

MathCastle

Number Theory

Complete course booklet • 11 topics

Contents

1	Divisibility	3
1.1	The Division Algorithm	3
1.2	Divisibility Rules	3
1.3	Why It Works	4
2	Primes and Factorization	4
2.1	Primes	4
2.2	The Fundamental Theorem of Arithmetic	5
2.3	Why It Works	6
3	GCD, LCM and the Euclidean Algorithm	6
3.1	The Euclidean Algorithm	6
3.2	LCM and the Product Formula	7
4	Modular Arithmetic	7
4.1	Congruences	7
4.2	Inverses and Linear Congruences	8
4.3	Why It Works	9
5	Digits and Bases	9
5.1	Base b Representation	9
5.2	Digit Problems	10
6	Diophantine Equations	10
6.1	Linear Diophantine Equations	10
6.2	Factoring and Bounding	11
7	Fermat, Euler and Wilson	12
7.1	Fermat's Little Theorem	12
7.2	Euler's Theorem and φ	12

7.3	Why It Works	13
8	Arithmetic Functions	13
8.1	τ , σ and φ	13
8.2	Divisor Problems	14
9	The Chinese Remainder Theorem	14
9.1	CRT	15
9.2	Why It Works	15
10	Orders and Primitive Roots	16
10.1	The Order of an Element	16
10.2	Quadratic Residues	16
10.3	Why It Works	17
11	Hard Number Theory	17
11.1	Strategy	17

1 Divisibility

What it means for one integer to divide another

1.1 The Division Algorithm

Divides, quotient, remainder

We write $a \mid b$ ("a divides b") when $b = ak$ for some integer k . For any integer b and positive a there are unique integers q, r with $b = aq + r$ and $0 \leq r < a$ — the **division algorithm**. Divisibility is the case $r = 0$.

Everything in number theory grows from this one sentence. It says the integers sort into a classes by remainder, that "divides" is a yes/no question with a computable answer, and that repeated division must terminate — which is what makes the Euclidean algorithm and base representations work. The uniqueness of q and r is what lets us say "the remainder" rather than "a remainder".

Basic facts

If $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for all integers x, y . If $a \mid b$ and $b \mid c$ then $a \mid c$. If $a \mid b$ with $b \neq 0$ then $|a| \leq |b|$.

Using linear combinations

Show that $7 \mid (2^{n+2} + 3^{2n+1})$ for all $n \geq 0$. Write $2^{n+2} + 3^{2n+1} = 4 \cdot 2^n + 3 \cdot 9^n$. Modulo 7, $9 \equiv 2$, so this is $4 \cdot 2^n + 3 \cdot 2^n = 7 \cdot 2^n \equiv 0$.

Where it goes wrong

Writing $a \mid b$ when you mean a/b . The bar is a statement (true or false), not a number.

Try it: remainder

Find q and r for $b = -37$, $a = 8$.

Answer. $-37 = 8(-5) + 3$: $q = -5$, $r = 3$. (Not $q = -4$, $r = -5$: the remainder must be non-negative.)

1.2 Divisibility Rules

Digit tests

A number is divisible by 2, 5, 10 according to its last digit; by 4 or 25 according to its last two

digits; by 8 by its last three. By 3 or 9 when its digit sum is; by 11 when the alternating digit sum is. By 6 when by both 2 and 3.

Every rule is the same idea: $10 \equiv 1 \pmod{9}$ so a number is congruent to its digit sum mod 9; $10 \equiv -1 \pmod{11}$ so it is congruent to its alternating digit sum mod 11; $10^2 \equiv 0 \pmod{4}$ so only the last two digits matter mod 4. Once you see them as congruences you can invent rules for 7, 13, or any modulus you like.

Test 11

918,082: alternating sum $9 - 1 + 8 - 0 + 8 - 2 = 22$, divisible by 11. So $11 \mid 918082 (= 11 \cdot 83462)$.

Try it: fill the digit

For which digit d is $4d,512$ divisible by 9?

Answer. Digit sum $4 + d + 5 + 1 + 2 = 12 + d$; need a multiple of 9: $d = 6$.

