
"AL.I.Cuza" University of Iaşi
Iaşi, Romania
E-mail: fltiplea@mail.dntis.ro

Spring 2014

Outline

The division theorem

The absolute value of an integer a, denoted $|a|$, is defined by:

$$|a| = \begin{cases} a, & \text{if } a \geq 0 \\ -a, & \text{otherwise.} \end{cases}$$

Theorem 1 (The Division Theorem)

For any two integers a and b with $b \neq 0$, there are unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.

In the equality $a = bq + r$ in the division theorem, a is called the dividend, b is called the divisor, q is called the quotient, and r is called the remainder. We usually write:

$$q = a \text{ div } b \quad \text{and} \quad r = a \bmod b$$

Divisibility relation

Definition 2

The binary relation $|\subseteq \mathbb{Z}\times\mathbb{Z}$ given by

$$a|b \quad\Leftrightarrow\quad (\exists c\in\mathbb{Z})(b=ac),$$

for any $a,b\in\mathbb{Z}$, is called the divisibility relation on $\mathbb{Z}$.

If $a|b$ then we will say that a divides b, or a is a divisor/factor of b, or b is divisible by a, or b is a multiple of a.

Remark 1

If $a\neq 0$, then $a|b$ iff b *mod* $a=0$.

If $a|b$ and $a\notin\{-1,1,-b,b\}$, then a is called a proper divisor of b.

Basic properties of divisibility

Proposition 1

Let $a, b, c \in \mathbb{Z}$. Then:

1. 0 divides only 0;
2. a divides 0 and a;
3. 1 divides a;
4. $a|b$ iff $a|-b$;
5. if $a|b$ and $b|c$, then $a|c$;
6. if $a|b+c$ and $a|b$, then $a|c$;
7. if $a|b$, then $ac|bc$. Conversely, if $c \neq 0$ and $ac|bc$, then $a|b$;
8. if $a|b$ and $a|c$, then $a|\beta b + \gamma c$, for any $\beta, \gamma \in \mathbb{Z}$;
9. if $a|b$ and $b \neq 0$, then $|a| \leq |b|$. Moreover, if a is a proper divisor of b, then $1 < |a| < |b|$.

Prime numbers

Definition 3

*A natural number $n \geq 2$ is called **prime** if the only positive factors of n are 1 and n. A natural number $n \geq 2$ that is not a prime is called **composite**.*

Definition 4

*Let $a_1, \ldots, a_m \in \mathbb{Z}$, where $m \geq 2$. We say that $a_1, \ldots, a_m$ are **co-prime** or **relatively prime**, denoted $(a_1, \ldots, a_m) = 1$, if the only common factors of these numbers are 1 and -1.*

Example 5

- *2, 3, 5, 7, and 11 are prime numbers and 4, 6, and 9 are composite numbers.*
- *$(0, 1) = 1$ (0 and 1 are co-prime) and $(4, 6, 8) \neq 1$ (4, 6, and 8 are not co-prime).*

Characterization of co-prime numbers

Theorem 6

Let $a_1, \ldots, a_m \in \mathbb{Z}$, where $m \geq 2$. Then, $(a_1, \ldots, a_m) = 1$ iff there are $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}$ such that $\sum_{i=1}^{m} \alpha_i a_i = 1$.

Corollary 7

Let $a_1, \ldots, a_m, b \in \mathbb{Z}$, where $m \geq 2$. Then:

1. if $(b, a_i) = 1$, for any i, then $(b, a_1 \cdots a_m) = 1$;
2. if $a_1, \ldots, a_m$ are pairwise co-prime and $a_i | b$, for any i, then $a_1 \cdots a_m | b$;
3. if $(b, a_1) = 1$ and $b | a_1 \cdots a_m$, then $b | a_2 \cdots a_m$;
4. if b is prime and $b | a_1 \cdots a_m$, then there exists i such that $b | a_i$.

The fundamental theorem of arithmetic

Theorem 8 (The Fundamental Theorem of Arithmetic)

Every natural number $n \geq 2$ can be written uniquely in the form

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

where $k \geq 1$, $p_1, \ldots, p_k$ are prime numbers written in order of increasing size, and $e_1, \ldots, e_k > 0$.

