Integers

Intro to Number Theory

Number theory is the theory of integers and their properties.

The principles of number theory
- divisibility,
- greatest common divisors (gcd),
- least common multiples (lcm), and
- modular arithmetic

And some related algorithms.

Division

Definition. If **a** and **b** are integers such that **a** $\neq 0$, we say that **a** divides **b** if there is an integer **c** such that **b = ac**. If a divides **b**, then we say that **a** is a factor of **b** and that **b** is a multiple of **a**.

Notation **a | b means a divides** b.

Notation **a $\not|$ b means a does not divide** b.

Divisibility

Theorem. For integers a, b, and c, the following holds

1. if a|b and a|c, then a|(b + c)
2. if a|b, then a|bc for any integer c
3. if a|b and b|c, then a|c

Corollary. If a, b, and c are integers such that a|b and a|c, then a|(mb+nc), where m and n are integers.

Illustration

- **Division theorem**:
- if a | b and a | c, then a | (b + c)

Example: 3 | 6 and 3 | 9, so 3 | 15.

- if a | b, then a | bc for any integer c

Example: 5 | 10, so 5 | 20, 5 | 30, 5 | 40, …

- if a | b and b | c, then a | c

Example: 4 | 8 and 8 | 24, then 4 | 24.

- **Corollary**
- If a|b and a|c, then a|(mb+nc), for integer a,b,c,m,n

Example: 3|6 and 3|12, take m=5, n=7, then 3|(5.6+ 7.12) → 3| (30+84) → 3|114

Prime Number

Definition. A positive integer p greater than one is called a prime number if the only positive factors of p are 1 and p.

A positive integer greater than 1 that is not a prime number is called a composite number.

Example:

Are the following numbers prime, composite, or neither?

-1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

Fundamental Theorem of Arithmetic

- Every positive integer can be written **uniquely as a product of prime numbers**, whose prime factors are written in increasing order.

Prime Numbers

Example

$15 = 3 \cdot 5$

$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$

$17 = 17$

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

$512 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^9$

$515 = 5 \cdot 103$

$28 = 2 \cdot 2 \cdot 7 = 2^2 \cdot 7$

Prime Numbers

Theorem. If n is a composite integer, then n has one prime divisor less than or equal to $\sqrt{n}$.

Reasoning: if n is composite, then n has two divisors p_1 and p_2 such that $p_1 p_2 = n$ and $p_1 \geq 2$and $p_2 \geq 2$.

p_1 and p_2 cannot both be greater than $\sqrt{n}$, because then $p_1 p_2$ would be greater than n.

If the numbers p_1 and p_2 are not themselves prime, then they can be decomposed into prime factors smaller than themselves but$\geq$ 2.

Infinite number of prime numbers

- **Theorem.** There are infinite prime numbers.

- This theorem was proven by Euclid in his book *Elements, using the technique of reductio ad absurdum* or proof by contradiction.

Proof: We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $p_1, p_2, \ldots, p_n$. Let

$$Q = p_1 p_2 \cdots p_n + 1.$$

By the fundamental theorem of arithmetic, Q is prime or else it can be written as the product of two or more primes. However, none of the primes p_j divides Q, for if $p_j \mid Q$, then p_j divides $Q - p_1 p_2 \cdots p_n = 1$. Hence, there is a prime not in the list $p_1, p_2, \ldots, p_n$. This prime is either Q, if it is prime, or a prime factor of Q. This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes. ◁

"*Reductio ad absurdum*, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game ". (G.H. Hardy, 1877-1947)

[Src: PPT Tao]

Chess Pieces: pawn, knight, bishop, rook, queen, king

*) Marsenne Primes

- Marsenne primes are prime numbers of the form 2^p-1, where p is a prime number.
- Not all Marsenne primes are true primes

- Mid 2002: largest primes $2^{13.466.917}$-1, which is 4 million digits long, found through the GIMPS (Great Internet Marsenne Prime Search) project

