Complexity and Cryptography

Thomas Zeugmann

Hokkaido University
Laboratory for Algorithmics

https://www-alg.ist.hokudai.ac.jp/~thomas/COCR/

Lecture 3: Number Theoretic Problems

Motivation

We want to have a closer look at the complexity of several problems arising in number theory.

Clearly, we cannot provide an exhaustive study of all interesting problems. Instead, we concentrate ourselves on problems that will be needed when dealing with *cryptography*.

Motivation

We want to have a closer look at the complexity of several problems arising in number theory.

Clearly, we cannot provide an exhaustive study of all interesting problems. Instead, we concentrate ourselves on problems that will be needed when dealing with *cryptography*.

Before we start to study the complexity of several problems arising in number theory, it is helpful to recall a bit group theory.

Groups I

Definition 1

Let $G \neq \emptyset$ be any set, and let $\circ\colon G \times G \to G$ be any binary operation. We call $(G, \circ)$ a *group* if

(1) $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$, (i.e., $\circ$ is associative);

(2) there exists a *neutral element* $e \in G$ such that $a \circ e = e \circ a = a$ for all $a \in G$;

(3) for every $a \in G$ there exists an *inverse element* $b \in G$ such that $a \circ b = b \circ a = e$.

(4) A group is called *Abelian group* if $\circ$ is also commutative, i.e., $a \circ b = b \circ a$ for all $a, b \in G$.

(5) A group is said to be *finite* if $|G|$ is finite.

(6) If $(G, \circ)$ is a finite group then we call $|G|$ the *order* of $(G, \circ)$.

Groups II

Note that the neutral element e and the inverse elements defined above are uniquely determined. In order to have an example, consider the Abelian group $(\mathbb{Z}, +)$. Clearly, addition over the integers is associative and commutative. The neutral element is 0, and for every $a \in \mathbb{Z}$, the number $-a$ is the inverse element of a. Below we shall see more examples.

Groups II

Note that the neutral element e and the inverse elements defined above are uniquely determined. In order to have an example, consider the Abelian group $(\mathbb{Z}, +)$. Clearly, addition over the integers is associative and commutative. The neutral element is 0, and for every $a \in \mathbb{Z}$, the number $-a$ is the inverse element of a. Below we shall see more examples.

It is advantageous to have the following definition:

Definition 2

Let $(G, \circ)$ be a group and let $S \subseteq G$ be non-empty. Then $(S, \circ)$ is said to be a *subgroup* of $(G, \circ)$ if

(1) $a \circ b \in S$ for all $a, b \in S$;

(2) for every $a \in S$ also the inverse b of a is in S.

Groups III

For example, let E be the set of all even integers, and let O be the set of all odd integers. Then $(E, +)$ is a subgroup of $(\mathbb{Z}, +)$, while $(O, +)$ is not. Also, for every group $(G, \circ)$ the group $(\{e\}, \circ)$ and the group $(G, \circ)$ itself are subgroups of $(G, \circ)$.

Groups III

For example, let E be the set of all even integers, and let O be the set of all odd integers. Then $(E, +)$ is a subgroup of $(\mathbb{Z}, +)$, while $(O, +)$ is not. Also, for every group $(G, \circ)$ the group $(\{e\}, \circ)$ and the group $(G, \circ)$ itself are subgroups of $(G, \circ)$.

For having another example, we introduce the following notation: Let $(G, \circ)$ be a group, let $a \in G$, and let b be the inverse of a. We set $a^0 =_{df} e$, $a^{n+1} =_{df} a^n \circ a$ for all $n \in \mathbb{N}$, and $a^{-(n+1)} =_{df} b^n \circ b$ for all $n \in \mathbb{N}$.

Groups III

For example, let E be the set of all even integers, and let O be the set of all odd integers. Then $(E, +)$ is a subgroup of $(\mathbb{Z}, +)$, while $(O, +)$ is not. Also, for every group $(G, \circ)$ the group $(\{e\}, \circ)$ and the group $(G, \circ)$ itself are subgroups of $(G, \circ)$.

For having another example, we introduce the following notation: Let $(G, \circ)$ be a group, let $a \in G$, and let b be the inverse of a. We set $a^0 =_{df} e$, $a^{n+1} =_{df} a^n \circ a$ for all $n \in \mathbb{N}$, and $a^{-(n+1)} =_{df} b^n \circ b$ for all $n \in \mathbb{N}$.

Let $S = \{a^n \mid n \in \mathbb{Z}\}$; then $(S, \circ)$ is always a subgroup of $(G, \circ)$.

Groups III

For example, let E be the set of all even integers, and let O be the set of all odd integers. Then $(E, +)$ is a subgroup of $(\mathbb{Z}, +)$, while $(O, +)$ is not. Also, for every group $(G, \circ)$ the group $(\{e\}, \circ)$ and the group $(G, \circ)$ itself are subgroups of $(G, \circ)$.

For having another example, we introduce the following notation: Let $(G, \circ)$ be a group, let $a \in G$, and let b be the inverse of a. We set $a^0 =_{df} e$, $a^{n+1} =_{df} a^n \circ a$ for all $n \in \mathbb{N}$, and $a^{-(n+1)} =_{df} b^n \circ b$ for all $n \in \mathbb{N}$.

Let $S = \{a^n \mid n \in \mathbb{Z}\}$; then $(S, \circ)$ is always a subgroup of $(G, \circ)$.

The importance of the latter example suggests the following definitions:

Groups IV

Definition 3

A group $(G, \circ)$ is said to be a *cyclic group* if there exists an element $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\}$. We refer to a as a *generator* of G.

Groups IV

Definition 3

A group $(G, \circ)$ is said to be a *cyclic group* if there exists an element $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\}$. We refer to a as a *generator* of G.

Definition 4

Let $(G, \circ)$ be any group with neutral element e, and let $a \in G$. The least number $n \in \mathbb{N}^+$ such that $a^n = e$ is called *order of a* provided such an n exists. If $a^n \neq e$ for all $n \in \mathbb{N}^+$ then we define the order of a to be ∞. We denote the order of a by $\mathrm{ord}(a)$.

