ZENITH EDUCATION, JAIPUR

Estd. 1998 | Zenith Point Publishers

HPRCA Teacher (Mathematics) — Mathematics

UNIT 1

Number Systems, Polynomials and Equations

online.zenitheducation.net | notes.zenitheducation.net | 8302450450, 9829607122

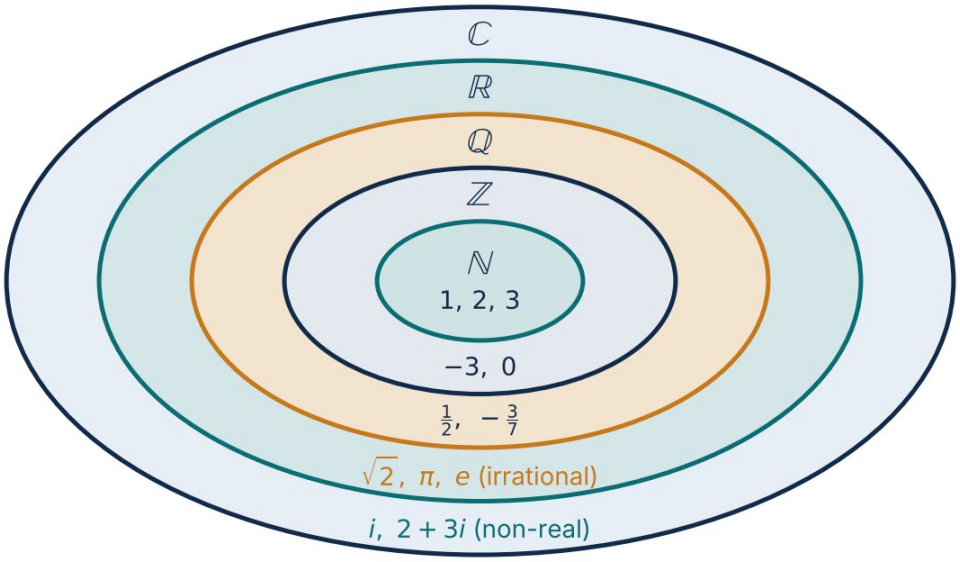
Number Systems and Real Number Properties

1. Overview

This chapter builds the number systems $N \subset Z \subset Q \subset R \subset C$ and the arithmetic facts that every later chapter silently uses. It covers the algebraic and order structure of each system, divisibility in Z (division algorithm, HCF/LCM, Euclid's algorithm, Bezout's identity, Euclid's lemma, the Fundamental Theorem of Arithmetic), rational and irrational numbers, the completeness of R (least upper bound property, Archimedean property, density, countability), and decimal expansions (terminating, recurring, non-unique).

The material serves the "Number System", "Real Numbers" and "Complex Numbers" items of the KVS, NVS, DSSSB and State PGT mathematics syllabi, and it is the base for the real-analysis and algebra units of the degree-level portion. Typical question types: HCF/LCM word problems, divisor counting, irrationality proofs, converting recurring decimals, sup/inf of a set, and "which statement is true" items on Q versus R.

Throughout, $N=\{1,2,3,\ldots\}$ and $N_0=N \cup \{0\}$. (Some books include 0 in N; read the question's convention.)



The chain of number systems; each set sits properly inside the next.

2. The Number Systems

2.1 Natural numbers and induction

The natural numbers satisfy the Peano axioms: $1 \in N$; every n has a successor n+1; 1 is not a successor; distinct numbers have distinct successors; and the induction axiom: a subset of N containing 1 and closed under successor is all of N.

> **Well-Ordering Principle (WOP).** Every non-empty subset of N has a least element. WOP, ordinary induction and strong induction are logically equivalent. The proofs below use WOP freely.

2.2 Integers, rationals, reals, complex numbers

- $Z=\{\ldots,-2,-1,0,1,2,\ldots\}$ is a commutative ring with unity: closed under $+,-,\times$, but not under division.
- $Q=\{p/q : p,q \in Z,\ q \neq 0\}$ is a field (with $p/q=r/s \Leftrightarrow ps=qr$). Every non-zero element has a multiplicative inverse.
- R is a complete ordered field (Section 5).
- $C=\{a+ib : a,b \in R\}$, $i^2=-1$, is a field but cannot be ordered (Section 7).

> **Field axioms.** A set F with + and $\cdot$ is a field if: $(F,+)$ is an abelian group with identity 0; $(F \setminus \{0\}, \cdot)$ is an abelian group with identity $1 \neq 0$; and $a(b+c)=ab+ac$.
> **Ordered field.** A field with a relation $<$ that is a total order, with $a<b \Rightarrow a+c<b+c$, and $a>0,\ b>0 \Rightarrow ab>0$.

Consequences used constantly: $0 \cdot a=0$; $(-1)(-1)=1$; in an ordered field, $a^2>0$ for every $a \neq 0$ (so $1>0$).

2.3 Closure summary

Operation	N	Z	Q	R\Q	R
+	yes	yes	yes	no	yes
-	no	yes	yes	no	yes
×	yes	yes	yes	no	yes
÷ (non-zero)	no	no	yes	no	yes

For the irrationals: $\sqrt{2}+(-\sqrt{2})=0$ and $\sqrt{2} \cdot \sqrt{2}=2$ are rational, so the irrationals are not closed under any of the four operations. However, rational + irrational

is irrational, and non-zero rational × irrational is irrational (otherwise the irrational would equal a rational).

2.4 Order, absolute value and intervals in R

The absolute value is $|x|=x$ for $x\geq 0$ and $|x|=-x$ for $x<0$. For $a>0$: $|x|<a \Leftrightarrow -a<x<a$, and $|x|>a \Leftrightarrow x>a$ or $x<-a$.

Triangle inequality. $|x+y|\leq|x|+|y|$ and $||x|-|y||\leq|x-y|$ for all real x,y.
AM-GM. For $a,b\geq 0$: $(a+b)/2\geq\sqrt{(ab)}$, with equality iff $a=b$.

Proof. Since $-|x|\leq x\leq|x|$ and $-|y|\leq y\leq|y|$, adding gives $-(|x|+|y|)\leq x+y\leq|x|+|y|$, i.e. $|x+y|\leq|x|+|y|$. For the second form apply the first to $x=(x-y)+y$. AM-GM follows from $(\sqrt{a}-\sqrt{b})^2\geq 0$. ▫

Intervals are the connected subsets of R: open (a,b), closed $[a,b]$, half-open, and the unbounded rays. A set is an interval iff it contains every point between any two of its points; this property depends on completeness (the corresponding subset of Q has "holes"). Order facts that exam questions test: multiplying an inequality by a negative number reverses it; $x<y$ with $x,y>0$ gives $1/x>1/y$; and $x^2<y^2 \Leftrightarrow |x|<|y|$, so $x^2<y^2$ does **not** imply $x<y$ (take $x=-3$, $y=2$).

3. Divisibility in the Integers

3.1 Definitions

Divisibility. For $a,b\in Z$, $a\mid b$ means $b=ak$ for some $k\in Z$. Basic rules: 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 $a\mid b$ and $b\neq 0$ then $|a|\leq|b|$.
HCF (GCD). $\gcd(a,b)$ is the largest positive integer dividing both (not both zero). a,b are coprime if $\gcd(a,b)=1$.
LCM. $\operatorname{lcm}(a,b)$ is the smallest positive integer divisible by both.
Prime. An integer $p>1$ whose only positive divisors are 1 and p. An integer $n>1$ that is not prime is composite. The number 1 is neither.

