Computational Introduction to Number Theory

Part II

Ferucio Laurențiu Țiplea

Department of Computer Science
"Al.I.Cuza" University of Iași
Iași 700506, Romania

e-mail: `ferucio.tiplea@uaic.ro`

Spring 2020

Outline

Outline

Linear congruential equations

Theorem 1

Let $a, b, m \in \mathbb{Z}$ with $m \geq 1$. Then, the equation

$$ax \equiv b \ mod \ m$$

is solvable in $\mathbb{Z}$ iff $(a, m)|b$. Moreover, if it is solvable, then it has exactly (a, m) solutions in $\mathbb{Z}_m$ which are of the form

$$\left(x_0 + i\frac{m}{(a, m)}\right) \ mod \ m,$$

where x_0 is an arbitrary integer solution and $0 \leq i < (a, m)$.

Example 2

The equation

$$5x \equiv 25 \ mod \ 10$$

has $(5, 10) = 5$ *solutions in* $\mathbb{Z}_{10}$*:* 1, 3, 5, 7, 9.

Linear congruential equations

Algorithm 1: Solving linear congruential equations

input : $m \geq 1$ *and* $a, b \in \mathbb{Z}$;
output: *all solutions modulo* m *of* $ax \equiv b$ *mod* m;

begin
    compute $gcd(a, m) := \alpha a + \beta m$;
    if $gcd(a, m)|b$ **then**
        $b' := b/gcd(a, m)$;
        $x_0 := \alpha b'$;
        for $i := 0$ **to** $gcd(a, m) - 1$ **do**
            print $((x_0 + im/gcd(a, m))$ *mod* $m)$
    else
        "*no integer solutions*"

Outline

The Chinese remainder theorem

According to D.Wells, the following problem was posed by Sun Tsu Suan-Ching (4th century AD):

> *There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5, the remainder is 3; and by 7, the remainder is 2. What will be the number?*

The mathematical form of this problem is:

$$\begin{cases} x \equiv 2 \ mod \ 3 \\ x \equiv 3 \ mod \ 5 \\ x \equiv 2 \ mod \ 7 \end{cases}$$

This system of equations has a least integer solution which is $x = 23$.

The Chinese remainder theorem

Theorem 3 (Chinese Remainder Theorem)

Let $k \geq 1$ and $m_1, \ldots, m_k$ be pairwise co-prime integers. Then, for any $b_1, \ldots, b_k \in \mathbb{Z}$, the following system (S) of equations has a unique solution modulo $m_1 \cdots m_k$

$$(S) \begin{cases} x \equiv b_1 \ mod \ m_1 \\ \cdots \\ x \equiv b_k \ mod \ m_k \end{cases}$$

The solution can be obtained as follows:

- compute $c_i = \prod_{j=1,\ j \neq i}^{k} m_j$;
- compute an integer solution x_i of the equation $c_i x \equiv b_i \ mod \ m_i$, for any i;
- $x = (c_1 x_1 + \cdots + c_k x_k) \ mod \ (m_1 \cdots m_k)$ is the unique solution modulo $m_1 \cdots m_k$ of the system.

The Chinese remainder theorem: example

Example 4

Let (S) be the system

$$(S)\begin{cases} x \equiv 2 \ mod\ 3 \\ x \equiv 3 \ mod\ 5 \\ x \equiv 2 \ mod\ 7 \end{cases}$$

Then:

- $c_1 = 35$, $c_2 = 21$, *and* $c_3 = 15$;
- $x_1 = 1$ *is a solution of* $35x \equiv 2 \ mod\ 3$;
- $x_2 = 3$ *is a solution of* $21x \equiv 3 \ mod\ 5$;
- $x_3 = 2$ *is a solution of* $15x \equiv 2 \ mod\ 7$;
- $x = (35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2) \ mod\ 105 = 128 \ mod\ 105 = 23$ *is the unique solution modulo* 105 *of the system* (S).

The Chinese remainder theorem: application

There is an important application of CRT to the problem of solving equations of the form $f(x) \equiv 0 \ mod \ m$, where $f(x)$ is a polynomial with integer coefficients and variables x.

Theorem 5

Let $f(x)$ be a polynomial with integer coefficients, and $m_1, \ldots, m_k$ be pairwise co-prime integers. Then, $a \in \mathbb{Z}$ is a solution to the equation

$$f(x) \equiv 0 \ mod \ m_1 \cdots m_k \tag{1}$$

if and only if a is a solution to each of the equations

$$f(x) \equiv 0 \ mod \ m_i, \quad 1 \leq i \leq k. \tag{2}$$

Moreover, the number of solutions in $\mathbb{Z}_{m_1 \cdots m_k}$ of the equation (1) is the product of the numbers of solutions in $\mathbb{Z}_{m_i}$ of the equations (2).

