Discrete Mathematics

Sylwia Cichacz

Akademia Górniczo-Hutnicza w Krakowie

October 24, 2021, Kraków

Literature

1. R. J. Wilson, Wprowadzenie do teorii grafów, PWN, Warszawa, 2002
2. K.H. Rosen, Discrete Mathematics & Its Applications (7th Edition).
3. R.A. Brualdi, Introductory combinatorics 5th Edition, Prentice Hall 2010.

Symbols

$\forall$ for all

$\exists$ exists

$\exists!$ exists exactly one

$\mathbb{N} = \{0, 1, 2, \ldots\}$

$\mathbb{N}^+$ – set of positive natural numbers

$\mathbb{Z} = \{x : x \in \mathbb{N} \lor -x \in \mathbb{N}\}$ – set of integers

$\mathbb{Q} = \{x : x = \frac{a}{b},\ a, b \in \mathbb{Z}, b \neq 0\}$ – set of rational numbers

$\mathbb{R}$ – set of real numbers

$\mathbb{R}^+$, the set of positive real numbers

$\mathbb{C}$, the set of complex numbers

$$\sum_{i=1}^{k} a_i = a_1 + a_2 + \ldots + a_k$$

$$\prod_{i=1}^{k} a_i = a_1 \cdot a_2 \cdot \ldots \cdot a_k$$

Definition:

A prime number is a positive integer that has no divisors other than and itself.

Definition:

A prime number is a positive integer that has no divisors other than and itself.

$\mathbb{P}$ – the set of all prime numbers (there is infinite number of primes)

Prime numbers

Definition:

A prime number is a positive integer that has no divisors other than and itself.

$\mathbb{P}$ – the set of all prime numbers (there is infinite number of primes)

Example:

Goldbach Conjecture

Every even integer can be written as sum of two primes.

Prime numbers

Definition:

A prime number is a positive integer that has no divisors other than and itself.

$\mathbb{P}$ – the set of all prime numbers (there is infinite number of primes)

Example:

Goldbach Conjecture

Every even integer can be written as sum of two primes.

The best result is by Chen (1966) Every even number is either

Prime numbers

Definition:

A prime number is a positive integer that has no divisors other than and itself.
$\mathbb{P}$ – the set of all prime numbers (there is infinite number of primes)

Example:

Goldbach Conjecture

Every even integer can be written as sum of two primes.

The best result is by Chen (1966) Every even number is either

(i) sum of two primes or

Definition:

A prime number is a positive integer that has no divisors other than and itself.
$\mathbb{P}$ – the set of all prime numbers (there is infinite number of primes)

Example:

Goldbach Conjecture

Every even integer can be written as sum of two primes.

The best result is by Chen (1966) Every even number is either

(i) sum of two primes or
(ii) sum of a prime and a product of two primes.

Theorem: THE DIVISION ALGORITHM

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.

Theorem: THE DIVISION ALGORITHM

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Definition:

For a positive integer n, two integers a and b are said to be congruent modulo n, written:

$$a \equiv b \pmod{n},$$

if their difference $a - b$ is an integer multiple of n.
We say that $a \equiv b \pmod{n}$ is a congruence and that m is its modulus (plural **moduli**).

Theorem: THE DIVISION ALGORITHM

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Definition:

For a positive integer n, two integers a and b are said to be congruent modulo n, written:

$$a \equiv b \pmod{n},$$

if their difference $a - b$ is an integer multiple of n.
We say that $a \equiv b \pmod{n}$ is a congruence and that m is its modulus (plural **moduli**).
$a \equiv b \pmod{n}$ can also be thought of as asserting that both **divisions** a/n and b/n have the same remainder.

Example:

$-3 \equiv 11 \pmod{7}$

Theorem:

If integers a_1 and a_2 are such that $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then:

Theorem:

If integers a_1 and a_2 are such that $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then:

- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$,

Theorem:

If integers a_1 and a_2 are such that $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then:

- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$,
- $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$,

Theorem:

If integers a_1 and a_2 are such that $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then:

- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$,
- $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$,
- $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Theorem:

The following are equivalent.

1. $a \equiv b \pmod{n}$,
2. $a = b + nt$ for some integer t,
3. a and b have the same remainder when divided by n.

