

[ OLYMPIAD MATHEMATICS ]

IOQM · PRE-RMO

2027

# IOQM *Handbook*

CLASS 8 TO 12

OLYMPIAD

THEORY AND PROBLEMS

## IN THIS HANDBOOK

PAPER ..... IOQM MATHEMATICS  
THIS VOLUME ..... PART I · NUMBER THEORY  
EACH CHAPTER ..... THEORY · EXAMPLES · EXERCISES

# IITIANFORUM

REAL STUDY, GENUINE RESULTS.

---

## IOQM Mathematics Handbook

### *Part I · Number Theory*

FOR IOQM 2027 | EDITION 1 | 2026

---

© 2026 IITian Forum. All rights reserved.

This handbook is for the personal use of the student to whom it is issued. No part of it may be copied, photographed, scanned, uploaded, shared in messaging groups, sold or distributed, in print or electronically, without the written permission of IITian Forum.

Questions taken from IOQM 2026 and from other mathematical olympiads are marked with their source and are used here for teaching. The theory, the solutions, the hints and the figures in this handbook are the work of IITian Forum.

Every answer in this handbook has been checked by computer. If you still find an error, or if you have a suggestion, please write to [ritesh@iitianforum.com](mailto:ritesh@iitianforum.com) or [academics@iitianforum.com](mailto:academics@iitianforum.com), with the page number. Corrections are made in the next edition.

Published by IITian Forum | [iitianforum.com](https://iitianforum.com)

Practice online | [domath.in](https://domath.in)

IITian Forum and doMath are marks of IITian Forum.

[ IOQM · PART I ]

# Preface

---

IOQM is the first stage of the Indian mathematical olympiad programme, and for most students it is the first paper in which a formula is not enough. The questions are short and every answer is a whole number from 00 to 99, but almost every question needs an idea. This handbook is written to build those ideas, one chapter at a time.

The handbook follows the paper. It will have four parts, one each for number theory, combinatorics, geometry and algebra, and every part is tied to the IOQM 2026 paper, so that you can see where each idea was actually tested. This volume is Part I, Number Theory, the largest area of the paper.

Everything here stays within school mathematics. Nothing needs more than the algebra of Classes 10 to 12, and every result that is used is either proved in the text or stated with its conditions. The examples and exercises come from the IOQM 2026 paper, from olympiads of many countries, and from our own classes. Every solution has been written afresh, in the way we teach it, and every answer has been checked by computer.

This book is meant to be worked through, not only read. Keep a notebook beside it, attempt every example before you read its solution, and come back later to the questions you could not do.

If something is not clear, if you find a mistake, or if you have a suggestion, write to me at [ritesh@iitianforum.com](mailto:ritesh@iitianforum.com) or to our academic team at [academics@iitianforum.com](mailto:academics@iitianforum.com). Your message will help every student who uses this book after you.

---

**Ritesh Raj**

Founder, IITian Forum · IIT Delhi

[ IOQM · PART I ]

# How to use this handbook

This page is for you, the student. Part I has five chapters, in the order in which they are taught. Chapters 1 to 3 build divisibility, the gcd and congruences. Chapter 4 covers Legendre's formula, digits, perfect squares and equations in integers. Chapter 5 shows how to choose the right method, and ends with a mixed problem set. The answers to all exercises, each with a one-line hint, are at the end of the part.

## HOW TO STUDY A CHAPTER

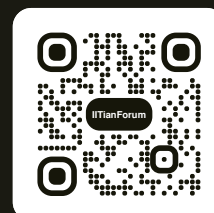
- 01** Read the theory slowly, once. Write out each short proof in your own notebook; that is how a result becomes yours.
- 02** Before reading a worked example, cover its solution and try the question for five minutes. Then read the solution and compare it with yours.
- 03** Learn the gold cards by heart. They hold the definitions, theorems and key ideas that the paper uses again and again.
- 04** Read the dark cards twice. Each one marks a point where students often lose marks.
- 05** Attempt every exercise before you look at the answers. Read the one-line hint only when you are stuck, then finish the question yourself.
- 06** Keep a list of the questions you got wrong, and try them again a week later without looking at the solution.

Questions from IOQM 2026 are marked with their question number, and questions from other olympiads with their source. Stuck on a question, or found a mistake? Write to [ritesh@iitianforum.com](mailto:ritesh@iitianforum.com) or [academics@iitianforum.com](mailto:academics@iitianforum.com).

IITianForum · Real study, genuine results

## The course behind this handbook

Modules, assignments and solutions, live classes and mentorship for JEE and the mathematics olympiads.

[Open iitianforum.com](https://iitianforum.com) →

SCAN FOR THE COURSE

[ IOQM · PART I ]

# Notation and conventions

Each symbol is defined in the section shown, where it first appears.

| SYMBOL                                 | MEANING                                                                               | SECTION |
|----------------------------------------|---------------------------------------------------------------------------------------|---------|
| $a \mid b, a \nmid b$                  | $a$ divides $b$ , that is $b = ak$ for an integer $k$ ; $a$ does not divide $b$       | 1.1     |
| $a \bmod b$                            | the remainder of $a$ on division by $b$ , one of $0, 1, \dots, b-1$                   | 1.2     |
| $\overline{a_k \cdots a_1 a_0}$        | the number whose decimal digits are $a_k, \dots, a_1, a_0$                            | 1.3     |
| $n!$                                   | $1 \cdot 2 \cdot 3 \cdots n$ , with $0! = 1$                                          | 1.4     |
| $\tau(n), \sigma(n)$                   | the number of positive divisors of $n$ ; their sum                                    | 1.6     |
| $\sum_{d \mid n}, \prod_{p \mid n}$    | sum over the positive divisors $d$ of $n$ ; product over the primes $p$ dividing $n$  | 1.6     |
| $\gcd(a, b), \operatorname{lcm}(a, b)$ | greatest common divisor; least common multiple                                        | 2.1     |
| $F_n$                                  | Fibonacci numbers: $F_1 = F_2 = 1, F_{n+2} = F_{n+1} + F_n$                           | 2.4     |
| $\mathbb{Z}$                           | the set of all integers                                                               | 2.5     |
| $a \equiv b \pmod{m}$                  | $m \mid a - b$ , that is $a$ and $b$ leave the same remainder on division by $m$      | 3.1     |
| $\varphi(n)$                           | the number of integers in $1, 2, \dots, n$ coprime to $n$                             | 3.6     |
| $\operatorname{ord}_m(a)$              | the smallest $d \geq 1$ with $a^d \equiv 1 \pmod{m}$ , for $a$ coprime to $m$         | 3.8     |
| $v_p(N)$                               | the exponent of the prime $p$ in $N$ : $p^{v_p(N)} \mid N$ but $p^{v_p(N)+1} \nmid N$ | 4.1     |
| $\binom{n}{k}$                         | $n! / (k!(n-k)!)$ , the number of ways to choose $k$ things from $n$                  | 4.1     |
| $S(n), \lceil x \rceil$                | the sum of the decimal digits of $n$ ; the least integer $\geq x$                     | 4.3     |
| $\lfloor x \rfloor, \{x\}$             | the greatest integer $\leq x$ ; the fractional part $x - \lfloor x \rfloor$           | 4.4     |
| $(a_k \cdots a_0)_b, s_p(n)$           | a number written in base $b$ ; the digit sum of $n$ in base $p$                       | 4.9     |
| $\Rightarrow, \Leftrightarrow$         | "implies"; "exactly when" (if and only if)                                            |         |

## CONVENTIONS

- (i) **Integers.** A positive integer is one of  $1, 2, 3, \dots$ ; a non-negative integer may also be 0. "Number" means an integer unless stated otherwise.
- (ii) **Primes and divisors.** Primes are positive, and 1 is not a prime. When divisors are counted or listed, they are the positive divisors.
- (iii) **Remainders.** On division by  $b > 0$  the remainder  $r$  always satisfies  $0 \leq r < b$ ; it is never negative.
- (iv) **Digits.** Digits are decimal unless a base is given,

and the leading digit of a number is never 0. With a bar,  $\overline{ab}$  is the two-digit number  $10a + b$ ; without it,  $ab$  is the product  $a \times b$ .