Groups IV

Definition 3

A group $(G, \circ)$ is said to be a *cyclic group* if there exists an element $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\}$. We refer to a as a *generator* of G.

Definition 4

Let $(G, \circ)$ be any group with neutral element e, and let $a \in G$. The least number $n \in \mathbb{N}^+$ such that $a^n = e$ is called *order of a* provided such an n exists. If $a^n \neq e$ for all $n \in \mathbb{N}^+$ then we define the order of a to be ∞. We denote the order of a by $\mathrm{ord}(a)$.

Let $a, b \in \mathbb{Z}$ be given. We say that a *divides* b (or b is *divisible* by a) if there exists a $d \in \mathbb{Z}$ such that $b = ad$. If a divides b we write $a|b$, and a is called a *divisor* of b.

Groups V

Next, we establish an important property of subgroups of finite groups.

Theorem 1 (Lagrange's theorem)

Let $(G, \circ)$ be a finite group and let $(H, \circ)$ be any subgroup of $(G, \circ)$. Then the order of $(H, \circ)$ divides the order of $(G, \circ)$.

Groups V

Next, we establish an important property of subgroups of finite groups.

Theorem 1 (Lagrange's theorem)

Let $(G, \circ)$ be a finite group and let $(H, \circ)$ be any subgroup of $(G, \circ)$. Then the order of $(H, \circ)$ divides the order of $(G, \circ)$.

Proof. Let $H = \{h_1, \ldots, h_m\} \subseteq G$ be any subgroup of G. If $G = H$, we are done.
Otherwise, we have $H \subset G$, and hence there exists an element $x \in G \setminus H$. Consider the set $Hx = \{h_1 \circ x, \ldots, h_m \circ x\}$. Then $h_i \circ x = h_j \circ x$ implies $h_i = h_j$. Furthermore, $h_i \circ x = h_j$ would imply $x = h_i^{-1} \circ h_j \in H$, a contradiction to $x \notin H$ (here h_i^{-1} is the inverse of h_i).

Groups VI

Thus, the elements of Hx are pairwise distinct and do not belong to H. We conclude that

$$|Hx| = |H| = m \quad \text{and} \quad Hx \cap H = \emptyset\,. \tag{1}$$

Now, if $Hx \cup H = G$, the theorem follows. Otherwise, there is an element $x_1 \in G \setminus (Hx \cup H)$ and we form the set $Hx_1 = \{h_1 \circ x_1, \ldots, h_m \circ x_1\}$. Analogously to the above, we can show that the elements of Hx_1 are pairwise distinct and do not belong to $Hx \cup H$. Since G is finite, we thus obtain a finite partition $H,\ Hx,\ Hx_1,\ \ldots,\ Hx_\ell$ of G, where each of the sets $H,\ Hx,\ Hx_1,\ \ldots,\ Hx_\ell$ has precisely m elements. Hence, we have shown that $|G| = (\ell + 2)m$. ∎

Groups VII

Theorem 1 allows for a nice corollary which is needed later.

Corollary 1

Let $(G, \circ)$ *be any group with neutral element* e*, and let* $a \in G$ *be any element such that* $\text{ord}(a) \neq \infty$*. Then* $\text{ord}(a)$ *divides* $|G|$*.*

Definitions I

We need the following notations and definitions:
Consider $m \in \mathbb{N}^+$ and $a \in \mathbb{Z}$. Then there are uniquely determined numbers q, r such that $a = qm + r$, where $0 \leqslant r < m$. We call q the *integer quotient* and r the *remainder*.

Definitions I

We need the following notations and definitions:
Consider $m \in \mathbb{N}^+$ and $a \in \mathbb{Z}$. Then there are uniquely determined numbers q, r such that $a = qm + r$, where $0 \leqslant r < m$. We call q the *integer quotient* and r the *remainder*.

Quite often, one is not interested in a number a itself but in its remainder when divided by a number m.
Let $m \in \mathbb{N}^+$, and let $a, b \in \mathbb{Z}$; we write $a \equiv b \mod m$ if and only if m divides $a - b$ (abbr. $m|(a - b)$).

Definitions I

We need the following notations and definitions:
Consider $m \in \mathbb{N}^+$ and $a \in \mathbb{Z}$. Then there are uniquely determined numbers q, r such that $a = qm + r$, where $0 \leqslant r < m$. We call q the *integer quotient* and r the *remainder*.

Quite often, one is not interested in a number a itself but in its remainder when divided by a number m.
Let $m \in \mathbb{N}^+$, and let $a, b \in \mathbb{Z}$; we write $a \equiv b \mod m$ if and only if m divides $a - b$ (abbr. $m|(a - b)$).

Thus, $a \equiv b \mod m$ if and only if a and b have the *same* remainder when divided by m.
If $a \equiv b \mod m$ then we say that a is *congruent* b modulo m, and we refer to "$\equiv$" as the *congruence relation*.

Definitions II

It is easy to see that "$\equiv$" is an equivalence relation, i.e., it is *reflexive*, *symmetric* and *transitive*. Thus, we may consider the equivalence classes $[a] =_{df} \{x \in \mathbb{Z} \mid a \equiv x \mod m\}$.

Consequently, $[a] = [b]$ iff $a \equiv b \mod m$. Therefore, there are precisely the m equivalence classes $[0], [1], \ldots, [m-1]$. We set $\mathbb{Z}_m =_{df} \{[0], [1], \ldots, [m-1]\}$.

Definitions II

It is easy to see that "$\equiv$" is an equivalence relation, i.e., it is *reflexive*, *symmetric* and *transitive*. Thus, we may consider the equivalence classes $[a] =_{df} \{x \in \mathbb{Z} \mid a \equiv x \mod m\}$.
Consequently, $[a] = [b]$ iff $a \equiv b \mod m$. Therefore, there are precisely the m equivalence classes $[0], [1], \ldots, [m-1]$. We set $\mathbb{Z}_m =_{df} \{[0], [1], \ldots, [m-1]\}$.

