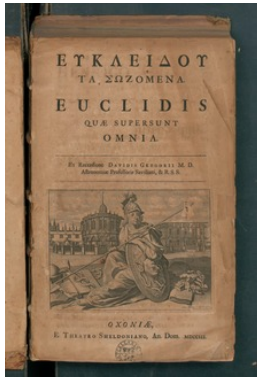
Session 53: Division

- Division
- Properties of Division
- Division Algorithm

Some History of Number Theory

- Euclid: wrote the most successful mathematics book ever “The Elements” (over 1000 editions)
- Gauss: “mathematics is the queen of sciences, number theory is the queen of mathematics”
- Wiles: proved Fermat’s last theorem (358 years after it was conjectured)
- Tao: proved famous theorem on arbitrarily long arithmetic progressions of primes



Euclid, 400-300 BC


Karl-Friedrich Gauss, 1777-1855


Andrew Wiles, 1958 -


Terence Tao, 1975 -

Number Theory and Computer Science

- Representation and Computation of Integers
- Cryptography
- Coding
- Pseudo-random number generation

- Computing is also used to explore open problems in number theory

Division

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

Notations

- The notation $a \mid b$ denotes that a divides b.
- If a does not divide b, we write $a \nmid b$
- If $a \mid b$, then $\dfrac{b}{a}$ is an integer.

Example: $3 \nmid 7$ and $3 \mid 12$

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
ii. If $a \mid b$, then $a \mid bc$ for all integers c;
iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

If $a|b$ and $a|c$, then $a|b+c$

Proof: $b = a \cdot k_1$, $c = a \cdot k_2$

k_1, k_2 Integers (Definition of Division)

Therefore $b + c = a k_1 + a k_2 = a(k_1 + k_2)$

Since $k_1 + k_2$ is an Integer, $a|b+c$

Properties of Divisibility

Corollary: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Direct consequence of Points (i) and (ii) in Theorem 1.

Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder.

This is traditionally called the "Division Algorithm," but it is in fact a theorem.

Division Algorithm (Theorem 2): If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Notation for Division

a = dq + r

d is called the **divisor**.

a is called the **dividend**.

q is called the **quotient**.

r is called the **remainder**.

We write

q = a **div** *d*	**div** is a function:	$\mathbf{div} : \mathbb{Z} \times \mathbb{Z}^{+} \rightarrow \mathbb{Z}$
r = a **mod** *d*	**mod** is a function:	$\mathbf{mod} : \mathbb{Z} \times \mathbb{Z}^{+} \rightarrow \mathbb{N}$

Example

What are the quotient and remainder when 101 is divided by 11?

$q = 101 \text{ div } 11 = 9$

$r = 101 \text{ mod } 11 = 2$

$101 = 9 * 11 + 2$

What are the quotient and remainder when −11 is divided by 3?

$q = -11 \text{ div } 3 = -4$

$r = -11 \text{ mod } 3 = 1$

$-11 = -4 * 3 + 1$

Note

$11 \text{ div } 3 = 3$

$11 \text{ mod } 3 = 2$

Property of mod: $\quad a \bmod m = (a \bmod m) \bmod m$

$a = dq + r \quad , \quad r = a \bmod m$

$r = d \cdot 0 + r \quad , \quad r = r \bmod m$

Therefore: $\quad a \bmod m = (a \bmod m) \bmod m$

Summary

- Division
- Divisibility under arithmetic operations
- Division Algorithm