The Chinese remainder theorem: application

Example 6

1. The equation
$$x^2 \equiv 1 \ mod \ p,$$
where $p > 2$ is a prime number, has exactly 2 solutions in $\mathbb{Z}_p$, namely $x = 1$ and $x = p - 1$.
2. The equation
$$x^2 \equiv 1 \ mod \ p_1 \cdots p_k,$$
where $p_1, \ldots, p_k$ are distinct odd primes ($k \geq 2$), has exactly 2^k solutions in $\mathbb{Z}_{p_1 \cdots p_k}$.

Outline

Quadratic residues - motivation

Proposition 1 (Solving quadratic congruences)

Let $p > 2$ be a prime and $a, b, c \in \mathbb{Z}$ such that $(a, p) = 1$. Then, the quadratic congruence

$$ax^2 + bx + c \equiv 0 \ mod \ p$$

has

1. two roots in $\mathbb{Z}_p$, if $\Delta \equiv y^2 \ mod \ p$ for some $y \in \mathbb{Z}$ with $p \not| y$;
2. one root in $\mathbb{Z}_p$, if $\Delta \equiv 0 \ mod \ p$;
3. no roots, otherwise,

where $\Delta = b^2 - 4ac$.

How hard is to decide if a given $a \in \mathbb{Z}_p^*$ satisfies $a \equiv y^2 \ mod \ p$ for some $y \in \mathbb{Z}$?

Quadratic residues and non-residues

Definition 7

Let $p > 2$ be a prime and $a \in \mathbb{Z}$ non-divisible by p. a is called a quadratic residue modulo p if $a \equiv x^2 \bmod n$ for some integer x.

If a is neither divisible by p nor a quadratic residue modulo p then a is called a quadratic non-residue modulo p.

Remark 1

An integer a non-divisible by a prime $p > 2$ is a quadratic (non-)residue modulo p if and only if $a \bmod p$ is a quadratic (non-)residue modulo p.

Denote

- $QR_p = \{a \in \mathbb{Z}_p^* | a \text{ is a quadratic residue modulo } p\}$
- $QNR_p = \{a \in \mathbb{Z}_p^* | a \text{ is a quadratic non-residue modulo } p\}$

Quadratic residues. Basic properties

Proposition 2

Let $p > 2$ be a prime. Then, $|QR_p| = |QNR_p| = \frac{p-1}{2}$.

Proposition 3

Let $p > 2$ be a prime. Then:

1. $a, b \in QR_p \quad \Rightarrow \quad (ab \bmod p) \in QR_p$;
2. $a \in QR_p \ \wedge \ b \in QNR_p \quad \Rightarrow \quad (ab \bmod p) \in QNR_p$;
3. $a, b \in QNR_p \quad \Rightarrow \quad (ab \bmod p) \in QR_p$.

Theorem 8 (Euler's Criterion)

Let $p > 2$ be a prime and $a \in \mathbb{Z}_p^*$. Then,

1. $a \in QR_p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \ mod \ p$;
2. $a \in QNR_p$ if and only if $a^{\frac{p-1}{2}} \equiv -1 \ mod \ p$.

Outline

The Legendre symbol

Introduced by Adrien-Marie Legendre in 1798 when trying to prove the law of quadratic reciprocity.

Definition 9

Let $p > 2$ be a prime. The Legendre symbol of $a \in \mathbb{Z}$, denoted $\left(\frac{a}{p}\right)$, is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a \\ 1, & \text{if } p \not| a \text{ and } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } p \not| a \text{ and } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

Remark that the Legendre symbol is only defined for primes $p > 2$. For $p = 2$, all even integers are divisible by p and all odd integers are quadratic residues modulo p.

The Legendre symbol

Proposition 4

Let $p > 2$ be a prime and $a, b \in \mathbb{Z}$. If $a \equiv b \ mod\ p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Therefore, $\left(\frac{a}{p}\right) = \left(\frac{a\ mod\ p}{p}\right)$.

Proposition 5

Let $p > 2$ be a prime. Then, for any $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ mod\ p$.

Proposition 6

Let $p > 2$ be a prime. Then, for any $a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

The Legendre symbol

According to the above properties, computing the Legendre symbol modulo p comes down to computing $\left(\frac{-1}{p}\right)$ and $\left(\frac{q}{p}\right)$, for any prime q with $2 \leq q < p$.