- Sept. 2015: the largest prime number is
  $2^{57.885.161}$ –1, whch is **17,425,170** digits long

*) Prime Number Theorem

- **Theorem.** The ratio of the number of primes not greater than x , π(x), to x/ln(x) approaches 1, as x grows without bound, or

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

Divisibility

Divisibility

Suppose **a** is an integer and **d** is a positive integer. Then there are unique integers **q** and **r**, with **0 ≤ r < d**, such that

$$a = dq + r$$

In the equation above:

- **d** is called the divisor,
- **a** is called the dividend,
- **q** is called the quotient, and
- **r** is called the remainder.

Divisibility

Example:

If we divide 17 by 5, we get $17 = 5.3 + 2$

17 is the dividend,
5 is the divisor,
3 is the quotient, and
2 is the remainder.

Divisibility of Division

Another example:

What if -11 is divided by 3?

Remember that remainder cannot be negative.

$-11 = 3.(-4) + 1$

-11 is the dividend,
3 is the divisor,
-4 is the quotient, and
1 is the remainder.

Greatest Common Divisors

Suppose **a** and **b** are integers that are not both zero. The largest integer **d** such that **d | a** and **d | b** is called the **greatest common divisor** of **a** and **b**.

The greatest common divisor of **a** and **b** is written as **gcd(a, b).**

Example 1: What is gcd(48, 72) ?
The positive common divisors of 48 and 72 are
1, 2, 3, 4, 6, 8, 12, 16, and 24, so gcd(48, 72) = 24.

Example 2: What is gcd(19, 72) ?
The only positive common divisor of 19 and 72 is
1, so gcd(19, 72) = 1.

Greatest Common Divisors

Using prime factorization

$a = p_1^{a_1}\ p_2^{a_2} \ldots p_n^{a_n}$, $b = p_1^{b_1}\ p_2^{b_2} \ldots p_n^{b_n}$,

where $p_1 < p_2 < \ldots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \le i \le n$

$\gcd(a, b) = p_1^{\min(a_1, b_1)}\ p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)}$

Example:

$a = 60 = 2^2\ 3^1\ 5^1$

$b = 54 = 2^1\ 3^3\ 5^0$

$\gcd(a, b) = 2^1\ 3^1\ 5^0 = 6$

Relatively Prime Number

Definition.
Two integers **a** and **b** are called relatively prime if gcd(a, b) = 1.

Example:
Are 15 and 28 relatively prime? Yes, gcd(15, 28) = 1.

Are 55 and 28 relatively prime? Yes, gcd(55, 28) = 1.

Are 35 and 28 relatively prime? No, gcd(35, 28) = $7 \neq 1$.

Pairwise Relatively Prime

Definition:
The numbers $a_1, a_2, \ldots, a_n$ are **pairwise relatively prime** numbers if $\gcd(a_i, a_j) = 1$ for $1 \leq i < j \leq n$.

Example:
Are 15, 17, and 27 relatively prime in pairs?
No, because gcd(15, 27) = 3.

Are 15, 17, and 28 relatively prime in pairs?
Yes, because gcd(15, 17) = 1, gcd(15, 28) = 1 and gcd(17, 28) =1.

Least Common Multiples (LCM)

Definition:

The least common multiple of positive integers a and b is the smallest positive integer that is divisible by both a and b.

The **least common multiple** of **a** and **b** is denoted as **lcm(a, b)**.

