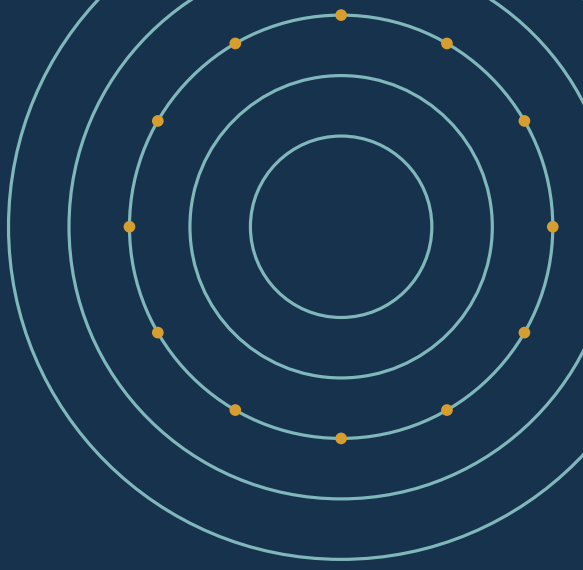
AN INTRODUCTION TO NUMBER THEORY



Patterns, Proofs, and Primes

A visual, inquiry-driven course with exercises

One-semester course packet

Euclid → continued fractions → congruences → groups → prime counting

How to use this course

Big idea

Number theory is an unusually good place to learn what proof feels like. The objects are familiar, experiments are cheap, and elementary questions quickly demand new ways of thinking. This course repeatedly follows the same rhythm:

$$\text{compute} \longrightarrow \text{notice} \longrightarrow \text{conjecture} \longrightarrow \text{prove} \longrightarrow \text{reuse}.$$

Audience and prerequisites

This packet is designed for a first proof-oriented course: strong secondary students, first- or second-year undergraduates, or mathematically mature non-majors. Students should be comfortable with algebra, functions, and mathematical induction. No calculus or abstract algebra is required. A short "proof studio" in the first week can supply any missing experience with direct proof, contradiction, and induction.

Learning goals

By the end, students should be able to:

1. use the Euclidean algorithm both computationally and as a source of proofs;
2. prove unique factorization from Euclid's lemma;
3. read, compute, and interpret finite and infinite continued fractions;
4. calculate in $\mathbb{Z}/n\mathbb{Z}$, solve linear congruences, and use the Chinese remainder theorem;
5. explain Fermat's little theorem through cyclic symmetry and through finite groups;
6. prove basic identities and divisibility statements for binomial coefficients;
7. understand why central binomial coefficients control the density of primes;
8. write short proofs that clearly separate evidence, claim, and justification.

A 14-week route

The design assumes two 75-minute meetings per week. "Studio" means that at least half the meeting is devoted to student work at boards or in small groups.

Week	Core mathematics	Suggested studio or assessment
1	Divisibility; gcd; Euclidean algorithm	Tiling model; proof diagnostic
2	Bézout identity; linear Diophantine equations	Extended Euclid relay
3	Primes; Euclid's lemma; unique factorization	Repair a flawed proof; Problem Set 1
4	Finite continued fractions; convergents	Rational reconstruction lab
5	Approximation; $\sqrt{2}$ and Pell's equation	Continued-fraction gallery; Problem Set 2
6	Congruences; units; linear congruences	Clock arithmetic and affine ciphers
7	Chinese remainder theorem	CRT construction studio; short quiz
8	Necklace colorings and Fermat's theorem	Orbit counting with physical beads; Problem Set 3
9	Groups, subgroups, cyclic groups	Cayley-table investigation
10	Lagrange's theorem; group proof of Fermat	Compare two proofs; Problem Set 4
11	Binomial coefficients and Pascal's triangle	Identity stations
12	p-adic valuations; Kummer's carry idea	Color divisibility patterns; Problem Set 5
13	Central binomial coefficient; Chebyshev functions	Prime-counting proof workshop
14	Chebyshev estimate; synthesis	Capstone presentations or oral exam

Assessment design

One workable balance is 45% problem sets, 20% two short proof interviews, 15% computational or visual labs, and 20% capstone. Problem sets should mix three modes:

- **Fluency**: focused calculations that make later proofs readable.
- **Reasoning**: multi-step proofs, often with a hint or intermediate claim.
- **Exploration**: generate data, state a conjecture, then test its limits.

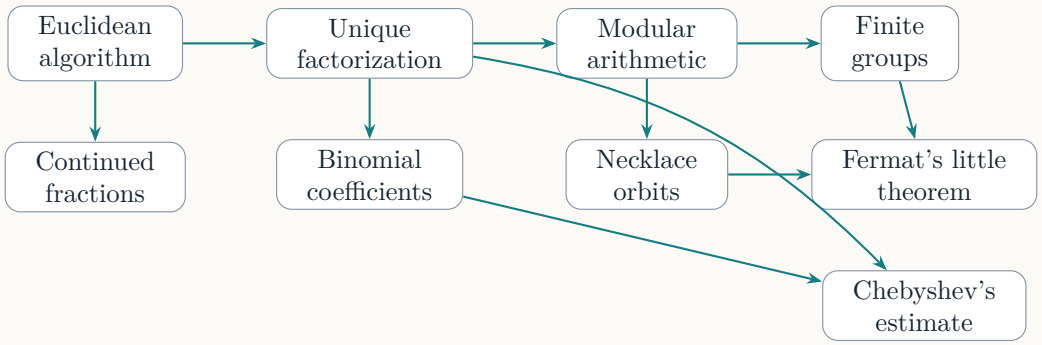
The exercises in each chapter carry these labels. A typical weekly assignment is two fluency problems, two reasoning problems, and one exploration. Selected hints and solutions appear in Appendix A; an instructor can remove those pages when distributing assignments.

Teaching principles

- **Let the picture precede the notation.** Tiling, winding around a clock, rotating a necklace, and counting lattice paths give students something to reason about before symbols compress the idea.
- **Prove one theorem twice.** Fermat's little theorem is the deliberate centerpiece: orbit counting supplies a concrete proof, while groups reveal the reusable structure.
- **Make proof choices visible.** Ask not only "Is this correct?" but "Why did this definition unlock that step?"

- **Use computation as a microscope, not an oracle.** The optional Sage notebook helps students find examples and conjectures; written work must still explain why a pattern continues.

Dependency map



Checkpoint

A good opening prompt. Write 391 and 299 on the board. Ask: "What is the largest square tile that covers a 391×299 rectangle without cutting? How could you be certain?" Do not define gcd until the class has invented the subtraction or division process.

Contents

Chapter 1

The algorithm hidden in a rectangle

Divisibility, gcd, and Bézout's identity

Guiding question 1.1. What is the largest square tile that exactly covers a 391×299 rectangle?

If a square has integer side length d, then it fits precisely only when $d \mid 391$ and $d \mid 299$. We are looking for the *greatest common divisor*, written $\gcd(391, 299)$.

1.1 Divisibility as structure

For integers a, b, we say $a \mid b$ when $b = ak$ for some $k \in \mathbb{Z}$. Divisibility is not an operation like division; it is a yes-or-no relation.