- (v) **"Find all".** A complete answer gives every solution and also shows that there are no others.
- (vi) **Numbering.** 3.8 is section 8 of Chapter 3. Examples are numbered in the same way, and Exercise 2.5 is question 5 of Exercises 2.
- (vii) **Sources.** "(IOQM 2026, Q14)" is question 14 of the IOQM 2026 paper. The name of another olympiad, as in "(RMO 2013)", gives the source of that question.

## [ CONTENTS ]

# Part I *number theory*

## BEFORE YOU BEGIN

|     |                          |   |
|-----|--------------------------|---|
| i   | Preface                  | 3 |
| ii  | How to use this handbook | 4 |
| iii | Notation and conventions | 5 |

## 01 · DIVISIBILITY AND PRIMES

|     |                        |    |
|-----|------------------------|----|
| 1.1 | Divisibility           | 7  |
| 1.2 | The division algorithm | 7  |
| 1.3 | Divisibility tests     | 8  |
| 1.4 | Primes                 | 8  |
| 1.5 | Unique factorisation   | 9  |
| 1.6 | Counting divisors      | 10 |
| 1.7 | Primes of special form | 10 |
| 1.8 | Useful factorisations  | 11 |

## 02 · GCD, LCM AND LINEAR EQUATIONS

|     |                              |    |
|-----|------------------------------|----|
| 2.1 | GCD and LCM                  | 12 |
| 2.2 | The Euclidean algorithm      | 13 |
| 2.3 | Bezout's identity            | 14 |
| 2.4 | Coprimality facts            | 14 |
| 2.5 | Linear Diophantine equations | 14 |
| 2.6 | The coin problem             | 15 |
| 2.7 | Factorising equations        | 16 |

## 03 · MODULAR ARITHMETIC

|     |                           |    |
|-----|---------------------------|----|
| 3.1 | Congruences               | 17 |
| 3.2 | Inverses and cancellation | 17 |

|      |                                 |    |
|------|---------------------------------|----|
| 3.3  | Linear congruences              | 18 |
| 3.4  | Powers modulo small numbers     | 18 |
| 3.5  | Fermat's little theorem         | 19 |
| 3.6  | Euler's theorem                 | 19 |
| 3.7  | Wilson's theorem                | 20 |
| 3.8  | Order, and cycles of powers     | 20 |
| 3.9  | The Chinese remainder theorem   | 21 |
| 3.10 | Last digits and last two digits | 21 |

## 04 · DIGITS, SQUARES AND EQUATIONS

|     |                                |    |
|-----|--------------------------------|----|
| 4.1 | Legendre's formula             | 22 |
| 4.2 | Digits and place value         | 23 |
| 4.3 | Digit sums                     | 24 |
| 4.4 | The floor function in counting | 25 |
| 4.5 | Perfect squares                | 25 |
| 4.6 | Sums of two squares            | 26 |
| 4.7 | Pythagorean triples            | 26 |
| 4.8 | Bounding, parity and descent   | 27 |
| 4.9 | Other bases                    | 28 |

## 05 · PROBLEM SOLVING

|     |                                   |    |
|-----|-----------------------------------|----|
| 5.1 | Choosing the method               | 29 |
| 5.2 | Standard results to remember      | 30 |
| 5.3 | Primes in equations               | 30 |
| 5.4 | Periodic remainders               | 31 |
| 5.5 | IOQM 2026 number theory questions | 32 |
| 5.6 | Common mistakes                   | 32 |
| 5.7 | A mixed problem set               | 33 |
| A   | Answers to the exercises          | 33 |
| N   | A note before you close it        | 35 |

## CHAPTER 01 DIVISIBILITY AND PRIMES

Number theory is the study of the integers, and almost all of it rests on one relation: one integer dividing another. This chapter sets up that relation, the division algorithm that comes with it, and the primes, which are the building blocks every integer is made from. Nothing here is hard, but every later chapter depends on it, so read it slowly.

## 1.1 DIVISIBILITY

## DEFINITION · DIVIDES

For integers  $a \neq 0$  and  $b$ , we say  $a$  **divides**  $b$ , and write  $a \mid b$ , when  $b = ak$  for some integer  $k$ . We also say  $a$  is a **divisor** of  $b$  and  $b$  is a **multiple** of  $a$ . If  $a$  does not divide  $b$  we write  $a \nmid b$ .

So  $3 \mid 12$ ,  $-4 \mid 12$ ,  $7 \nmid 12$ , and every non-zero integer divides 0, since  $0 = a \cdot 0$ . The numbers  $\pm 1$  divide every integer.

Four rules follow straight from the definition, and they are used constantly.

- (i) If  $a \mid b$  and  $b \mid c$ , then  $a \mid c$ .
- (ii) If  $a \mid b$  and  $a \mid c$ , then  $a \mid bx + cy$  for all integers  $x, y$ .
- (iii) If  $a \mid b$  and  $b \neq 0$ , then  $|a| \leq |b|$ .
- (iv) If  $a \mid b$  and  $b \mid a$ , then  $a = \pm b$ .

The second rule is worth proving, because its proof is the whole idea. If  $b = ak$  and  $c = al$ , then  $bx + cy = a(kx + ly)$ , and  $kx + ly$  is an integer. The third rule is what makes divisor problems finite: a non-zero number has only finitely many divisors, all of them between  $-|b|$  and  $|b|$ .

## KEY IDEA · REMOVE THE VARIABLE

If  $d$  divides two expressions, it divides every combination of them. Choose the combination that removes the variable; then  $d$  must divide a fixed number.

## EXAMPLE 1.1

Find all integers  $n$  for which  $n + 2$  divides  $n^2 + 5$ .

For  $n = 1$ :  $n + 2 = 3$ ,  $n^2 + 5 = 6$  and  $3 \mid 6$ .

$n + 2$  divides

$$(n + 2)(n - 2) = n^2 - 4$$

So  $n + 2$  also divides the difference

$$(n^2 + 5) - (n^2 - 4) = 9$$

Hence  $n + 2$  is one of the six divisors of 9 (key idea *Remove the variable*):

$$\begin{array}{cccccc} n + 2 & 1 & -1 & 3 & -3 & 9 & -9 \\ n & -1 & -3 & 1 & -5 & 7 & -11 \end{array}$$

Each of these works, as  $n^2 + 5 = (n + 2)(n - 2) + 9$  and  $n + 2$  divides both terms. For  $n = 7, 9 \mid 54$ .