Definition 5

We define addition and multiplication of these equivalence classes by

$$
\begin{aligned}
[a] + [b] &=_{df} [a + b] \quad \text{and} \\
[a] \cdot [b] &=_{df} [a \cdot b] \,.
\end{aligned}
$$

Definitions III

Exercise 1. *Show that the definition of $+$ and $\cdot$ over $\mathbb{Z}_m$ are independent of the choice of the representation.*

Now, it is easy to see that $(\mathbb{Z}_m, +, \cdot)$ constitutes a commutative ring.

Definitions III

Exercise 1. *Show that the definition of $+$ and $\cdot$ over $\mathbb{Z}_m$ are independent of the choice of the representation.*

Now, it is easy to see that $(\mathbb{Z}_m, +, \cdot)$ constitutes a commutative ring.

Clearly, the neutral element for addition is $[0]$ and the identity element with respect to multiplication is $[1]$.
Moreover, by the definition of a ring, it is immediate that $(\mathbb{Z}_m, +)$ is an Abelian group. We refer to this group also as to $\mathbb{Z}_m$ for short.

Definitions III

Exercise 1. *Show that the definition of $+$ and $\cdot$ over $\mathbb{Z}_m$ are independent of the choice of the representation.*

Now, it is easy to see that $(\mathbb{Z}_m, +, \cdot)$ constitutes a commutative ring.

Clearly, the neutral element for addition is $[0]$ and the identity element with respect to multiplication is $[1]$.
Moreover, by the definition of a ring, it is immediate that $(\mathbb{Z}_m, +)$ is an Abelian group. We refer to this group also as to $\mathbb{Z}_m$ for short.

Note, however, that in general $(\mathbb{Z}_m, +, \cdot)$ is *not* a field. For example, let $m = 6$ and consider $[2]$. Then $[2]$ does not have a multiplicative inverse in $(\mathbb{Z}_6, +, \cdot\,)$.

Definitions IV

In order to see under what circumstances $(\mathbb{Z}_m, +, \cdot)$ is a field, we have to answer the question under which conditions the multiplicative inverses do always exist. Note that these multiplicative inverses are also called *modular inverses*. The existence of modular inverses is completely characterized by Theorem 6 below.

First we have to establish some useful rules for performing calculations with congruences.

Definitions IV

In order to see under what circumstances $(\mathbb{Z}_m, +, \cdot)$ is a field, we have to answer the question under which conditions the multiplicative inverses do always exist. Note that these multiplicative inverses are also called *modular inverses*. The existence of modular inverses is completely characterized by Theorem 6 below.
First we have to establish some useful rules for performing calculations with congruences.

We shall also look at the complexity of some of the more important algorithms provided. For doing this, we measure the length of the inputs by the number of bits needed to write the input down. Moreover, whenever dealing with elements from $\mathbb{Z}_m$, we assume that they are represented by their canonical representations, i.e., by $0, \ldots, m-1$.

Basics

Theorem 2

Let $m \in \mathbb{N}^+$, *let* $a, b, c, d \in \mathbb{Z}$ *be any integers such that* $a \equiv b \mod m$ *and* $c \equiv d \mod m$, *and let* $n \in \mathbb{N}$. *Then we have the following:*

(1) $a + c \equiv b + d \mod m$;

(2) $a - c \equiv b - d \mod m$;

(3) $ac \equiv bd \mod m$;

(4) $a^n \equiv b^n \mod m$.

The proof is left as an *exercise*.

So, we can calculate with congruences almost as convenient as with equations. The main difference is division. *Division* cannot be used.

GCD I

Before we can study modular inverses, we need the following:

Greatest Common Divisor (abbr. gcd)

Input: Numbers $a, b \in \mathbb{N}$.

Problem: Compute the greatest $d \in \mathbb{N}$ dividing both a and b.

It is convenient to set $\gcd(0,0) = 0$. Also, $\gcd(a,0) = a$ and $\gcd(a,a) = a$ for all $a \in \mathbb{N}$. Thus, we may assume $a > b > 0$.

Since we are also interested in the complexity of the number theoretic problems we are dealing with, we have to say how we do present numbers. In the following, we always assume numbers to be represented in binary notation. Thus, we need $n = \lfloor \log a \rfloor + 1$ many bits to represent number a, and we refer to n as to the *length* of input a.

GCD I

Before we can study modular inverses, we need the following:

Greatest Common Divisor (abbr. gcd)

Input: Numbers $a, b \in \mathbb{N}$.

Problem: Compute the greatest $d \in \mathbb{N}$ dividing both a and b.

It is convenient to set $\gcd(0, 0) = 0$. Also, $\gcd(a, 0) = a$ and $\gcd(a, a) = a$ for all $a \in \mathbb{N}$. Thus, we may assume $a > b > 0$.

Since we are also interested in the complexity of the number theoretic problems we are dealing with, we have to say how we do present numbers. In the following, we always assume numbers to be represented in binary notation. Thus, we need $n = \lfloor \log a \rfloor + 1$ many bits to represent number a, and we refer to n as to the *length* of input a.

We say that a computation can be performed in time *polynomial in the length m of the input* if there is a constant $c > 0$ such that the running time is $O(m^c)$ for all $m \in \mathbb{N}$.

GCD II

Theorem 3

Algorithm ECL below computes the gcd of numbers $a, b \in \mathbb{N}^+$ *and numbers* $x, y \in \mathbb{Z}$ *such that* $d = ax + by$. *It uses at most* $1.5 \log a$ *many divisions of numbers less than or equal to* a.

GCD II

Theorem 3

Algorithm ECL below computes the gcd of numbers $a, b \in \mathbb{N}^+$ and numbers $x, y \in \mathbb{Z}$ such that $d = ax + by$. It uses at most $1.5 \log a$ many divisions of numbers less than or equal to a.

Proof. Algorithm ECL is the so-called extended Euclidean algorithm. We use the following formulation of it:

Algorithm ECL: "Set $x_0 = 1,\ x_1 = 0, y_0 = 0,\ y_1 = 1$, and
$r_0 = a,\ r_1 = b$.
Compute successively

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i, && \text{where } q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor, \\ x_{i+1} &= x_{i-1} - q_i x_i, && \text{and} \\ y_{i+1} &= y_{i-1} - q_i y_i && \text{until } r_{i+1} = 0. \end{aligned}$$

Output $r_i,\ x_i,\ y_i$."