1.3 Why It Works

Existence: among the integers $b - ak$ ($k \in \mathbb{Z}$) some are non-negative (take k very negative). Let r be the smallest non-negative one, with q the corresponding k . If $r \geq a$ then $r - a = b - a(q + 1)$ is a smaller non-negative member, contradiction; so $0 \leq r < a$. Uniqueness: if $aq + r = aq' + r'$ with both remainders in $[0, a)$, then $a(q - q') = r' - r$ has absolute value less than a , so it must be 0. The well-ordering of the non-negative integers — every non-empty set has a least element — is the engine, and it will power almost every proof in this course.

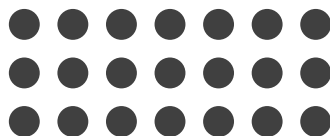
2 Primes and Factorization

The atoms of arithmetic and the unique way numbers split into them

2.1 Primes

Definition and infinitude

A **prime** is an integer $p > 1$ whose only positive divisors are 1 and p . There are infinitely many: given any finite list $p_1, \dots, p_k$, the number $N = p_1 p_2 \cdots p_k + 1$ has a prime factor, and it is none of the p_i (each leaves remainder 1).



3 rows of 7

Euclid's argument does not say N is prime — $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$. It says N has a NEW prime factor, which is all that is needed. To test whether n is prime, trial-divide by primes up to $\sqrt{n}$: a composite $n = ab$ with $a \leq b$ has $a \leq \sqrt{n}$.

Is 221 prime?

$\sqrt{221} < 15$; test 2, 3, 5, 7, 11, 13. $221 = 13 \cdot 17$. Composite.

Try it: primality

Is 197 prime?

Answer. $\sqrt{197} < 15$; not divisible by 2, 3, 5, 7, 11, 13 (check: $197 = 13 \cdot 15 + 2$). **Prime.**

2.2 The Fundamental Theorem of Arithmetic

Unique factorization

Every integer $n > 1$ is a product of primes, and the factorization is unique up to order: $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. The exponents answer most questions about n : the number of divisors is $(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$; n is a perfect square exactly when every e_i is even.

Uniqueness is the deep half. Existence is easy (keep splitting); uniqueness needs Euclid's lemma — if a prime divides a product, it divides a factor — which in turn rests on Bzout. In number systems where uniqueness fails, like $\mathbb{Z}[\sqrt{-5}]$ where $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, almost every familiar argument breaks. Prime factorizations are the coordinates of the integers.

Count divisors

$360 = 2^3 \cdot 3^2 \cdot 5$: $(3+1)(2+1)(1+1) = 24$ divisors. Sum of divisors: $(1+2+4+8)(1+3+9)(1+5) = 15 \cdot 13 \cdot 6 = 1170$.

Legendre's formula

The exponent of a prime p in $n!$ is $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$ — count the multiples of p , then

of p^2 (which contribute a second factor), and so on.

Where it goes wrong

Counting divisors by listing them and missing one. The exponent formula is exact; use it and then list only if asked.

Try it: trailing zeros

How many zeros end 100!?

Answer. Zeros come from factors of $10 = 2 \cdot 5$, and 5 is scarcer: $\lfloor 100/5 \rfloor + \lfloor 100/25 \rfloor = 20 + 4 = 24$.

2.3 Why It Works

Lemma: if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. Proof: if $p \nmid a$ then $\gcd(p, a) = 1$, so by Bzout $1 = px + ay$ for some integers x, y . Multiply by b : $b = pbx + aby$, and p divides both terms, so $p \mid b$. Uniqueness of factorization follows: if $p_1 \cdots p_r = q_1 \cdots q_s$, then p_1 divides the right side, hence (by the lemma, repeatedly) divides some q_j , hence equals it; cancel and repeat. The lemma is exactly what fails in $\mathbb{Z}[\sqrt{-5}]$, where 2 divides $(1 + \sqrt{-5})(1 - \sqrt{-5})$ but neither factor.

3 GCD, LCM and the Euclidean Algorithm

Greatest common divisors, Bzout, and fast computation

3.1 The Euclidean Algorithm

Repeated remainders

Since $\gcd(a, b) = \gcd(b, a \bmod b)$, dividing repeatedly and keeping remainders reaches $\gcd(a, b)$ as the last nonzero remainder. It takes at most about $5 \times (\text{number of digits})$ steps — far faster than factoring.