Proposition 1.2 (Division algorithm)**.** *If $a \in \mathbb{Z}$ and $b > 0$, there are unique integers q, r such that*

$$a = bq + r, \qquad 0 \le r < b.$$

The quotient q says how many full copies of b fit inside a; the remainder r is what is left. The crucial observation is

$$\gcd(a, b) = \gcd(b, r) \quad \text{whenever } a = bq + r.$$

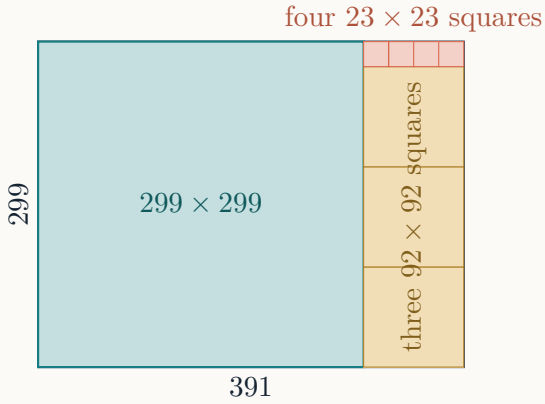
Indeed, an integer divides both a and b exactly when it divides both b and $a - bq = r$.

1.2 Euclid's algorithm

Repeat the division algorithm until the remainder is zero:

$$\begin{aligned} 391 &= 1 \cdot 299 + 92, \\ 299 &= 3 \cdot 92 + 23, \\ 92 &= 4 \cdot 23 + 0. \end{aligned}$$

The last nonzero remainder is 23, so $\gcd(391, 299) = 23$.



The same remainders appear when successively removing the largest possible squares.

Theorem 1.3 (Euclidean algorithm)**.** *For positive integers $a \geq b$, repeated division terminates, and the last nonzero remainder is* $\gcd(a, b)$.

Proof. Each remainder is a nonnegative integer smaller than the previous positive remainder, so the process must stop. Replacing (a, b) by (b, r) does not change the common divisors. At the last line $r_{k-1} = qr_k$, hence the common divisors are precisely the divisors of r_k. □

1.3 Running the movie backward

The remainders do more than find the gcd. Reverse the equations:

$$\begin{aligned} 23 &= 299 - 3 \cdot 92 \\ &= 299 - 3(391 - 299) \\ &= 4 \cdot 299 - 3 \cdot 391. \end{aligned}$$

Thus 23 is an integer linear combination of 391 and 299.

Theorem 1.4 (Bézout's identity)**.** *For integers a, b, not both zero, there are integers x, y such that*

$$ax + by = \gcd(a, b).$$

Moreover, $\gcd(a, b)$ *is the smallest positive integer of the form $ax + by$.*

Corollary 1.5. *The equation $ax + by = c$ has integer solutions exactly when* $\gcd(a, b) \mid c$.

Proof. If $ax + by = c$, every common divisor of a, b divides c. Conversely, multiply a Bézout identity for the gcd by $c/\gcd(a, b)$. □

Common trap

The gcd is positive, but Bézout coefficients need not be. Restricting x, y to positive integers makes the statement false.

Explore

Choose two 3-digit integers. Make a two-column record: Euclid's divisions on the left, backward substitutions on the right. How large can the coefficients become? The optional Sage notebook automates the arithmetic but also asks you to certify its output by substitution.

Exercises

1. Compute $\gcd(2024, 748)$ by Euclid's algorithm. [Fluency]

2. Express $\gcd(527, 341)$ in the form $527x + 341y$. [Fluency]

3. Prove: if $d \mid a$ and $d \mid b$, then $d \mid (ma + nb)$ for all $m, n \in \mathbb{Z}$. [Reasoning]

4. Find all integer solutions to $35x + 22y = 1$. Describe how one solution generates all the others. [Reasoning]

5. Show that $\gcd(a, b) = \gcd(a + kb, b)$ for every $k \in \mathbb{Z}$. Explain why this is the engine of Euclid's algorithm. [Reasoning]

6. A rectangle has integer sides $a > b$. Repeatedly remove the largest square available. Prove that the final square has side $\gcd(a, b)$. [Exploration]

7. Consecutive Fibonacci numbers make Euclid's algorithm take many steps. Test this claim, then prove $\gcd(F_{n+1}, F_n) = 1$. [Exploration]

Chapter 2

Every integer has an address

Primes and the fundamental theorem of arithmetic

Positive integers factor. But why should the factorization into primes be unique? The arithmetic step that makes uniqueness possible is modest enough to miss.

Definition 2.1. An integer $p > 1$ is *prime* if its only positive divisors are 1 and p. An integer $n > 1$ that is not prime is *composite*.

2.1 Euclid's lemma

Lemma 2.2 (Euclid)**.** *If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. Suppose $p \nmid a$. Since the only positive divisors of p are $1, p$, we have $\gcd(p, a) = 1$. Bézout gives $px + ay = 1$. Multiply by b:

$$pbx + aby = b.$$

Both terms on the left are divisible by p, so $p \mid b$. □

Common trap

The word "prime" is essential. We have $6 \mid 2 \cdot 3$, but 6 divides neither factor.

Applying the lemma repeatedly shows: if a prime divides $a_1 a_2 \cdots a_k$, it divides at least one factor.

2.2 Existence and uniqueness

Theorem 2.3 (Fundamental theorem of arithmetic)**.** *Every integer $n > 1$ can be written as a product of primes. Apart from rearranging the factors, this product is unique.*

Existence. Use strong induction on n. If n is prime, we are done. If it is composite, write $n = ab$ with $1 < a, b < n$. By induction, both a and b are products of primes, so n is too. □

Uniqueness. Suppose

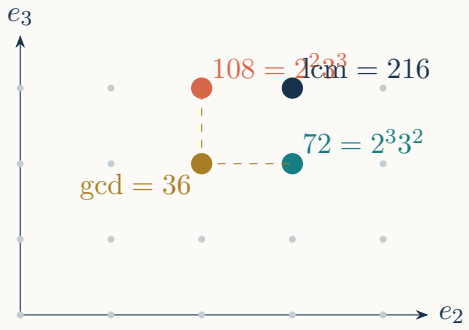
$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

with all p_i, q_j prime. Since p_1 divides the right side, Euclid's lemma says $p_1 = q_j$ for some j. Cancel this common factor. Repeat. No factor can remain on only one side, so the lists agree up to order. □

Collecting repeated primes gives a coordinate system

$$n = 2^{e_2} 3^{e_3} 5^{e_5} \cdots,$$

where only finitely many exponents are nonzero. Multiplication adds exponent vectors; gcd takes coordinatewise minima; lcm takes coordinatewise maxima.



Prime exponents turn gcd and lcm into geometry.

Proposition 2.4. *If* $n = \prod p^{e_p}$ *and* $m = \prod p^{f_p}$*, then*

$$\gcd(n,m) = \prod p^{\min(e_p, f_p)}, \qquad \operatorname{lcm}(n,m) = \prod p^{\max(e_p, f_p)}.$$

In particular, $\gcd(n,m)\operatorname{lcm}(n,m) = nm$.