ANSWER **six integers:  $-11, -5, -3, -1, 1, 7$**

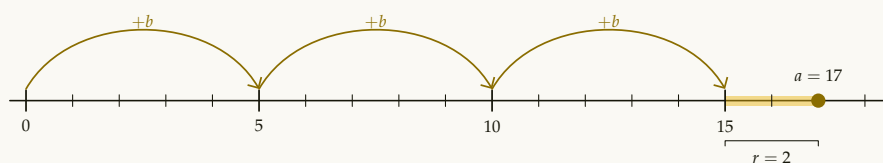
## 1.2 THE DIVISION ALGORITHM

## THEOREM · DIVISION ALGORITHM

For any integer  $a$  and any integer  $b > 0$  there is exactly one pair of integers  $q, r$  with

$$a = bq + r, \quad 0 \leq r < b.$$

$q$  is the **quotient** and  $r$  the **remainder**.



$$17 = 5 \cdot 3 + 2: \text{ three whole jumps of } b = 5, \text{ then } 0 \leq r < b$$

To see why, take  $q$  to be the largest integer with  $bq \leq a$ , that is  $q = \lfloor a/b \rfloor$ . Then  $r = a - bq$  is at least 0, and it is less than  $b$ , because otherwise  $b(q+1)$  would still be at most  $a$ . Uniqueness holds because two remainders both lie in  $0, 1, \dots, b-1$  and differ by a multiple of  $b$ , so they are equal.

Two consequences are used all the time.

- (i) **The remainder is never negative.**  $-17 = 5 \cdot (-4) + 3$ , so  $-17$  leaves remainder 3 on division by 5, not  $-2$ .
- (ii) **Every integer has one of  $b$  forms:**  $bk, bk+1, \dots, bk+(b-1)$ . Splitting a problem into these forms is the cleanest proof by cases.

#### EXAMPLE 1.2

An integer  $M$  is divisible by 4 but not by 256. How many different remainders can  $M$  leave on division by 256? (IOQM 2026, Q2)

For  $M = 1000$ :  $1000 = 256 \cdot 3 + 232$ , and the remainder  $232 = 4 \cdot 58$  is again a multiple of 4.

In general, by the division algorithm,

$$M = 256q + r, \quad 0 \leq r < 256$$

$4 \mid M$  and  $4 \mid 256q$ , so  $4 \mid M - 256q = r$ .  $\therefore r$  is one of  $0, 4, 8, \dots, 252$ , i.e.,  $252/4 + 1 = 64$  values.

$r = 0$  is not possible, as then  $256 \mid M$ . Every other value of  $r$  occurs: take  $M = r$ , a multiple of 4 between 0 and 256.

ANSWER  $64 - 1 = 63$

### 1.3 DIVISIBILITY TESTS

A test lets you decide divisibility from the digits alone.

Write  $N = \overline{a_k \cdots a_1 a_0} = a_0 + 10a_1 + 100a_2 + \cdots$ .

| DIVISOR   | TEST ON $N$                                             |
|-----------|---------------------------------------------------------|
| 2, 5      | the last digit                                          |
| 4         | the number formed by the last two digits                |
| 8         | the number formed by the last three digits              |
| 3, 9      | the sum of the digits                                   |
| 11        | $a_0 - a_1 + a_2 - \cdots$ , alternating from the units |
| 7, 11, 13 | alternating sum of three-digit blocks from the right    |

Each test is a statement about remainders. Since  $10 = 9 + 1$ , every power of 10 leaves remainder 1 on division by 9, so  $N$  and its digit sum leave the same remainder on division by 9, and by 3. Since  $10 = 11 - 1$ , the powers of 10 alternate between remainder 1 and  $-1$  on division by 11, which gives the alternating sum. And  $1000 = 1001 - 1$  with  $1001 = 7 \cdot 11 \cdot 13$  gives the block test.

#### WHERE MARKS GO · COPRIME FACTORS ONLY

To test divisibility by 36, test 4 and 9, which share no prime. Testing 6 and 6, or 2 and 18, proves nothing: 18 passes a test for 2 and for 18 and is not a multiple of 36.

#### EXAMPLE 1.3

Find all five-digit numbers  $\overline{34a5b}$  that are divisible by 36.

$36 = 4 \cdot 9$ , and 4, 9 have no common prime, so the number must be divisible by 4 and by 9 (tip *Coprime factors only*).

For 4:  $4 \mid \overline{5b}$ . From 50 to 59 the multiples of 4 are 52 and 56, so  $b = 2$  or 6.

For 9: the digit sum  $3 + 4 + a + 5 + b = 12 + a + b$  is a multiple of 9, and  $0 \leq a + b \leq 18$ , so  $12 + a + b = 18$  or 27, i.e.,  $a + b = 6$  or 15.

|         |             |              |
|---------|-------------|--------------|
|         | $a + b = 6$ | $a + b = 15$ |
| $b = 2$ | $a = 4$     | $a = 13$     |
| $b = 6$ | $a = 0$     | $a = 9$      |

$a = 13$  is not a digit, so three numbers remain.

ANSWER 34452, 34056, 34956

### 1.4 PRIMES

#### DEFINITION · PRIME

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**. The number 1 is neither.

The primes below 50 are the fifteen highlighted in the sieve: cross out the multiples of 2, 3, 5 and 7, and the numbers left are prime.

|    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|
| 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |

fifteen primes below 50; striking multiples

of 2, 3, 5, 7 is enough, since  $7 < \sqrt{50} < 11$ 

**The square-root test.** If  $n = ab$  with  $1 < a \leq b$ , then  $a^2 \leq ab = n$ , so  $a \leq \sqrt{n}$ . Hence a composite  $n$  always has a prime factor at most  $\sqrt{n}$ , and to test a number for primality it is enough to try the primes up to  $\sqrt{n}$ . That is why the sieve to 50 could stop at 7: the next prime, 11, already has  $11^2 > 50$ .

**THEOREM · EUCLID**

There are infinitely many primes.

Suppose  $p_1, \dots, p_k$  were all of them, and look at  $N = p_1 p_2 \cdots p_k + 1$ . Each  $p_i$  leaves remainder 1 on dividing  $N$ , so none divides it. But  $N > 1$  has some prime factor, which is then a prime missing from the list.

The primes thin out, and the gaps between them can be as long as you like:  $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$  are  $n$  consecutive composites, the  $j$ th of them divisible by  $j$ .

**EXAMPLE 1.4***Is 851 prime?*

$29^2 = 841 < 851 < 900 = 30^2$ , so it is enough to try the primes up to 29 (square-root test).

851 is odd, its digit sum 14 is not a multiple of 3, and its last digit is not 0 or 5. So none of 2, 3, 5 divides 851. For the next primes:

|           |   |    |    |    |    |    |
|-----------|---|----|----|----|----|----|
| $p$       | 7 | 11 | 13 | 17 | 19 | 23 |
| remainder | 4 | 4  | 6  | 1  | 15 | 0  |

$\therefore 851 = 23 \cdot 37$ , which is not prime.

**ANSWER no,  $851 = 23 \cdot 37$** **1.5 UNIQUE FACTORISATION****THEOREM · FUNDAMENTAL THEOREM OF ARITHMETIC**Every integer  $n > 1$  is a product of primes,

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

and this product is unique apart from the order of the factors.

Existence is easy: keep splitting a composite factor until every piece is prime. Uniqueness rests on one lemma.

**LEMMA · EUCLID**

If a prime  $p$  divides a product  $ab$ , then  $p \mid a$  or  $p \mid b$ .

The lemma fails for composite numbers:  $6 \mid 4 \cdot 9$ , yet  $6 \nmid 4$  and  $6 \nmid 9$ . We prove it in Chapter 2, from Bezout's identity.

Unique factorisation turns many questions into questions about exponents.