The key fact $\gcd(a, b) = \gcd(b, r)$ where $a = bq + r$ holds because any common divisor of a and b divides $r = a - bq$, and any common divisor of b and r divides a . The two pairs have the same common divisors, so the same greatest one. Running the algorithm backwards expresses the gcd as a combination of a and b — Bzout's identity — which is the tool behind modular inverses and Euclid's lemma.

Compute $\gcd(252, 105)$

$252 = 2 \cdot 105 + 42$; $105 = 2 \cdot 42 + 21$; $42 = 2 \cdot 21 + 0$. So $\gcd = 21$. Backwards: $21 = 105 - 2 \cdot 42 = 105 - 2(252 - 2 \cdot 105) = 5 \cdot 105 - 2 \cdot 252$.

Bzout's identity

For integers a, b not both zero there exist integers x, y with $ax + by = \gcd(a, b)$. In particular a and b are coprime exactly when $ax + by = 1$ is solvable.

Try it: Euclid

Compute $\gcd(1071, 462)$ and write it as $1071x + 462y$.

Answer. $1071 = 2 \cdot 462 + 147$; $462 = 3 \cdot 147 + 21$; $147 = 7 \cdot 21$. $\gcd = \mathbf{21}$; $21 = 462 - 3 \cdot 147 = 462 - 3(1071 - 2 \cdot 462) = \mathbf{7 \cdot 462 - 3 \cdot 1071}$.

3.2 LCM and the Product Formula

$$\gcd \cdot \text{lcm} = ab$$

For positive a, b : $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$. In terms of prime exponents, the $\gcd$ takes the minimum exponent of each prime and the lcm the maximum, and $\min + \max = \text{the sum of the two exponents}$.

Find the lcm

$\text{lcm}(252, 105) = 252 \cdot 105 / 21 = 1260$. Check: $252 = 2^2 \cdot 3^2 \cdot 7$, $105 = 3 \cdot 5 \cdot 7$, $\text{lcm} = 2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$.

Where it goes wrong

Applying $\gcd \cdot \text{lcm} = \text{product}$ to THREE numbers. It is false in general: $\gcd(2, 2, 2) \cdot \text{lcm}(2, 2, 2) = 4 \neq 8$.

Try it: from gcd and lcm

Two numbers have $\gcd = 6$ and $\text{lcm} = 180$, and one of them is 30. Find the other.

Answer. $6 \cdot 180 / 30 = \mathbf{36}$. Check: $\gcd(30, 36) = 6$, $\text{lcm} = 180$. ✓

4 Modular Arithmetic

Congruences, inverses and linear congruences

4.1 Congruences

Working mod m

$a \equiv b \pmod{m}$ means $m \mid (a - b)$. Congruences can be added, subtracted and multiplied like

equations: if $a \equiv b$ and $c \equiv d$ then $a + c \equiv b + d$ and $ac \equiv bd$. So you may reduce at every step of a computation — which is what makes $2^{100} \bmod 7$ easy.

Reducing mod m is forgetting everything about a number except its remainder, and the miracle is that arithmetic still works on remainders alone. The one operation that needs care is division: you may cancel a factor c from both sides only when $\gcd(c, m) = 1$, and then "dividing by c " means multiplying by the inverse of c .

Big powers

$2^{100} \bmod 7$: $2^3 = 8 \equiv 1$, so $2^{100} = 2^{99} \cdot 2 = (2^3)^{33} \cdot 2 \equiv 2$. Answer 2.

Cancellation

If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$. If $\gcd(c, m) = d$, you can only conclude $a \equiv b \pmod{m/d}$.

Try it: last digit

Find the last digit of 7^{2025} .

Answer. Powers of 7 mod 10 cycle 7, 9, 3, 1 with period 4; $2025 \equiv 1 \pmod{4}$, so the last digit is 7.

4.2 Inverses and Linear Congruences

Modular inverses

a has an inverse mod m (a number a^{-1} with $aa^{-1} \equiv 1$) exactly when $\gcd(a, m) = 1$; find it from Bzout. The congruence $ax \equiv b \pmod{m}$ has a solution iff $\gcd(a, m) \mid b$, and then exactly $\gcd(a, m)$ solutions mod m .