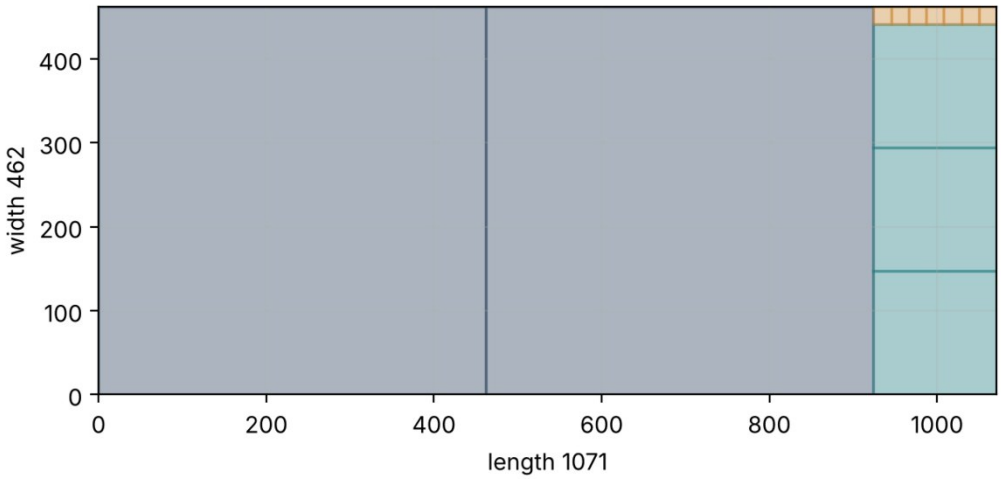
3.2 Division algorithm

Theorem (Division Algorithm). For integers a and $b>0$ there exist unique integers q,r with
$a=bq+r, \quad 0\leq r<b$.

Proof. Let $S=\{a-bk : k\in Z,\ a-bk\geq 0\}$. It is non-empty (take $k=-|a|$), so by WOP it has a least element $r=a-bq\geq 0$. If $r\geq b$ then $r-b=a-b(q+1)\in S$ is smaller than r, a contradiction; so $0\leq r<b$. For uniqueness, if $bq+r=bq'+r'$ with $0\leq r,r'<b$ then $b(q-q')=r'-r$ has absolute value $<b$ and is a multiple of b, hence 0. ▫

3.3 Euclid's algorithm and Bezout's identity

Repeated division gives $\gcd(a,b)=\gcd(b,r)$ because the common divisors of (a,b) and of (b,r) coincide (as $r=a-bq$). Continue until the remainder is 0; the last non-zero remainder is the HCF.



Euclid's algorithm for gcd(1071,462) as a rectangle-tiling process: two 462-squares, then three 147-squares, then seven 21-squares exhaust the rectangle, so gcd=21.

Theorem (Bezout). If $d=\gcd(a,b)$ then there exist integers x,y with $ax+by=d$. Moreover d is the smallest positive value of $ax+by$ over all integers x,y.

Proof. Let d' be the least positive element of $\{ax+by\}$ (non-empty set; WOP). Divide: $a=d'q+r$ with $0\leq r<d'$. Then $r=a-q(ax_0+by_0)$ is again of the form $ax+by$ and is smaller than d', so $r=0$ and $d'\mid a$. Likewise $d'\mid b$. Conversely any common divisor of a,b divides $ax_0+by_0=d'$, so d' is the greatest common divisor. ▫

Corollary. a,b are coprime iff $ax+by=1$ is solvable in integers. If $\gcd(a,c)=1$ and $\gcd(b,c)=1$ then $\gcd(ab,c)=1$. If $c\mid ab$ and $\gcd(c,a)=1$ then $c\mid b$.

3.4 Euclid's lemma

Euclid's Lemma. If p is prime and $p\mid ab$, then $p\mid a$ or $p\mid b$. By induction, $p\mid a_1a_2\cdots a_n$ implies $p\mid a_i$ for some i.

Proof. Suppose $p\nmid a$. The only positive divisors of p are $1,p$, so $\gcd(p,a)=1$. By Bezout, $px+ay=1$. Multiply by b: $b=pbx+(ab)y$. Both terms on the right are divisible by p, so $p\mid b$. □

The lemma fails for composite moduli: $6\mid 2\cdot 3$ but $6\nmid 2$ and $6\nmid 3$.

3.5 Fundamental Theorem of Arithmetic

Theorem (FTA). Every integer n>1 can be written as a product of primes, and this factorisation is unique apart from the order of the factors: $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, $p_1<p_2<\dots<p_k$ primes, $a_i\geq 1$.

Proof. Existence, by strong induction: 2 is prime. If n>2 is prime we are done; otherwise n=rs with 1<r,s<n, and each of r,s is a product of primes by hypothesis.

Uniqueness: suppose $p_1\cdots p_m=q_1\cdots q_n$ with all p_i,q_j prime. Then $p_1 \mid q_1\cdots q_n$, so by Euclid's lemma $p_1 \mid q_j$ for some j; as q_j is prime, $p_1=q_j$. Cancel and repeat (induction on m). □

Infinitude of primes. If $p_1,\dots,p_k$ were all the primes, $N=p_1\cdots p_k+1>1$ has a prime factor p_i by FTA; then $p_i \mid N-p_1\cdots p_k=1$, absurd.

3.6 Consequences of FTA

Let $a=\prod p_i^{\alpha_i}$ and $b=\prod p_i^{\beta_i}$ (exponents ≥ 0, over a common set of primes). Then

$\gcd(a,b)=\prod p_i^{\min(\alpha_i,\beta_i)}$, $\operatorname{lcm}(a,b)=\prod p_i^{\max(\alpha_i,\beta_i)}$, $\gcd(a,b)\cdot\operatorname{lcm}(a,b)=ab$.

The last identity holds because $\min+\max=\alpha_i+\beta_i$. It is valid for **two** numbers only; for three numbers $\gcd\cdot\operatorname{lcm}\neq abc$ in general.

For $n=p_1^{a_1}\cdots p_k^{a_k}$:

$\tau(n)=\prod_i (a_i+1)$, $\sigma(n)=\prod_i \frac{p_i^{a_i+1}-1}{p_i-1}$, $\varphi(n)=n\prod_i \left(1-\frac{1}{p_i}\right)$,

where $\tau(n)$ is the number of positive divisors, $\sigma(n)$ their sum, and $\varphi(n)$ the number of integers in $\{1,\dots,n\}$ coprime to n. Also n is a perfect square iff every a_i is even, iff $\tau(n)$ is odd. The number of divisors of n that are perfect squares is $\prod\left(\lfloor a_i/2\rfloor+1\right)$.

Legendre's formula. The exponent of a prime p in n! is

$v_p(n!)=\sum_{k\geq 1}\lfloor n/p^k\rfloor$.

The number of trailing zeros of n! is $v_5(n!)$, since powers of 2 are always more plentiful.

3.7 HCF and LCM of fractions and word-problem rules

For fractions in lowest terms,

$\mathrm{HCF}\left(\frac{a_1}{b_1},\frac{a_2}{b_2},\dots\right)=\frac{\mathrm{HCF}(a_i)}{\mathrm{LCM}(b_i)}$, $\mathrm{LCM}\left(\frac{a_1}{b_1},\frac{a_2}{b_2},\dots\right)=\frac{\mathrm{LCM}(a_i)}{\mathrm{HCF}(b_i)}$.

Standard word-problem translations:

Situation	Answer
Greatest number dividing a,b,c exactly	HCF(a,b,c)
Greatest number dividing a,b,c leaving remainders r_1,r_2,r_3	HCF$(a-r_1,b-r_2,c-r_3)$ (must exceed every r_i)
Least number divisible by a,b,c	LCM(a,b,c)
Least number leaving the same remainder r on division by a,b,c	LCM(a,b,c)+r
Events repeating every a,b,c units, together again after	LCM(a,b,c)

3.8 Linear Diophantine equations

Theorem. The equation $ax+by=c$ (with a,b not both zero) has an integer solution iff $\gcd(a,b) \mid c$. If (x_0,y_0) is one solution and $d=\gcd(a,b)$, all solutions are $x=x_0+b/d\,t$, $y=y_0-a/d\,t$, $t\in\mathbb{Z}$.