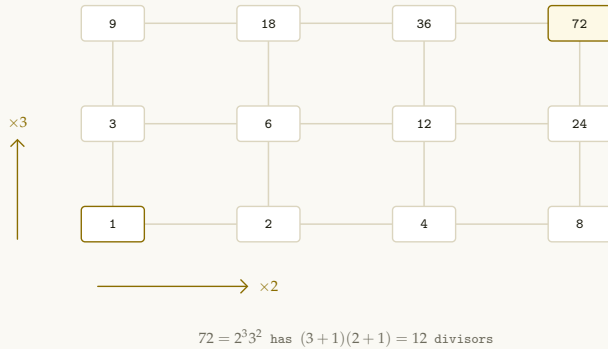
- (i)  $m \mid n$  exactly when every prime appears in  $m$  to a power no larger than in  $n$ .
- (ii)  $n$  is a perfect square exactly when every exponent  $a_i$  is even, and a perfect  $k$ th power when every  $a_i$  is a multiple of  $k$ .
- (iii) If  $a, b > 0$ ,  $\gcd(a, b) = 1$  and  $ab$  is a perfect square, then  $a$  and  $b$  are both perfect squares, since no prime is shared between them.

**WHERE MARKS GO · COPRIME IS ESSENTIAL**

$ab$  square does not make  $a$  and  $b$  squares in general:  $2 \cdot 8 = 16$ . The conclusion needs  $\gcd(a, b) = 1$ , so prove coprimality first.

## 1.6 COUNTING DIVISORS

Write  $n = p_1^{a_1} \cdots p_k^{a_k}$ . A positive divisor of  $n$  chooses the power of each  $p_i$  independently, anywhere from 0 to  $a_i$ .



## FORMULAS · DIVISOR FUNCTIONS

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

$$\sigma(n) = \prod_{i=1}^k \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

$$\text{product of all divisors} = n^{\tau(n)/2}$$

$\tau$  counts the divisors and  $\sigma$  adds them;  $\sigma$  is the product over the primes of  $1 + p + \cdots + p^a$ . The product formula comes from pairing each divisor  $d$  with  $n/d$ : each pair multiplies to  $n$ , and there are  $\tau(n)/2$  pairs.

## THEOREM · ODD NUMBER OF DIVISORS

$\tau(n)$  is odd exactly when  $n$  is a perfect square.

The divisors pair up as  $d \leftrightarrow n/d$ ; only  $d = \sqrt{n}$  is paired with itself, and that happens only when  $n$  is a square.

## EXAMPLE 1.5

How many positive divisors does  $10!$  have, and how many of them are perfect squares?

Power of each prime in  $10! = 1 \cdot 2 \cdot 3 \cdots 10$ :

$$2 : 2, 4, 6, 8, 10 \text{ give } 1 + 2 + 1 + 3 + 1 = 8,$$

$$3 : 3, 6, 9 \text{ give } 1 + 1 + 2 = 4,$$

$$5 : 5, 10 \text{ give } 2; \quad 7 : 1$$

So  $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$  and, by the formula for  $\tau$ ,

$$\tau(10!) = 9 \cdot 5 \cdot 3 \cdot 2 = 270$$

A divisor is a perfect square exactly when every exponent in it is even (Section 1.5):

| $p$ | even exponent | choices |
|-----|---------------|---------|
| 2   | 0, 2, 4, 6, 8 | 5       |
| 3   | 0, 2, 4       | 3       |
| 5   | 0, 2          | 2       |
| 7   | 0             | 1       |

$$5 \cdot 3 \cdot 2 \cdot 1 = 30$$

ANSWER 270 divisors, 30 of them squares

## 1.7 PRIMES OF SPECIAL FORM

Every integer is one of  $6k, 6k \pm 1, 6k \pm 2, 6k + 3$ . The forms  $6k, 6k \pm 2$  are even and  $6k + 3$  is a multiple of 3, so:

## THEOREM · PRIMES ABOVE THREE

Every prime  $p > 3$  has the form  $6k \pm 1$ , and  $24 \mid p^2 - 1$ .

For the second part write  $p^2 - 1 = (p - 1)(p + 1)$ . These are consecutive even numbers, so one of them is a multiple of 4 and together they supply  $2 \cdot 4 = 8$ . Also one of the three consecutive numbers  $p - 1, p, p + 1$  is a multiple of 3, and it is not  $p$ . So  $8 \cdot 3 = 24$  divides  $p^2 - 1$ .

**EXAMPLE 1.6**

Find the largest integer that divides  $p^4 + p^2 - 2$  for every prime  $p > 3$ . (IOQM 2026, Q25)

For  $p = 5$  and  $p = 7$ :

$$p = 5 : 625 + 25 - 2 = 648,$$

$$p = 7 : 2401 + 49 - 2 = 2448$$

**Not more than 72.** The answer divides both numbers.  $648 = 2^3 \cdot 3^4$  and  $2448 = 2^4 \cdot 3^2 \cdot 17$ , so their gcd is

$$2^3 \cdot 3^2 = 72$$

**72 always divides.**

$$p^4 + p^2 - 2 = (p^2 + 2)(p^2 - 1)$$

$24 \mid p^2 - 1$  (theorem *Primes above three*, Section 1.7).

In particular  $3 \mid p^2 - 1$ , so  $p^2 + 2 = (p^2 - 1) + 3$  is a multiple of 3.

Hence  $24 \cdot 3 = 72$  divides the product.

**ANSWER 72**

**WHERE MARKS GO · BOTH HALVES**

“Largest number dividing every value” needs two halves: a proof that some  $D$  always divides, and two cases whose gcd is exactly  $D$ . Either half alone earns nothing.

**1.8 USEFUL FACTORISATIONS**

Most “show this divides” questions become one line once the expression is factorised. The identities used most:

- (i)  $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$ , so  $a - b \mid a^n - b^n$ .
- (ii) For odd  $n$ ,  $a + b \mid a^n + b^n$ ; for even  $n$ ,  $a + b \mid a^n - b^n$ .
- (iii) **Sophie Germain:**  $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$ .
- (iv) **Difference of squares:**  $n = x^2 - y^2 = (x - y)(x + y)$ , where both factors have the same parity.

The last point gives a neat criterion. If  $n = x^2 - y^2$  then  $x - y$  and  $x + y$  are both odd or both even, so  $n$  is odd or a multiple of 4. Conversely an odd  $n$  is  $(\frac{n+1}{2})^2 - (\frac{n-1}{2})^2$  and  $n = 4m$  is  $(m+1)^2 - (m-1)^2$ . So an integer is a difference of two squares exactly

when it does not leave remainder 2 on division by 4.

**EXAMPLE 1.7**

For which positive integers  $n$  is  $n^4 + 4$  prime?

For small  $n$ :

| $n$       | 1 | 2  | 3  | 4   |
|-----------|---|----|----|-----|
| $n^4 + 4$ | 5 | 20 | 85 | 260 |

Only  $n = 1$  gives a prime. By the Sophie Germain identity with  $a = n$ ,  $b = 1$ ,

$$n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$$

The first factor is at least  $1 + 2 + 2 = 5$ , as  $n \geq 1$ .

The second factor is  $(n - 1)^2 + 1$ : it is 1 at  $n = 1$ , and at least 2 for  $n \geq 2$ .

So for  $n \geq 2$ ,  $n^4 + 4$  is a product of two numbers greater than 1, i.e., composite. At  $n = 1$  it is 5, a prime.

**ANSWER only  $n = 1$**

**EXAMPLE 1.8**

Show that 30 divides  $n^5 - n$  for every integer  $n$ .

For  $n = 2$ :  $2^5 - 2 = 30$ .

$30 = 2 \cdot 3 \cdot 5$ , so it is enough to show that 2, 3 and 5 each divide  $n^5 - n$ .

$$n^5 - n = n(n^4 - 1) = (n - 1)n(n + 1)(n^2 + 1)$$

$n - 1$ ,  $n$ ,  $n + 1$  are three consecutive integers, so one of them is even and one is a multiple of 3.