Solve $7x \equiv 3 \pmod{20}$

$\gcd(7, 20) = 1$; $7 \cdot 3 = 21 \equiv 1$, so $7^{-1} \equiv 3$. $x \equiv 3 \cdot 3 = 9$. Check: $63 = 3 \cdot 20 + 3$. ✓

Solve $6x \equiv 4 \pmod{10}$

$\gcd(6, 10) = 2 \mid 4$: divide through: $3x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{5}$. Two solutions mod 10: $x = 4, 9$.

Where it goes wrong

Dividing both sides of a congruence by a number that shares a factor with the modulus. $2x \equiv 2 \pmod{4}$ does NOT give $x \equiv 1$; $x = 3$ also works.

Try it: inverse

Find the inverse of 11 modulo 26.

Answer. $26 = 2 \cdot 11 + 4$; $11 = 2 \cdot 4 + 3$; $4 = 3 + 1$. Back: $1 = 4 - 3 = 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 = 3(26 - 2 \cdot 11) - 11 = 3 \cdot 26 - 7 \cdot 11$. So $11^{-1} \equiv -7 \equiv \mathbf{19}$. Check: $11 \cdot 19 = 209 = 8 \cdot 26 + 1$. ✓

4.3 Why It Works

If $ax \equiv 1 \pmod{m}$ then $ax - my = 1$ for some y , so any common divisor of a and m divides 1: $\gcd(a, m) = 1$. Conversely, if $\gcd(a, m) = 1$, Bzout gives $ax + my = 1$, and reducing mod m leaves $ax \equiv 1$. The residues coprime to m therefore form a group under multiplication — closed, with identity 1, every element invertible — and the size of that group is Euler's $\varphi(m)$, which is where the next topic begins.

5 Digits and Bases

Place value in any base and the tricks it enables

5.1 Base b Representation

Every integer, every base

For any base $b \geq 2$, every positive integer has a unique representation $n = d_k b^k + \cdots + d_1 b + d_0$ with digits $0 \leq d_i < b$. Convert to base b by repeated division (the remainders are the digits, last to first); convert back by evaluating the polynomial.

Base representation is the division algorithm applied repeatedly: $n = bq_0 + d_0$, then $q_0 = bq_1 + d_1$, and so on until the quotient is 0. Uniqueness comes from uniqueness of remainders. Base 2 underlies computers, base 16 compresses base 2, and base 3 with digits $-1, 0, 1$ (balanced ternary) solves the classic weighing puzzles.

Convert 2024 to base 7

$2024 = 7 \cdot 289 + 1$; $289 = 7 \cdot 41 + 2$; $41 = 7 \cdot 5 + 6$; $5 = 7 \cdot 0 + 5$. Digits from the last: 5621_7 . Check: $5 \cdot 343 + 6 \cdot 49 + 2 \cdot 7 + 1 = 1715 + 294 + 14 + 1 = 2024$. ✓

Try it: base 2

Write 200 in binary, and say how many 1s it has.

Answer. $200 = 128 + 64 + 8 = 11001000_2$: **three** ones.

5.2 Digit Problems

Digits as unknowns

A two-digit number with digits a, b is $10a + b$; reversing gives $10b + a$; their difference is $9(a - b)$. Writing the number in terms of its digits turns a digit puzzle into an equation with small integer unknowns, solvable by bounding and casework.

A reversal puzzle

A two-digit number is 4 times the sum of its digits. $10a + b = 4(a + b)$ gives $6a = 3b$, $b = 2a$: 12, 24, 36, 48.

Digit sums and 9

A number and its digit sum are congruent mod 9. Repeatedly taking digit sums (the "digital root") gives $n \bmod 9$, with 9 in place of 0.

Where it goes wrong

Forgetting the digit range: leading digits are 1–9, others 0–9. A "solution" with $a = 12$ is not a digit.

Try it: digital root

Find the digital root of $2^{20} = 1048576$.

Answer. Digit sum $1 + 0 + 4 + 8 + 5 + 7 + 6 = 31 \rightarrow 4$. (Check: $2^{20} \equiv (2^6)^3 \cdot 4 \equiv 1 \cdot 4 \pmod{9}$.) 4.