Necessity is immediate (the left side is a multiple of d). Sufficiency: Bezout gives $ax_1+by_1=d$; multiply by c/d. The general solution follows because $a(x-x_0)=-b(y-y_0)$ forces $b/d \mid (x-x_0)$.

3.9 Congruence in one paragraph

$a\equiv b \pmod m$ means $m \mid (a-b)$. Congruence respects $+,-,\times$ and powers. A congruence $ax\equiv c \pmod m$ is solvable iff $\gcd(a,m) \mid c$, with $\gcd(a,m)$ solutions modulo m when solvable. A perfect square is $\equiv 0,1 \pmod 4$ and $\equiv 0,1,4 \pmod 8$; this is the usual tool for "can n be a sum of two squares" and "is n a square" items.

3.10 Primes: testing and standard facts

Trial division test. A positive integer n>1 is composite iff it has a prime divisor $p\leq\sqrt{n}$. Reason: if n=rs with $1<r\leq s$ then $r^2\leq rs=n$, so the smaller factor is at most $\sqrt{n}$, and any prime factor of r is a prime factor of n that is at most $\sqrt{n}$.

Form $6k\pm1$. Every prime p>3 is $\equiv\pm1 \pmod 6$ (otherwise 2 or 3 divides it). Hence $p^2\equiv 1 \pmod{24}$ for every prime p>3.

Consecutive integers. $\gcd(n,n+1)=1$, so $n(n+1)$ is a product of coprime numbers; a product of k consecutive integers is divisible by k!.

For example, to test 367: $\sqrt{367}\approx 19.2$, so it suffices to try the primes 2,3,5,7,11,13,17,19; none divides 367, hence 367 is prime. The primes below 60 are 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59. A perfect number equals the sum of its proper divisors, equivalently $\sigma(n)=2n$; if 2^p-1 is prime then $2^{p-1}(2^p-1)$ is perfect (e.g. 6, 28, 496).

Proof that $p^2\equiv 1 \pmod{24}$. Write $p^2-1=(p-1)(p+1)$. Both factors are even, and one of them is divisible by 4 (they are consecutive even numbers), so $8 \mid p^2-1$. Among $p-1,p,p+1$ exactly one is divisible by 3, and it is not p, so $3 \mid p^2-1$. As $\gcd(8,3)=1$, $24 \mid p^2-1$. □

3.11 Inverses modulo m

By Bezout, a has a multiplicative inverse modulo m iff $\gcd(a,m)=1$: from $ax+my=1$ we get $ax\equiv 1 \pmod m$. For example, $7\cdot 8=56=5\cdot 11+1$ so $7^{-1}\equiv 8$

(mod 11); this is the integer-world counterpart of the fact that every non-zero rational has an inverse in Q, and it shows Z_p is a field exactly when p is prime.

4. Rational and Irrational Numbers

4.1 Irrational numbers

A real number is irrational if it is not of the form p/q with p,q∈Z, q≠0. Every rational can be written with gcd(p,q)=1, q>0 (lowest terms); this representation is unique.

Theorem 1. If p is prime, √p is irrational.
Theorem 2. For a positive integer n, √n is either an integer or irrational. More generally, if a positive integer n is not a perfect k-th power then k√n is irrational.
Theorem 3 (Rational Root Theorem). If p/q in lowest terms is a root of $a_n x^n+\dots+a_1x+a_0$ with integer coefficients, then $p \mid a_0$ and $q \mid a_n$. In particular a monic integer polynomial has only integer rational roots.

Proof of Theorem 1. Suppose √p=a/b in lowest terms. Then $a^2=pb^2$, so $p \mid a^2$, and by Euclid's lemma $p \mid a$. Write a=pc: $p^2c^2=pb^2$, so $b^2=pc^2$ and likewise $p \mid b$. This contradicts gcd(a,b)=1. ▫

Proof of Theorem 2. If n=∏p_i^(a_i) and √n=a/b then $nb^2=a^2$. Compare the exponent of each prime on both sides: a_i+2v_(p_i)(b)=2v_(p_i)(a), so every a_i is even and n is a perfect square. The k-th root case is identical with exponents divisible by k. ▫

Proof of Theorem 3. Substitute x=p/q and multiply by q^n: $a_n p^n+a_{n-1}p^{n-1}q+\dots+a_0q^n=0$. Every term except a_0q^n is divisible by p, so $p \mid a_0q^n$ and, as gcd(p,q)=1, $p \mid a_0$. Symmetrically $q \mid a_n p^n$ gives $q \mid a_n$. ▫

Theorem 3 gives a quick irrationality test: $\sqrt[3]{2}$ is a root of x^3-2, whose only possible rational roots are ±1,±2, and none works. Similarly √2+√3 is a root of x^4-10x^2+1 (verified in Worked Example 7), with only candidates ±1; neither is a root, so √2+√3 is irrational.

Other standard irrationals. $\log_{10}2$ is irrational (if $\log_{10}2=p/q$ with p,q>0 then 2^q=10^p=2^p5^p, impossible by uniqueness of factorisation). The number e=∑_(n≥0) 1/n! is irrational: if e=a/b then b! e−∑_(n≤b) b!/n! is a positive integer smaller than ∑_(k≥1) 1/(b+1)^k≤1, a contradiction. The irrationality of π is true but harder; e and π are in fact transcendental (not roots of any non-zero integer polynomial). Numbers that are roots of integer polynomials are called algebraic.

4.2 Numbers of the form a+b√d

For a positive integer d that is not a perfect square, $\mathbb{Q}(\sqrt{d})=\{a+b\sqrt{d} : a,b\in\mathbb{Q}\}$ is a field: it is closed under the four operations because $(a+b\sqrt{d})(a-b\sqrt{d})=a^2-db^2\neq 0$ unless a=b=0, which lets us rationalise denominators:

$1/(a+b\sqrt{d})=(a-b\sqrt{d})/(a^2-db^2)$.

Equating parts. If a,b,c,e∈Q and a+b√d=c+e√d then a=c and b=e. (Otherwise √d=(a−c)/(e−b) would be rational.) In particular a+b√d=0 with a,b rational forces a=b=0.

This is the standard tool for questions such as "find rational a,b with $(a+b\sqrt{2})^2=17+12\sqrt{2}$" (Worked Example 16).

4.3 Density

Theorem (Density). Between any two distinct real numbers a<b there are infinitely many rationals and infinitely many irrationals.

The rational case follows from the Archimedean property (Section 5.3): choose n with n(b−a)>1; then some integer m satisfies na<m<nb, so m/n∈(a,b). For the irrational case apply this to $a/\sqrt{2}<b/\sqrt{2}$ to get a non-zero rational r there (there are infinitely many, so 0 can be avoided), and then $r\sqrt{2}\in(a,b)$ is irrational. Neither set has a "next" element: there is no smallest positive rational or irrational.

5. Completeness of the Real Numbers

5.1 Bounds, supremum and infimum

Let S⊆R be non-empty. An upper bound u satisfies s≤u for all s∈S; S is bounded above if one exists. The supremum supS is the least upper bound.

Characterisation. M=supS iff (i) M is an upper bound of S, and (ii) for every ε>0 there is s∈S with s>M−ε. Similarly m=infS iff m is a lower bound and for each ε>0 some s∈S has s<m+ε.
Completeness Axiom (LUB property). Every non-empty subset of R that is bounded above has a supremum in R. Equivalently, every non-empty set bounded below has an infimum in R.

The supremum need not belong to the set: sup{1−1/n:n∈N}=1∉S, while sup[0,1]=max[0,1]=1. If supS∈S it is the maximum.