Greatest common divisor

Definition:

The greatest common divisor (gcd), also known as the greatest common factor (gcf) of two or more non-zero integers, is the largest positive integer that divides the numbers without a remainder.

Definition:

The greatest common divisor (gcd), also known as the greatest common factor (gcf) of two or more non-zero integers, is the largest positive integer that divides the numbers without a remainder.

Example:

$\gcd(18, 24) =$

Greatest common divisor

Definition:

The greatest common divisor (gcd), also known as the greatest common factor (gcf) of two or more non-zero integers, is the largest positive integer that divides the numbers without a remainder.

Example:

$\gcd(18, 24) =$

Definition:

The integers a and b are relatively prime if their greatest common divisor is 1.

Definition:

The greatest common divisor (gcd), also known as the greatest common factor (gcf) of two or more non-zero integers, is the largest positive integer that divides the numbers without a remainder.

Example:

$\gcd(18, 24) =$

Definition:

The integers a and b are relatively prime if their greatest common divisor is 1.

Example:

$\gcd(7, 24) =$

The Euclidean Algorithm

From Wikipedia

The Euclidean Algorithm

Given: $a, b \in \mathbb{Z} \setminus \{0\}$

Given: $a, b \in \mathbb{Z} \setminus \{0\}$
Find: $\gcd(a, b)$

Given: $a, b \in \mathbb{Z} \setminus \{0\}$
Find: $\gcd(a, b)$

Note: $\gcd(|a|, |b|) = \gcd(a, b)$, with $a \geq b > 0$.

The Euclidean Algorithm

Given: $a, b \in \mathbb{Z} \setminus \{0\}$
Find: $\gcd(a, b)$

Note: $\gcd(|a|, |b|) = \gcd(a, b)$, with $a \geq b > 0$.

Step 1. If $b = 0$ return a

The Euclidean Algorithm

Given: $a, b \in \mathbb{Z} \setminus \{0\}$
Find: $\gcd(a, b)$

Note: $\gcd(|a|, |b|) = \gcd(a, b)$, with $a \geq b > 0$.

Step 1. If $b = 0$ return a

Step 2. Since $a > 0$ write $a = bq + r$ with $r \in \{0, 1, \ldots, a - 1\}$.
Replace (a, b) with (b, r) and go to **Step 1**.

The Euclidean Algorithm

$$a = q_0 b + r_0$$

The Euclidean Algorithm

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

The Euclidean Algorithm

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

The Euclidean Algorithm

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\dots$$

Example:

Find $\gcd(121, 114)$.

Theorem:

Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Example:

Find $\gcd(54, 102)$.

Bézout's Theorem

From Wikipedia

From Wikipedia

Theorem: Bézout's Theorem

For any integers a, b there exist integers α, β such that:

$$\gcd(a, b) = \alpha \cdot a + \beta \cdot b.$$

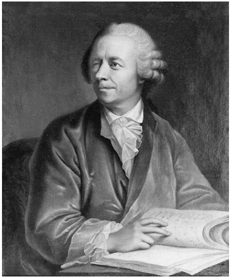
Example:

Find α, β such that: $\gcd(121, 114) = \alpha \cdot 121 + \beta \cdot 114$.

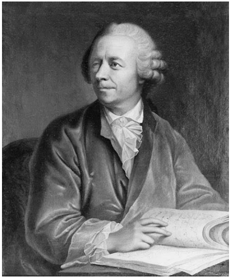
Example:

Find α, β such that: $\gcd(54, 102) = \alpha \cdot 54 + \beta \cdot 102$.

Euler's totient



From Wikipedia



From Wikipedia

Definition:

Euler's totient or phi function, $\varphi(n)$ is an arithmetic function that counts the number of positive integers less than or equal to n that are relatively prime to n.

Example:

$\varphi(5) =$

Example:

$\varphi(5) = 4$
$\varphi(9) =$

Euler's totient

Theorem:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product is over the distinct prime numbers dividing n.

Euler's totient

Theorem:

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right),$$

where the product is over the distinct prime numbers dividing n.

Example:

Count $\varphi(450)$.

Theorem:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product is over the distinct prime numbers dividing n.

Example:

Count $\varphi(450)$.

Theorem:

If $n = p \cdot q$, where p, q are different primes, then
$\varphi(n) = (p - 1)(q - 1)$.