2.3 There is no last prime

Theorem 2.5 (Euclid)**.** *There are infinitely many primes.*

Proof. If $p_1, \ldots, p_k$ were all primes, consider $N = p_1 \cdots p_k + 1$. Some prime divides N, but none of the listed primes does: division by any p_i leaves remainder 1. Contradiction. □

This proof does not say that N is prime. It says that N has a prime factor missing from the proposed complete list.

Exercises

1. Factor 7560 and use the exponent vectors to find the number of its positive divisors. [Fluency]
2. Compute $\gcd(2^7 3^2 11, 2^4 3^5 5)$ and the lcm without multiplying first. [Fluency]
3. Prove that if $\gcd(a,b) = 1$ and $a \mid c$, $b \mid c$, then $ab \mid c$. [Reasoning]

4. Prove that $\sqrt{p}$ is irrational for every prime p. State exactly where unique factorization is used. [Reasoning]

5. Show that every integer $n > 1$ has a prime divisor at most $\sqrt{n}$, unless n itself is prime. Turn this into a primality test. [Reasoning]

6. Is $n! + 1$ always prime? Find the first counterexample, then explain why Euclid's proof is unaffected. [Exploration]

7. Prove that infinitely many primes are congruent to 3 modulo 4 by adapting Euclid's idea to $4p_1 \cdots p_k - 1$. You may use the fact that a product of numbers congruent to 1 modulo 4 is again 1 modulo 4. [Challenge]

Chapter 3

Fractions inside fractions

Continued fractions and best approximations

The quotients from Euclid's algorithm are not bookkeeping debris. Read them forward and they produce a new numerical language.

3.1 Euclid, folded up

From

$$415 = 4 \cdot 93 + 43, quad 93 = 2 \cdot 43 + 7, quad 43 = 6 \cdot 7 + 1, quad 7 = 7 \cdot 1,$$

we obtain

$$\frac{415}{93} = 4 + \cfrac{1}{2 + \cfrac{1}{6 + \cfrac{1}{7}}} = [4; 2, 6, 7].$$

Definition 3.1. A finite simple continued fraction is

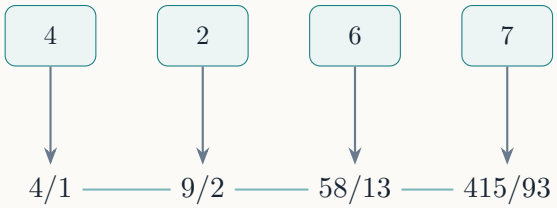
$$[a_0; a_1, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}},$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for $i \geq 1$.

The truncations $[a_0; \dots, a_k] = p_k/q_k$ are called *convergents*. They can be computed without rebuilding the nested fraction:

$$p_k = a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2},$$

with $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$.



Each convergent remembers all earlier partial quotients.

Theorem 3.2 (Determinant identity)**.** *Consecutive convergents satisfy*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Consequently, each p_k/q_k is in lowest terms and

$$\left| \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} \right| = \frac{1}{q_k q_{k-1}}.$$

Proof. Substitute the recurrences:

$$\begin{aligned} p_k q_{k-1} - p_{k-1} q_k &= (a_k p_{k-1} + p_{k-2}) q_{k-1} - p_{k-1}(a_k q_{k-1} + q_{k-2}) \\ &= -(p_{k-1} q_{k-2} - p_{k-2} q_{k-1}). \end{aligned}$$

The initial value is 1, so the sign alternates. □

3.2 Infinite continued fractions

For an irrational real number x, repeatedly take integer parts:

$$a_0 = \lfloor x \rfloor, \qquad x_1 = \frac{1}{x - a_0}, \qquad a_1 = \lfloor x_1 \rfloor, \quad \dots$$

This produces $x = [a_0; a_1, a_2, \dots]$.

Example 3.3 (The silver staircase)**.** Let $x = \sqrt{2}$. Since

$$\frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 = 2 + (\sqrt{2} - 1),$$

the same remainder repeats, so

$$\sqrt{2} = [1; \overline{2}] = [1; 2, 2, 2, \dots].$$

Its first convergents are

$$1, \quad \frac{3}{2}, \quad \frac{7}{5}, \quad \frac{17}{12}, \quad \frac{41}{29}, \dots$$

They alternately fall below and above $\sqrt{2}$.

Theorem 3.4 (Approximation by convergents)**.** *If p_k/q_k is a convergent of an irrational x, then*

$$\left|x - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}} < \frac{1}{q_k^2}.$$

Moreover, if $0 < q < q_{k+1}$, then no fraction p/q is closer to x than both neighboring convergents in the appropriate interval. In this precise sense, convergents are best approximations with small denominators.

The determinant identity is the engine: distinct reduced fractions $a/b, c/d$ are at least $1/(bd)$ apart. There is simply not enough room for another small-denominator fraction between a convergent and x.

3.3 Pell's equation appears

For the convergents p/q to $\sqrt{2}$, direct computation gives

$$p^2 - 2q^2 = \pm 1.$$

Thus excellent rational approximations produce integer points very near the curve $p^2 = 2q^2$. The solutions to $p^2 - 2q^2 = 1$ begin $(3, 2), (17, 12), (99, 70)$.

Checkpoint

Compute $99/70$ as a decimal. The striking accuracy is not a floating-point accident: $99^2 - 2 \cdot 70^2 = 1$ forces

$$\left|\sqrt{2} - 99/70\right| = \frac{1}{70^2(\sqrt{2} + 99/70)}.$$

Exercises

1. Find the continued fraction of $355/113$. List all convergents. [Fluency]
2. Compute the first six convergents of $[1; \overline{1}]$. What familiar sequence appears? [Fluency]
3. Prove the determinant identity by induction. Use it to prove $\gcd(p_k, q_k) = 1$. [Reasoning]
4. Show that $[a_0; \ldots, a_n] = [a_0; \ldots, a_n - 1, 1]$ when $a_n > 1$. Explain the only ambiguity in finite expansions. [Reasoning]
5. Derive $\sqrt{3} = [1; \overline{1, 2}]$ and compute four convergents. [Reasoning]
6. A calendar year is about 365.2422 days. Use continued fractions to find a simple leap-year rule. Compare the Julian and Gregorian rules. [Exploration]
7. Investigate which convergents to $\sqrt{2}$ solve $p^2 - 2q^2 = 1$ and which solve -1. State and prove a pattern using the recurrence. [Challenge]

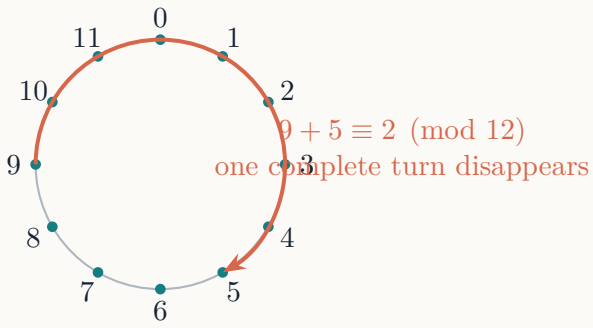
Chapter 4

Arithmetic on a clock

Congruences, inverses, and the Chinese remainder theorem

Definition 4.1. For $n \geq 2$, we write $a \equiv b \pmod{n}$ if $n \mid (a - b)$. The equivalence class of a is written $[a]$ or $\bar{a}$.