5.2 Q is not complete

Let $S=\{x\in\mathbb{Q} : x>0,\ x^2<2\}$. It is bounded above by 2 but has no least upper bound in Q. Indeed, for rational x>0 put

$y=(2x+2)/(x+2)$, $y^2-2=(2(x^2-2))/((x+2)^2)$, $y-x=(2-x^2)/(x+2)$.

If x∈S then y>x and $y^2<2$, so y∈S and S has no largest element. If x is a rational upper bound then $x^2>2$ (as $x^2=2$ is impossible), whence y<x and $y^2>2$, so y is a smaller rational upper bound. Thus no rational is a least upper bound, although √2∈R is one. This is the precise sense in which Q has "holes" and R does not.

5.3 Consequences of completeness

Archimedean Property. For every real x there is n∈N with n>x. Equivalently, for a,b>0 there is n with na>b; and inf{1/n:n∈N}=0.
Nested Interval Property. If $I_1\supseteq I_2\supseteq\cdots$ are closed bounded intervals, then ⋂_nI_n≠∅ (the intersection is a single point if the lengths tend to 0).

Monotone Convergence. A bounded monotone sequence of reals converges (to its sup if increasing, to its inf if decreasing).
Cauchy completeness. Every Cauchy sequence of reals converges. This fails in Q: the rational sequence 1,1.4,1.41,1.414,… is Cauchy and converges to $\sqrt{2} \notin Q$.

Proof of the Archimedean property. If N were bounded above, it would have a supremum M; then M−1 is not an upper bound, so n>M−1 for some n∈N, and n+1>M contradicts M being an upper bound. ▫

The Archimedean property, density of Q, nested intervals, monotone convergence, Dedekind cuts and Cauchy completeness are all consequences of (or, with the Archimedean property, equivalent to) the LUB axiom. A Dedekind cut is a partition of Q into two non-empty sets A<B with A having no greatest element; in R every cut is produced by a real number (the cut for $\sqrt{2}$ has $A=\{x \in Q : x \leq 0 \text{ or } x^2<2\}$).

5.4 Countability

A set is countable if it is finite or can be put in one-to-one correspondence with N.

- Z and Q are countably infinite. For Q: list the positive fractions p/q along the diagonals p+q=2,3,4,… skipping repeated values; negatives and 0 are handled as for Z. A countable union of countable sets is countable, and so is a finite Cartesian product of countable sets.
- The set of algebraic numbers is countable (countably many integer polynomials, each with finitely many roots).
- R, every non-degenerate interval, and R\Q are uncountable.

Proof that (0,1) is uncountable (Cantor). Suppose the numbers of (0,1) are listed as $x_1, x_2, \ldots$ with non-terminating decimal expansions x_n=0.d_(n1)d_(n2)d_(n3)…. Define $y=0.e_1e_2e_3\ldots$ with e_n=5 if d_(nn)≠5 and e_n=6 if d_(nn)=5. Then y∈(0,1) has digits only 5,6 (so no ambiguity of expansion) and differs from each x_n in the n-th digit, so y is not in the list. ▫

Since Q is countable and R is not, “most” real numbers are irrational, indeed transcendental. Yet both Q and R\Q are dense.

6. Decimal Expansions

Every real number has a decimal expansion $a_0.d_1d_2d_3\ldots$ (obtained by successive division, or as sup of its truncations). Real numbers with a terminating expansion have exactly two expansions, e.g. $0.5 = 0.4999\ldots$; all other reals have exactly one.

$0.\overline{9} = 1$. $\sum_{(k \geq 1)} 9 \cdot 10^{(-k)} = (9/10)/(1-1/10) = 1$. Equivalently, $x = 0.\overline{9} \Rightarrow 10x - x = 9 \Rightarrow x = 1$.
Theorem (Rational iff terminating or recurring). A real number is rational iff its decimal expansion is terminating or eventually periodic.
Theorem (Terminating criterion). Let p/q be in lowest terms, q>1. Then p/q has a terminating decimal expansion iff q=2^a5^b with a,b≥0. The number of decimal places is max(a,b).
Pure/mixed recurrence. If q=2^a5^bq′ with gcd(q′,10)=1 and q′>1, the expansion is eventually periodic with pre-period (non-repeating digits) of length max(a,b) and period equal to the multiplicative order of 10 modulo q′, i.e. the least k with q′ | 10^k−1. The period divides φ(q′) and is less than q′.

Proof sketch. In long division of p by q each step produces a remainder in {0,1,…,q−1}. If 0 appears the expansion terminates; otherwise some remainder repeats within q steps and from then on the digits repeat. Conversely, a periodic tail is a geometric series, giving a rational (see the conversions below). For the terminating criterion: p/q=m/(10^k) forces q | 10^k=2^k5^k, so q has no prime factors other than 2,5; conversely q=2^a5^b with k=max(a,b) gives p/q=(p · 2^(k−a)5^(k−b))/(10^k). ▫

Converting recurring decimals to fractions

For a pure recurrence with a block of k digits,
$0.d_1\ldots d_\overline{k} = (d_1\ldots d_k)/(10^k-1)$.
For a mixed recurrence $0.a_1\ldots a_md_1\ldots d_\overline{k}$,
value=$(a_1\ldots a_md_1\ldots d_\overline{k} - a_1\ldots a_\overline{m})/(10^m(10^k-1))$,
where $a_1\ldots a_md_1\ldots d_\overline{k}$ and $a_1\ldots a_\overline{m}$ denote the integers formed by those digit strings. In words: (digit string up to the end of the first period) minus (the non-repeating part), over as many 9s as the period length followed by as many 0s as the pre-period length.

Fraction	Decimal	Pre-period	Period
1/3	$0.\overline{3}$	0	1
1/7	$0.14285\overline{7}$	0	6
1/11	$0.0\overline{9}$	0	2
1/13	$0.07692\overline{3}$	0	6
1/6	$0.1\overline{6}$	1	1
1/17	period 16	0	16

An irrational number has a non-terminating, non-recurring expansion. Conversely, any expansion that is visibly non-recurring is irrational, e.g. 0.101001000100001… (the gaps of zeros grow without bound) and 0.123456789101112… (concatenated integers).

7. Complex Numbers (Structure)

Formally $C = R^2$ with
(a,b)+(c,d)=(a+c,b+d), (a,b)(c,d)=(ac−bd, ad+bc),

and a+ib is notation for (a,b), with R embedded as {(a,0)}. This is a field; 1/(a+ib)=(a−ib)/(a²+b²).

Conjugate and modulus. For z=a+ib: $\overline{z}$=a−ib, |z|=√(a²+b²), z$\overline{z}$=|z|², z$\overline{w}$=$\overline{z}$ $\overline{w}$, |zw|=|z||w|, |z+w|≤|z|+|w|.
Square root. For z=a+ib with b≠0,
√z=±(√((|z|+a)/2)+i sgn(b)√((|z|−a)/2)).
No ordering. C admits no order making it an ordered field: in such a field 1=1²>0 and −1=i²>0 (squares of non-zero elements are positive), contradicting 1+(−1)=0. So statements like "i>0" or "2+i<3+i" are meaningless.

C is algebraically closed: every non-constant polynomial over C has a root in C. It is not complete in the order sense (no order) but is complete as a metric space under |z−w|. The n-th roots of unity e^(2πik/n) (k=0,…,n−1) sum to 0 for n≥2.