Theorem: Chinese remainder theorem

Suppose $m_1, m_2, \dots, m_k$ are positive integers which are pairwise coprime. Then, for any given sequence of integers $a_1, a_2, \dots, a_k$, there exists an integer x solving the following system of congruences:

$$\begin{cases} x \equiv a_1 \pmod{m}_1 \\ x \equiv a_2 \pmod{m}_2 \\ \dots \\ x \equiv a_k \pmod{m}_k \end{cases} \qquad (\star)$$

Furthermore, all solutions x of this system are congruent modulo the product, $M = m_1 m_2 \dots m_k$. Hence $x \equiv y \pmod{m}_i$ for all $1 \le i \le k$, if and only if $x \equiv y \pmod{M}$.

Example:

Solve the system

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 5 \pmod{6} \end{cases}$$

Let:

$M = m_1 m_2 \dots m_k$

Let:

$M = m_1 m_2 \dots m_k$

$M_i = \frac{M}{m_i}$ for $i \in \{1, 2, \dots, k\}$

Let:

$M = m_1 m_2 \ldots m_k$

$M_i = \frac{M}{m_i}$ for $i \in \{1, 2, \ldots, k\}$

Note: $\gcd(M_i, m_i) = 1 \ \forall i \in \{1, 2, \ldots, k\}$

Let:
$M = m_1 m_2 \dots m_k$
$M_i = \frac{M}{m_i}$ for $i \in \{1, 2, \dots, k\}$
Note: $\gcd(M_i, m_i) = 1 \; \forall i \in \{1, 2, \dots, k\}$
Thus $\exists \alpha_i, \beta_i : \alpha_i \cdot M_i + \beta_i \cdot m_i = 1$

Let:

$M = m_1 m_2 \dots m_k$

$M_i = \frac{M}{m_i}$ for $i \in \{1, 2, \dots, k\}$

Note: $\gcd(M_i, m_i) = 1 \ \forall i \in \{1, 2, \dots, k\}$

Thus $\exists \alpha_i, \beta_i : \alpha_i \cdot M_i + \beta_i \cdot m_i = 1$

Then: $\alpha_i \cdot M_i \equiv 1 \pmod{m_i}$ and $\alpha_i \cdot M_i \equiv 0 \pmod{m_j}$ for $i \neq j$

Let:
$M = m_1 m_2 \dots m_k$
$M_i = \frac{M}{m_i}$ for $i \in \{1, 2, \dots, k\}$
Note: $\gcd(M_i, m_i) = 1 \ \forall i \in \{1, 2, \dots, k\}$
Thus $\exists \alpha_i, \beta_i : \alpha_i \cdot M_i + \beta_i \cdot m_i = 1$
Then: $\alpha_i \cdot M_i \equiv 1 \pmod{m_i}$ and $\alpha_i \cdot M_i \equiv 0 \pmod{m_j}$ for $i \neq j$
Hence

$$x = \sum_{i=1}^{k} a_i \cdot \alpha_i \cdot M_i$$

is solution of system $(\star)$ modulo M

Example:

Solve the system

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 0 \pmod{4} \\ x \equiv 8 \pmod{25} \end{cases}$$

Fermat's Little Theorem

From Wikipedia

From Wikipedia

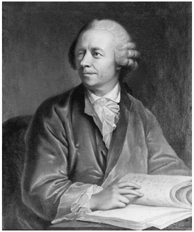
Theorem: Fermat's Little Theorem

If $p \in \mathbb{P}$ and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every integer n we have

$$n^{p} \equiv n \pmod{p}.$$

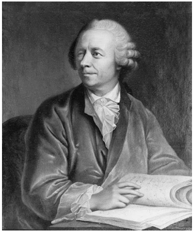


From Wikipedia

Theorem: Euler's Totient Theorem

If n and a are coprime positive integers, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$



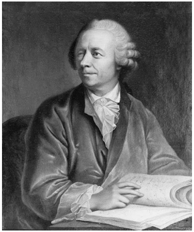
From Wikipedia

Theorem: Euler's Totient Theorem

If n and a are coprime positive integers, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

If $p \in \mathbb{P}$ then $\varphi(p) = p - 1$ thus Fermat's Little Theorem follows from Euler's Totient Theorem.



From Wikipedia

Theorem: Euler's Totient Theorem

If n and a are coprime positive integers, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Example:

$(34)^{67} \pmod{15} =$