6 Diophantine Equations

Integer solutions: linear equations, factoring tricks and bounding

6.1 Linear Diophantine Equations

$$ax + by = c$$

The equation $ax + by = c$ has integer solutions iff $\gcd(a, b) \mid c$. From one solution (x_0, y_0) (found by the extended Euclidean algorithm), all solutions are $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$ with

$$d = \gcd(a, b) \text{ and } t \in \mathbb{Z}.$$

Geometrically the solutions are the lattice points on a line, spaced evenly along it. The spacing $(b/d, -a/d)$ is the smallest integer step along the line, which is why d appears: with $d > 1$ the naive step $(b, -a)$ skips solutions. Constraints like "positive solutions" become inequalities in t — usually leaving finitely many.

Positive solutions

$7x + 11y = 200$. $7 \cdot (-3) + 11 \cdot 2 = 1$, so $x_0 = -600$, $y_0 = 400$. General: $x = -600 + 11t$, $y = 400 - 7t$. Positive: $t \geq 55$ and $t \leq 57$: $t = 55, 56, 57$ give $(5, 15), (16, 8), (27, 1)$.

Try it: stamps

In how many ways can \$1.00 be made from 5-cent and 7-cent stamps (order irrelevant)?

Answer. $5x + 7y = 100$ with $x, y \geq 0$. y must be a multiple of 5: $y = 0, 5, 10$ give $x = 20, 13, 6$. **3** ways.

6.2 Factoring and Bounding

Simon's Favorite Factoring Trick

$xy + ax + by = c$ becomes $(x + b)(y + a) = c + ab$: add the missing constant to complete the product, then list factor pairs. More generally, get one side to factor and the other to be a constant, and the equation reduces to finitely many cases.

The trick is a change of variables that turns a hyperbola into one with axes parallel to the coordinate axes; the integer points on $XY = N$ are the divisor pairs of N , of which there are finitely many. For equations without such a factorization, bound one variable — by size, by parity, or by a modulus in which the equation has no solutions.

SFFT

Solve $xy - 3x - 2y = 7$ in positive integers. $(x - 2)(y - 3) = 13$: pairs $(1, 13), (13, 1)$ give $(x, y) = (3, 16), (15, 4)$.

No solutions, mod 4

$x^2 + y^2 = 2023$: squares are 0 or 1 mod 4, so $x^2 + y^2 \in \{0, 1, 2\}$ mod 4; but $2023 \equiv 3$. No solutions.

Where it goes wrong

Forgetting negative factor pairs when the variables may be negative, and forgetting that (a, b) and (b, a) are different pairs when x and y play different roles.

Try it: SFFT

Find all positive integer solutions of $xy + x + y = 23$.

Answer. $(x + 1)(y + 1) = 24$: pairs $(2, 12), (3, 8), (4, 6), (6, 4), (8, 3), (12, 2)$ give $(x, y) = (1, 11), (2, 7), (3, 5), (5, 3), (7, 2), (11, 1)$ — six solutions.

7 Fermat, Euler and Wilson

The three theorems behind every big power

7.1 Fermat's Little Theorem

$$a^{p-1} \equiv 1$$

If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$; equivalently $a^p \equiv a$ for every a . So exponents can be reduced mod $p - 1$: $a^n \equiv a^{n \bmod (p-1)} \pmod{p}$ when $p \nmid a$.

The exponent $p - 1$ is the number of nonzero residues mod p , and the theorem says multiplying by a permutes them: $a, 2a, \dots, (p - 1)a$ are the same residues in a different order, so their products agree, $a^{p-1}(p-1)! \equiv (p-1)!$, and $(p-1)!$ cancels. This is a group-theory fact in disguise (Lagrange's theorem), and Euler's theorem is the same argument with the coprime residues mod m .

Reduce the exponent

$3^{1000} \bmod 7$: $1000 = 6 \cdot 166 + 4$, so $3^{1000} \equiv 3^4 = 81 \equiv 4 \pmod{7}$.

Try it: Fermat

Find $2^{2025} \bmod 13$.

Answer. $2025 = 12 \cdot 168 + 9$, so $2^{2025} \equiv 2^9 = 512 = 39 \cdot 13 + 5 \equiv 5$.

7.2 Euler's Theorem and φ

Euler's totient

$\varphi(m)$ counts the integers in $1, \dots, m$ coprime to m . For $m = p_1^{e_1} \cdots p_k^{e_k}$: $\varphi(m) = m \prod \left(1 - \frac{1}{p_i}\right)$.