Proposition 7

Let $p > 2$ be a prime. Then,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \ mod \ 4 \\ -1, & \text{if } p \equiv 3 \ mod \ 4 \end{cases}$$

The Legendre symbol

Theorem 10 (Gauss' Criterion)

Let $p > 2$ be a prime and $a \in \mathbb{Z}$ non-divisible by p. Then, $\left(\frac{a}{p}\right) = (-1)^r$, where

$$r = |\{i \in \{1, \ldots, (p-1)/2\} | ia \ mod \ p > p/2\}|.$$

Proposition 8

Let $p > 2$ be a prime. Then,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \ mod \ 8 \\ -1, & \text{if } p \equiv \pm 3 \ mod \ 8 \end{cases}$$

The Legendre symbol

Theorem 11 (Quadratic reciprocity law)

Let $p, q > 2$ be distinct primes. Then,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Equivalently,

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right), & \text{if } p, q \equiv 3 \ mod\ 4 \\ \left(\frac{p}{q}\right), & \text{otherwise} \end{cases}$$

Example 12

$$\left(\frac{7}{59}\right) = -\left(\frac{59}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$$

The Legendre symbol

Basic rules for computing the Legendre symbol (review):

1. if $a \equiv b \ mod \ p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{1}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \ mod \ 4 \\ -1, & \text{if } p \equiv 3 \ mod \ 4 \end{cases}$
5. $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \ mod \ 8 \\ -1, & \text{if } p \equiv \pm 3 \ mod \ 8 \end{cases}$
6. $\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{if } p \equiv 1 \ mod \ 4 \text{ or } q \equiv 1 \ mod \ 4 \\ -\left(\frac{p}{q}\right), & \text{if } p \equiv q \equiv 3 \ mod \ 4 \end{cases}$

for any distinct primes $p, q > 2$ and $a, b \in \mathbb{Z}$.

Outline

The Jacobi symbol

Introduced by Carl Gustav Jacob Jacobi in 1837 as a generalization of the Legendre symbol.

Definition 13

Let $n > 0$ be an odd integer. The Jacobi symbol *of $a \in \mathbb{Z}$, denoted $\left(\frac{a}{n}\right)$, is defined by*

$$\left(\frac{a}{n}\right) = \begin{cases} 1, & \text{if } n=1 \\ \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}, & \text{otherwise} \end{cases}$$

where $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n.

Remark 2

1. The Jacobi symbol is defined only for odd integers $n > 0$.
2. $(a, n) = 1$ if and only if $\left(\frac{a}{n}\right) \neq 0$, for all $a \in \mathbb{Z}$ and $n > 0$ odd.

The Jacobi symbol

Theorem 14

The following properties hold:

1. if $a \equiv b \; mod \; n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
3. $\left(\frac{1}{n}\right) = 1$
4. $\left(\frac{-1}{n}\right) = \begin{cases} 1, & \text{if } n \equiv 1 \; mod \; 4 \\ -1, & \text{if } n \equiv 3 \; mod \; 4 \end{cases}$
5. $\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{if } n \equiv \pm 1 \; mod \; 8 \\ -1, & \text{if } n \equiv \pm 3 \; mod \; 8 \end{cases}$
6. $\left(\frac{m}{n}\right) = \begin{cases} \left(\frac{n}{m}\right), & \text{if } n \equiv 1 \; mod \; 4 \text{ or } m \equiv 1 \; mod \; 4 \\ -\left(\frac{n}{m}\right), & \text{if } n \equiv m \equiv 3 \; mod \; 4 \end{cases}$

for any distinct odd integers $n, m > 0$ and $a, b \in \mathbb{Z}$.

The Jacobi symbol

Algorithm 2: Computing the Jacobi symbol

input : integer a and odd integer $n > 0$;
output: $\left(\frac{a}{n}\right)$

begin
  $b := a \bmod n$; $c := n$; $s := 1$;
  while $b \geq 2$ **do**
    while $4|b$ **do** $b := b/4$;
    if $2|b$ **then**
      if $c \bmod 8 \in \{3, 5\}$ **then** $s := -s$;
      $b := b/2$;
    if $b = 1$ **then quit**;
    if $b \bmod 4 = 3 = c \bmod 4$ **then**
      $s := -s$;
      $(b, c) := (c \bmod b, b)$;
  return $s \cdot b$;

Outline

Linear congruential equations

The Chinese remainder theorem

Quadratic residues

The Legendre symbol

The Jacobi symbol

Course readings

Course readings

1. F.L. Țiplea: *Fundamentele Algebrice ale Informaticii*, Ed. Polirom, Iași, 2006, pag. 164–172.

2. M. B. Nathanson: *Elementary Methods in Number Theory*, Graduate Texts in Mathematics, Springer-Verlag, 2000, pag. 100–120.