Example

lcm(3, 7) = 21

lcm(4, 6) = 12

lcm(5, 10) = 10

Least Common Multiples

Using prime factorization

$a = p_1^{a_1}\ p_2^{a_2} \ldots p_n^{a_n}$, $b = p_1^{b_1}\ p_2^{b_2} \ldots p_n^{b_n}$,
where $p_1 < p_2 < \ldots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \leq i \leq n$

$$\text{lcm}(a, b) = p_1^{\max(a_1, b_1)}\ p_2^{\max(a_2, b_2)} \ldots p_n^{\max(a_n, b_n)}$$

Example

$a = 60 = 2^2\ 3^1\ 5^1$

$b = 54 = 2^1\ 3^3\ 5^0$

$\text{lcm}(a, b) = 2^2\ 3^3\ 5^1 = 4 \cdot 27 \cdot 5 = 540$

GCD dan LCM

$a = 60 = 2^2 \; 3^1 \; 5^1$

$b = 54 = 2^1 \; 3^3 \; 5^0$

$\gcd(a, b) = 2^1 \, 3^1 \, 5^0 = 6$

$\text{lcm}(a, b) = 2^2 \, 3^3 \, 5^1 = 540$

Theorem: $a \cdot b = \gcd(a,b) \cdot \text{lcm}(a,b)$

Modular Arithmetics

Modular Arithmetics

Suppose **a** is an integer and **m** is a positive integer. The notation **a** mod **m** is the remainder if **a** is divided by **m**.

Example

9 mod 4 = 1

9 mod 3 = 0

9 mod 10 = 9

-13 mod 4 = 3

Congruent

Suppose **a** and b are integers and **m** is a positive integer. We **say a is congruent to b modulo m** if **m** divides **a – b**.

We use the notation **a ≡ b (mod m)** to say that **a** is congruent to **b modulo m.**

In other words:
a ≡ b (mod m) if and only if **a mod m = b mod m**.

Congruent

Examples:

Does $46 \equiv 68 \pmod{11}$?
Yes, 11 | (46 – 68).

Does $46 \equiv 68 \pmod{22}$?
Yes, 22 | (46 – 68).

For z integer, what is $z \equiv 12 \pmod{10}$?
Answer: $z \in \{\ldots,-28, -18, -8, 2, 12, 22, 32, \ldots\}$

Theorem: Let **m** be a positive integer. The integers **a** and **b** are congruent modulo **m** if and only if there is an integer k such that **a = b + km**.

Congruent

Theorem: Suppose *m* is positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, hence $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Proof:

We know that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies that there are integers s and t with $b = a + sm$ and $d = c + tm$.

Therefore,

$\mathbf{b + d} = (a + sm) + (c + tm) = (\mathbf{a + c}) + \mathbf{m}(s + t)$

and $\mathbf{bd} = (a + sm)(c + tm) = \mathbf{ac} + \mathbf{m}(at + cs + stm)$.

Thus, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Mathematician of The Day

KARL FRIEDRICH GAUSS (1777–1855) Karl Friedrich Gauss, the son of a bricklayer, was a child prodigy. He demonstrated his potential at the age of 10, when he quickly solved a problem assigned by a teacher to keep the class busy. The teacher asked the students to find the sum of the first 100 positive integers. Gauss realized that this sum could be found by forming 50 pairs, each with the sum 101: $1 + 100, 2 + 99, \ldots, 50 + 51$. This brilliance attracted the sponsorship of patrons, including Duke Ferdinand of Brunswick, who made it possible for Gauss to attend Caroline College and the University of Göttingen. While a student, he invented the method of least squares, which is used to estimate the most likely value of a variable from experimental results. In 1796 Gauss made a fundamental discovery in geometry, advancing a subject that had not advanced since ancient times. He showed that a 17-sided regular polygon could be drawn using just a ruler and compass.

In 1799 Gauss presented the first rigorous proof of the fundamental theorem of algebra, which states that a polynomial of degree n has exactly n roots (counting multiplicities). Gauss achieved worldwide fame when he successfully calculated the orbit of the first asteroid discovered, Ceres, using scanty data.

Gauss was called the Prince of Mathematics by his contemporary mathematicians. Although Gauss is noted for his many discoveries in geometry, algebra, analysis, astronomy, and physics, he had a special interest in number theory, which can be seen from his statement "Mathematics is the queen of the sciences, and the theory of numbers is the queen of mathematics." Gauss laid the foundations for modern number theory with the publication of his book *Disquisitiones Arithmeticae* in 1801.