8. Formula and Result Sheet

Divisibility. a=bq+r, 0≤r<b; gcd(a,b)=gcd(b,r); gcd(a,b)lcm(a,b)=ab (two numbers only).
Counting. n=∏p_i^(a_i): τ(n)=∏(a_i+1); σ(n)=∏(p_i^(a_i+1)−1)/(p_i−1); φ(n)=n∏(1−1/(p_i)); product of all divisors =n^(τ(n)/2); v_p(n!)=∑⌊n/p^k⌋.
Fractions. HCF=(HCF(num))/(LCM(den)), LCM=(LCM(num))/(HCF(den)).
Diophantine. ax+by=c solvable iff gcd(a,b)|c; x=x₀+b/dt, y=y₀−a/dt.
Special gcds. gcd(2^m−1,2^n−1)=2^(gcd(m,n))−1; gcd(F_m,F_n)=F_(gcd(m,n)) for Fibonacci numbers; consecutive integers are coprime; gcd(n,n+k)=gcd(n,k).
Irrationality. √n∉Q unless n is a perfect square; rational ± irrational and non-zero rational × irrational are irrational; √2,√3,∛2,log₁₀2,e,π are irrational.
Sup/inf. supS is the least upper bound; completeness of R ⇔ every non-empty bounded-above set has a sup ⇔ Cauchy completeness plus Archimedean.
Decimals. p/q (lowest terms) terminates iff q=2^a5^b; 0.d₁…d_$\overline{k}$=(d₁…d_k)/(10^k−1); 0.$\overline{9}$=1; rational ⇔ terminating or recurring.
Cardinality. N,Z,Q, algebraic numbers: countable. R,R\Q,C: uncountable.

9. Worked Examples

Worked Example 1. Find the HCF and LCM of 396 and 540 and verify gcd · lcm=ab.
Solution. By FTA, 396=2² · 3² · 11 and 540=2² · 3³ · 5. Take the minimum exponents for the HCF and the maximum for the LCM:
gcd=2² · 3²=36, lcm=2² · 3³ · 5 · 11=5940.
Check: 36×5940=213840=396×540. ✓
Worked Example 2. Use Euclid's algorithm to find gcd(1071,462) and express it as 1071x+462y.
Solution. Divide repeatedly:
[1071, =2 · 462+147,; 462, =3 · 147+21,; 147, =7 · 21+0.]
So gcd=21. Back-substitute:
[21, =462−3 · 147; , =462−3 (1071−2 · 462); , =7 · 462−3 · 1071.]
Hence x=−3, y=7: indeed −3213+3234=21. ✓ (The figure in Section 3.3 shows the tiling picture of these three steps.)
Worked Example 3. For n=360 find the number of divisors, their sum, the number of integers up to 360 coprime to 360, and the number of divisors that are perfect squares.
Solution. 360=2³ · 3² · 5.
τ=(3+1)(2+1)(1+1)=24, σ=(2⁴−1)/1 · (3³−1)/2 · (5²−1)/4=15 · 13 · 6=1170.
φ(360)=360 · 1/2 · 2/3 · 4/5=96.
Square divisors need even exponents: 2^(0 or 2), 3^(0 or 2), 5⁰, giving 2 · 2 · 1=4 (namely 1,4,9,36).
Worked Example 4. Find the number of trailing zeros in 100! and the highest power of 7 dividing 200!.
Solution. Trailing zeros =v₅(100!)=⌊100/5⌋+⌊100/25⌋=20+4=24 (powers of 2 are plentiful, v₂(100!)=97). For 7 in 200!: ⌊200/7⌋+⌊200/49⌋=28+4=32 (and 343>200 adds nothing). So $7^{32} \mid\mid 200!$.
Worked Example 5. (PGT style.) Find the greatest number that divides 1251, 9377 and 15628 leaving remainders 1, 2 and 3 respectively.
Solution. The required number divides 1250, 9375 and 15625 and exceeds 3. Factorise: 1250=2 · 5⁴, 9375=3 · 5⁵, 15625=5⁶. So HCF=5⁴=625. Check: 1251=625 · 2+1, 9377=625 · 15+2, 15628=625 · 25+3. Since 625>3, the answer is 625.
Worked Example 6. (PGT style.) Find the HCF and LCM of 2/3, 8/9, (16)/(81). Also find the least number which leaves remainder 5 when divided by 12, 15 and 20.
Solution. Numerators 2,8,16: HCF =2, LCM =16. Denominators 3,9,81: HCF =3, LCM =81. Therefore
HCF=2/(81), LCM=(16)/3.
(Check: (16)/3/2/3=8, (16)/3/8/9=6, (16)/3/(16)/(81)=27, all integers.) For the second part, lcm(12,15,20)=60, so the number is 60+5=65.
Worked Example 7. Prove that √2+√3 is irrational.
Solution. Suppose √2+√3=r∈Q. Squaring, 5+2√6=r², so √6=(r²−5)/2 would be rational. But 6 is not a perfect square, so √6 is irrational (Theorem 2), a contradiction.
Alternative: x=√2+√3 satisfies (x²−5)²=24, i.e. x⁴−10x²+1=0. The only candidates for rational roots are ±1, and 1−10+1=−8≠0, so x is irrational by the Rational Root Theorem.
Worked Example 8. Express 0.43$\overline{7}$ as a fraction, and write (13)/(84) as a decimal, stating its pre-period and period.
Solution. Let x=0.4373737…. Then 10x=4.3737… and 1000x=437.3737…, so 990x=437−4=433 and x=(433)/(990). By the formula: (digits 437) - (non-repeating digit 4) over 990, the same.
For 13/84: 84=2² · 3 · 7 has the 2² factor, so the pre-period is max(2,0)=2. The remaining denominator is q′=21, and the period is the order of 10 modulo 21, which is 6 (as 10⁶−1=999999=21 · 47619 and no smaller power works). Long division gives
(13)/(84)=0.1547619$\overline{0}$.

Worked Example 9. Determine whether 7/(80) and (13)/(84) have terminating decimal expansions and, if so, the number of decimal places.

Solution. 7/(80): gcd(7,80)=1 and $80=2^4\cdot 5$, so it terminates, with max(4,1)=4 decimal places: 0.0875. (13)/(84): gcd(13,84)=1 and $84=2^2\cdot 3\cdot 7$ contains primes other than 2,5, so it does not terminate (Example 8). Note that the test applies only **after** reducing to lowest terms: (21)/(84)=1/4=0.25 terminates even though 84 contains 3 and 7.

Worked Example 10. Find all positive integer solutions of 18x+30y=66.

Solution. gcd(18,30)=6 and $6\mid 66$, so solutions exist. Divide by 6: 3x+5y=11. A particular solution is $(x_0,y_0)=(2,1)$. The general solution is

$x=2+5t,\qquad y=1-3t,\qquad t\in Z.$

Both positive requires t>−2/5 and t<1/3, i.e. t=0. The only positive solution is (x,y)=(2,1).

Worked Example 11. (NET/lecturer style.) Let $S=\{(-1)^n+1/n : n\in N\}$. Find supS and infS and state whether they belong to S.

Solution. The terms: n=1: 0; n=2: 3/2; n=3: −2/3; n=4: 5/4; and so on. For even n the term is 1+1/n, decreasing from 3/2 towards 1. For odd n the term is −1+1/n, which starts at 0 (n=1) and decreases (−2/3,−4/5,…) towards −1, always staying above −1.

Hence every element lies in (−1,3/2], and 3/2 is attained at n=2, so supS=maxS=3/2∈S. The odd-index terms −1+1/n get arbitrarily close to −1, but are never equal to it, so infS=−1∉S (there is no minimum).

Worked Example 12. (NET/lecturer style.) Show that gcd(2^12−1, 2^18−1)=2^(gcd(12,18))−1=63, and prove the general identity gcd(2^m−1,2^n−1)=2^(gcd(m,n))−1.

Solution. Numerically, $2^{12}-1=4095=3^2\cdot 5\cdot 7\cdot 13$ and $2^{18}-1=262143=3^3\cdot 7\cdot 19\cdot 73$, so the gcd is $3^2\cdot 7=63=2^6-1$. ✓

General proof: for m>n, write m=n+k. Then 2^m−1=2^k(2^n−1)+(2^k−1), so gcd(2^m−1,2^n−1)=gcd(2^n−1,2^k−1) with k=m−n. Thus the pair of exponents (m,n) is replaced by (m−n,n), exactly the subtractive form of Euclid's algorithm, which ends at the pair (d,d) with d=gcd(m,n). There gcd(2^d−1,2^d−1)=2^d−1.