Congruence remembers the remainder and forgets the number of complete turns around the clock.



4.1 Legal arithmetic

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n}, \qquad ac \equiv bd \pmod{n}.$$

Powers are therefore legal too. Division is different.

Definition 4.2. A residue a is a *unit modulo* n if there exists b with $ab \equiv 1 \pmod{n}$. Such a b is an inverse of a.

Theorem 4.3 (Invertibility criterion)**.** *a has an inverse modulo n exactly when* $\gcd(a, n) = 1$.

Proof. The congruence $ab \equiv 1 \pmod{n}$ means $ab + nk = 1$ for some k. This is precisely a Bézout identity. Such an identity exists exactly when $\gcd(a, n) = 1$. □

Common trap

Cancellation can fail. Modulo 6, $2 \cdot 1 \equiv 2 \cdot 4$, but $1 \not\equiv 4$. You may cancel a modulo n only when a is a unit, or after carefully reducing the modulus.

Proposition 4.4 (Linear congruence)**.** *The congruence $ax \equiv b \pmod{n}$ has a solution exactly when $d = \gcd(a, n)$ divides b. When it does, there are exactly d incongruent solutions modulo n.*

4.2 Reassembling remainders

Suppose a number leaves remainder 2 modulo 3 and remainder 3 modulo 5. Listing possibilities gives 8 modulo 15. The Chinese remainder theorem says this always works for coprime clocks.

Theorem 4.5 (Chinese remainder theorem)**.** *If $n_1, \dots, n_r$ are pairwise coprime, then for any $a_1, \dots, a_r$, the system*

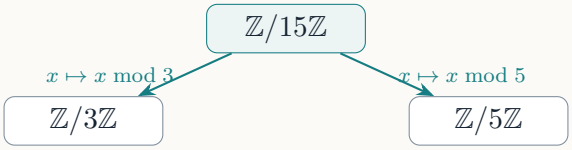
$$x \equiv a_i \pmod{n_i} \qquad (i = 1, \dots, r)$$

has a solution, unique modulo $N = n_1 \cdots n_r$.

Construction. Set $N_i = N/n_i$. Since $\gcd(N_i, n_i) = 1$, choose M_i with $N_i M_i \equiv 1 \pmod{n_i}$. Then

$$x = \sum_{i=1}^{r} a_i N_i M_i$$

has every prescribed remainder: modulo n_i, its ith term is a_i and every other term is 0. If x, y both work, each n_i divides $x - y$; coprimality makes $N \mid x - y$. □



One clock of size 15 is equivalent to two independent clocks.

4.3 Fast powers and patterns

Modular reduction prevents numbers from exploding. To compute $7^{222} \pmod{13}$, square and reduce:

$$7^2 \equiv 10, quad 7^4 \equiv 9, quad 7^8 \equiv 3, quad 7^{16} \equiv 9 \pmod{13},$$

then use the binary expansion $222 = 128 + 64 + 16 + 8 + 4 + 2$. Later, Fermat's theorem will make this even faster.

Explore

Make a multiplication table modulo n and highlight the rows that are permutations of all residues. Conjecture which row labels have inverses. Then compare with the gcd criterion.

Exercises

1. Find the inverse of 37 modulo 101 using extended Euclid. [Fluency]

2. Solve $18x \equiv 30 \pmod{42}$ and list all solutions modulo 42. [Fluency]

3. Prove that congruence modulo n is an equivalence relation. [Reasoning]

4. Show that an integer is divisible by 9 exactly when its decimal digit sum is divisible by 9. [Reasoning]

5. Solve $x \equiv 2 \pmod{7}$, $x \equiv 3 \pmod{8}$, $x \equiv 4 \pmod{9}$ by the constructive CRT proof. [Reasoning]

6. Determine every possible last two digits of a square. Explain how CRT can split the work into moduli 4 and 25. [Exploration]

7. Prove that $x^2 \equiv 1 \pmod{p}$ has only the solutions $x \equiv \pm 1$ when p is prime. Find a composite modulus where there are more than two solutions. [Challenge]

Chapter 5

A theorem you can rotate

Necklace colorings and Fermat's little theorem

Why should a prime p divide $a^p - a$ for every integer a? Instead of manipulating the expression, we count objects that naturally arrive in packets of p.

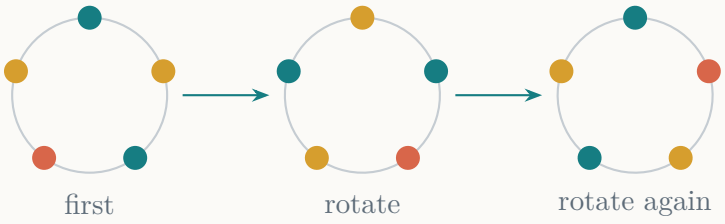
5.1 Words on a circular loom

Fix a prime p and a colors. First imagine p labeled positions around a circle. A coloring is a word

$$(c_0, c_1, \ldots, c_{p-1}),$$

and there are a^p such words. Rotation by one step sends it to

$$(c_{p-1}, c_0, \ldots, c_{p-2}).$$



Group words together when one is a rotation of another. Such a group is called a rotational *orbit*. How large can an orbit be?

Lemma 5.1 (Prime orbit dichotomy)**.** *For p prime, a length-p word has either 1 or p distinct rotations. It has one exactly when it is constant.*

Proof. If rotation by k positions, with $1 \le k < p$, fixes the word, then entries i and $i + k$ have the same color (indices modulo p). Since $\gcd(k, p) = 1$, repeatedly adding k visits every position. Thus all entries have one color. A nonconstant word has no repeated rotation before the pth, so its orbit has size p. □

There are a constant words, one for each color. The remaining $a^p - a$ words split into orbits of exactly p words.

Theorem 5.2 (Fermat's little theorem, necklace form)**.** *If p is prime, then for every integer a,*

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

If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. For $a \geq 0$, the orbit count above shows $p \mid a^p - a$. This congruence depends only on the residue of a modulo p, so it holds for every integer a. If $p \nmid a$, then a has an inverse modulo p, and we may cancel it from $a^p \equiv a$. □

Big idea

Divisibility by p appears because symmetry packages nonexceptional objects into groups of p. The exceptions are exactly the colorings fixed by rotation. This pattern – count, isolate fixed points, divide the rest into orbits – reaches far beyond number theory.

5.2 A subtle choice: labeled words or necklaces?

A physical necklace usually ignores where position 0 is. Here we first count *labeled* circular words, then use rotation to partition them. Calling each orbit a necklace is convenient, but the proof depends on keeping those two levels distinct.