GCD III

Claim A. Algorithm ECL computes d, x, and y correctly.

Looking at the sequence of the r_i's computed by Algorithm ECL, we see that $r_{i-1} = q_i r_i + r_{i+1}$. That is, q_i is the integer quotient and r_{i+1} is the remainder obtained when dividing r_{i-1} by r_i. So we have $0 \leqslant r_i < r_{i-1}$ during the execution of Algorithm ECL, and thus it must terminate.

GCD III

Claim A. *Algorithm ECL computes* d, x, *and* y *correctly.*
Looking at the sequence of the r_i's computed by Algorithm ECL, we see that $r_{i-1} = q_i r_i + r_{i+1}$. That is, q_i is the integer quotient and r_{i+1} is the remainder obtained when dividing r_{i-1} by r_i. So we have $0 \leqslant r_i < r_{i-1}$ during the execution of Algorithm ECL, and thus it must terminate.

Let $i+1$ be the number such that $r_{i+1} = 0$. We prove inductively that

$$r_0 x_\ell + r_1 y_\ell = r_\ell \quad \text{for } \ell = 0, \ldots, i\,. \tag{2}$$

For $i = 0$ and $i = 1$ we directly obtain $r_0 x_0 + r_1 y_0 = r_0$ and $r_0 x_1 + r_1 y_1 = r_1$, respectively. Thus, we may assume the induction hypothesis for $\ell - 1$ and ℓ, where $\ell = 1, \ldots, i-1$.

GCD IV

By definition

$x_{\ell+1} = x_{\ell-1} - q_\ell x_\ell$, and $y_{\ell+1} = y_{\ell-1} - q_\ell y_\ell$; thus

$$\begin{aligned}
r_0 x_{\ell+1} + r_1 y_{\ell+1} &= r_0 x_{\ell-1} - r_0 q_\ell x_\ell + r_1 y_{\ell-1} - r_1 q_\ell y_\ell \\
&= \underbrace{r_0 x_{\ell-1} + r_1 y_{\ell-1}}_{=r_{\ell-1} \text{ by ind. hyp.}} - q_\ell \underbrace{(r_0 x_\ell + r_1 y_\ell)}_{=r_\ell \text{ by ind. hyp.}} \\
&= r_{\ell-1} - q_\ell r_\ell = r_{\ell+1} \,.
\end{aligned}$$

GCD IV

By definition

$x_{\ell+1} = x_{\ell-1} - q_\ell x_\ell$, and $y_{\ell+1} = y_{\ell-1} - q_\ell y_\ell$; thus

$$\begin{aligned} r_0 x_{\ell+1} + r_1 y_{\ell+1} &= r_0 x_{\ell-1} - r_0 q_\ell x_\ell + r_1 y_{\ell-1} - r_1 q_\ell y_\ell \\ &= \underbrace{r_0 x_{\ell-1} + r_1 y_{\ell-1}}_{=r_{\ell-1} \text{ by ind. hyp.}} - q_\ell \underbrace{(r_0 x_\ell + r_1 y_\ell)}_{=r_\ell \text{ by ind. hyp.}} \\ &= r_{\ell-1} - q_\ell r_\ell = r_{\ell+1} \,. \end{aligned}$$

It remains to show that $r_i = \gcd(a, b)$. Let $d = \gcd(a, b)$.
By (2), we have $r_i = r_0 x_i + r_1 y_i = a x_i + b y_i$. So d divides r_i.
On the other hand, every divisor of r_i divides $a x_i + b y_i$. Since $r_{i+1} = 0$, we know that $r_{i-1} = q_i r_i$.
Therefore, r_i divides r_{i-1}, too. Consequently, $r_{i-2} = r_i + q_{i-1} r_{i-1}$ implies $r_i | r_{i-2}$. Iterating this argument directly yields that r_i divides a and b. Thus, $r_i = d$.
This proves Claim A, i.e., the correctness.

GCD V

Claim B. *Algorithm ECL uses at most* $1.5 \log a$ *many divisions of numbers less than or equal to* a.

We have already seen that Algorithm ECL must terminate. To obtain a better bound for the number of divisions necessary, we show that

$$r_{\ell+1} + r_\ell \leqslant r_{\ell-1} \quad \text{for all} \quad \ell = 1, \ldots, i\,. \tag{3}$$

This can be seen as follows: By construction, $r_{\ell+1} = r_{\ell-1} - q_\ell r_\ell$; hence $r_{\ell+1} + r_\ell = r_{\ell-1} + r_\ell(1 - q_\ell) \leqslant r_{\ell-1}$ provided $(1 - q_\ell) \leqslant 0$. The latter inequality obviously holds in accordance with q_ℓ's definition.

GCD V

Claim B. *Algorithm ECL uses at most* $1.5 \log a$ *many divisions of numbers less than or equal to* a.

We have already seen that Algorithm ECL must terminate. To obtain a better bound for the number of divisions necessary, we show that

$$r_{\ell+1} + r_\ell \leqslant r_{\ell-1} \quad \text{for all} \quad \ell = 1, \ldots, i\,. \tag{3}$$

This can be seen as follows: By construction, $r_{\ell+1} = r_{\ell-1} - q_\ell r_\ell$; hence $r_{\ell+1} + r_\ell = r_{\ell-1} + r_\ell(1 - q_\ell) \leqslant r_{\ell-1}$ provided $(1 - q_\ell) \leqslant 0$. The latter inequality obviously holds in accordance with q_ℓ's definition.

By Inequality (3), we see that the number of divisions is maximal iff $r_{\ell+1} + r_\ell = r_{\ell-1}$ for all $\ell = 1, \ldots, i-1$.