For 5, the five forms of  $n$  (division algorithm):

| $n$        | multiple of 5                 |
|------------|-------------------------------|
| $5k$       | $n$                           |
| $5k + 1$   | $n - 1$                       |
| $5k - 1$   | $n + 1$                       |
| $5k \pm 2$ | $n^2 + 1 = 25k^2 \pm 20k + 5$ |

In every case one factor is a multiple of 5.

2, 3, 5 are distinct primes, so their product 30 divides  $n^5 - n$ . Hence proved.

**ANSWER  $30 \mid n^5 - n$  for all  $n$**

## EXERCISES 1

- 1.1 Find the sum of all positive integers  $n$  for which  $n + 3$  divides  $n^2 + 15$ .
- 1.2 The six-digit number  $\overline{a1989b}$  is divisible by 72. Find  $a + b$ .
- 1.3 How many positive divisors of 7200 are perfect squares?
- 1.4 Find the smallest positive integer with exactly 12 positive divisors.
- 1.5 Find the sum of all positive divisors of 360.
- 1.6 The product of all positive divisors of 36 is  $6^k$ . Find  $k$ .
- 1.7 How many primes  $p$  are there for which  $p^2 + 2$  is also prime?
- 1.8 How many integers  $n$  with  $1 \leq n \leq 100$  can be written as  $x^2 - y^2$  with  $x, y$  integers?
- 1.9 Find the largest prime factor of  $2^{16} - 1$ .
- 1.10 For how many integers  $n$  with  $1 \leq n \leq 10$  is  $n^4 + n^2 + 1$  prime?
- 1.11 Find the largest integer that divides  $n^3 - n$  for every integer  $n$ .
- 1.12 Find the number of positive integers  $n \leq 1000$  for which  $\tau(n)$  is odd.

## CHAPTER 02 GCD, LCM AND LINEAR EQUATIONS

This chapter is about the greatest common divisor and the least common multiple of two numbers. The Euclidean algorithm finds the gcd without factorising, and from it comes Bezout's identity. Bezout's identity in turn gives the complete solution of the equation  $ax + by = c$  in integers, a type of question that appears in IOQM almost every year.

## 2.1 GCD AND LCM

## DEFINITION · GCD AND LCM

For integers  $a, b$  not both zero,  $\gcd(a, b)$  is the largest integer dividing both. For non-zero  $a, b$ ,  $\text{lcm}(a, b)$  is the smallest positive integer that both divide. If  $\gcd(a, b) = 1$ , the numbers are **coprime**.

Prime factorisation gives both at once. Write the two numbers over the same primes, allowing exponent 0. Then the gcd takes the **smaller** exponent of each prime, and the lcm the **larger**. Since  $\min(x, y) + \max(x, y) = x + y$  for every pair of exponents:

## THEOREM · PRODUCT OF GCD AND LCM

For positive integers  $a, b$ :  
 $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$ .

Two more facts are used often. Every common divisor of  $a$  and  $b$  divides  $\gcd(a, b)$ , and every common multiple is a multiple of  $\text{lcm}(a, b)$ .

## KEY IDEA · TAKE OUT THE GCD

With  $g = \gcd(a, b)$ , write  $a = gx$  and  $b = gy$ . Then  $\gcd(x, y) = 1$  and  $\text{lcm}(a, b) = gxy$ .

## EXAMPLE 2.1

Find  $\gcd(360, 756)$  and  $\text{lcm}(360, 756)$ .

$$360 = 2^3 \cdot 3^2 \cdot 5, \quad 756 = 2^2 \cdot 3^3 \cdot 7$$

Exponent of each prime (0 if the prime is absent); the gcd takes the smaller exponent and the lcm the larger:

| prime | 360 | 756 | gcd | lcm |
|-------|-----|-----|-----|-----|
| 2     | 3   | 2   | 2   | 3   |
| 3     | 2   | 3   | 2   | 3   |
| 5     | 1   | 0   | 0   | 1   |
| 7     | 0   | 1   | 0   | 1   |

$$\gcd = 2^2 \cdot 3^2 = 36$$

$$\text{lcm} = 2^3 \cdot 3^3 \cdot 5 \cdot 7 = 7560$$

Check by  $\gcd \cdot \text{lcm} = ab$  (Section 2.1):

$$36 \cdot 7560 = 272160 = 360 \cdot 756$$

ANSWER 36 and 7560

**EXAMPLE 2.2**

How many ordered pairs  $(a, b)$  of positive integers have  $\gcd(a, b) = 12$  and  $\text{lcm}(a, b) = 360$ ?

Taking out the gcd (Section 2.1), let  $a = 12x$ ,  $b = 12y$  with  $\gcd(x, y) = 1$ . Then

$$\text{lcm}(a, b) = 12xy = 360$$

so  $xy = 30 = 2 \cdot 3 \cdot 5$ .

$\gcd(x, y) = 1$ , so no prime is shared: each of 2, 3, 5 goes wholly into  $x$  or wholly into  $y$ . 2 choices for each prime, so  $2^3 = 8$  pairs.

The four with  $x < y$ :

| $x$ | $y$ | $(a, b)$  |
|-----|-----|-----------|
| 1   | 30  | (12, 360) |
| 2   | 15  | (24, 180) |
| 3   | 10  | (36, 120) |
| 5   | 6   | (60, 72)  |

Swapping  $x$  and  $y$  gives the other four.

**ANSWER 8 pairs**

**WHERE MARKS GO · TWO NUMBERS ONLY**

$\gcd \cdot \text{lcm} = \text{product}$  is an identity for two numbers. For three it holds only when they are pairwise co-prime: for 2, 2, 2 the gcd and lcm are both 2, with product 4, while  $2 \cdot 2 \cdot 2 = 8$ .

**2.2 THE EUCLIDEAN ALGORITHM**

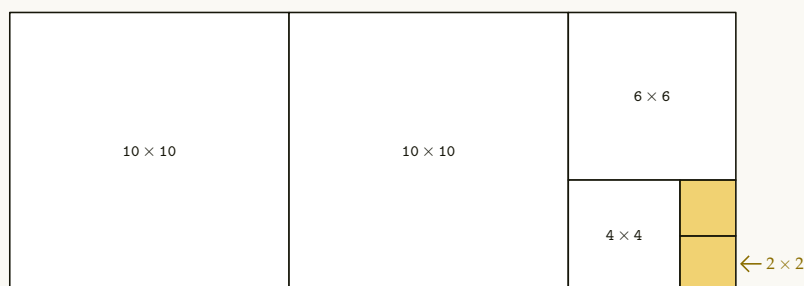
Factorising large numbers is slow. The Euclidean algorithm finds the gcd by division alone.

**THEOREM · EUCLID'S STEP**

If  $a = bq + r$ , then  $\gcd(a, b) = \gcd(b, r)$ . In particular

$\gcd(a, b) = \gcd(b, a \bmod b) = \gcd(a - kb, b)$  for every integer  $k$ .

Any common divisor of  $a$  and  $b$  divides  $r = a - bq$ ; any common divisor of  $b$  and  $r$  divides  $a = bq + r$ . So the two pairs have the same common divisors, and hence the same greatest one.



$$26 = 2 \cdot 10 + 6, \quad 10 = 1 \cdot 6 + 4, \quad 6 = 1 \cdot 4 + 2, \quad 4 = 2 \cdot 2$$

the last square is the gcd:  $\gcd(26, 10) = 2$

Repeat: replace the larger number by its remainder on division by the smaller, until the remainder is 0. The last non-zero remainder is the gcd. The remainders at least halve every two steps, so the algorithm ends quickly even for large numbers.