Common trap

When the length is composite, an orbit can have an intermediate size. The word $RBRB$ has two distinct rotations, not 1 or 4. Primality is doing real work.

5.3 Using the theorem

To compute $3^{1000} \pmod{7}$, note that $3^6 \equiv 1$ and $1000 = 6 \cdot 166 + 4$:

$$3^{1000} \equiv (3^6)^{166} 3^4 \equiv 81 \equiv 4 \pmod{7}.$$

Fermat's theorem also explains the first layer of binomial divisibility. For $1 \leq k \leq p-1$,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

is divisible by p, because the denominator contains no factor p. Therefore

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

We will return to this "freshman's dream" after developing binomial coefficients systematically.

Exercises

1. List the rotational orbits of binary words of length 3. Identify the constant words. [Fluency]

2. Compute $11^{2026} \pmod{17}$ using Fermat's theorem. [Fluency]

3. In the orbit lemma, prove carefully that $0, k, 2k, \ldots, (p-1)k$ are all distinct modulo p. [Reasoning]

4. Give an orbit-counting proof that $p \mid a^p - a$ using linear strings and cyclic shift, without drawing a circle. [Reasoning]

5. Find every possible orbit size for binary words of length 6, and give an example of each. [Exploration]

6. Prove that if p is prime, then $(x+y)^p \equiv x^p + y^p \pmod{p}$. Use induction to deduce $(x_1 + \cdots + x_m)^p \equiv x_1^p + \cdots + x_m^p$. [Reasoning]

7. If n is composite, must there be an a with $a^n \not\equiv a \pmod{n}$? Test $n = 341$ and 561. This opens the door to pseudoprimes and Carmichael numbers. [Challenge]

Chapter 6

The reusable machine

A quick introduction to finite groups

The necklace proof is vivid, but it was tailored to one symmetry. Group theory isolates the small collection of rules shared by rotations, invertible residues, permutations, and many other systems.

6.1 One operation, four rules

Definition 6.1. A *group* is a set G with an operation $*$ such that:

1. $a * b \in G$ for all $a, b \in G$ (closure);

2. $(a * b) * c = a * (b * c)$ (associativity);

3. there is an identity e with $e * a = a * e = a$;

4. each a has an inverse a^{-1} with $a * a^{-1} = a^{-1} * a = e$.

If also $a * b = b * a$, the group is *abelian*.

Group	Operation	Identity / inverse
$\mathbb{Z}/n\mathbb{Z}$	addition	0 / $-a$
$(\mathbb{Z}/n\mathbb{Z})^\times$	multiplication of units	1 / modular inverse
rotations of a regular n-gon	composition	no rotation / reverse rotation
permutations of a set	composition	do nothing / undo

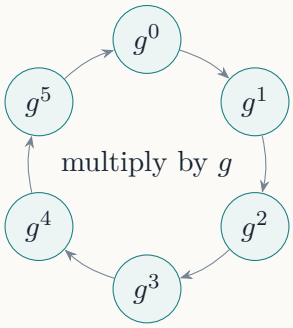
Not every familiar set works: all residues modulo n under multiplication fail because nonunits have no inverse.

6.2 Powers and cyclic subgroups

For $g \in G$, the list

$$e, g, g^2, g^3, \dots$$

eventually repeats when G is finite. The first positive m with $g^m = e$ is the *order* of g, written $\operatorname{ord}(g)$. The powers form the cyclic subgroup $\langle g \rangle$.



A cyclic group of order 6: repeated multiplication traces a loop.

6.3 Cosets and Lagrange's theorem

If H is a subgroup of G and $g \in G$, the left coset

$$gH = \{gh : h \in H\}$$

is a translated copy of H. Two cosets are either equal or disjoint, and every coset has $|H|$ elements because $h \mapsto gh$ is a bijection.

Theorem 6.2 (Lagrange)**.** *If G is finite and $H \leq G$, then $|H|$ divides $|G|$.*

Proof. The distinct cosets of H partition G into equally sized blocks. If there are r blocks, then $|G| = r\,|H|$. □

Corollary 6.3. *For every g in a finite group G, $\operatorname{ord}(g) \mid |G|$ and hence $g^{|G|} = e$.*

6.4 Fermat's theorem, now in one line

For prime p, every nonzero residue has an inverse, so

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \dots, p-1\}$$

is a group of order $p - 1$. Lagrange immediately yields the standard group-theoretic proof:

$$a^{p-1} \equiv 1 \pmod{p} \qquad (p \nmid a).$$

The gain is not a shorter proof at any price. The gain is a theorem that can be reused.

Theorem 6.4 (Euler)**.** *If $\gcd(a, n) = 1$, then*

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

where $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Proof. Apply the corollary of Lagrange to the group $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Big idea

The necklace proof uses orbits of a cyclic action; Lagrange uses cosets of a subgroup. Both prove divisibility by partitioning a finite set into equal blocks. Group theory turns that shared move into a portable language.

6.5 A second standard proof without naming Lagrange

If $a \not\equiv 0 \pmod{p}$, multiplication by a permutes the nonzero residues:

$$a, 2a, \ldots, (p-1)a \pmod{p}$$

is just $1, 2, \ldots, p-1$ in another order. Multiply all entries:

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

Since $(p-1)!$ is invertible, cancel it. This is the group proof with the machinery folded away.

Exercises

1. List $(\mathbb{Z}/12\mathbb{Z})^\times$ and make its multiplication table. Find the order of every element. [Fluency]
2. Find $\varphi(20)$ and use Euler's theorem to reduce 3^{2026} modulo 20. [Fluency]
3. Prove that the identity of a group is unique and that each element has a unique inverse. [Reasoning]
4. Prove that two left cosets of H are equal or disjoint. [Reasoning]
5. Show that a group of prime order is cyclic. [Reasoning]
6. Draw the subgroup lattice of $(\mathbb{Z}/12\mathbb{Z}, +)$. Check Lagrange's theorem at every node. [Exploration]
7. Prove $\varphi(mn) = \varphi(m)\varphi(n)$ when $\gcd(m, n) = 1$ by using the Chinese remainder theorem. [Challenge]
8. Compare the necklace, permutation, and Lagrange proofs of Fermat's theorem. For each, identify the set being partitioned or permuted and the exact place primality enters. [Synthesis]

Chapter 7

Arithmetic in Pascal's triangle

Binomial coefficients and divisibility

Definition 7.1. For $0 \le k \le n$,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

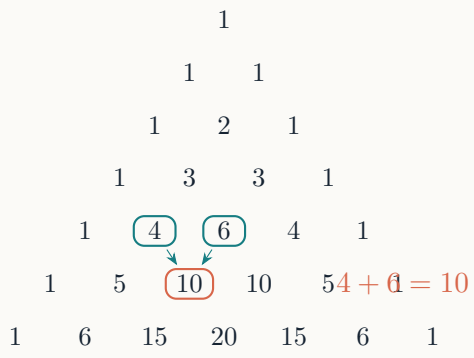
It counts the k-element subsets of an n-element set.

The counting meaning proves integrality without asking the fraction to look integral. It also makes identities visible.