Example 9

- $4 = 2^2$, $9 = 3^2$, $12 = 2^2 \cdot 3$, $36 = 2^2 \cdot 3^2$.
- $105 = 3 \cdot 5 \cdot 7$.

The prime number theorem

Theorem 10

There are infinitely many primes.

Theorem 11 (The Prime Number Theorem)

Let $\pi(n) = |\{p|p \text{ is a prime and } p \leq n\}|$. Then,

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1.$$

We write

$$\pi(n) \sim \frac{n}{\ln n}$$

and say that $\pi(n)$ and $\frac{n}{\ln n}$ are asymptotically equivalent.

Values of $\pi(n)$

A few values of $\pi(n)$:

n	10^1	10^2	10^3	10^4	10^5	10^6	10^7
$\pi(n)$	4	25	168	1229	9592	78496	664579

How many 100-digit primes are there?

$$
\begin{aligned}
\pi(10^{100}) - \pi(10^{99}) &\approx \frac{10^{100}}{100 \ln 10} - \frac{10^{99}}{99 \ln 10} \\
&= \frac{10^{99}}{\ln 10}\left(\frac{1}{10} - \frac{1}{99}\right) \\
&> 0.39 \cdot 10^{98} \\
&\approx 4 \cdot 10^{97}
\end{aligned}
$$

Large numbers

How large is 10^{97}? Below are a few interesting estimates and comparisons:

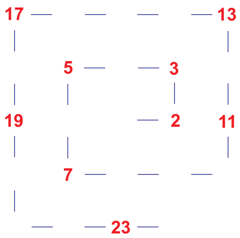
- the number of cells in the human body is estimated at 10^{14};
- the number of neuronal connections in the human brain is estimated at 10^{14};
- the universe is estimated to be $5 \cdot 10^{17}$ seconds old;
- the total number of particles in the universe has been variously estimated at numbers from 10^{72} up to 10^{87}.

Very large numbers often occur in fields such as mathematics, cosmology and cryptography. They are particularly important to cryptography where security of cryptosystems (ciphers) is usually based on solving problems which require, say, 2^{128} operations (which is about what would be required to break the 128-bit SSL commonly used in web browsers).

The prime spiral

There is no known formula for generating prime numbers in a row which is more efficient than the ancient sieve of Eratosthenes or the modern sieve of Atkin.

The Ulam spiral (or prime spiral), discovered by Stanislaw Ulam in 1963, is a simple method of graphing the prime numbers.



The prime numbers tend to line up along diagonal lines !

The greatest common divisor

Definition 12

Let $a_1, \ldots, a_m \in \mathbb{Z}$, not all zero, where $m \geq 2$. The **greatest common divisor** *of these numbers, denoted $gcd(a_1, \ldots, a_m)$ or $(a_1, \ldots, a_m)$, is the largest integer d such that $d|a_i$, for all i.*

Example 13

- $(2, 5, 7) = 1$.
- $(9, 3, 15) = 3$.

Proposition 2

Let $a_1, \ldots, a_m \in \mathbb{Z}$, not all zero, where $m \geq 2$. Then:

1. $(0, a_1, \ldots, a_m) = (a_1, \ldots, a_m)$;
2. $(0, a_1) = |a_1|$, provided that $a_1 \neq 0$;
3. $(a_1, a_2) = (a_2, a_1 \; mod \; a_2)$, provided that $a_2 \neq 0$.

Linear combination of the greatest common divisor

Theorem 14

Let $a_1, \ldots, a_m \in \mathbb{Z}$, not all zero, where $m \geq 2$. Then,

$$(a_1, \ldots, a_m) = \alpha_1 a_1 + \cdots + \alpha_m a_m$$

for some $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}$.

Corollary 15

Let $a_1, \ldots, a_m \in \mathbb{Z}$, not all zero, where $m \geq 2$. Then, the equation

$$a_1 x_1 + \cdots + a_m x_m = b$$

has solutions in $\mathbb{Z}$ iff $(a_1, \ldots, a_m) | b$.