The picture is the same algorithm drawn as squares: cut the largest possible squares off a  $26 \times 10$  rectangle, then off what is left, and so on. The last square fits exactly, and its side is the gcd.

**EXAMPLE 2.3**

Show that  $\frac{21n+4}{14n+3}$  is in lowest terms for every positive integer  $n$ .

Putting  $n = 1$ ,

$$\frac{21+4}{14+3} = \frac{25}{17}, \quad \gcd(25, 17) = 1$$

For any  $n$ , let  $d$  be a positive common divisor of  $21n+4$  and  $14n+3$ . Making the coefficients of  $n$  equal,

$$2(21n+4) = 42n+8, \quad 3(14n+3) = 42n+9$$

$d$  divides both, so  $d$  divides their difference

$$(42n + 9) - (42n + 8) = 1$$

$\therefore d = 1$ , i.e., the gcd is 1 for every  $n$ .

ANSWER always in lowest terms

## 2.3 BEZOUT'S IDENTITY

### THEOREM · BEZOUT

For integers  $a, b$  not both zero there are integers  $x, y$  with

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

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

Let  $s$  be the smallest positive number of the form  $ax + by$ . Divide  $a$  by  $s$ :  $a = sq + r$  with  $0 \leq r < s$ . Then  $r = a - sq$  is again of the form  $ax + by$ , and it is smaller than  $s$ , so it cannot be positive:  $r = 0$  and  $s \mid a$ . Likewise  $s \mid b$ , so  $s \leq \gcd(a, b)$ . But  $\gcd(a, b)$  divides  $ax + by = s$ , so  $\gcd(a, b) \leq s$ . Hence  $s = \gcd(a, b)$ .

Bezout's identity proves the lemma stated in Chapter 1. If a prime  $p$  divides  $ab$  but not  $a$ , then  $\gcd(p, a) = 1$ , so  $px + ay = 1$  for some  $x, y$ . Multiply by  $b$ :  $pbx + aby = b$ . Both terms on the left are multiples of  $p$ , so  $p \mid b$ .

To find  $x$  and  $y$  in practice, run the Euclidean algorithm and substitute back from the last line.

### EXAMPLE 2.4

Find integers  $x, y$  with  $143x + 63y = 1$ .

By the Euclidean algorithm (Section 2.2), with each remainder on the left,

$$17 = 143 - 2 \cdot 63$$

$$12 = 63 - 3 \cdot 17$$

$$5 = 17 - 12$$

$$2 = 12 - 2 \cdot 5$$

$$1 = 5 - 2 \cdot 2$$

Now work backwards from the last line, replacing one remainder at a time.

Putting  $2 = 12 - 2 \cdot 5$ ,

$$1 = 5 - 2(12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12$$

Putting  $5 = 17 - 12$ ,

$$1 = 5(17 - 12) - 2 \cdot 12 = 5 \cdot 17 - 7 \cdot 12$$

Putting  $12 = 63 - 3 \cdot 17$ ,

$$1 = 5 \cdot 17 - 7(63 - 3 \cdot 17) = 26 \cdot 17 - 7 \cdot 63$$

Putting  $17 = 143 - 2 \cdot 63$ ,

$$\begin{aligned} 1 &= 26(143 - 2 \cdot 63) - 7 \cdot 63 \\ &= 26 \cdot 143 - 59 \cdot 63 \end{aligned}$$

Check:  $26 \cdot 143 = 3718$ ,  $59 \cdot 63 = 3717$ , difference 1.

ANSWER  $x = 26$ ,  $y = -59$

## 2.4 COPRIMALITY FACTS

- (i)  $\gcd(n, n+k)$  divides  $k$ . So consecutive integers are coprime, and so are consecutive odd numbers.
- (ii) If  $a \mid bc$  and  $\gcd(a, b) = 1$ , then  $a \mid c$ .
- (iii) If  $a \mid n$ ,  $b \mid n$  and  $\gcd(a, b) = 1$ , then  $ab \mid n$ .
- (iv)  $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1$  for integers  $a \geq 2$ ,  $m, n \geq 1$ .
- (v) Consecutive Fibonacci numbers are coprime, and  $\gcd(F_m, F_n) = F_{\gcd(m, n)}$ .

The second item is Euclid's lemma again, with Bezout: from  $ax + by = 1$  get  $acx + bcy = c$ , and  $a$  divides both terms on the left.

### WHERE MARKS GO · SPLIT INTO PRIME POWERS

To prove  $72 \mid N$ , prove  $8 \mid N$  and  $9 \mid N$ . Writing  $72 = 6 \cdot 12$  proves nothing, because 6 and 12 share primes:  $4 \mid 12$  and  $6 \mid 12$ , yet  $24 \nmid 12$ .

## 2.5 LINEAR DIOPHANTINE EQUATIONS

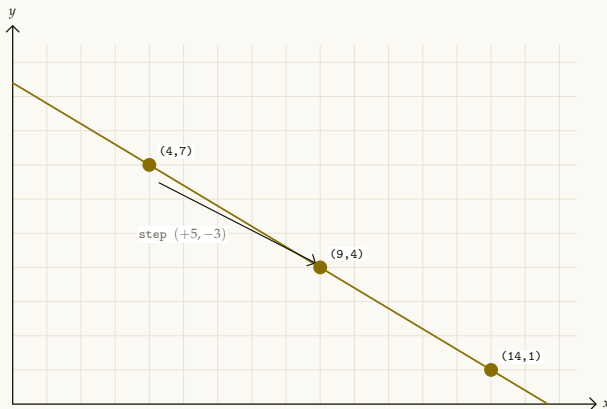
An equation to be solved in integers is called **Diophantine**. The linear equation in two unknowns can be solved completely.

## THEOREM · LINEAR EQUATION IN TWO UNKNOWN

$ax + by = c$  has integer solutions exactly when  $g = \gcd(a, b)$  divides  $c$ . If  $(x_0, y_0)$  is one solution, all of them are

$$x = x_0 + \frac{b}{g}t, \quad y = y_0 - \frac{a}{g}t, \quad t \in \mathbb{Z}.$$

If a solution exists,  $g$  divides the left side, so  $g \mid c$ . Conversely, if  $c = gm$ , multiply the Bezout pair by  $m$ . For the general solution, subtract two solutions:  $a(x - x_0) = -b(y - y_0)$ . Dividing by  $g$ , the coprime number  $\frac{a}{g}$  divides  $y - y_0$ , which gives the stated form. Geometrically, the solutions are the lattice points on a straight line, spaced at a fixed step. For **positive** solutions, turn  $x > 0$  and  $y > 0$  into two inequalities for  $t$  and count the integers between them.



$3x + 5y = 47$ : a lattice point every  $(5, -3)$ , three of them positive

## EXAMPLE 2.5

How many solutions in positive integers does  $7x + 11y = 200$  have?

For one solution,  $200 - 7x$  must be a multiple of 11. Putting  $x = 1, 2, 3, 4, 5$ ,

$$200 - 7x = 193, 186, 179, 172, 165$$

Only  $165 = 11 \cdot 15$  works, so  $(5, 15)$  is one solution.  $\gcd(7, 11) = 1$ , so by the linear-equation theorem (Section 2.5), all solutions are

$$x = 5 + 11t, \quad y = 15 - 7t$$

For positive solutions,

$$x > 0: 11t > -5, \text{ so } t \geq 0$$

$$y > 0: 7t < 15, \text{ so } t \leq 2$$

| $t$ | $x$ | $y$ |
|-----|-----|-----|
| 0   | 5   | 15  |
| 1   | 16  | 8   |
| 2   | 27  | 1   |

Check  $(27, 1)$ :  $7 \cdot 27 + 11 \cdot 1 = 189 + 11 = 200$ .