Proposition 7.2 (Pascal and symmetry)**.**

$$\binom{n}{k} = \binom{n}{n-k}, \qquad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

For Pascal's identity, distinguish k-subsets that contain a chosen element from those that do not.



7.1 Three ways to see the binomial theorem

Theorem 7.3 (Binomial theorem)**.**

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

In expanding $(x+y)^n$, choose which k of the n factors contribute y. This proof also explains why the coefficients are integers and why their sum is 2^n.

Proposition 7.4 (Vandermonde)**.** *For nonnegative integers r, s, n,*

$$\sum_k \binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n}.$$

Count n-person committees from two groups: either all at once, or according to how many come from the first group.

7.2 Prime rows

Theorem 7.5. *If p is prime and $1 \le k \le p-1$, then*

$$p \mid \binom{p}{k}.$$

Proof. The identity $k\binom{p}{k} = p\binom{p-1}{k-1}$ shows p divides $k\binom{p}{k}$. Since $p \nmid k$, Euclid's lemma gives $p \mid \binom{p}{k}$. □

Thus the pth row of Pascal's triangle becomes $1, 0, \ldots, 0, 1$ modulo p, which again yields

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

7.3 Measuring divisibility one prime at a time

Definition 7.6. For nonzero integer m, $v_p(m)$ is the exponent of p in its prime factorization. Thus $v_2(40) = 3$.

Valuations turn multiplication into addition:

$$v_p(ab) = v_p(a) + v_p(b), \qquad v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

when the quotient is an integer.

Theorem 7.7 (Legendre)**.**

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots.$$

Proof. Among $1, \ldots, n$, exactly $\lfloor n/p \rfloor$ contribute at least one p; $\lfloor n/p^2 \rfloor$ contribute one additional p; and so on. □

Consequently,

$$v_p\binom{n}{k} = \sum_{j \ge 1} \left(\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{k}{p^j} \right\rfloor - \left\lfloor \frac{n-k}{p^j} \right\rfloor \right).$$

Each parenthesis is 0 or 1: it records whether adding k and $n-k$ creates a carry at the p^j place.

Theorem 7.8 (Kummer's carry rule)**.** *$v_p\binom{n}{k}$ equals the number of carries when k and $n-k$ are added in base p.*

The formula above is already the proof once carries are read from right to left. It gives a remarkable visual test: $\binom{n}{k}$ is not divisible by p precisely when subtracting k from n in base p needs no borrowing.

Example 7.9. To find $v_2\binom{10}{3}$, add $3 = 0011_2$ and $7 = 0111_2$:

$$\begin{array}{r} 0011 \\ +0111 \\ \hline 1010 \end{array}$$

There are three carries, so $v_2\binom{10}{3} = 3$. Indeed, $\binom{10}{3} = 120 = 2^3 \cdot 15$.

Explore

Color entry $\binom{n}{k}$ when it is nonzero modulo 2, then modulo 3. Zoom out. The self-similar patterns are the visual shadow of base-p digits and lead to Lucas's theorem.

Exercises

1. Prove $\sum_k \binom{n}{k} = 2^n$ and $\sum_k (-1)^k \binom{n}{k} = 0$ for $n > 0$. [Fluency]

2. Compute $v_2(100!)$, $v_5(100!)$, and the number of trailing zeros of $100!$. [Fluency]

3. Give a counting proof of $k\binom{n}{k} = n\binom{n-1}{k-1}$. [Reasoning]

4. Use Vandermonde's identity to prove $\sum_k \binom{n}{k}^2 = \binom{2n}{n}$. [Reasoning]

5. Determine all n for which every interior entry of row n is even. Use Kummer's rule. [Reasoning]

6. For a fixed prime p, explore the first p^2 rows of Pascal's triangle modulo p. State a digit-based conjecture for when $\binom{n}{k} \not\equiv 0 \pmod{p}$. [Exploration]

7. Prove that $\operatorname{lcm}(1, 2, \ldots, 2n)$ is divisible by $\binom{2n}{n}$ by comparing p-adic valuations. [Bridge]

Chapter 8

How crowded are the primes?

Chebyshev's estimate from the middle of Pascal's triangle

Euclid proved that the primes never end. A sharper question asks how many lie below x:

$$\pi(x) = \#\{p \le x : p \text{ prime}\}.$$

The prime number theorem says $\pi(x) \sim x/\log x$, but its proof lies beyond this course. Chebyshev's elementary argument already captures the correct scale.

8.1 The central binomial squeeze

The largest coefficient in $(1+1)^{2n}$ is central. Since there are $2n+1$ nonnegative coefficients with sum 4^n,

$$\frac{4^n}{2n+1} \le \binom{2n}{n} < 4^n. \tag{8.1}$$

This elementary inequality contains surprising information about primes.

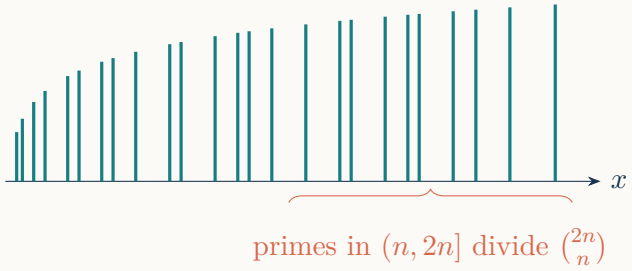
Define two weighted prime counts:

$$\vartheta(x) = \sum_{p \le x} \log p, \qquad \psi(x) = \sum_{p^k \le x} \log p.$$

The first logs the product of primes at most x; the second logs the least common multiple:

$$\psi(x) = \log \operatorname{lcm}(1, 2, \dots, \lfloor x \rfloor).$$

A logarithmic weight turns products into sums.



8.2 An upper bound for the prime product

Every prime $n < p \le 2n$ occurs in the numerator $(n+1)(n+2)\cdots(2n)$ and not in $n!$. Therefore it divides $\binom{2n}{n}$, and

$$\vartheta(2n) - \vartheta(n) \le \log \binom{2n}{n} < 2n \log 2.$$

Adding these inequalities over dyadic intervals gives the following deliberately non-optimized bound.

Lemma 8.1. *For $x \ge 2$,*

$$\vartheta(x) \le 2(\log 2)x.$$

Proof. Split $(1, x]$ into $(x/2, x], (x/4, x/2], \ldots$ and apply the preceding estimate, with integer endpoints rounded outward. The resulting geometric series is bounded by

$$x \log 2 + \frac{x}{2} \log 2 + \frac{x}{4} \log 2 + \cdots = 2x \log 2.$$

Endpoint rounding can only add primes already included in the neighboring interval. □

8.3 A lower bound from an lcm

The bridge exercise in the last chapter showed

$$\binom{2n}{n} \mid \operatorname{lcm}(1, 2, \ldots, 2n).$$

Taking logarithms and using (8.1),

$$\psi(2n) \ge \log \binom{2n}{n} \ge 2n \log 2 - \log(2n+1). \tag{8.2}$$

Prime powers make ψ larger than ϑ, but not by too much:

$$\psi(x) = \vartheta(x) + \vartheta(x^{1/2}) + \vartheta(x^{1/3}) + \cdots.$$

By Lemma 8.1, all terms after the first contribute at most

$$2\sqrt{x} \log x$$

for $x \ge 4$: there are at most $\log_2 x$ terms, and every argument is at most $\sqrt{x}$. Combining this with (8.2) shows that, once x is sufficiently large,

$$\vartheta(x) \ge \frac{\log 2}{2} x. \tag{8.3}$$

The constant $1/2$ is chosen for convenience; better bookkeeping improves it.