GCD VI

Hence, the worst-case occurs if $a_0 = a_1 = 1$ and $a_\ell = a_{\ell-1} + a_{\ell-2}$ for all $n \geqslant \ell \geqslant 2$, where $a = a_{n+1}$ and $b = a_n$; i.e., if a equals the $(n+2)$th member and b equals the $(n+1)$th member of the well-known Fibonacci sequence. Therefore, all we have to do is to estimate the size of the nth member of the Fibonacci sequence.

GCD VII

Recall that

$$a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right). \tag{4}$$

GCD VII

Recall that

$$a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right) . \qquad (4)$$

Let $\phi =_{df} \left(\frac{1+\sqrt{5}}{2}\right)$; then one can show inductively that

$$\phi^{n-1} \leqslant a_n \leqslant \phi^n \quad \text{for all } n \geqslant 1 . \qquad (5)$$

That is, if $a = a_{n+1}$ and $b = a_n$ then Algorithm ECL has to perform n division steps. By the left-hand side of (5), we know that $a = a_{n+1} \geqslant \phi^n$ and thus $\log_\phi a \geqslant n$ gives the desired upper bound for the number of divisions to be performed. Since $\log_\phi a = \frac{\ln 2}{\ln \phi} \log a$, Claim B follows.

Putting Claim A and B together, directly yields Theorem 3. ∎

GCD VIII

It remains to estimate the time complexity of the Algorithm ECL. The only remaining issue that needs clarification is the size of the numbers x and y.

Theorem 4

During the execution of Algorithm ECL we always have $|x_\ell| \leqslant b/(2d)$ and $|y_\ell| \leqslant a/(2d)$ for $\ell = 0, \ldots i$, where i is the smallest number such that $r_{i+1} = 0$.

Proof. By construction, all $x_\ell,\, y_\ell \in \mathbb{Z}$. Let D_ℓ be the determinant

$$D_\ell =_{df} \begin{vmatrix} x_\ell & y_\ell \\ x_{\ell+1} & y_{\ell+1} \end{vmatrix} .$$

GCD IX

Then we obtain

$$\begin{aligned}
D_{\ell+1} &= \begin{vmatrix} x_{\ell+1} & y_{\ell+1} \\ x_{\ell+2} & y_{\ell+2} \end{vmatrix} = \begin{vmatrix} x_{\ell+1} & y_{\ell+1} \\ x_{\ell} - q_{\ell+1}x_{\ell+1} & y_{\ell} - q_{\ell+1}y_{\ell+1} \end{vmatrix} \\
&= \begin{vmatrix} x_{\ell+1} & y_{\ell+1} \\ x_{\ell} & y_{\ell} \end{vmatrix} = -D_{\ell}\ .
\end{aligned}$$

GCD IX

Then we obtain

$$
\begin{aligned}
D_{\ell+1} &= \begin{vmatrix} x_{\ell+1} & y_{\ell+1} \\ x_{\ell+2} & y_{\ell+2} \end{vmatrix} = \begin{vmatrix} x_{\ell+1} & y_{\ell+1} \\ x_\ell - q_{\ell+1}x_{\ell+1} & y_\ell - q_{\ell+1}y_{\ell+1} \end{vmatrix} \\
&= \begin{vmatrix} x_{\ell+1} & y_{\ell+1} \\ x_\ell & y_\ell \end{vmatrix} = -D_\ell\,.
\end{aligned}
$$

We have $D_0 = 1$ and so $D_\ell = (-1)^\ell$ for all $\ell = 0, \ldots, i$. Since $D_\ell = x_\ell y_{\ell+1} - y_\ell x_{\ell+1} = (-1)^\ell$, we see that $\gcd(x_\ell, y_\ell) = 1$. By Equality (2) we know that $ax_{i+1} + by_{i+1} = r_{i+1} = 0$. Thus, $ax_{i+1} = -by_{i+1}$, and dividing this equality by $d = \gcd(a, b)$ gives us $(a/d)x_{i+1} = -(b/d)y_{i+1}$. Since $\gcd(a/d, b/d) = 1$ and $\gcd(x_{i+1}, y_{i+1}) = 1$, we obtain $x_{i+1} = \pm b/d$ and $y_{i+1} = \pm a/d$. The appropriate signs are determined by observing that the signs of the sequences (x_ℓ) and (y_ℓ) alternate for $\ell \geqslant 2$.

GCD X

From the recursive definition of the integers x_ℓ, we see that $x_2 = 1$, $x_3 = -q_2$, $x_4 = 1 + q_3 q_2$, and in general $|x_\ell| < |x_{\ell+1}|$ for all $\ell \geqslant 3$. Analogously, we have $|y_\ell| < |y_{\ell+1}|$ for all $\ell \geqslant 3$. Finally, $x_{i+1} = x_{i-1} - q_i x_i$, and thus

$$|q_i x_i| = |x_{i-1} - x_{i+1}| \leqslant |x_{i+1}| = |b/d| \, .$$

Since $r_{i+1} = 0$ and $q_i = \lfloor r_{i-1}/r_i \rfloor$, we must have $q_i \geqslant 2$. Hence, $|x_i| \leqslant b/(2d)$. Similarly, one obtains that $|y_i| \leqslant a/(2d)$. $\blacksquare$

GCD X

From the recursive definition of the integers x_ℓ, we see that $x_2 = 1$, $x_3 = -q_2$, $x_4 = 1 + q_3 q_2$, and in general $|x_\ell| < |x_{\ell+1}|$ for all $\ell \geqslant 3$. Analogously, we have $|y_\ell| < |y_{\ell+1}|$ for all $\ell \geqslant 3$. Finally, $x_{i+1} = x_{i-1} - q_i x_i$, and thus

$$|q_i x_i| = |x_{i-1} - x_{i+1}| \leqslant |x_{i+1}| = |b/d| \,.$$

Since $r_{i+1} = 0$ and $q_i = \lfloor r_{i-1}/r_i \rfloor$, we must have $q_i \geqslant 2$. Hence, $|x_i| \leqslant b/(2d)$. Similarly, one obtains that $|y_i| \leqslant a/(2d)$. ∎

Consequently, we arrive at the following theorem:

Theorem 5

The time complexity of Algorithm ECL is $O((\log a)^3)$.