ANSWER 3

## 2.6 THE COIN PROBLEM

## THEOREM · TWO COINS

Let  $a, b \geq 2$  be coprime. The largest integer that **cannot** be written as  $ax + by$  with  $x, y \geq 0$  is  $ab - a - b$ , and exactly  $\frac{(a-1)(b-1)}{2}$  positive integers cannot be so written.

Every integer larger than  $ab - a - b$  can be paid. If  $\gcd(a, b) = d > 1$ , only multiples of  $d$  can ever be paid, so there is no largest unpayable amount.

## EXAMPLE 2.6

Pens come in packs of 5 and packs of 9. What is the largest number of pens that cannot be bought exactly, and how many numbers cannot?

$\gcd(5, 9) = 1$ , so by the two-coins theorem (Section 2.6) with  $a = 5, b = 9$ ,

$$\text{largest} = 5 \cdot 9 - 5 - 9 = 31$$

$$\text{how many} = \frac{(5-1)(9-1)}{2} = \frac{4 \cdot 8}{2} = 16$$

Check 31 by hand: with  $y = 0, 1, 2, 3$  packs of 9 ( $9 \cdot 4 > 31$ ), the pens left over are

$$31 - 9y = 31, 22, 13, 4$$

None is a multiple of 5, so 31 cannot be bought.

The 16 numbers that cannot be bought are

$$1, 2, 3, 4, 6, 7, 8, 11, 12, 13$$

$$16, 17, 21, 22, 26, 31$$

ANSWER 31, and 16 numbers

## 2.7 FACTORISING EQUATIONS

Many nonlinear equations in integers become a short divisor list once they are factorised.

## KEY IDEA · COMPLETING THE RECTANGLE

$$xy + ax + by = c \iff (x+b)(y+a) = c + ab$$

Two related methods:

- (i) **Isolate one variable.** Solve for one variable as a fraction. It must be an integer, so the denominator divides a fixed number.
- (ii) **Unit fractions.**  $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$  is  $(x-n)(y-n) = n^2$ , so it has  $\tau(n^2)$  ordered solutions in positive integers.

## EXAMPLE 2.7

Solve  $xy = 2x + 3y$  in positive integers.

$$xy - 2x - 3y = 0$$

Completing the rectangle (Section 2.7), i.e., adding  $6 = 2 \cdot 3$  to both sides,

$$xy - 2x - 3y + 6 = 6$$

$$(x-3)(y-2) = 6$$

$x, y \geq 1$ , so  $x-3 \geq -2$  and  $y-2 \geq -1$ .

The product 6 is positive, so both factors have the same sign. If both are negative, then  $y-2 = -1$  and  $x-3 = -1$  or  $-2$ , so the product is at most 2, not 6. Hence both factors are positive:

| $x-3$ | $y-2$ | $(x, y)$ |
|-------|-------|----------|
| 1     | 6     | (4, 8)   |
| 2     | 3     | (5, 5)   |
| 3     | 2     | (6, 4)   |
| 6     | 1     | (9, 3)   |

Check (5, 5):  $xy = 25$  and  $2x + 3y = 10 + 15 = 25$ .

ANSWER (4, 8), (5, 5), (6, 4), (9, 3)

## EXAMPLE 2.8

Find the number of two-digit numbers  $n = \overline{ab}$  with  $n = 26 + ab$ , where  $a, b$  are the digits of  $n$ . (IOQM 2026, Q6)

$n = 10a + b$ , so

$$10a + b = 26 + ab$$

$$b(a-1) = 10a - 26 = 10(a-1) - 16$$

$a = 1$  gives  $0 = -16$ , which is not possible. So  $a \geq 2$  and, on dividing by  $a-1$ ,

$$b = 10 - \frac{16}{a-1}$$

$b$  is an integer, so  $(a-1) \mid 16$ . As  $2 \leq a \leq 9$ ,  $a-1 = 1, 2, 4$  or  $8$ :

| $a-1$ | $a$ | $b$ | $n$ |
|-------|-----|-----|-----|
| 1     | 2   | -6  | no  |
| 2     | 3   | 2   | 32  |
| 4     | 5   | 6   | 56  |
| 8     | 9   | 8   | 98  |

$a = 2$  is rejected, as a digit cannot be negative.

Check:  $26 + 3 \cdot 2 = 32$ ,  $26 + 5 \cdot 6 = 56$ ,  $26 + 9 \cdot 8 = 98$ .

ANSWER 3

## WHERE MARKS GO · NEGATIVE PAIRS AND RANGES

After factorising, list the negative divisor pairs as well, then apply the given conditions. Forgetting the negative pairs loses solutions; forgetting the digit range or the sign conditions gives false ones.

## EXERCISES 2

- Find  $\gcd(2^{30} - 1, 2^{18} - 1)$ .
- How many ordered pairs  $(a, b)$  of positive integers have  $\gcd(a, b) = 6$  and  $\text{lcm}(a, b) = 360$ ?
- Find the smallest positive value of  $84x + 126y$  over all integers  $x, y$ .
- How many solutions in positive integers does  $3x + 5y = 100$  have?
- Find the largest integer that cannot be written as  $8a + 13b$  with  $a, b$  non-negative integers.
- How many positive integers cannot be written as  $4a + 7b$  with  $a, b$  non-negative integers?
- How many ordered pairs  $(x, y)$  of positive integers satisfy  $\frac{1}{x} + \frac{1}{y} = \frac{1}{12}$ ?
- For how many positive integers  $n$  is  $\frac{n+20}{n+2}$  an integer?

- 2.9 For how many  $n$  with  $1 \leq n \leq 100$  is the fraction  $\frac{n+4}{n+1}$  **not** in lowest terms?
- 2.10 How many ordered pairs of positive integers satisfy  $xy = 4x + 3y$ ?

- 2.11 In how many ways can 1000 be written as a sum of one or more consecutive positive integers?
- 2.12 Find  $\gcd(F_{30}, F_{45})$ , where  $F_1 = F_2 = 1$  and  $F_{n+2} = F_{n+1} + F_n$ .

## CHAPTER 03 MODULAR ARITHMETIC

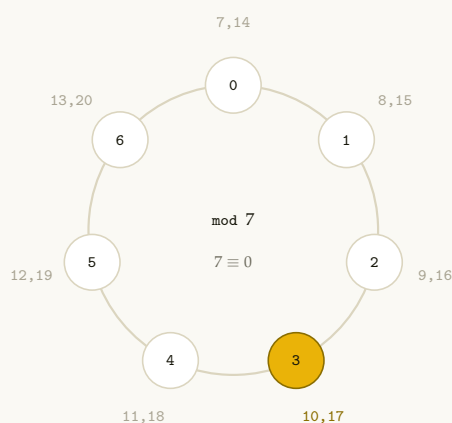
Many number theory questions ask only for a remainder. Congruence notation lets us add, subtract and multiply remainders, and raise them to powers, as if they were ordinary numbers. This chapter develops this arithmetic, then the theorems of Fermat, Euler and Wilson, then the order of a number, and finally the Chinese remainder theorem, which combines remainders for different moduli into one.

### 3.1 CONGRUENCES

#### DEFINITION · CONGRUENT MODULO $m$

For a positive integer  $m$ , we write  $a \equiv b \pmod{m}$  when  $m \mid a - b$ . Equivalently,  $a$  and  $b$  leave the same remainder on division by  $m$ .

