Number Theory & Abstract Algebra

From divisibility to groups, rings, and fields

one thread
structure

Lesson `gre.algebra.ch6`

Explore this live Watch the walk-through

Two halves, one idea: structure

*This chapter is about the **structure** hiding in arithmetic. Part A — number theory — studies the integers: divisibility, primes, and arithmetic "that wraps around" (modular arithmetic). Part B — abstract algebra — names the structure itself: a set with an operation obeying a few axioms is a **group**, and adding a second operation gives **rings** and **fields**.*

Part A: divisibility • primes • Euclid & Bézout • congruences • CRT • Fermat/Euler

Part B: groups • subgroups & cyclic • Lagrange • homomorphisms • rings & fields

The bridge: the Chinese Remainder Theorem is secretly a statement about isomorphic groups.

Divisibility and unique factorization

$d \mid n$ means $n = dk$ for some integer k. Every integer above 1 factors into primes in exactly one way — the Fundamental Theorem of Arithmetic.

$$360 = 2^3 \cdot 3^2 \cdot 5$$

The divisor count multiplies each exponent plus one:

$$\#\text{divisors} = (3{+}1)(2{+}1)(1{+}1) = 24$$

The Euclidean algorithm and Bézout

? *How do you find* $\gcd(a, b)$ *without factoring?*

Repeatedly replace the larger by its remainder on division by the smaller; the last nonzero remainder is the gcd. Back-substitution writes it as $\gcd = ax + by$ *(Bézout).*

$$\gcd(252, 198): \; 252 = 1 \cdot 198 + 54, \; 198 = 3 \cdot 54 + 36,$$
$$54 = 1 \cdot 36 + 18, \; 36 = 2 \cdot 18 + 0 \Rightarrow 18$$

The last nonzero remainder, 18*, is the gcd.*

Modular arithmetic

$a \equiv b \pmod{n}$ means $n \mid (a-b)$ — "same remainder mod n." You can add, subtract, and multiply congruences freely; division needs an inverse, which exists iff $\gcd(a,n)=1$.

$$7 \cdot 8 = 56 \equiv 2 \pmod{9}$$

Watch out

You cannot always divide mod n. $2x \equiv 4 \pmod{6}$ has *two* solutions, not one, because $\gcd(2,6) \neq 1$.

Worked example — Chinese Remainder Theorem

Find x with $x \equiv 2 \pmod 3$ and $x \equiv 3 \pmod 5$.

$$
\begin{aligned}
x &= 3k + 2 && \text{first congruence} \\
3k + 2 \equiv 3 \pmod 5 &\Rightarrow 3k \equiv 1 && \text{substitute} \\
k &\equiv 2 \pmod 5 && \text{since } 3^{-1} \equiv 2 \\
x &= 3(5m + 2) + 2 = 15m + 8
\end{aligned}
$$

$$x \equiv 8 \pmod{15}$$

Coprime moduli combine into one modulus $3 \cdot 5 = 15$ with a unique solution.

Fermat's Little Theorem and Euler

If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. This collapses giant powers instantly.

$$3^{100} \pmod 7 : \; 3^6 \equiv 1 \Rightarrow 3^{100} = 3^{96} \cdot 3^4 \equiv 3^4 = 81 \equiv 4$$

Euler generalizes: $a^{\varphi(n)} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$.

Groups: the structure behind arithmetic

? *What do clock arithmetic, symmetries, and matrices share?*

*A **group** is a set with an associative operation, an identity, and inverses. That is the entire definition — and it is enough to prove a surprising amount.*

closure • associativity • identity • inverses

The order of an element g is the smallest $n > 0$ with $g^n = e$.

Cyclic groups and Lagrange's theorem

*A **cyclic** group is generated by one element: $\mathbb{Z}_n$ under addition. Its subgroups correspond to divisors of n.*

Lagrange: the order of a subgroup divides the order of the group.

Consequence: an element's order divides the group's order — so a group of prime order has no proper subgroups and must be cyclic.

Worked example — order divides the group

In $\mathbb{Z}_{12}$ (addition mod 12), what is the order of the element 8?

$$8,\ 16 \equiv 4,\ 24 \equiv 0 \Rightarrow \text{order } 3$$

$$\text{and } 3 \mid 12 \ \checkmark \ \text{(Lagrange)}$$

$$\text{order of } 8 \text{ is } 3$$

The order 3 divides the group order 12, exactly as Lagrange promises.

Homomorphisms and isomorphisms

*A **homomorphism** preserves the operation: $f(ab) = f(a)f(b)$. An **isomorphism** is a bijective homomorphism — the two groups are "the same" relabeled.*

$$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \times), \qquad e^{x+y} = e^x e^y$$

The kernel (what maps to the identity) measures how far a homomorphism is from one-to-one.

Rings and fields

*A **ring** has two operations (add and multiply) with distributivity; a **field** is a ring where every nonzero element has a multiplicative inverse.*

$$\mathbb{Z}_p \text{ is a field } \iff p \text{ is prime}$$

$\mathbb{Z}$ is a ring but not a field (only ± 1 have inverses); $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Worked example — is $\mathbb{Z}_6$ a field?

Check whether every nonzero element of $\mathbb{Z}_6$ has a multiplicative inverse.

$$2 \cdot 3 = 6 \equiv 0 \pmod 6$$

$$\Rightarrow 2, 3 \text{ are zero divisors, no inverses}$$

$\mathbb{Z}_6$ is not a field (not even an integral domain)

$\mathbb{Z}_n$ is a field exactly when n is prime — 6 fails because $6 = 2 \cdot 3$.

The through-line

Divisibility and primes build the integers; the Euclidean algorithm computes gcds and, via Bézout, modular inverses; congruences and the CRT organize arithmetic mod n; Fermat and Euler tame large powers. Then abstraction: a group is a set with one good operation, Lagrange constrains its subgroups, homomorphisms compare groups, and rings and fields add a second operation — with $\mathbb{Z}_p$ a field exactly when p is prime.

30 practice problems ($\star$ to $\star\star\star$) in the manuscript.

Explore this live Watch the walk-through