Modular Inverse I

The following theorem completely characterizes the existence of modular inverses:

Theorem 6

The congruence $ax \equiv 1 \mod m$ *is solvable iff* $\gcd(a, m) = 1$. *Moreover, if* $ax \equiv 1 \mod m$ *is solvable, then the solution is uniquely determined.*

Modular Inverse I

The following theorem completely characterizes the existence of modular inverses:

Theorem 6

The congruence $ax \equiv 1 \mod m$ *is solvable iff* $\gcd(a, m) = 1$. *Moreover, if* $ax \equiv 1 \mod m$ *is solvable, then the solution is uniquely determined.*

Proof. First, assume $\gcd(a, m) = 1$. We have to show that $ax \equiv 1 \mod m$ is solvable.
Since $\gcd(a, m) = 1$, there are integers x, y such that $1 = ax + my$. Hence, m divides $1 - ax$, i.e., $ax \equiv 1 \mod m$.
Thus, $x \mod m$ is the wanted solution.

Modular Inverse II

Next, assume $ax \equiv 1 \mod m$ to be solvable.
Hence, there exists an x_0 such that $ax_0 \equiv 1 \mod m$.

Consequently, m divides $ax_0 - 1$, and therefore, there exists a y such that $my = ax_0 - 1$.

Modular Inverse II

Next, assume $ax \equiv 1 \mod m$ to be solvable.
Hence, there exists an x_0 such that $ax_0 \equiv 1 \mod m$.

Consequently, m divides $ax_0 - 1$, and therefore, there exists a y such that $my = ax_0 - 1$.

Let d be any natural number dividing both m and a. Dividing the left side of the latter equation by d leaves the remainder 0. Hence, dividing the right side must also yield the remainder 0. Since $d|a$, we may conclude $d|1$, and thus $d = 1$.

Modular Inverse III

Finally, assume $ax \equiv 1 \mod m$ to be solvable. Suppose, there are solutions $x_1,\ x_2$. Thus, we have

$$
\begin{aligned}
ax_1 &\equiv 1 \mod m \qquad (6)\\
ax_2 &\equiv 1 \mod m \qquad (7)
\end{aligned}
$$

By our Theorem 2, we can subtract (7) from (6) and obtain $a(x_1 - x_2) \equiv 0 \mod m$, i.e., m divides $a(x_1 - x_2)$. Since $\gcd(a, m) = 1$, we may conclude that m divides $x_1 - x_2$, i.e., $x_1 \equiv x_2 \mod m$. Thus, the solution is unique modulo m. ∎

Modular Inverse IV

Question

What can be said about the complexity of computing modular inverses?

Modular Inverse IV

Question

What can be said about the complexity of computing modular inverses?

The answer is given by the following theorem:

Theorem 7

Modular inverse can be computed in time $O(\max\{\log a, \log m\}^3)$.

Modular Inverse IV

Question

What can be said about the complexity of computing modular inverses?

The answer is given by the following theorem:

Theorem 7

Modular inverse can be computed in time $O(\max\{\log a, \log m\}^3)$.

Proof. As the proof of Theorem 6 shows, all we have to do is to apply Algorithm ECL presented above. Thus, the assertion follows. ∎

Remarks

By Theorem 6 it is appropriate to consider

$$\mathbb{Z}_m^* = \{[a] \in \mathbb{Z}_m \mid \gcd(a, m) = 1\} .$$

Note that Theorem 6 directly implies that $(\mathbb{Z}_m^*, \cdot)$ constitutes a *finite Abelian group* (cf. Definition 1).

Remarks

By Theorem 6 it is appropriate to consider

$$\mathbb{Z}_m^* = \{[a] \in \mathbb{Z}_m \mid \gcd(a, m) = 1\} .$$

Note that Theorem 6 directly implies that $(\mathbb{Z}_m^*, \cdot)$ constitutes a *finite Abelian group* (cf. Definition 1).

Again, we simplify notation and refer to $(\mathbb{Z}_m^*, \cdot)$ as to $\mathbb{Z}_m^*$ for short. Furthermore, we usually omit the brackets when referring to members of $\mathbb{Z}_m$ and $\mathbb{Z}_m^*$, respectively.

That is, we write $a \in \mathbb{Z}_m$ and $a \in \mathbb{Z}_m^*$ instead of $[a] \in \mathbb{Z}_m$ and of $[a] \in \mathbb{Z}_m^*$, respectively.

Divisibility I

In order to get more familiarity with the congruence relation "$\equiv$", let us derive a rule for deciding whether or not an integer given in decimal notation is divisible by 3.

Divisibility I

In order to get more familiarity with the congruence relation "$\equiv$", let us derive a rule for deciding whether or not an integer given in decimal notation is divisible by 3.

Since the divisibility by 3 is not affected by the sign, it suffices to consider

$$z = \sum_{i=0}^{n} z_i 10^i ,$$

where $z_i \in \{0, 1, \ldots, 9\}$ for all $i = 0, \ldots, n$.

Divisibility II

Then, by the reflexivity of "$\equiv$" we have

$$z_i \equiv z_i \mod 3 \tag{8}$$

for all $i = 0, \ldots, n$. Moreover, $10 \equiv 1 \mod 3$ and thus by Property (4) of Theorem 2 we know that

$$10^i \equiv 1^i \equiv 1 \mod 3 \quad \text{for all } i = 0, \ldots, n\,. \tag{9}$$

Next, we apply Property (1) of Theorem 2 to (8) and (9) exactly n many times and obtain

$$\sum_{i=0}^{n} z_i 10^i \equiv \sum_{i=0}^{n} z_i \mod 3\,.$$

Divisibility III

Consequently, we directly get the following theorem:

Theorem 8

A number given in decimal notation is divisible by 3 if and only if the sum of its digits is divisible by 3.

Divisibility III

Consequently, we directly get the following theorem:

Theorem 8

A number given in decimal notation is divisible by 3 if and only if the sum of its digits is divisible by 3.