Example 16

$2x + 3y = 5$ has solutions in $\mathbb{Z}$ because $(2, 3) = 1$ divides 5, but $4x + 2y = 3$ does not have solutions in $\mathbb{Z}$ because $(4, 2) = 2$ does not divide 3.

The least common multiple

Definition 17

Let $a_1, \ldots, a_m \in \mathbb{Z}$, where $m \geq 2$. The **least common multiple** *of these numbers, denoted* $lcm(a_1, \ldots, a_m)$ *or* $[a_1, \ldots, a_m]$, *is*

- *0, if at least one of these numbers is 0;*
- *the smallest integer $b > 0$ such that $a_i | b$, for all i, otherwise.*

Example 18

- $[0, a] = 0$, *for any a.*
- $[4, 6, 2] = 12$.

Theorem 19

Let $a, b \in \mathbb{N}$, not both zero. Then, $ab = (a, b)[a, b]$.

The Euclidean Algorithm

If $a = 0$ or $b = 0$, but not both zero, then $(a, b) = max\{|a|, |b|\}$.

Let $a > b > 0$ and

$$\begin{array}{lcll} r_{-1} & = & r_0 q_1 + r_1, & 0 < r_1 < r_0 \\ r_0 & = & r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ \cdots & & & \\ r_{n-2} & = & r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_n q_{n+1} + r_{n+1}, & r_{n+1} = 0, \end{array}$$

where $r_{-1} = a$ şi $r_0 = b$. Then,

$$(a, b) = (r_{-1}, r_0) = (r_0, r_1) = \cdots = (r_n, 0) = r_n$$

The Euclidean algorithm

Algorithm 1: Computing gcd

input : $a, b \in \mathbb{Z}$ *not both* 0;
output: $gcd(a, b)$;

begin
  while $b \neq 0$ **do**
    $r := a \; mod \; b$;
    $a := b$;
    $b := r$
  $gcd(a, b) := |a|$;

Theorem 20 (Lamé, 1844)

Let $a \geq b > 0$ be integers. The number of division steps performed by **Euclid**(a, b) does not exceed 5 times the number of decimal digits in b.

The extended Euclidean algorithm

The Euclidean algorithm can be easily adapted to compute a linear combination of the gcd as well. The resulting algorithm is called the Extended Euclidean Algorithm.

Given a and b there are α and β such that $(a, b) = \alpha a + \beta b$. The numbers α and β can be computed as follows:

$$
\begin{array}{rlcl@{\qquad}lcl}
 & & & & V_a & = & (1,0) \\
 & & & & V_b & = & (0,1) \\
1. & a & = & bq_1 + r_1 & V_{r_1} & = & V_a - q_1 V_b \\
2. & b & = & r_1 q_2 + r_2 & V_{r_2} & = & V_b - q_2 V_{r_1} \\
3. & r_1 & = & r_2 q_3 + r_3 & V_{r_3} & = & V_{r_1} - q_3 V_{r_2} \\
 & \ldots & & & & & \\
n. & r_{n-2} & = & r_{n-1} q_n + r_n & V_{r_n} & = & V_{r_{n-2}} - q_n V_{r_{n-1}} \\
n+1. & r_{n-1} & = & r_n q_{n+1} & & &
\end{array}
$$

$r_n = (a, b)$ and $V_{r_n} = (\alpha, \beta)$.

Algorithm 2: Computing gcd and a linear combination of it

input : $a, b \in \mathbb{Z}$ *not both* 0;
output: $gcd(a, b)$ *and* $V = (\alpha, \beta)$ *s.t.* $gcd(a, b) = \alpha a + \beta b$;

begin
    $V_0 := (1, 0)$;
    $V_1 := (0, 1)$;
    while $b \neq 0$ **do**
        $q := a \ div \ b$;
        $r := a \ mod \ b$;
        $a := b$;
        $b := r$;
        $V := V_0$;
        $V_0 := V_1$;
        $V_1 := V - qV_1$
    $gcd(a, b) := |a|$;
    $V := V_0$;

