Lesson - Number theory and discrete mathematics

Year: University Year 1

Number theory and discrete mathematics study integers, congruences, counting and graphs. They underpin cryptography, algorithms and computer science.

Starter activity

A cinema prints ticket numbers from 1 to 1000. How many ticket numbers are multiples of 3? Of 5? Of both? Can you work out quickly how many are multiples of 3 or 5? Now think about a clock: 9 hours after 7 o'clock it is 4 o'clock, so in clock arithmetic $7 + 9 = 4$. What is 5×5 on a 12-hour clock? These two ideas, careful counting and arithmetic that wraps around, are the start of this chapter.

Divisibility and the Euclidean algorithm

Definition: divisibility and gcd

For integers, $a \mid b$ means $b = ka$ for some integer k. The **greatest common divisor** $\gcd(a, b)$ is the largest integer dividing both.

Method: Euclidean algorithm and Bezout

1. Replace (a, b) by $(b,\ a \bmod b)$ repeatedly until the remainder is 0.
2. The last non-zero remainder is the gcd.
3. Back-substitute through the lines to write $\gcd = ax + by$.

Example 1

Find $\gcd(252, 198)$ and write it as $252x + 198y$.

$252 = 1 \cdot 198 + 54$, $198 = 3 \cdot 54 + 36$, $54 = 1 \cdot 36 + 18$, $36 = 2 \cdot 18$. So $\gcd = 18$. Then $18 = 54 - 36 = 54 - (198 - 3 \cdot 54) = 4 \cdot 54 - 198 = 4(252 - 198) - 198 = 4 \cdot 252 - 5 \cdot 198$.

Theorem: Bezout and the fundamental theorem of arithmetic

Bezout's identity: there are integers x, y with $ax + by = \gcd(a, b)$. The **fundamental theorem of arithmetic** says every integer > 1 factorises uniquely into primes, and there are infinitely many primes (a classic proof by contradiction).

Modular arithmetic

Definition: congruence

$a \equiv b \pmod{n}$ means $n \mid (a-b)$. Congruences can be added, subtracted and multiplied, so $ab \bmod n$ depends only on $a \bmod n$ and $b \bmod n$.

Rule: inverses and linear congruences

a has an **inverse** modulo n if and only if $\gcd(a,n)=1$, found by Bezout. To solve $ax \equiv c \pmod{n}$ with $g=\gcd(a,n)$: solutions exist if and only if $g \mid c$; divide through by g.

Example 2

Find $7^{-1} \bmod 26$ and solve $14x \equiv 6 \pmod{20}$.

$7 \cdot 15 = 105 = 4 \cdot 26 + 1$, so $7^{-1} \equiv 15$. For the second, $g=2$ divides 6, so $7x \equiv 3 \pmod{10}$, giving $x \equiv 9 \pmod{10}$, that is $x \equiv 9$ or $19 \pmod{20}$.

Fermat, Euler and the Chinese remainder theorem

Theorem: Fermat and Euler

Fermat's little theorem: if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. Euler's totient $\varphi(n)$ counts integers in $1,\dots,n$ coprime to n; $\varphi(p^k) = p^k - p^{k-1}$ and φ is multiplicative on coprime arguments. **Euler's theorem:** $a^{\varphi(n)} \equiv 1 \pmod{n}$ when $\gcd(a,n)=1$.

Example 3

Find $3^{100} \bmod 7$ and the last digit of 7^{2025}.

$3^6 \equiv 1$ and $100 = 96+4$, so $3^{100} \equiv 3^4 = 81 \equiv 4$. Also $7^4 \equiv 1 \pmod{10}$ and $2025 \equiv 1 \pmod{4}$, so the last digit is 7.

Theorem: Chinese remainder theorem

If $\gcd(m,n)=1$ then $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ has a unique solution modulo mn.

Example 4

Solve $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$.

The numbers $3, 8, 13, \dots$ satisfy the second; $8 \equiv 2 \pmod{3}$, so $x \equiv 8 \pmod{15}$.