The proof given above directly allows for a corollary concerning the divisibility by 9. By reflexivity we also have

$$z_i \equiv z_i \mod 9 \tag{10}$$

and (9) also holds modulo 9, i.e.,

$$10^i \equiv 1^i \equiv 1 \mod 9 \quad \text{for all } i = 0, \ldots, n\,. \tag{11}$$

Thus, putting (10) and (11) together directly yields the following corollary:

Divisibility IV

Corollary 2

A number given in decimal notation is divisible by 9 if and only if the sum of its digits is divisible by 9.

Divisibility V

In order to see that decimal notation is crucial here, let us consider numbers given in binary, i.e., $z = \sum_{i=0}^{n} z_i 2^i$, where $z_i \in \{0,1\}$ for all $i = 0, \ldots, n$. Again, we have

$$z_i \equiv z_i \mod 3 \tag{12}$$

as before, but (9) translates into

$$2^i \equiv (-1)^i \mod 3 \quad \text{for all } i = 0, \ldots, n\,. \tag{13}$$

Thus, now we get

$$\sum_{i=0}^{n} z_i 2^i \equiv \sum_{i=0}^{n} (-1)^n z_i \mod 3\,.$$

Divisibility V

In order to see that decimal notation is crucial here, let us consider numbers given in binary, i.e., $z = \sum_{i=0}^{n} z_i 2^i$, where $z_i \in \{0,1\}$ for all $i = 0, \ldots, n$. Again, we have

$$z_i \equiv z_i \mod 3 \tag{12}$$

as before, but (9) translates into

$$2^i \equiv (-1)^i \mod 3 \quad \text{for all } i = 0, \ldots, n\,. \tag{13}$$

Thus, now we get

$$\sum_{i=0}^{n} z_i 2^i \equiv \sum_{i=0}^{n} (-1)^n z_i \mod 3\,.$$

Consequently, a number given in binary notation is divisible by 3 if and only if the alternating sum of its digits is divisible by 3.

Chinese Remaindering I

Finally, we prove an important theorem that will be needed later. Before we can present it, we need the following definition:

Definition 6

Integers a and b are said to be *relatively prime* if $\gcd(a, b) = 1$.

Integers $m_1, \ldots, m_r$ are said to be *pairwise relatively prime* if every pair m_i, m_j, $i \neq j$ is relatively prime.

Chinese Remaindering II

Theorem 9

Let $m_1, \ldots, m_r$ *be pairwise relatively prime numbers, and let* $M = \prod_{i=1}^{r} m_i$. *Furthermore, let* $a_1, \ldots, a_r$ *be any integers. Then there is a unique* $y \in \mathbb{Z}_M$ *such that* $y \equiv a_i \mod m_i$ *for* $i = 1, \ldots, r$. *Moreover,* y *can be computed in time polynomial in the length of the input.*

Chinese Remaindering III

Proof. For each $i = 1, \ldots, r$, we set $n_i = M/m_i$. Then for all $i = 1, \ldots, r$, the number n_i satisfies $n_i \in \mathbb{N}$, and $\gcd(m_i, n_i) = 1$.

Chinese Remaindering III

Proof. For each $i = 1, \ldots, r$, we set $n_i = M/m_i$. Then for all $i = 1, \ldots, r$, the number n_i satisfies $n_i \in \mathbb{N}$, and $\gcd(m_i, n_i) = 1$. Consequently, the modular inverses n_i^{-1} modulo m_i do exist for all $i = 1, \ldots, r$.

Chinese Remaindering III

Proof. For each $i = 1, \ldots, r$, we set $n_i = M/m_i$. Then for all $i = 1, \ldots, r$, the number n_i satisfies $n_i \in \mathbb{N}$, and $\gcd(m_i, n_i) = 1$. Consequently, the modular inverses n_i^{-1} modulo m_i do exist for all $i = 1, \ldots, r$. Now, let

$$\hat{y} = \sum_{i=1}^{r} n_i \cdot n_i^{-1} \cdot a_i$$

and let y be $\hat{y}$ reduced modulo M. Taking into account that $m_i | n_j$ for all $i = 1, \ldots, r$, $j = 1, \ldots, r$, provided $j \neq i$, we conclude

$$y \equiv \hat{y} \equiv n_i n_i^{-1} a_i \equiv a_i \mod m_i \ .$$

Thus, we have found a number y simultaneously fulfilling all the wanted congruences.

Chinese Remaindering IV

It remains to show that y is uniquely determined modulo M.

Chinese Remaindering IV

It remains to show that y is uniquely determined modulo M.

Suppose the converse; i.e., there exists an x such that $x \equiv a_i \mod m_i$ for $i = 1, \ldots, r$ and $x \not\equiv y \mod M$.
Subtracting $y \equiv a_i \mod m_i$ from $x \equiv a_i \mod m_i$ for all $i = 1, \ldots, r$ yields $x - y \equiv 0 \mod m_i$ for all $i = 1, \ldots, r$, and thus m_i divides $x - y$.

Chinese Remaindering IV

It remains to show that y is uniquely determined modulo M.

Suppose the converse; i.e., there exists an x such that $x \equiv a_i \mod m_i$ for $i = 1, \ldots, r$ and $x \not\equiv y \mod M$. Subtracting $y \equiv a_i \mod m_i$ from $x \equiv a_i \mod m_i$ for all $i = 1, \ldots, r$ yields $x - y \equiv 0 \mod m_i$ for all $i = 1, \ldots, r$, and thus m_i divides $x - y$.

However, all the m_i are pairwise relatively prime. Hence, $\prod_{i=1}^{r} m_i$ must divide $(x - y)$, too. But this means

$$x - y \equiv 0 \mod M ,$$

a contradiction. Thus, y is uniquely determined modulo M.

Chinese Remaindering V

Finally, by Theorem 7 we know that the modular inverses can be each computed in time polynomial in the input. All other computations, i.e., multiplication, addition and reduction modulo M are known to be performable in polynomial time, too. $\blacksquare$

Chinese Remaindering V

Finally, by Theorem 7 we know that the modular inverses can be each computed in time polynomial in the input. All other computations, i.e., multiplication, addition and reduction modulo M are known to be performable in polynomial time, too. $\blacksquare$

Please solve the exercises and the problem set given in the book.