Worked Example 13. Show that n^3-n is divisible by 6 for every integer n, and that $\log_{10}2$ is irrational.

Solution. $n^3-n=(n-1)n(n+1)$ is a product of three consecutive integers. One of them is even and one is a multiple of 3; since gcd(2,3)=1 the product is divisible by $2\cdot 3=6$.

If $\log_{10}2=p/q$ with positive integers p,q, then 2=10^(p/q), so 2^q=10^p=2^p5^p. The right side has the prime factor 5 ($p\geq 1$) but the left does not, contradicting the uniqueness part of FTA. Hence $\log_{10}2$ is irrational.

Worked Example 14. (PGT style, complex numbers.) Find √(3+4i) and simplify (3+4i)/(1−2i).

Solution. Here |3+4i|=5, so

√(3+4i)=±(√((5+3)/2)+i√((5−3)/2))=±(2+i).

Check: $(2+i)^2=4+4i-1=3+4i$. ✓ For the quotient, multiply by the conjugate:

(3+4i)/(1−2i)=(3+4i)(1+2i)/(1+4)=(3+6i+4i−8)/5=(−5+10i)/5=−1+2i.

Worked Example 15. (PGT style.) Show that if p>3 is a prime then $24\mid p^2-1$, and hence find the remainder when p^2+23 is divided by 24 for p=7.

Solution. $p^2-1=(p-1)(p+1)$. The two factors are consecutive even numbers, so one is a multiple of 4 and the product is divisible by 8. Among p−1,p,p+1 one is a multiple of 3 and it is not p, so $3\mid p^2-1$. Therefore $24\mid p^2-1$. For p=7: $p^2-1=48=2\cdot 24$, and $p^2+23=49+23=72=3\cdot 24$, so the remainder is 0.

Worked Example 16. Find rational numbers a,b such that $(a+b\sqrt{2})^2=17+12\sqrt{2}$.

Solution. Expanding, $(a^2+2b^2)+2ab\sqrt{2}=17+12\sqrt{2}$. Equating rational and irrational parts (legitimate because √2 is irrational): $a^2+2b^2=17$ and ab=6. Substituting b=6/a: $a^2+72/a^2=17$, so $a^4-17a^2+72=0$, i.e. $(a^2-8)(a^2-9)=0$. Rational a forces $a^2=9$, a=±3, b=±2. Hence $a+b\sqrt{2}=\pm(3+2\sqrt{2})$, and indeed $(3+2\sqrt{2})^2=9+8+12\sqrt{2}=17+12\sqrt{2}$. ✓ (The root $a^2=8$ would give $a=2\sqrt{2}$, which is not rational.)

Worked Example 17. Show that gcd(5n+3, 7n+4)=1 for every integer n, and find the least positive integer leaving remainders 2,3,2 on division by 3,5,7.

Solution. Any common divisor d divides 7(5n+3)−5(7n+4)=21−20=1, so d=1.

For the second part, the conditions are $N\equiv 2 \pmod 3$, $N\equiv 3 \pmod 5$, $N\equiv 2 \pmod 7$. The first and third combine to $N\equiv 2 \pmod{21}$ (since gcd(3,7)=1), so N=2+21k. Then $2+21k\equiv 3 \pmod 5$ gives $k\equiv 1 \pmod 5$ (as $21\equiv 1$), so k=1 is the least choice and N=23. Check: $23=3\cdot 7+2$, $23=5\cdot 4+3$, $23=7\cdot 3+2$. ✓ Note that the "LCM+r" shortcut of Section 3.7 does not apply, because the remainders 2,3,2 are not equal; one must solve the congruences, as above.

Worked Example 18. (NET/lecturer style.) True or false, with reason: (a) the set $\{x\in Q : x^2<3\}$ has a supremum in Q; (b) $\{x\in R : x^2<3\}$ has a supremum in R; (c) between √2 and √3 there is a rational and an irrational number.

Solution. (a) False. $T=\{x\in Q : x^2<3\}$ is bounded above (by 2), and its real supremum is √3, which is irrational; since a rational supremum would also be a real supremum and the real supremum is unique, T has no supremum in Q. (b) True: the set is (−√3,√3), bounded above and non-empty, so sup=√3 by the LUB axiom (not attained). (c) True by density: $1.5\in(\sqrt{2},\sqrt{3})$ since $\sqrt{2}\approx 1.414<1.5<1.732\approx\sqrt{3}$, and $(11)/(10)\sqrt{2}\approx 1.556$ also lies in the interval and is irrational (a non-zero rational times an irrational).

10. Exam Traps

Exam Trap. "gcd(a,b,c) · lcm(a,b,c)=abc." This is false. The identity gcd · lcm=product holds for exactly two numbers. Counter-example: 2,4,8 have gcd=2, lcm=8, so gcd · lcm=16 while abc=64.

Exam Trap. Applying the terminating-decimal test before reducing. (21)/(84) looks non-terminating because $84=4\cdot 3\cdot 7$, but (21)/(84)=1/4=0.25. Always cancel to lowest terms first.

Exam Trap. Believing the sum or product of two irrationals is irrational. $\sqrt{2}+(-\sqrt{2})=0$ and $\sqrt{2}\cdot\sqrt{2}=2$. Likewise $(\sqrt{2}+1)(\sqrt{2}-1)=1$. Only rational ± irrational and non-zero rational × irrational are guaranteed irrational. Also $0\times\sqrt{2}=0$ is rational: the word "non-zero" matters.

Exam Trap. Treating Euclid's lemma as true for composite divisors, i.e. "$n\mid ab\Rightarrow n\mid a$ or $n\mid b$". It fails ($6\mid 4\cdot 9$ but $6\nmid 4$, $6\nmid 9$). The correct statement for general n needs gcd(n,a)=1 to conclude $n\mid b$.

Exam Trap. Saying supS always belongs to S, or that a bounded set has a maximum. $S=\{1-1/n\}$ is bounded with supS=1∉S and no maximum. Also, completeness is about R: the same bounded set $\{x\in Q : x^2<2\}$ has a sup in R ($\sqrt{2}$) but none in Q.

Exam Trap. "$0.\overline{9}<1$" or "0.999… is the number just below 1". There is no real number between $0.\overline{9}$ and 1; they are equal. Consequently terminating decimals have two expansions, and decimal expansions are unique only if one forbids a tail of nines.

Exam Trap. In "greatest number dividing a,b,c leaving remainders r_1,r_2,r_3" using HCF(a,b,c) directly, or forgetting the condition that the divisor must exceed each remainder. Always subtract the remainders first, then check the answer is larger than every remainder. (If the HCF came out as 2 with a remainder of 5, the problem is inconsistent.)

Exam Trap. Assuming C can be compared like R, e.g. "i>0" or "|z| is ≥ 0 so $z \geq 0$". Only moduli are ordered; complex numbers themselves are not. Also $\sqrt{(-a)}\sqrt{(-b)} \neq \sqrt{(ab)}$ in general: $\sqrt{(-1)} \cdot \sqrt{(-1)} = i \cdot i = -1$, not $\sqrt{1}=1$.

Exam Trap. Confusing "Q is dense in R" with "Q is complete" or "uncountable". Q is dense and countable but not complete; $R \setminus Q$ is also dense but uncountable. A set can be dense and still miss most of R in size.

Exam Trap. Squaring inequalities blindly. From $x^2<4$ one gets $-2<x<2$, not just $x<2$; from $x<y$ one cannot conclude $x^2<y^2$ unless both are non-negative. Also $\sqrt{(x^2)}=|x|$, not x.