8.4 From weighted primes to ordinary counting

The lower bound is immediate because every term in $\vartheta(x)$ is at most $\log x$:

$$\vartheta(x) \le \pi(x)\log x \quad \Longrightarrow \quad \pi(x) \ge \frac{\log 2}{2}\frac{x}{\log x}.$$

For the upper bound, primes between $\sqrt{x}$ and x each contribute at least $\frac{1}{2}\log x$:

$$\vartheta(x) \ge (\pi(x) - \pi(\sqrt{x}))\frac{\log x}{2}.$$

Using $\pi(\sqrt{x}) \le \sqrt{x}$ and Lemma 8.1 gives

$$\pi(x) \le 4\log 2\,\frac{x}{\log x} + \sqrt{x} \le 4\frac{x}{\log x}$$

for all sufficiently large x.

Theorem 8.2 (Chebyshev estimate)**.** *For all sufficiently large x,*

$$\boxed{\frac{\log 2}{2}\frac{x}{\log x} \le \pi(x) \le 4\frac{x}{\log x}}$$

In particular, $\pi(x) \asymp x/\log x$: their ratio stays between two positive constants.

Common trap

The symbol $\asymp$ does not mean $\sim$. Chebyshev's estimate gets the correct order of magnitude. The prime number theorem makes the much stronger claim

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

Big idea

Why did binomial coefficients see primes? Factorials contain every integer up to a boundary. Dividing $(2n)!$ by two copies of $n!$ cancels most small-scale information while exposing primes that cross the boundary from n to $2n$. The central coefficient is both arithmetically rich and analytically easy to estimate.

Exercises

1. Compute $\pi(10^k)$ and $10^k/\log(10^k)$ for $k = 1, 2, 3, 4$. Track the ratio. [Fluency]
2. Prove both sides of the central binomial squeeze (8.1). [Reasoning]
3. Prove that every prime p with $n < p \le 2n$ divides $\binom{2n}{n}$ exactly once. [Reasoning]
4. Fill in the valuation proof that $\binom{2n}{n}$ divides $\operatorname{lcm}(1, \ldots, 2n)$. [Reasoning]
5. Starting from the dyadic inequality, write a fully detailed proof of Lemma 8.1, including floors and ceilings. [Challenge]

6. Use a computer to graph $\pi(x)$, $x/\log x$, and the two Chebyshev bounds. Which statement is visible at moderate x, and which remains too coarse? [Exploration]

7. Show that Chebyshev's estimate implies the nth prime p_n has order of magnitude $n \log n$. [Synthesis]

Chapter 9

Capstone studio

Choose a thread, extend it, and explain it

The capstone is not a miniature research paper. It is a carefully explained mathematical journey: a motivating question, small examples, one substantial proof, and a clear account of how course ideas connect.

9.1 Project menu

A. Rational approximation and Pell equations

Choose a nonsquare d. Compute the continued fraction of $\sqrt{d}$, identify convergents that solve $x^2 - dy^2 = \pm 1$, and prove at least one recurring pattern. Include a number-line or lattice illustration.

B. Symmetry, orbits, and divisibility

Generalize necklace counting to length n. Classify possible orbit sizes for one composite n, explain stabilizers in concrete language, and derive a divisibility identity. Möbius inversion is an optional extension, not a prerequisite.

C. Pascal's triangle modulo a prime

Visualize Pascal's triangle modulo p. Develop and prove a digit rule (Lucas's theorem is the natural destination), then explain how Kummer's carry rule and the visual pattern encode the same arithmetic.

D. Prime-counting laboratory

Compare $\pi(x)$ with $x/\log x$, $\mathrm{Li}(x)$, and the Chebyshev bounds over a range your computer can handle. Explain which plots are evidence and which claims are proved. Reconstruct one link in Chebyshev's proof in full detail.

9.2 Required deliverables

1. A four-to-six page mathematical exposition.
2. At least one original diagram or data visualization.
3. One theorem stated precisely and proved completely.
4. A one-page "proof map" naming the definitions and earlier results used.
5. A five-minute oral explanation, followed by questions.

9.3 Evaluation rubric

Criterion	Evidence of strong work	Weight
Mathematical correctness	Claims are true, hypotheses are visible, examples are checked, and the main proof closes every logical gap.	35%
Exposition	The question motivates the definitions; notation is stable; paragraphs explain why steps matter.	25%
Connection	At least two course strands are linked in a mathematically meaningful way.	15%
Visual or computational insight	A diagram or computation reveals structure and is interpreted rather than merely displayed.	15%
Revision and response	The final version addresses peer/instructor feedback and the oral defense shows ownership.	10%

Checkpoint

Before submitting, underline every sentence that makes a mathematical claim. For each underline, ask: Is it a definition, an observed example, a cited theorem, or a claim I have proved? Ambiguous status is often the real source of unclear exposition.

9.4 A final synthesis prompt

In 500–700 words, respond to this statement:

> Number theory repeatedly converts multiplication into something easier to organize: remainders, exponent vectors, additive logarithms, or equal-sized orbits.

Use one precise example from three different chapters. Your response should include at least one equation and explain not only what the conversion does, but why it helps a proof.

Appendix A

Selected hints and solutions

For checking arguments, not replacing them

Only selected exercises are treated here. A useful routine is: write a complete attempt, mark the exact step where you are stuck, then consult only the first relevant sentence below.

Chapter 1

1. Euclid gives

$$2024 = 2(748) + 528, quad 748 = 528 + 220, quad 528 = 2(220) + 88,$$

$$220 = 2(88) + 44, quad 88 = 2(44),$$

so the gcd is 44.

2. The divisions are $527 = 341 + 186$, $341 = 186 + 155$, $186 = 155 + 31$, $155 = 5 \cdot 31$. Reverse:

$$31 = 186 - 155 = 2(186) - 341 = 2(527 - 341) - 341 = 2 \cdot 527 - 3 \cdot 341.$$

4. One solution is $35(-5) + 22(8) = 1$. All solutions are

$$x = -5 + 22t, qquad y = 8 - 35t \qquad (t \in \mathbb{Z}).$$

To prove completeness, subtract two solutions and use $35(x - x') = -22(y - y')$ with $\gcd(35, 22) = 1$.

Chapter 2

3. Write $c = ar = bs$. Since $a \mid bs$ and $\gcd(a, b) = 1$, repeated Euclid's lemma (or Bézout) gives $a \mid s$. Thus $s = at$ and $c = abt$.

