Lesson 3.1 — Integers: The Discrete Backbone

Mathematical Intuition · Module 3 — Numbers Spaces

Node 3.1

1. Why this matters (Hook)

Integers are the first numbers humans invented, and we stopped thinking about them too early.

We treat integers as "easy math" — counting, adding, multiplying whole numbers. But integers are the backbone of:

- **Cryptography** — RSA, Diffie-Hellman, elliptic curve methods all live in integer arithmetic
- **Computer science** — everything a computer does is ultimately integer operations on bits
- **Quantum computing** — measurement outcomes are integers; Shor's algorithm factors integers
- **Number theory** — the distribution of primes is one of the deepest unsolved structures in mathematics

The key insight: integers are **discrete**. There is nothing between 3 and 4. This gap — the absence of continuity — is not a limitation. It is a **structural feature** that makes counting, ordering, and exact computation possible.

---

2. Core Intuition

2.1 Integers are positions on a lattice

Picture the number line, but only the dots — no line connecting them.

$$\cdots \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad \cdots$$

Each dot is exactly one step from its neighbors. This regularity is what makes integers so useful: - You can always ask "what comes next?" $(n+1)$ - You can always count steps between two integers $(b-a)$ - You can always divide and ask about remainders

2.2 Closure tells you what stays inside

Integers are **closed** under addition, subtraction, and multiplication: - $3+5=8$ (integer) - $7-12=-5$ (integer) - $4\times 6=24$ (integer)

But NOT closed under division: - $7\div 3=2.333\ldots$ (not an integer)

This failure of closure is significant. It means that to divide integers, you must either leave the integers (going to rationals) or accept a **remainder**. The remainder is not a bug — it is the foundation of modular arithmetic.

2.3 Primes are the atoms

$$60=2^2\times 3\times 5$$

Every integer greater than 1 can be written as a product of primes, and this factorization is **unique** (the fundamental theorem of arithmetic).

Primes are to integers what atoms are to molecules: irreducible building blocks. You cannot decompose 7 into a product of smaller integers (other than 1×7).

The distribution of primes — where they appear, how they thin out, their mysterious patterns — is one of the central questions of mathematics.

2.4 Modular arithmetic wraps the line into a circle

$$17 \equiv 5 \pmod{12}$$

Read: "17 and 5 are the same, if you only care about the remainder when dividing by 12."

This is clock arithmetic: after 12, you wrap back to 0. The integers mod n form a finite system with n elements: $\{0, 1, 2, \ldots, n-1\}$.

Modular arithmetic converts the infinite integer line into a finite circle. This is why it appears in: - **Cryptography**: operations in $\mathbb{Z}/n\mathbb{Z}$ are efficient but hard to invert - **Hashing**: mapping arbitrary data to fixed-size buckets - **Signal processing**: periodic signals, the discrete Fourier transform - **Error detection**: checksums, CRC codes

---

3. Formal Lens (Light)

3.1 Divisibility: a structural relation

$$a \mid b \iff b = ka \text{ for some } k \in \mathbb{Z}$$

Sentence: "a divides b means b is a multiple of a — there is no remainder."

Divisibility organizes the integers into a hierarchy. The greatest common divisor $\gcd(a, b)$ is the largest number that divides both. The least common multiple $\text{lcm}(a, b)$ is the smallest number both divide into.

3.2 The Euclidean algorithm: finding structure efficiently

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Sentence: "The GCD of a and b equals the GCD of b and the remainder of a divided by b. Repeat until the remainder is zero."

This 2300-year-old algorithm is still used in modern cryptography (computing modular inverses for RSA).

3.3 Fermat's little theorem: structure inside modular arithmetic

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{for prime } p,\ \gcd(a, p) = 1$$

Sentence: "Raise any integer to the power $p-1$, and the result is always 1 modulo p. The prime p creates a periodic structure in exponentiation."

This is the mathematical foundation of RSA: the periodicity of modular exponentiation makes encryption possible, while the difficulty of factoring makes decryption hard.

3.4 The integers as a ring

The integers form a **ring**: a set with addition and multiplication that obeys associativity, commutativity, and distributivity.

$$(\mathbb{Z}, +, \times)$$

This is the algebraic structure that makes integer arithmetic work. Rings appear throughout mathematics: polynomials form a ring, matrices form a ring, modular integers form a ring. Understanding $\mathbb{Z}$ as a ring prepares you for abstract algebra.

---

4. Cross-Domain Examples

4.1 Cryptography — RSA key generation

$$n = p \cdot q, \quad e \cdot d \equiv 1 \pmod{\phi(n)}$$

Reading: "Choose two large primes p and q. Their product n is easy to compute but hard to factor. The encryption exponent e and decryption exponent d are modular inverses. Security rests on the difficulty of recovering p and q from n."

Every online transaction depends on the hardness of integer factorization.

4.2 Computer Science — binary representation

$$42 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 = 101010_2$$

Reading: "Every integer has a unique representation as a sum of powers of 2. Computers exploit this: each bit stores one binary digit, and all computation reduces to integer operations on bit strings."

Integer arithmetic is the physical substrate of all digital computation.

4.3 Quantum Computing — Shor's algorithm

$$\text{Order-finding: find } r \text{ such that } a^r \equiv 1 \pmod{N}$$

Reading: "Shor's algorithm uses quantum phase estimation to find the period of modular exponentiation. Once you know the period, classical number theory extracts the prime factors of N."

Quantum computers threaten RSA because they turn the hard problem (factoring) into an easy problem (period-finding) by exploiting superposition.

4.4 Music — frequency ratios and harmony

Consonant musical intervals correspond to simple integer ratios:

Interval	Ratio
Octave	2:1
Perfect fifth	3:2
Perfect fourth	4:3
Major third	5:4

Reading: "Two frequencies sound harmonious when their ratio is a ratio of small integers. The simpler the ratio, the more consonant the interval."

The Pythagoreans discovered this, and it remains true: integer structure underlies musical perception.

---

5. Micro Drills

Answer in words where possible.

1. **Closure test:** Is the set of even integers closed under addition? Under multiplication? Under division? Explain each.
2. **Modular reading:**
$$2^{10} \equiv 1 \pmod{11}$$
What does this tell you about the structure of powers of 2 modulo 11?
3. **Prime decomposition:** Factor 2520 into primes. Why does knowing the prime factorization tell you everything about the number's divisibility?
4. **GCD interpretation:** $\gcd(12, 18) = 6$. In one sentence: what does this tell you about the common structure of 12 and 18?
5. **Discrete vs continuous:** Why can a computer represent 7 exactly but not $\frac{1}{3}$ exactly? What property of integers makes exact representation possible?

---

6. Reflection

Integers feel simple, but they support: - the security of the internet (cryptography) - the operation of all computers (binary arithmetic) - the deepest open problems in mathematics (Riemann hypothesis, Goldbach conjecture)

Pick one of these domains. In a few sentences, explain why the **discreteness** of integers — the fact that there is nothing between consecutive integers — is essential to how that domain works.

Mathematical Intuition · Module 3 — Numbers Spaces · Node 3.1
Prerequisites: 1.1, 1.2, 1.3
Enables: 3.2, 3.3

hbar.university — own.your.cognition