11. Exam Pointers

Exam Pointers —

- gcd(a,b)=gcd(b,r) for a=bq+r; the last non-zero remainder in Euclid's algorithm is the HCF; Bezout: gcd(a,b)=ax+by.
- gcd(a,b) · lcm(a,b)=ab for two numbers only; HCF uses minimum exponents, LCM maximum exponents.
- Euclid's lemma: p prime, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. FTA uniqueness rests on it.
- $\tau(n)=\prod(a_i+1)$, $\sigma(n)=\prod(p_i^{(a_i+1)}-1)/(p_i-1)$, $\varphi(n)=n\prod(1-1/p_i)$; $\tau(n)$ odd iff n is a perfect square.
- Trailing zeros of n! $=\lfloor n/5 \rfloor+\lfloor n/25 \rfloor+\lfloor n/125 \rfloor+\cdots$
- Fractions: HCF=(HCF of numerators)/(LCM of denominators), LCM=(LCM of numerators)/(HCF of denominators).
- $\sqrt{n}$ is irrational unless n is a perfect square; rational + irrational is irrational; irrational + irrational may be rational.
- p/q (lowest terms) terminates iff $q=2^a5^b$; $0.\overline{9}=1$; recurring $\Leftrightarrow$ rational.
- R is the complete ordered field: LUB property $\Rightarrow$ Archimedean, nested intervals, monotone convergence; Q fails the LUB property ($\sup\{x:x^2<2\}$).
- N,Z,Q countable; R and $R \setminus Q$ uncountable; both Q and $R \setminus Q$ dense.
- C is a field, algebraically closed, with no compatible order; $\sqrt{(a+ib)}$ has two values $\pm$.

12. Practice Set

1. Write 5/(16) as a terminating decimal and state the number of decimal places. Answer: 0.3125; 4 places (since $16=2^4$).
2. State the period of the decimal expansion of 1/(13) and write it. Answer: period 6; $0.\overline{076923}$.
3. Find the HCF and LCM of 144, 180 and 252. Answer: HCF=36, LCM=5040.
4. How many zeros does 150! end with? Answer: 30+6+1=37.
5. How many positive divisors of 360 are perfect squares? Answer: 4 (namely 1,4,9,36).
6. Express $0.21\overline{8}$ as a fraction in lowest terms. Answer: (218−2)/(990)=(216)/(990)=(12)/(55).
7. The HCF of two numbers is 12, their LCM is 180 and one number is 36. Find the other. Answer: (12 · 180)/(36)=60.
8. For $S=\{(-1)^n+1/n\}$ with n restricted to $n \geq 2$, find supS and infS. Answer: supS=maxS=3/2 (at n=2); infS=−1, not attained (odd n gives $-1+1/n>-1$).
9. Is $\log_{10}2$ rational? Give a one-line reason. Answer: No. If $\log_{10}2=p/q$ then $2^q=2^p5^p$, impossible by unique factorisation.
10. Find one integer solution of 7x+11y=1 and state the general solution. Answer: (x,y)=(−3,2) since −21+22=1; general solution x=−3+11t, y=2−7t.
11. Simplify (3+4i)/(1−2i). Answer: −1+2i.
12. How many integers in {1,2,…,60} are coprime to 60? Answer: $\varphi(60)=60 \cdot 1/2 \cdot 2/3 \cdot 4/5=16$.

Supplement: Number Systems and Real Number Properties — Advanced Problems and Extensions

Extended Theory and Techniques

Fermat, Euler and Wilson. The chapter introduced congruence briefly; the three classical theorems below turn most "remainder of a huge power" questions into one-line computations.

Euler's theorem. If gcd(a,m)=1 then $a^{\varphi(m)} \equiv 1 \pmod m$. For a prime p this is **Fermat's theorem**: $a^{p-1} \equiv 1 \pmod p$ when $p \nmid a$, and $a^p \equiv a \pmod p$ for every integer a.
Wilson's theorem. For a prime p, $(p-1)! \equiv -1 \pmod p$. Conversely, if $(n-1)! \equiv -1 \pmod n$ with n>1 then n is prime.

Proof of Euler's theorem. Let $r_1,\ldots,r_k$ ($k=\varphi(m)$) be the residues coprime to m. Multiplication by a permutes them modulo m, because $ar_i \equiv ar_j$ implies $r_i \equiv r_j$ and each ar_i is again coprime to m. Hence $a^k \prod r_i \equiv \prod r_i$, and cancelling the unit $\prod r_i$ gives the result. Proof of Wilson. In $\{1,\ldots,p-1\}$ each element has a unique inverse modulo p; the only self-inverse elements are ± 1 (since $x^2 \equiv 1$ means $p \mid (x-1)(x+1)$). Pairing the others leaves $1 \cdot (p-1) \equiv -1$.
Reduction of exponents. If gcd(a,m)=1, then $a^n \equiv a^{(n \bmod \varphi(m))} \pmod m$. If gcd(a,m)>1 do not use this; split m into prime powers and combine.

Chinese Remainder Theorem. If $m_1,\ldots,m_k$ are pairwise coprime, the system $x \equiv a_i \pmod{m_i}$ has a unique solution modulo $M=m_1 \cdots m_k$. Solve two congruences at a time: from $x \equiv a_1 \pmod{m_1}$ write $x=a_1+m_1t$ and substitute into the next.

The pairwise-coprime condition is essential; otherwise the system may have no solution (for example $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 6$).
Last digits and cyclicity. The last digit of a^n depends only on a mod 10 and n mod 4 (use exponent 4, not 0, when $4 \mid n$). For the last two digits, work modulo 100; useful anchors are $7^4=2401 \equiv 1$ and the fact that $a^{20} \equiv 1 \pmod{100}$ whenever gcd(a,10)=1 (the exponent of the unit group modulo 100 is lcm(2,20)=20, smaller than $\varphi(100)=40$).
Divisibility rules from 10^k**.** Since $10 \equiv -1 \pmod{11}$, a number is divisible by 11 iff the alternating digit sum is. Since $1001=7 \cdot 11 \cdot 13$ and $10^3 \equiv -1 \pmod$

1001), split the number into three-digit blocks from the right; it is divisible by 7, 11 or 13 iff the alternating sum of the blocks is. For 8 test the last three digits; for 9 the digit sum; for 72 test 8 and 9 together (coprime factors).

Trailing zeros in base b**.** If $b=\prod p_i^{e_i}$, the number of trailing zeros of n! in base b is $\min_i \lfloor v_{p_i}(n!)/e_i \rfloor$, where $v_p(n!)=\sum_{k\ge 1} \lfloor n/p^k \rfloor$.

Coprime-pair counting. If gcd(a,b)=h and lcm(a,b)=l, write a=hx, b=hy with gcd(x,y)=1 and xy=l/h. The number of ordered pairs is $2^{\omega(l/h)}$, where ω counts distinct primes of l/h (each prime power goes wholly to x or to y). Also $\sum_{[1\le k\le n;\ \gcd(k,n)=1]} k=n\varphi(n)/2$ for n>2, since $k \leftrightarrow n-k$ pairs the coprime residues.

Periods of decimals. If gcd(q,10)=1, the decimal of p/q is purely periodic and its period is the order of 10 modulo q, which divides $\varphi(q)$. For $q=2^{\alpha}5^{\beta}q'$ with gcd(q′,10)=1, the pre-period has length $\max(\alpha,\beta)$ and the period is the order of 10 modulo q′.

Inequalities on R**.**

> **Triangle inequalities.** $|a+b|\le|a|+|b|$ and $||a|-|b||\le|a-b|$. The sum $\sum|x-a_i|$ is minimised at a median of $a_1,\dots,a_n$ (any point of the middle interval when n is even). **Bernoulli:** $(1+x)^n\ge 1+nx$ for $x\ge -1$, $n\in\mathbb{N}$. **AM-GM:** for $a_i>0$, $(a_1+\cdots+a_n)/n\ge\sqrt[n]{a_1\cdots a_n}$ with equality iff all are equal.