Euler: if $\gcd(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Last two digits

$7^{222} \bmod 100$: $\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$, and $222 = 5 \cdot 40 + 22$, so $7^{222} \equiv 7^{22}$. $7^2 = 49$, $7^4 \equiv 49^2 = 2401 \equiv 1$. So $7^{22} = (7^4)^5 \cdot 7^2 \equiv 49$. Last two digits 49.

Wilson's theorem

For a prime p : $(p-1)! \equiv -1 \pmod{p}$. (For composite $m > 4$, $(m-1)! \equiv 0$.)

Where it goes wrong

Using Euler when $\gcd(a, m) \neq 1$ — $2^{\varphi(8)} = 16 \equiv 0 \pmod{8}$, not 1. Split the modulus into prime powers and treat the non-coprime part directly.

Try it: totient

Compute $\varphi(360)$, then find $7^{96} \bmod 360$.

Answer. $360 = 2^3 \cdot 3^2 \cdot 5$: $\varphi = 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = \mathbf{96}$. Since $\gcd(7, 360) = 1$, $7^{96} \equiv \mathbf{1} \pmod{360}$.

7.3 Why It Works

Let $p \nmid a$. The residues $a, 2a, \dots, (p-1)a$ are pairwise distinct mod p : if $ia \equiv ja$ then $p \mid (i-j)a$, and since $p \nmid a$, $p \mid i-j$, forcing $i = j$ (both lie in $1, \dots, p-1$). None is 0. So they are the residues $1, \dots, p-1$ in some order, and multiplying them together gives $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Since $p \nmid (p-1)!$ (all its factors are smaller than p), cancel it: $a^{p-1} \equiv 1$. Replace "1, ..., $p-1$ " by "the $\varphi(m)$ residues coprime to m " and the identical argument proves Euler's theorem.

8 Arithmetic Functions

Counting and summing divisors, and multiplicativity

8.1 τ , σ and φ

Multiplicative functions

$\tau(n)$ counts the divisors of n , $\sigma(n)$ sums them, $\varphi(n)$ counts the residues coprime to n . All three are **multiplicative**: $f(mn) = f(m)f(n)$ when $\gcd(m, n) = 1$. So each is determined by its values on prime powers: $\tau(p^e) = e + 1$, $\sigma(p^e) = \frac{p^{e+1} - 1}{p - 1}$, $\varphi(p^e) = p^e - p^{e-1}$.

Multiplicativity is the Chinese remainder theorem seen from the divisor side: a divisor of mn (coprime parts) is a divisor of m times a divisor of n , uniquely. That single bijection gives all three

formulas at once. Perfect numbers ($\sigma(n) = 2n$), abundant and deficient numbers, and the famous open questions about them all live inside σ .

Evaluate all three at 72

$$72 = 2^3 \cdot 3^2. \quad \tau = 4 \cdot 3 = 12. \quad \sigma = 15 \cdot 3 = 45. \quad \varphi = (8 - 4)(9 - 3) = 24.$$

Sum of φ over divisors

For every n : $\sum_{d|n} \varphi(d) = n$. (Sort $1, \dots, n$ by gcd with n : exactly $\varphi(n/d)$ of them have gcd d .)

Try it: from the formulas

Find $\tau(1000)$, $\sigma(1000)$ and $\varphi(1000)$.

Answer. $1000 = 2^3 \cdot 5^3$: $\tau = 16$; $\sigma = 15 \cdot 156 = 2340$; $\varphi = 4 \cdot 100 = 400$.

8.2 Divisor Problems

Reading off structure

Questions like "which n have exactly 6 divisors?" are questions about exponent patterns: $6 = 6$ or $2 \cdot 3$, so $n = p^5$ or $n = p^2 q$. "Perfect squares have an odd number of divisors" is $\tau(n)$ odd iff every $e_i + 1$ is odd.

Smallest with 12 divisors

$12 = 12, 6 \cdot 2, 4 \cdot 3, 3 \cdot 2 \cdot 2$: candidates $2^{11}, 2^5 \cdot 3, 2^3 \cdot 3^2, 2^2 \cdot 3 \cdot 5$, i.e. 2048, 96, 72, 60. Smallest: 60.

