



# Theory of algorithms (11th lecture)

Pál Pusztai  
[pusztai@sze.hu](mailto:pusztai@sze.hu)

## Outline

- Number-theoretic algorithms
  - Mathematical background
  - Euclid's algorithm
  - The extended form of Euclid's algorithm
  - Solving modular linear equations
- Exercises



# Number-theoretic algorithms

Number theory was once viewed as a beautiful but largely useless subject in pure mathematics.

Today number-theoretic algorithms are used widely, due in large part to the invention of cryptographic schemes based on **large prime** numbers.

These schemes are **feasible** because we can find large primes easily, and they are **secure** because we do not know how to factor the product of large primes.

The RSA public-key cryptosystem: Rivest-Shamir-Adleman (1978)



# Mathematical background

## ■ Divisibility and divisors

Let  $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$  be the set of integers.

The notation  $d \mid a$  means ( $a, d \in \mathbf{Z}, d \neq 0$ ) that  $a=kd$  for some integer  $k$ .

If  $d \mid a$  and  $d > 0$ , we say that  $d$  is a **divisor** of  $a$ , and  $a$  is a **multiple** of  $d$ .

**Remarks:** Note that  $d \mid a$  if and only if  $-d \mid a$ , so that no generality is lost by defining the divisors to be positive, with the understanding that the negative of any divisor of  $a$  also divides  $a$ . A divisor of a nonzero integer  $a$  is at least 1 but not greater than  $|a|$ .

For example, the divisors of 12 are 1, 2, 3, 4, 6, and 12.

Every positive integer  $a$  is divisible by the **trivial divisors** 1 and  $a$ . The nontrivial divisors of  $a$  are the **factors** of  $a$ .

For example, the factors of 12 are 2, 3, 4, and 6.



## Mathematical background

### ■ Prime and composite numbers

An integer  $a > 1$  whose only divisors are the trivial divisors 1 and  $a$  is a **prime number** or, more simply, a **prime**. Primes have many special properties and play a critical role in number theory.  
For example: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

An integer  $a > 1$  that is not prime is a **composite number** or, more simply, a **composite**.

For example: 15 is composite, because  $3 \mid 15$ .

We call the integer 1 a **unit**, and it is neither prime nor composite.

**Remark:** The integer 0 and all negative integers are neither prime nor composite.



## Mathematical background

### ■ Remainders and modular equivalence

**The division theorem** : For any integer  $a$  and any positive integer  $n$ , there exist unique integers  $q$  and  $r$  such that  $0 \leq r < n$  and  $a = qn + r$ .

The value  $q = \lfloor a / n \rfloor$  is the **quotient** of the division, and the value  $r = a \bmod n$  is the **remainder** (or **residue**) of the division. We have that  $n \mid a$  if and only if  $a \bmod n = 0$ .

If  $a \bmod n = b \bmod n$ , then  $a$  is **equivalent** (or **congruent**) to  $b$  modulo  $n$ .

Notation:  $a \equiv b \pmod{n}$ .

For example:  $61 \equiv 6 \pmod{11}$ ,  $-13 \equiv 22 \pmod{5}$ .

**Properties:** If  $a \equiv a' \pmod{n}$  and  $b \equiv b' \pmod{n}$ , then  $a + b \equiv a' + b' \pmod{n}$  and  $ab \equiv a'b' \pmod{n}$ .

**Corollary:**  $ab \equiv a(b \bmod n) \pmod{n}$ , since  $b \equiv b \bmod n \pmod{n}$ .



# Mathematical background

## ■ Equivalence classes

We can partition the integers into  $n$  equivalence classes according to their remainders modulo  $n$ .

The **equivalence class modulo  $n$**  containing an integer  $a$  is

$$[a]_n = \{a + kn : k \in \mathbf{Z}\}.$$

For example:  $[3]_7 = \{\dots, -11, -4, 3, 10, 17, \dots\}$ , we can also denote this set by  $[-4]_7$  or  $[10]_7$ .

Writing  $a \in [b]_n$  is the same as writing  $a \equiv b \pmod{n}$ .

The set of all such equivalence classes is

$$\mathbf{Z}_n = \{[a]_n : 0 \leq a \leq n-1\}.$$

**Remarks:** The definition  $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$  is also used where 0 represents  $[0]_n$ , 1 represents  $[1]_n$ , and so on; each class is represented by its smallest nonnegative element. You should keep the underlying equivalence classes in mind, however. For example,  $-1$  is referring to  $[n-1]_n$ , since  $-1 \equiv n-1 \pmod{n}$ .



## Mathematical background

### ■ Common divisors and greatest common divisors

If  $d$  is a divisor of  $a$  and  $d$  is also a divisor of  $b$ , then  $d$  is a **common divisor** of  $a$  and  $b$ .

For example, the common divisors of 24 and 30 are 1, 2, 3, and 6.

Properties of common divisors is that:

If  $d \mid a$  and  $d \mid b$ , then  $d \mid (a+b)$  and  $d \mid (a-b)$ , more generally  $d \mid (ax+by)$  for any  $x, y$  integers.