Cube roots of unity. With $\omega=e^{(2\pi i/3)}$: $\omega^3=1$, $1+\omega+\omega^2=0$, $\bar{\omega}=\omega^2$, $1+\omega=-\omega^2$, $1+\omega^2=-\omega$, and ω^n depends only on n mod 3. Also $a^3+b^3+c^3-3abc=(a+b+c)(a+\omega b+\omega^2 c)(a+\omega^2 b+\omega c)$.

Divisor structure beyond counting. Let $n=\prod p_i^{a_i}$ and $d(n)=\prod(a_i+1)$. Pairing each divisor e with n/e shows that the product of all divisors is $n^{d(n)/2}$; for example the divisors of 36 multiply to $36^{9/2}=6^9$. The pairing has a fixed point $e=\sqrt{n}$ exactly when n is a perfect square, so d(n) is odd if and only if n is a perfect square. A positive integer n can be written as a sum of consecutive positive integers (one term allowed) in exactly as many ways as it has odd divisors: if $n=k(m+(k-1)/2)$ with k terms starting at m, then $2n=k(2m+k-1)$, the two factors have opposite parity, and each odd divisor of n supplies one admissible factorisation. For n=45 the odd divisors 1,3,5,9,15,45 give six representations, five of them with at least two terms.

Standard divisibility facts. For every integer n: $6\mid n^3-n$, $30\mid n^5-n$, and $p\mid n^p-n$ for every prime p (Fermat). The product of k consecutive integers is divisible by k!, because ((n+k−1)/k) is an integer. The possible remainders of a perfect square are {0,1} modulo 3, {0,1} modulo 4, {0,1,4} modulo 5 and {0,1,4} modulo 8; these tables are the quickest ways to prove that an equation such as $x^2-8y=3$ has no integer solution.

Irrationality bookkeeping. The sum or product of a nonzero rational and an irrational number is irrational. The sum of two irrationals can be rational ($\sqrt{2}$ and $1-\sqrt{2}$), and so can their product ($\sqrt{2}\cdot\sqrt{2}=2$), so no closure statement holds for the irrationals. $\sqrt{n}$ is irrational unless n is a perfect square, and $\log_a b$ (with a,b>1 coprime integers) is irrational: if $\log_a b=p/q$ then $a^p=b^q$, contradicting unique factorisation.

Floor function. $\lfloor x\rfloor\le x<\lfloor x\rfloor+1$; $\lfloor x+m\rfloor=\lfloor x\rfloor+m$ for integer m; $\lfloor x\rfloor+\lfloor -x\rfloor=-1$ when $x\notin\mathbb{Z}$ and 0 otherwise; and Hermite's identity $\lfloor x\rfloor+\lfloor x+1/2\rfloor=\lfloor 2x\rfloor$. Legendre's formula for $v_p(n!)$ is a floor-function sum, which is why it appears in the same questions.

Equality of decimals. A terminating decimal has a second representation ending in $\overline{9}$: $0.5=0.4\overline{9}$ since $0.\overline{9}=9/9=1$. Comparison of real numbers through decimals must therefore use the unique expansion not ending in $\overline{9}$.

Linear congruences. The congruence $ax\equiv b \pmod m$ is solvable if and only if g=gcd(a,m) divides b; in that case there are exactly g solutions modulo m, and dividing through by g reduces it to $a/g\,x\equiv b/g \pmod{m/g}$, which has a unique solution because a/g is invertible modulo m/g. When gcd(a,m)=1 the solution is $x\equiv a^{\varphi(m)-1}b$, though Euclid's algorithm is usually faster. For example $6x\equiv 9 \pmod{15}$ has g=3, reduces to $2x\equiv 3 \pmod 5$, so $x\equiv 4 \pmod 5$, giving the three solutions $x\equiv 4,9,14 \pmod{15}$.

Digital root and casting out nines. Because $10\equiv 1 \pmod 9$, every integer is congruent to its digit sum modulo 9 (and modulo 3). A quick check of a product $A\cdot B=C$ is therefore that the digit sums satisfy $s(A)s(B)\equiv s(C) \pmod 9$. This test can only reject a wrong answer, never confirm a correct one. The same idea with $10\equiv -1 \pmod{11}$ gives casting out elevens.

Order of an element. For gcd(a,m)=1 the least $k>0$ with $a^k\equiv 1 \pmod m$ is the order of a; it divides $\varphi(m)$, and $a^n\equiv 1$ if and only if order$\mid n$. This single fact explains the cycle of last digits, the period of a decimal expansion, and results such as $\gcd(a^m-1,a^n-1)=a^{\gcd(m,n)}-1$.

Place value in other bases. A number $(d_k d_{k-1}\dots d_0)_b=\sum d_i b^i$. Since $b\equiv 1 \pmod{b-1}$, divisibility by b−1 is tested by the digit sum in base b, and since $b\equiv -1 \pmod{b+1}$ divisibility by b+1 is tested by the alternating sum. To convert a fraction, multiply repeatedly by b and record integer parts; the expansion terminates in base b exactly when every prime factor of the reduced denominator divides b.

Complex numbers: modulus inequalities. For complex z,w: $|zw|=|z||w|$, $|z+w|\le|z|+|w|$, $||z|-|w||\le|z-w|$ and the parallelogram law $|z+w|^2+|z-w|^2=2|z|^2+2|w|^2$. The nth roots of unity are the vertices of a regular n-gon on the unit circle and their sum is 0 for $n\ge 2$; their product is $(-1)^{n-1}$.

Advanced Worked Examples

Worked Example S.1. Find the last two digits of $7^{2^{023}}$.

Solution. $7^2=49$ and $7^4=2401\equiv 1 \pmod{100}$. Since $2023=4\cdot 505+3$, $7^{2^{023}}\equiv 7^3=343\equiv 43 \pmod{100}$. The last two digits are 43.

Worked Example S.2. Find the remainder when 3^{200} is divided by 35.

Solution. gcd(3,35)=1 and $\varphi(35)=4\cdot 6=24$, so $3^{24}\equiv 1$. As $200=24\cdot 8+8$, $3^{200}\equiv 3^8=6561$. Now $35\cdot 187=6545$, so the remainder is $6561-6545=16$.

Worked Example S.3. Find the remainder when 28! is divided by 31.

Solution. By Wilson, $30!\equiv -1 \pmod{31}$. Now $30!=30\cdot 29\cdot 28!\equiv(-1)(-2)\,28!=2\cdot 28!$. So $2\cdot 28!\equiv -1\equiv 30$, giving $28!\equiv 15 \pmod{31}$ (cancelling 2, which is invertible). The remainder is 15.

Worked Example S.4. (a) Find the least positive N with $N\equiv 3 \pmod 4$, $N\equiv 2 \pmod 5$, $N\equiv 5 \pmod 7$. (b) How many ordered pairs of positive integers have HCF 12 and LCM 360?

Solution. (a) From the first two, $N=3+4t\equiv 2 \pmod 5$ gives $4t\equiv -1$, $t\equiv 1$, so $N\equiv 7 \pmod{20}$. Put $N=7+20k$; modulo 7 this is $6k\equiv 5$, i.e. $-k\equiv 5$, $k\equiv 2 \pmod 7$. Hence N=47 (unique modulo 140). Check: $47=4\cdot 11+3=5\cdot 9+2=7\cdot 6+5$.

(b) Write $a=12x$, $b=12y$ with gcd(x,y)=1 and $xy=360/12=30=2\cdot 3\cdot 5$. Each of the three primes goes to x or y: $2^3=8$ ordered pairs.

Worked Example S.5. Find the number of trailing zeros of 1000! when written in base 12.