Counting

Property: counting principles

- $n!$ arranges n distinct objects; with repeats divide by the factorials of the repeat counts.
- The number of ways to choose r from n is $\binom{n}{r}$.
- Binomial theorem: $(a+b)^n = \sum \binom{n}{k} a^{n-k} b^k$.
- Inclusion-exclusion: $|A \cup B| = |A| + |B| - |A \cap B|$.
- Pigeonhole: if $n+1$ objects go into n boxes, some box has two.

Example 5

Count the arrangements of LETTER; find the x^3 coefficient in $(1+2x)^6$; count the numbers in $1, \dots, 100$ divisible by 2 or 3.

$\frac{6!}{2!\,2!} = 180$. The coefficient is $\binom{6}{3} \cdot 2^3 = 160$. And $50 + 33 - 16 = 67$.

Graph theory

Definition: graph, degree, tree

A **graph** consists of vertices and edges. The **degree** of a vertex is the number of edges at it. A **tree** is a connected graph with no cycles; a tree on n vertices has exactly $n-1$ edges.

Theorem: handshaking lemma and Euler circuits

The sum of degrees equals twice the number of edges, so it is even. A connected graph has an **Euler circuit** (using every edge once and returning) if and only if every vertex has even degree. The **chromatic number** is the least number of colours for a proper vertex colouring.

Example 6

Degrees $3, 3, 2, 2, 1, 1$: how many edges? Does K_5 or K_4 have an Euler circuit?

The sum is 12, so there are 6 edges. Five vertices of degree 3 are impossible (sum 15, odd). K_5 has all degrees 4, so it has a circuit; K_4 has degrees 3, so it does not. An odd cycle such as C_5 needs 3 colours; bipartite graphs need 2.

Recurrences and induction

Example 7: Fibonacci

Prove that $F_1 + \cdots + F_n = F_{n+2} - 1$, where $F_1 = F_2 = 1$ and $F_{n+1} = F_n + F_{n-1}$.

Assume it for $n = k$. Then $F_1 + \cdots + F_{k+1} = F_{k+2} - 1 + F_{k+1} = F_{k+3} - 1$. Check $n = 5$: $1 + 1 + 2 + 3 + 5 = 12 = F_7 - 1 = 13 - 1$.

Watch out

- Cancelling a common factor in a congruence without checking it is coprime to the modulus.
- Fermat requires $p \nmid a$.
- Counting ordered arrangements when order does not matter.
- Applying the Euler circuit criterion to a disconnected graph.

Number theory and discrete maths in practice

Key fact: fast modular powers

To compute $a^k \bmod n$ for a large k we never compute a^k itself. Write k in binary, square repeatedly ($a, a^2, a^4, a^8, \ldots$), reducing modulo n after each step, and multiply together the powers that correspond to the binary digits equal to 1. Only about $2\log_2 k$ multiplications are needed, which is why computers can work with exponents hundreds of digits long in cryptography. Fermat's and Euler's theorems give a second shortcut: reduce the exponent modulo $p - 1$ or modulo $\varphi(n)$ first, provided a is coprime to the modulus.

Method: solving the linear congruence ax ≡ b (mod n)

1. Compute $d = \gcd(a, n)$ with the Euclidean algorithm.
2. If d does not divide b there is no solution.
3. Otherwise divide everything by d: $a'x \equiv b' \pmod{n'}$ with $\gcd(a', n') = 1$.
4. Find the inverse of a' modulo n' by working the Euclidean algorithm backwards, and multiply: $x \equiv (a')^{-1} b' \pmod{n'}$.
5. Write the d solutions modulo n: $x_0,\ x_0 + n',\ \ldots,\ x_0 + (d-1)n'$, and check one of them in the original congruence.

Worked example 8: Repeated squaring

Find $3^{45} \bmod 17$.

In binary $45 = 32 + 8 + 4 + 1$. Squaring repeatedly modulo 17: $3^1 = 3$, $3^2 = 9$, $3^4 = 81 \equiv 13$, $3^8 \equiv 13^2 = 169 \equiv 16$, $3^{16} \equiv 16^2 = 256 \equiv 1$, $3^{32} \equiv 1$. So $3^{45} \equiv 1 \times 16 \times 13 \times 3 = 624 \equiv 624 - 36 \times 17 = 12$. Check with Fermat: $3^{16} \equiv 1$ and $45 = 2 \times 16 + 13$, so $3^{45} \equiv 3^{13} = 3^8 \cdot 3^4 \cdot 3 \equiv 16 \times 13 \times 3 \equiv 12$. Both methods give 12.