If  $a \mid b$ , then either  $|a| \leq |b|$  or  $b=0$ , which implies that if  $a \mid b$  and  $b \mid a$ , then  $a = \pm b$ .

The **greatest common divisor** of two integers  $a$  and  $b$ , not both zero, is the largest of the common divisors of  $a$  and  $b$ ; we denote it by  $\gcd(a, b)$ .

For example:  $\gcd(24, 30)=6$ ,  $\gcd(14, 15)=1$ ,  $\gcd(5, 7)=1$ ,  $\gcd(0, 9)=9$ .

If  $a$  and  $b$  are both nonzero, then  $1 \leq \gcd(a, b) \leq \min(|a|, |b|)$ .

We define  $\gcd(0, 0)$  to be 0.



## Mathematical background

### ■ Common divisors and greatest common divisors

The elementary properties of the gcd function:

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

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

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

$$\gcd(a, 0) = |a|,$$

$$\gcd(a, ka) = |a| \text{ for any } k \in \mathbb{Z}.$$

**Theorem:** If  $a$  and  $b$  are any integers, not both zero, then  $\gcd(a, b)$  is the smallest positive element of the set  $\{ax+by: x, y \in \mathbb{Z}\}$  of linear combinations of  $a$  and  $b$ .

### Corollaries:

- For any integers  $a$  and  $b$ , if  $d \mid a$  and  $d \mid b$ , then  $d \mid \gcd(a, b)$ .
- For all integers  $a$  and  $b$  and any nonnegative integer  $n$ ,  $\gcd(an, bn) = n \gcd(a, b)$ .
- For all positive integers  $n$ ,  $a$ , and  $b$ , if  $n \mid ab$  and  $\gcd(a, n)=1$ , then  $n \mid b$ .

**Remark:** Since  $\gcd(a, b) = \gcd(|a|, |b|)$  in the following we assume that  $a$  and  $b$  are nonnegative integers.



## Mathematical background

### ■ Relatively prime integers

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

For example: 8 and 15 are relatively prime, since the divisors of 8 are 1, 2, 4, and 8, and the divisors of 15 are 1, 3, 5, and 15.

**Theorem:** For any integers  $a$ ,  $b$ , and  $p$ , if both  $\gcd(a, p) = 1$  and  $\gcd(b, p) = 1$ , then  $\gcd(ab, p) = 1$ .

**Theorem:** For all primes  $p$  and all integers  $a$  and  $b$ , if  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$  (or both).

### ■ The Euler's $\Phi$ function

Let  $\mathbf{Z}_n^* = \{[a]_n \in \mathbf{Z}_n : \gcd(a, n) = 1\}$  be the set of the elements of  $\mathbf{Z}_n$  that are relatively prime to  $n$ .

For example:  $\mathbf{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ .

Let  $\Phi(n)$  be the number of elements of  $\mathbf{Z}_n^*$ . This is the Euler's  $\Phi$  function. For example:  $\Phi(15) = 8$ .

Property:  $\Phi(n) = n \prod_{p : p \text{ is prime and } p \mid n} \left(1 - \frac{1}{p}\right)$ . For example:  $\Phi(15) = 15 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 15 \left(\frac{2}{3}\right) \left(\frac{4}{5}\right) = 8$ .

If  $p$  is prime, then  $\mathbf{Z}_p^* = \{1, 2, 3, \dots, p-1\}$ , and  $\Phi(p) = p-1$ .



## Exercises

- Calculate the value of  $\Phi(n)$  with below given  $n$ .
  - 9, 30, 42, 100



## Mathematical background

### ■ Unique factorization

**Theorem:** There is exactly one way to write any composite integer  $a$  as a product of the form

$a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ , where the  $p_i$  are prime,  $p_1 < p_2 < \dots < p_r$ , and the  $e_i$  are positive integers.

For example:  $60 = 2^2 \cdot 3 \cdot 5$ .

### ■ Computing greatest common divisors

The  $\gcd(a, b)$  can be computed for positive integers  $a$  and  $b$  from the prime factorizations of  $a$  and  $b$ .

If  $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$  and  $b = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$ , with zero exponents being used to make the set of primes

$p_1, p_2, \dots, p_r$  the same for both  $a$  and  $b$ , then  $\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_r^{\min(e_r, f_r)}$ .

**Remark:** As factoring do not run in polynomial time, this approach does not give an efficient algorithm.

**Theorem:** For any nonnegative integer  $a$  and any positive integer  $b$ ,  $\gcd(a, b) = \gcd(b, a \bmod b)$ .

**Remark:** Based on it an efficient algorithm can be given to calculate the greatest common divisor.



## Euclid's algorithm

- An efficient algorithm to calculate the greatest common divisor

EUCLID( $a, b$ )

```
1  if  $b == 0$ 
2      return  $a$ 
3  else
4      return EUCLID( $b, a \bmod b$ )
```

For example, to compute  $\text{gcd}(30, 21)$  the below given recursive calls will produce the result:

$$\text{EUCLID}(30, 21) = \text{EUCLID}(21, 9) = \text{EUCLID}(9, 3) = \text{EUCLID}(3, 0) = 3$$

**Theorem** (Lamé): For any integer  $k \geq 1$ , if  $a > b \geq 1$  and  $b < F_{k+1}$ , then the call  $\text{EUCLID}(a, b)$  makes fewer than  $k$  recursive calls. ( $F_{k+1}$  is the  $k+1$ th Fibonacci number.)