The extended Euclidean algorithm can be used to compute integer solutions to linear Diophantine equations:

Algorithm 3: Computing solutions to linear Diophantine equations

input : $a, b, c \in \mathbb{Z}$ *such that not both a and b are* 0;
output: integer solution to $ax + by = c$, if it has;

begin
  compute $gcd(a, b) := \alpha a + \beta b$;
  if $gcd(a, b)|c$ **then**
    $c' := c/gcd(a, b)$;
    $x := \alpha c'$;
    $y := \beta c'$
  else
    "no integer solutions"

Congruences

Definition 21

Let $a, b, m \in \mathbb{Z}$. We say that *a is congruent to b modulo m*, denoted $a \equiv_m b$ or $a \equiv b \bmod m$, if $m|(a-b)$.

Example 22

- $6 \equiv 0 \bmod 2$.
- $-7 \equiv 1 \bmod 2$.
- $3 \not\equiv 2 \bmod 2$.
- $-11 \equiv 1 \bmod -4$ and $-11 \equiv 1 \bmod 4$.

Remark 2

If $m \neq 0$, then $a \equiv b \bmod m$ iff $a \bmod m = b \bmod m$.

Basic properties of congruences

Proposition 3

Let $a, b, c, d, m, m' \in \mathbb{Z}$ and $f : \mathbb{Z} \to \mathbb{Z}$ be a polynomial function with integer coefficients. Then:

1. $\equiv_m$ is an equivalence relation on $\mathbb{Z}$;
2. if $a \equiv_m b$, then $(a, m) = (b, m)$;
3. if $a \equiv_m b$ şi $c \equiv_m d$, then $a + c \equiv_m b + d$, $a - c \equiv_m b - d$, $ac \equiv_m bd$, and $f(a) \equiv_m f(b)$;
4.
   1. if $ac \equiv_{mc} bc$ and $c \neq 0$, then $a \equiv_m b$;
   2. if $ac \equiv_m bc$ and $d = (m, c)$, then $a \equiv_{m/d} b$;
   3. if $ac \equiv_m bc$ and $(m, c) = 1$, then $a \equiv_m b$;
5.
   1. if $a \equiv_{mm'} b$, then $a \equiv_m b$ and $a \equiv_{m'} b$;
   2. if $a \equiv_m b$ and $a \equiv_{m'} b$, then $a \equiv_{[m,m']} b$;
   3. if $a \equiv_m b$, $a \equiv_{m'} b$, and $(m, m') = 1$, then $a \equiv_{mm'} b$.

$\mathbb{Z}_m$

Let $\mathbb{Z}_m$ be the set of all equivalence classes induced by $\equiv_m$. Then:

- $[a]_m = [a]_{-m}$, for any $a \in \mathbb{Z}$. Therefore, we may consider only $m \geq 0$;
- for any $a, b \in \mathbb{Z}$, if $a \neq b$ then $[a]_0 \neq [b]_0$. Therefore, $\mathbb{Z}_0$ has as many elements as $\mathbb{Z}$;
- for $m \geq 1$, $\mathbb{Z}_m = \{[0]_m, \ldots, [m-1]_m\}$ has exactly m elements.

Example 23

- $\mathbb{Z}_1 = \{[0]_1\}$, $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$.

Remark 3

We usually write $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ instead of $\mathbb{Z}_m = \{[0]_m, \ldots, [m-1]_m\}$, for any $m \geq 1$.

Addition and multiplication modulo m

Define the following operations on $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$:

- $a + b = (a + b)\ mod\ m$; (binary operation)
- $a \cdot b = (a \cdot b)\ mod\ m$; (binary operation)
- $-a = (m - a)\ mod\ m$, (unary operation)

for any $a, b \in \mathbb{Z}_m$.

These operations fulfill the following properties:

- $+$ and $\cdot$ are associative and commutative;
- $a + 0 = 0 + a = a$, for any a;
- $a \cdot 1 = 1 \cdot a = a$, for any a;
- $a + (-a) = 0$, for any a.