Thank you!

Generating Functions I

Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of real (or complex) numbers. Then

$$g(z) = \sum_{n=0}^{\infty} a_n z^n$$

is called *generating function* of $(a_n)_{n\in\mathbb{N}}$. The following theorem is often applied to generating functions:

Generating Functions I

Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of real (or complex) numbers. Then

$$g(z) = \sum_{n=0}^{\infty} a_n z^n$$

is called *generating function* of $(a_n)_{n\in\mathbb{N}}$. The following theorem is often applied to generating functions:

Theorem 10

Let $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ be any sequences such that that their generating functions have a radius $r > 0$ of convergence. Then

$$\sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} b_n z^n$$

if and only if $a_n = b_n$ for all $n \in \mathbb{N}$.

Generating Functions II

Moreover, recall that power series can be differentiated by differentiating their summands. Thus, we also know that

$$g'(z) = \sum_{n=0}^{\infty} n \cdot a_n z^{n-1} .$$

Generating Functions II

Moreover, recall that power series can be differentiated by differentiating their summands. Thus, we also know that

$$g'(z) = \sum_{n=0}^{\infty} n \cdot a_n z^{n-1} .$$

Now, let $(a_n)_{n\in\mathbb{N}}$ be the Fibonacci sequence. Thus, we have the generating function

$$g(z) = \sum_{n=0}^{\infty} a_n z^n$$

which we use as follows:

Generating Functions III

$$\begin{aligned}
g(z) &= \sum_{n=0}^{\infty} a_n z^n = 1 + z + \sum_{n=2}^{\infty} a_n z^n \\
&= 1 + z + \sum_{n=2}^{\infty} (a_{n-1} + a_{n-2}) z^n \\
&= 1 + z + \sum_{n=2}^{\infty} a_{n-1} z^n + \sum_{n=2}^{\infty} a_{n-2} z^n \\
&= 1 + z + z \cdot \sum_{n=2}^{\infty} a_{n-1} z^{n-1} + z^2 \cdot \sum_{n=2}^{\infty} a_{n-2} z^{n-2} \\
&\quad (*\text{changing the summation indices yields}*) \\
&= 1 + z + z \cdot \left(\sum_{n=0}^{\infty} a_n z^n - 1 \right) + z^2 \cdot \sum_{n=0}^{\infty} a_n z^n \,.
\end{aligned}$$

Generating Functions IV

Next, we replace $\sum_{n=0}^{\infty} a_n z^n$ by $g(z)$ and obtain

$$g(z) = 1 + z - z + zg(z) + z^2 g(z) = 1 + zg(z) + z^2 g(z)\ .$$

Hence, we arrive at

$$g(z) = \frac{1}{1 - z - z^2}\ .$$

Thus, we have found a representation of g as a rational function.

Generating Functions V

All that is left for applying Theorem 10 is to develop this rational function in a power series. For that purpose, we have to calculate the zeros of the denominator. Solving

$$0 = z^2 + z - 1$$

directly yields

$$z_{0,1} = -\frac{1}{2} \pm \sqrt{\frac{1}{4} + 1}\,.$$

Next, we set

$$\alpha = \frac{-1 + \sqrt{5}}{2}$$

and

$$\widehat{\alpha} = \frac{-1 - \sqrt{5}}{2}\,.$$

Generating Functions VI

Now, we write

$$\frac{1}{1-z-z^2} = \frac{1}{(z-\alpha)(\widehat{\alpha}-z)} = \frac{A}{z-\alpha} + \frac{B}{\widehat{\alpha}-z}\,.$$

Generating Functions VI

Now, we write

$$\frac{1}{1-z-z^2} = \frac{1}{(z-\alpha)(\widehat{\alpha}-z)} = \frac{A}{z-\alpha} + \frac{B}{\widehat{\alpha}-z}\,.$$

An easy calculation yields $A = B = -\frac{1}{\sqrt{5}}$, and consequently we have

$$g(z) = -\frac{1}{\sqrt{5}}\frac{1}{(z-\alpha)} - \frac{1}{\sqrt{5}}\frac{1}{(\widehat{\alpha}-z)}\,.$$

Generating Functions VII

Recalling that

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$$

we can write

$$\frac{1}{z-\alpha} = -\frac{1}{\alpha} \cdot \frac{1}{1-\frac{1}{\alpha}z} = -\frac{1}{\alpha}\sum_{n=0}^{\infty} \frac{1}{\alpha^n} z^n$$

and

$$\frac{1}{\widehat{\alpha}-z} = \frac{1}{\widehat{\alpha}} \cdot \frac{1}{1-\frac{1}{\widehat{\alpha}}z} = \frac{1}{\widehat{\alpha}}\sum_{n=0}^{\infty} \frac{1}{\widehat{\alpha}^n} z^n .$$

Generating Functions VIII

This yields the desired power series for g; i.e., we get

$$
\begin{aligned}
g(z) &= \sum_{n=0}^{\infty} a_n z^n \\
&= \frac{1}{\sqrt{5}\cdot\alpha}\sum_{n=0}^{\infty}\frac{1}{\alpha^n}z^n - \frac{1}{\sqrt{5}\cdot\widehat{\alpha}}\sum_{n=0}^{\infty}\frac{1}{\widehat{\alpha}^n}z^n \\
&= \frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}\frac{1}{\alpha^{n+1}}z^n - \frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}\frac{1}{\widehat{\alpha}^{n+1}}z^n \\
&= \sum_{n=0}^{\infty}\left[\frac{1}{\sqrt{5}}\left(\frac{1}{\alpha^{n+1}} - \frac{1}{\widehat{\alpha}^{n+1}}\right)\right]z^n .
\end{aligned}
$$

Generating Functions IX

Thus, by Theorem 10 we obtain

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1}{\alpha^{n+1}} - \frac{1}{\widehat{\alpha}^{n+1}}\right)$$

Finally, putting this all together, after a short calculation we arrive at

$$a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right) . \tag{14}$$