4. If $\sqrt{p} = a/b$ in lowest terms, then $a^2 = pb^2$. The exponent of p on the left is even; on the right it is odd. Unique factorization forbids this.

6. No: $5! + 1 = 121 = 11^2$. Euclid's number only needs a prime divisor outside the proposed list; it need not itself be prime.

Chapter 3

1. Euclid gives

$$355/113 = [3; 7, 16],$$

with convergents 3, 22/7, and 355/113.

2. The convergents are

$$1,\ 2,\ \frac{3}{2},\ \frac{5}{3},\ \frac{8}{5},\ \frac{13}{8}.$$

Numerators and denominators are consecutive Fibonacci numbers; the recurrence with every $a_k = 1$ proves it.

4. Since $a_n = (a_n - 1) + 1/1$ at the bottom level,

$$[a_0; \ldots, a_n] = [a_0; \ldots, a_n - 1, 1].$$

Requiring the last partial quotient to exceed 1 selects a unique finite expansion.

Chapter 4

1. Extended Euclid yields

$$1 = 11 \cdot 101 - 30 \cdot 37,$$

so $37^{-1} \equiv -30 \equiv 71 \pmod{101}$.

2. Divide $18x \equiv 30 \pmod{42}$ by 6 while reducing the modulus: $3x \equiv 5 \pmod{7}$. Since $3^{-1} \equiv 5$, $x \equiv 4 \pmod{7}$. Modulo 42 the six solutions are $4, 11, 18, 25, 32, 39$.

5. Here $N = 504$. One convenient construction is

$$x = 2(72)(4) + 3(63)(7) + 4(56)(5) = 3019 \equiv 499 \pmod{504}.$$

The multipliers $4, 7, 5$ invert $72, 63, 56$ modulo $7, 8, 9$, respectively.

Chapter 5

1. The binary length-3 words form four orbits:

$$\{000\},\quad \{111\},\quad \{001, 010, 100\},\quad \{011, 110, 101\}.$$

3. If $ik \equiv jk \pmod{p}$, then $p \mid k(i - j)$. As $p \nmid k$, Euclid's lemma gives $p \mid i - j$. For $0 \le i, j < p$, this forces $i = j$.

5. Orbit sizes divide 6, and binary examples realize $1, 2, 3, 6$: 000000, 010101, 001001, and 000001.

Chapter 6

1. $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$. Every nonidentity element squares to 1, so their orders are 2; the identity has order 1.

4. If $aH \cap bH$ contains x, write $x = ah_1 = bh_2$. Then $a = bh_2h_1^{-1}$, so every $ah \in aH$ equals $b(h_2h_1^{-1}h) \in bH$. Thus $aH \subseteq bH$; symmetry gives equality.

5. For $g \neq e$, the order of g divides the prime $|G|$, so it is $|G|$. Hence $G = \langle g \rangle$.

Chapter 7

2. Legendre gives

$$v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97,$$

$$v_5(100!) = 20 + 4 = 24.$$

Each trailing zero consumes one 2 and one 5, so there are 24.

4. Choose n objects from two disjoint groups of n. If k come from the first group, then $n - k$ come from the second. Summing over k gives

$$\sum_k \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}.$$

7. Legendre gives

$$v_p\binom{2n}{n} = \sum_{j\geq 1}\left(\left\lfloor \frac{2n}{p^j}\right\rfloor - 2\left\lfloor \frac{n}{p^j}\right\rfloor\right).$$

Each summand is 0 or 1, and there are at most $\left\lfloor \log_p(2n)\right\rfloor$ nonzero candidates. This is the exponent of p in the lcm, so the valuation of the binomial coefficient is no larger for every prime p.

Chapter 8

2. The sum of the $2n + 1$ coefficients in row $2n$ is 4^n. The central coefficient is largest, so it is at least the average $4^n/(2n + 1)$ and strictly below the whole sum.

3. For $n < p \leq 2n$, the numerator $(n + 1)\cdots(2n)$ contains exactly one multiple of p, while $n!$ contains none. Because $p^2 > 2n$ for $p > n \geq 1$, the valuation is exactly one.

7 (hint). Insert $x = p_n$ into both Chebyshev bounds to compare n with $p_n/\log p_n$. First obtain coarse polynomial bounds on p_n so that $\log p_n$ can be compared with $\log n$, then substitute back.

Appendix B

Reference sheets

Definitions, algorithms, and proof moves

Core notation

Notation	Meaning
$a \mid b$	$b = ak$ for some integer k
$\gcd(a, b)$	greatest positive common divisor
$a \equiv b \pmod{n}$	$n \mid (a - b)$
$(\mathbb{Z}/n\mathbb{Z})^\times$	invertible residue classes modulo n
$\varphi(n)$	number of units modulo n
$v_p(m)$	exponent of p in m
$\pi(x)$	number of primes at most x
$\vartheta(x)$	$\sum_{p \le x} \log p$
$\psi(x)$	$\sum_{p^k \le x} \log p$
$f(x) \asymp g(x)$	their ratio stays between positive constants eventually

Algorithms at a glance

Extended Euclid. Divide until zero; the last nonzero remainder is the gcd; substitute backward to obtain $ax + by = \gcd(a, b)$.

Continued fraction. Repeatedly take the integer part, subtract it, and invert. Convergents satisfy

$$p_k = a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2}.$$

Linear congruence. For $ax \equiv b \pmod{n}$, first compute $d = \gcd(a, n)$. There are solutions iff $d \mid b$. Divide by d, reduce the modulus to n/d, and invert the new coefficient.

CRT. With $N = \prod n_i$, take $N_i = N/n_i$ and choose $M_i = N_i^{-1} \pmod{n_i}$. Then $x = \sum a_i N_i M_i \pmod{N}$.

Proof moves worth naming

- **Minimal counterexample / strong induction**: factor a composite object into smaller ones.
- **Bézout insertion**: replace 1 by $ax + by$ to transfer divisibility.
- **Exponent comparison**: use unique factorization or v_p to compare products and quotients.
- **Equal-block partition**: cosets and rotation orbits turn a count into divisibility.
- **Count two ways**: binomial identities become transparent when both sides count the same set.
- **Logarithmic weighting**: products of primes become the sums ϑ and ψ.
- **Dyadic decomposition**: split a range into $(x/2, x], (x/4, x/2], \ldots$ and sum a geometric series.

The two Fermat proofs

	Necklace proof	Group proof
Objects	a^p labeled colorings	nonzero residues modulo p
Structure	cyclic rotation orbits	group $(\mathbb{Z}/p\mathbb{Z})^\times$
Exceptional part	a constant colorings	identity/powers inside cyclic subgroups
Equal blocks	nonconstant orbits have size p	element orders divide $p-1$
Conclusion	$a^p \equiv a \pmod{p}$	$a^{p-1} \equiv 1 \pmod{p}$ for $p \nmid a$

Further reading

- G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*.
- I. Niven, H. Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*.
- J. Stillwell, *Elements of Number Theory*.
- J.-P. Serre, *A Course in Arithmetic* (for a more advanced next step).

Course packet designed as an adaptable teaching draft. Examples, exercises, and diagrams are original to this packet.