$a + (-b)$ is usually denoted by $a - b$.

Inverses modulo m

- additive inverse modulo m.

  We have seen that $a + (-a) = 0$, for any a. $-a$ is called the additive inverse of a modulo m (it is unique);

- multiplicative inverse modulo m.
  - Given $a \in \mathbb{Z}_m - \{0\}$, is there any $b \in \mathbb{Z}_m$ such that $a \cdot b = 1$? That is, does any $a \in \mathbb{Z}_m$ have a multiplicative inverse modulo m?
  - Let us consider $m = 6$. There is no $b \in \mathbb{Z}_6$ such that $2 \cdot b = 1$.
  - Moreover, $\mathbb{Z}_6$ exhibits the following interesting property:

    $$2 \cdot 3 = 0$$

    (the product of two non-zero numbers is zero !!!).

Inverses modulo m and the group of units

Proposition 4

$a \in \mathbb{Z}_m$ has a multiplicative inverse modulo m iff $(a, m) = 1$.

The multiplicative inverse of a, when it exists, is unique and it is denoted by a^{-1}.

$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m | (a, m) = 1\}$ is called the group of units of $\mathbb{Z}_m$ or the group of units modulo m.

Example 24

- $\mathbb{Z}_1^* = \{0\}$.
- $\mathbb{Z}_{26}^*$ *has 12 elements:*
  - $1^{-1} = 1$, $3^{-1} = 9$, $5^{-1} = 21$,
  - $7^{-1} = 15$, $11^{-1} = 19$, $17^{-1} = 23$,
  - $25^{-1} = 25$.

Computing multiplicative inverses

The extended Euclidean algorithm can be easily used to compute multiplicative inverses modulo m:

Algorithm 4: Computing multiplicative inverses

input : $m \geq 1$ *and* $a \in \mathbb{Z}_m$;
output: a^{-1} *modulo* m, *if* $(a, m) = 1$;

begin
  compute $gcd(a, m) := \alpha a + \beta m$;
  if $gcd(a, m) = 1$ **then**
    $a^{-1} := \alpha \bmod m$
  else
    "a^{-1} *does not exist*"

Euler's totient function

Euler's totient function ϕ is given by:

$$\phi(m) = |\mathbb{Z}_m^*|,$$

for any $m \geq 1$. That is, $\phi(m)$ is the number of positive integers less than or equal to m and co-prime to m.

Theorem 25

1. $\phi(1) = 1$;
2. $\phi(p) = p - 1$, for any prime p;
3. $\phi(ab) = \phi(a)\phi(b)$, for any co-prime integers $a, b \geq 1$;
4. $\phi(p^e) = p^e - p^{e-1}$, for any prime p and $e > 0$;
5. $\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$, for any $n \geq 1$, where $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime decomposition of n.

Euler's totient function: examples

Example 26

1. $\phi(5) = 4$.
2. $\phi(26) = \phi(2 \cdot 13) = 12$.
3. $\phi(245) = \phi(5 \cdot 7^2) = 168$.

Remark 4

- it is easy to compute $\phi(n)$ if the prime decomposition of n is known;
- it is hard to compute the prime decomposition of large numbers (512-bit numbers (about 155 decimals) or larger);
- it is hard to compute $\phi(n)$ if n is large and the prime decomposition of n is not known.

Euler's theorem

Theorem 27 (Euler's Theorem)

Let $m \geq 1$. Then, $a^{\phi(m)} \equiv 1 \ mod \ m$, for any integer a with $(a, m) = 1$.

Corollary 28 (Fermat's Theorem)

Let p be a prime. Then:

1. $a^{p-1} \equiv 1 \ mod \ p$, for any integer a with $p \not| a$;
2. $a^p \equiv a \ mod \ p$, for any integer a.

Example 29

$1359^4 \equiv 1 \ mod \ 5 \ and \ 3^{168} \equiv 1 \ mod \ 245.$

Course readings

1. F.L. Ţiplea: *Fundamentele Algebrice ale Informaticii*, Ed. Polirom, Iaşi, 2006, pag. 143–164.