**Efficiency:** The neighbor Fibonacci numbers cause the worst case. Since  $F_k$  is approximately  $\varphi^k / \sqrt{5}$ , where  $\varphi = (1 + \sqrt{5})/2 = 1.61803\dots$  is the golden ratio, the number of recursive calls in EUCLID (thus, the running time) is  $O(\lg b)$ .

**Remark:** Euclid describes „this” algorithm circa 300 B.C.



## Exercises

- What recursive calls are produced by EUCLID with below given input data?
  - 50, 35
  - 0, 8
  - 34, 21



## The extended form of Euclid's algorithm

### ■ The extension of Euclid's algorithm

We extend the algorithm to compute the integer coefficients  $x$  and  $y$  such that:

$$d = \gcd(a, b) = ax + by.$$

The new algorithm takes as input a pair of nonnegative integers and returns a triple of the form  $(d, x, y)$  that satisfies the equation.

EXTENDED-EUCLID( $a, b$ )

```
1  if  $b == 0$ 
2      return  $(a, 1, 0)$ 
3   $(d', x', y') = \text{EXTENDED-EUCLID}(b, a \bmod b)$ 
4   $(d, x, y) = (d', y', x' - \lfloor a / b \rfloor y')$ 
5  return  $(d, x, y)$ 
```

**Remark:** Note that  $x$  and  $y$  may be zero or negative.

**Efficiency:** Since the number of recursive calls made in EUCLID is equal to the number of recursive calls made in EXTENDED-EUCLID, the running times are the same, to within a constant factor. That is, for  $a > b > 0$ , the number of recursive calls is  $O(\lg b)$ .



## The extended form of Euclid's algorithm

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	—	3	1	0

### The operation of EXTENDED-EUCLID

The call EXTENDED-EUCLID(99, 78) returns (3, -11, 14), so that

$$\gcd(99, 78) = 3 = 99 \cdot (-11) + 78 \cdot 14.$$



## Exercises

- Compute the values  $(d, x, y)$  that the EXTENDED-EUCLID returns with below given input data.
  - 30, 75
  - 899, 493



## Modular linear equations

### ■ Solving modular linear equations

**Problem:** Find solutions to the equation  $ax \equiv b \pmod{n}$ , where  $b$  integer,  $a > 0$  and  $n > 0$  integers.

**Remark:** The equation may have 0, 1, or more than 1 such solution.

**Properties:**

- The equation  $ax \equiv b \pmod{n}$  is solvable for the unknown  $x$  if and only if  $d \mid b$ , where  $d = \gcd(a, n)$ .
- The equation  $ax \equiv b \pmod{n}$  either has  $d$  distinct solutions modulo  $n$ , where  $d = \gcd(a, n)$ , or it has no solutions.
- Let  $d = \gcd(a, n)$  and suppose that  $d = ax' + ny'$  for some integers  $x', y'$ . If  $d \mid b$ , then the equation  $ax \equiv b \pmod{n}$  has as one of its solutions the value  $x_0$ , where  $x_0 = x'(b/d) \pmod{n}$ .
- Suppose that the equation  $ax \equiv b \pmod{n}$  is solvable (that is,  $d \mid b$ , where  $d = \gcd(a, n)$ ) and that  $x_0$  is any solution to this equation. Then, this equation has exactly  $d$  distinct solutions, modulo  $n$ , given by  $x_i = x_0 + i(n/d) \pmod{n}$ , for  $i = 0, 1, 2, \dots, d-1$ .
- For any  $n > 1$ , if  $\gcd(a, n) = 1$ , then the equation  $ax \equiv b \pmod{n}$  has a unique solution, modulo  $n$ .

**Remark:** If  $b=1$ , the  $x$  we are looking for is a **multiplicative inverse** of  $a$ , modulo  $n$ . If  $\gcd(a, n) = 1$ , then the unique solution to the equation  $ax \equiv 1 \pmod{n}$  is the integer  $x$  returned by EXTENDED-EUCLID, since the equation  $\gcd(a, n) = 1 = ax + ny$  implies  $ax \equiv 1 \pmod{n}$ .



## Modular linear equations

MODULAR-LINEAR-EQUATION-SOLVER( $a, b, n$ )

```
1  ( $d, x', y'$ ) = EXTENDED-EUCLID( $a, n$ )
2  if  $d \mid b$ 
3       $x_0 = x'(b / d) \bmod n$ 
4      for  $i = 0$  to  $d-1$ 
5          write  $(x_0 + i (n / d)) \bmod n$ 
6  else
7      write „No solutions”
```

**Efficiency:** The running time is  $O(\lg n + \gcd(a, n))$ .



## Exercises

- Find all solutions to the below given equations.
  - $14x \equiv 30 \pmod{100}$
  - $35x \equiv 10 \pmod{50}$