Where it goes wrong

Assigning the larger exponents to the larger primes. To minimize n for a given τ , the biggest exponent goes on the smallest prime.

Try it: exactly 10 divisors

What is the smallest positive integer with exactly 10 divisors?

Answer. $10 = 10$ or $5 \cdot 2$: $2^9 = 512$ or $2^4 \cdot 3 = 48$. **48.**

9 The Chinese Remainder Theorem

Solving systems of congruences

9.1 CRT

Independent moduli combine

If $m_1, \dots, m_k$ are pairwise coprime, the system $x \equiv a_i \pmod{m_i}$ has exactly one solution mod $M = m_1 \cdots m_k$. To find it: solve two at a time, substituting $x = a_1 + m_1 t$ into the second congruence and solving for t .

The theorem says that knowing a number mod 3 and mod 5 is the same as knowing it mod 15 — no more, no less. That is why problems about a composite modulus split into prime-power pieces (Euler's theorem on each, then reassemble), and why φ and τ are multiplicative. It is also the reason a computer can do arithmetic on huge integers by working mod several small primes at once.

Solve the system

$x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$. From the first, $x = 2 + 3t$; mod 5: $2 + 3t \equiv 3$, $3t \equiv 1$, $t \equiv 2$, so $x = 8 + 15s$. Mod 7: $8 + 15s \equiv 1 + s \equiv 2$, $s \equiv 1$. $x \equiv 23 \pmod{105}$. Check: $23 = 7 \cdot 3 + 2 = 4 \cdot 5 + 3 = 3 \cdot 7 + 2$. ✓

Non-coprime moduli

If the moduli share factors, a solution exists iff $a_i \equiv a_j \pmod{\gcd(m_i, m_j)}$ for every pair, and it is then unique mod lcm.

Where it goes wrong

Claiming uniqueness mod the product when the moduli are not coprime, or solving mod m_1 and mod m_2 separately and then not combining.

Try it: CRT

Find the smallest positive x with $x \equiv 1 \pmod{4}$ and $x \equiv 4 \pmod{9}$.

Answer. $x = 1 + 4t$; mod 9: $1 + 4t \equiv 4$, $4t \equiv 3$, $t \equiv 3 \cdot 7 = 21 \equiv 3$ (since $4^{-1} \equiv 7$). $x = 13$. Check: $13 = 3 \cdot 4 + 1 = 9 + 4$. ✓

9.2 Why It Works

Consider the map from residues mod M to k -tuples of residues $(x \bmod m_1, \dots, x \bmod m_k)$. It is injective: if two residues agree mod every m_i , each m_i divides their difference, and since the m_i are pairwise coprime so does their product M — so the residues are equal mod M . Both sides have exactly M elements (M residues; $m_1 m_2 \cdots m_k$ tuples), and an injection between finite sets of the same size is a bijection. Hence every tuple of remainders is hit exactly once: existence and uniqueness together, with no formula needed.

10 Orders and Primitive Roots

How powers cycle, and quadratic residues

10.1 The Order of an Element

Order

For $\gcd(a, m) = 1$, the **order** of $a \bmod m$ is the least $d > 0$ with $a^d \equiv 1$. Key facts: $a^n \equiv 1$ iff $d \mid n$; hence $d \mid \varphi(m)$. A **primitive root** is an element of order exactly $\varphi(m)$; every prime modulus has one, and then every nonzero residue is a power of it.

The order is the period of the sequence $a, a^2, a^3, \dots \bmod m$. Fermat and Euler only say the period divides $p - 1$ or $\varphi(m)$; the order is the exact period. This is why "find the smallest n with $2^n \equiv 1 \pmod{p}$ " is not answered by Fermat alone, and why decimal expansions of $1/p$ have period equal to the order of $10 \bmod p$.

Order of 2 mod 13

Candidates divide 12: 1, 2, 3, 4, 6, 12. $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \equiv 3$, $2^6 = 64 \equiv 12 \equiv -1$. None is 1, so the order is 12: 2 is a primitive root mod 13.

Period of $1/p$

The decimal expansion of $1/p$ ($p \neq 2, 5$) has period equal to the order of 10 modulo p . For $p = 7$, the order of 10 is 6: $1/7 = 0.\overline{142857}$.