Worked example 9: All integer solutions of a linear equation

Find all integer solutions of $14x + 9y = 5$.

First $\gcd(14, 9) = 1$: $14 = 9 + 5$, $9 = 5 + 4$, $5 = 4 + 1$. Backwards, $1 = 5 - 4 = 5 - (9 - 5) = 2 \times 5 - 9 = 2(14 - 9) - 9 = 2 \times 14 - 3 \times 9$. Multiplying by 5 gives the particular solution $x_0 = 10$, $y_0 = -15$. Adding a multiple of 9 to x and subtracting the same multiple of 14 from y keeps the sum unchanged, so the general solution is $x = 10 + 9t$, $y = -15 - 14t$ for integers t. With $t = -1$ we get the small solution $(1, -1)$: indeed $14 - 9 = 5$.

Worked example 10: Derangements and Secret Santa

Four friends each put their name in a hat and draw one at random. In how many ways does nobody draw their own name?

Let A_i be the set of draws in which friend i gets their own name. Inclusion-exclusion gives the number of draws in at least one A_i: $\binom{4}{1}3! - \binom{4}{2}2! + \binom{4}{3}1! - \binom{4}{4}0! = 24 - 12 + 4 - 1 = 15$. So the number of good draws is $4! - 15 = 9$. In general the number of derangements is $D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^n}{n!}\right)$, and the probability that nobody gets their own name tends to $\frac{1}{e} \approx 0.368$.

Worked example 11: A graph question in context

A museum has five rooms; the doorways between rooms give the degrees $2, 2, 4, 3, 3$. Can a visitor walk through every doorway exactly once?

The degree sum is 14, so there are 7 doorways. Exactly two rooms have odd degree, so an Euler trail exists: the visitor must start in one of the rooms of degree 3 and finish in the other. A circuit returning to the start is impossible, because every time the visitor passes through a room they use two doorways, so all rooms except the start and end need even degree.

Worked example 12: Pigeonhole principle

Show that among any 5 points inside a square of side 2 there are two at distance at most $\sqrt{2}$.

Divide the square into four squares of side 1. With five points and four small squares, the pigeonhole principle says that two points lie in the same small square. The largest distance in a unit square is its diagonal $\sqrt{2}$, so these two points are at most $\sqrt{2}$ apart. The same idea proves that among 13 people two share a birth month, and many existence results in combinatorics. The principle never tells you which two objects coincide, only that two must exist, which is typical of counting arguments.

Note: why number theory matters today

For centuries number theory was regarded as the purest part of mathematics, with no practical use. That changed in the 1970s with public-key cryptography. Every time you pay online or send a private message, your device performs modular exponentiation, uses the Euclidean algorithm to find inverses, and relies on the fact that multiplying two large primes is easy while factorising the product is extremely hard. Check digits on barcodes, ISBNs and bank card numbers use simple congruences to catch typing errors, and graph theory organises everything from bus networks to exam timetables.

Watch out: typical mistakes

- Dividing a congruence by a number that is not coprime to the modulus: from $6x \equiv 4 \pmod{10}$ you must also divide the modulus.
- Applying Fermat's little theorem when the modulus is not prime, or when p divides a.
- Confusing arrangements (order matters) and selections (order does not matter).
- Forgetting that an Euler circuit needs all degrees even and that the graph must be connected.

Did you know?

The Euclidean algorithm appears in Book VII of Euclid's Elements, written about 300 BC, and is one of the oldest algorithms still in daily use. The RSA cryptosystem, published in 1977 by Rivest, Shamir and Adleman, turned Fermat's little theorem (1640) and Euler's theorem (1763) into the basis of secure internet communication. Graph theory began in 1736 when Euler proved that nobody could walk across all seven bridges of Königsberg exactly once.

Otto's tip

Reduce exponents using the order of the base before computing a huge power.