Try it: order

Find the order of 3 modulo 7, and the period of the decimal expansion of $1/13$.

Answer. $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^6 = 36 \equiv 1$: order **6** (a primitive root). For $1/13$: $10^2 = 100 \equiv 9$, $10^3 \equiv 90 \equiv 12 \equiv -1$, so $10^6 \equiv 1$: period **6** ($1/13 = 0.\overline{076923}$).

10.2 Quadratic Residues

Squares mod p

For an odd prime p , exactly half of the nonzero residues are squares (**quadratic residues**). **Euler's criterion:** a is a residue iff $a^{(p-1)/2} \equiv 1$; a non-residue gives -1 . In particular -1 is a square mod p iff $p \equiv 1 \pmod{4}$.

Half the residues are squares because x and $-x$ have the same square and no others do (from $x^2 \equiv y^2$, $p \mid (x - y)(x + y)$). The criterion is Fermat cut in half: $a^{p-1} = (a^{(p-1)/2})^2 \equiv 1$, so $a^{(p-1)/2} \equiv \pm 1$, and it is $+1$ exactly for the squares. The statement about -1 is what makes $x^2 + 1$ factor mod 5, 13, 17, ... and never mod 3, 7, 11, ... — and behind it sits quadratic reciprocity.

Is 2 a square mod 7?

$2^{(7-1)/2} = 2^3 = 8 \equiv 1$: yes. Indeed $3^2 = 9 \equiv 2$ and $4^2 = 16 \equiv 2$.

Where it goes wrong

Concluding $x^2 \equiv a$ has a solution because a is a perfect square as an integer — 4 is a square mod every p , but so is 2 mod 7 and not mod 5. Being a residue depends on p .

Try it: residues

List the quadratic residues mod 11, and decide whether $x^2 \equiv -1 \pmod{11}$ has a solution.

Answer. Squares of $1, \dots, 5$: 1, 4, 9, 5, 3. Residues: $\{1, 3, 4, 5, 9\}$. $-1 \equiv 10$ is not among them, as expected since $11 \equiv 3 \pmod{4}$: **no solution**.

10.3 Why It Works

Let d be the order of a and suppose $a^n \equiv 1$. Divide: $n = dq + r$ with $0 \leq r < d$. Then $1 \equiv a^n = (a^d)^q a^r \equiv a^r$. If $r > 0$ this contradicts the minimality of d ; so $r = 0$ and $d \mid n$. Apply it to $n = \varphi(m)$ (Euler) and $d \mid \varphi(m)$ follows. The division algorithm, once more, is the whole proof.

11 Hard Number Theory

Contest-level problems that combine everything

11.1 Strategy

The toolkit in one place

Hard number theory problems combine a few moves: reduce mod a well-chosen modulus to rule out solutions; factor (SFFT, difference of squares, sums of cubes); bound a variable by size or by the growth of a power; use orders to control exponents; and apply Fermat, Euler, Wilson or CRT to compute residues. Look for the invariant a modulus exposes.

Choose the modulus by what the equation contains: squares suggest mod 4 or mod 8 (squares are $0, 1 \pmod{4}$; $0, 1, 4 \pmod{8}$); cubes suggest mod 7 or 9 (cubes are $0, \pm 1$); powers of 2 suggest mod 3; fourth powers mod 16. If a modulus leaves too many residues, try a product of small primes and reason with CRT.

Bounding with growth

Find all positive n with $n! + 1$ a perfect square: $n! + 1 = m^2$ gives $n! = (m-1)(m+1)$. Small cases: $n = 4$ (25), $n = 5$ (121), $n = 7$ ($5041 = 71^2$). No others are known below 10^9 —

Brocard's problem, still open. Moral: some equations resist every tool, and recognizing that is part of the skill.

Combining orders and Fermat

Show $2^n + 1$ is never divisible by 7. The order of 2 mod 7 is 3, so $2^n \in \{1, 2, 4\} \pmod{7}$ and $2^n + 1 \in \{2, 3, 5\}$ — never 0.

Try it: a classic

Find all primes p such that $p^2 + 2$ is also prime.

Answer. For $p \neq 3$, $p^2 \equiv 1 \pmod{3}$, so $3 \mid p^2 + 2 > 3$: composite. Only $p = \mathbf{3}$ ($9 + 2 = 11$).