So  $17 \equiv 3 \pmod{7}$ ,  $-1 \equiv 6 \pmod{7}$ , and  $a \equiv 0 \pmod{m}$  means  $m \mid a$ . Every integer is congruent to exactly one of  $0, 1, \dots, m-1$ , its remainder. Think of a clock with  $m$  hours: counting round it, 3, 10 and 17 come to the same place.



3, 10, 17 are at one place:  $10 \equiv 17 \equiv 3 \pmod{7}$

The main use of this notation is that congruences can be added, subtracted and multiplied like equations.

#### RULES · ARITHMETIC OF CONGRUENCES

If  $a \equiv b$  and  $c \equiv d \pmod{m}$ , then  
 $a \pm c \equiv b \pm d$ ,  $ac \equiv bd$ ,  $a^k \equiv b^k \pmod{m}$ .

For the product,  $ac - bd = a(c - d) + d(a - b)$ , and both terms are multiples of  $m$ . The power rule is the product rule repeated. It follows that if  $P$  is a polynomial with integer coefficients and  $a \equiv b \pmod{m}$ , then  $P(a) \equiv P(b) \pmod{m}$ ; in other words  $a - b$  always divides  $P(a) - P(b)$ .

#### EXAMPLE 3.1

Find the remainder when  $2026^{2026}$  is divided by 7.

$2026 = 7 \cdot 289 + 3$ , so  $2026 \equiv 3 \pmod{7}$  and

$$2026^{2026} \equiv 3^{2026} \pmod{7}$$

Multiplying by 3 each time and reducing modulo 7:

| $k$            | 1 | 2 | 3 | 4 | 5 | 6 |
|----------------|---|---|---|---|---|---|
| $3^k \pmod{7}$ | 3 | 2 | 6 | 4 | 5 | 1 |

$3^6 \equiv 1$ , so the powers repeat every 6. Now  $2026 = 6 \cdot 337 + 4$ , so

$$3^{2026} = (3^6)^{337} \cdot 3^4 \equiv 3^4 \equiv 4$$

ANSWER 4

#### WHERE MARKS GO · EXPONENTS ARE NOT REDUCED MOD $m$

$2^{10} = 1024 \equiv 2 \pmod{7}$ , but  $2^{10 \pmod{7}} = 2^3 \equiv 1$ . An exponent may only be reduced modulo the length of the cycle of powers, here 3, which section 3.8 calls the order.

### 3.2 INVERSES AND CANCELLATION

Division is where congruences differ from equations.

## THEOREM · CANCELLATION

$$ac \equiv bc \pmod{m} \text{ implies } a \equiv b \pmod{\frac{m}{\gcd(c, m)}}.$$

So a common factor can be cancelled directly only when it is coprime to  $m$ . For example  $2 \cdot 3 \equiv 2 \cdot 8 \pmod{10}$ , yet  $3 \not\equiv 8 \pmod{10}$ ; what is true is  $3 \equiv 8 \pmod{5}$ .

An **inverse** of  $a$  modulo  $m$  is a number  $a'$  with  $aa' \equiv 1 \pmod{m}$ . By Bezout,  $ax + my = 1$  is solvable exactly when  $\gcd(a, m) = 1$ , so  $a$  has an inverse exactly when it is coprime to  $m$ , and the inverse is unique modulo  $m$ . Modulo a prime every non-zero residue has an inverse, so division by anything non-zero is allowed.

## EXAMPLE 3.2

Find the inverse of 13 modulo 21, and use it to solve  $13x \equiv 8 \pmod{21}$ .

We need  $a'$  with  $13a' \equiv 1 \pmod{21}$ . Numbers 1 more than a multiple of 21, up to the first multiple of 13:

$$22, 43, 64, 85, 106, 127, 148, 169$$

$169 = 13 \cdot 13$ , so  $13 \cdot 13 \equiv 1 \pmod{21}$ , i.e., the inverse of 13 is 13 itself.

Multiplying  $13x \equiv 8$  by 13, as  $13 \cdot 13 \equiv 1$ ,

$$x \equiv 13 \cdot 8 = 104 = 4 \cdot 21 + 20$$

$\therefore x \equiv 20 \pmod{21}$ . Check:  $13 \cdot 20 = 260 = 12 \cdot 21 + 8$ . (IOQM 2026, Q28 uses this inverse; see Example 5.6.)

$$\text{ANSWER } x \equiv 20 \pmod{21}$$

## 3.3 LINEAR CONGRUENCES

THEOREM · SOLVING  $ax \equiv b \pmod{m}$ 

The congruence is solvable exactly when  $g = \gcd(a, m)$  divides  $b$ , and then it has exactly  $g$  solutions modulo  $m$ .

The method: divide  $a$ ,  $b$  and  $m$  by  $g$ , so that  $a/g$  is coprime to  $m/g$ , then multiply by the inverse of  $a/g$  modulo  $m/g$ . A linear congruence is the same thing as the equation  $ax - my = b$  of section 2.5, written in another form.

## EXAMPLE 3.3

Solve  $9x \equiv 6 \pmod{15}$ .

$\gcd(9, 15) = 3$  and  $3 \mid 6$ , so there are exactly 3 solutions modulo 15 (theorem on linear congruences, Section 3.3).

On dividing 9, 6, 15 by 3,

$$3x \equiv 2 \pmod{5}$$

$3 \cdot 2 = 6 \equiv 1 \pmod{5}$ , so the inverse of 3 modulo 5 is 2. Multiplying by 2,

$$x \equiv 4 \pmod{5}$$

In  $0, 1, \dots, 14$ :  $x = 4, 9, 14$ .

Check:  $9x = 36, 81, 126$ , each 6 more than a multiple of 15.

$$\text{ANSWER } x \equiv 4, 9, 14 \pmod{15}$$

## 3.4 POWERS MODULO SMALL NUMBERS

Squares and cubes leave only a few remainders, and this alone shows that many equations have no solution.

| POWER, MODULUS               | POSSIBLE REMAINDERS    |
|------------------------------|------------------------|
| $x^2 \pmod{3 \text{ or } 4}$ | 0, 1                   |
| $x^2 \pmod{5}$               | 0, 1, 4                |
| $x^2 \pmod{8}$               | 0, 1, 4; odd squares 1 |
| $x^2 \pmod{9}$               | 0, 1, 4, 7             |
| $x^2 \pmod{16}$              | 0, 1, 4, 9             |
| $x^3 \pmod{7 \text{ or } 9}$ | 0, 1, -1               |
| $x^4 \pmod{16}$              | 0, 1                   |

Each row is a finite check: square the residues  $0, 1, \dots, m-1$ . Consequences:

- (i) A sum of two squares never leaves remainder 3 on division by 4.
- (ii) A sum of three squares never leaves remainder 7 on division by 8.
- (iii) A sum of two cubes never leaves remainder 3, 4, 5 or 6 on division by 9.

## EXAMPLE 3.4

Show that  $x^2 + y^2 = 2027$  has no solution in integers.

$2027 = 4 \cdot 506 + 3$ , so the right side is  $\equiv 3 \pmod{4}$ .

A square is  $\equiv 0$  or  $1 \pmod{4}$  (table in Section 3.4), so modulo 4 the left side can only be:

| $x^2$ | $y^2$ | $x^2 + y^2$ |
|-------|-------|-------------|
| 0     | 0     | 0           |
| 0     | 1     | 1           |
| 1     | 0     | 1           |
| 1     | 1     | 2           |

$x^2 + y^2$  is never  $\equiv 3$ , so the two sides are never equal.

ANSWER **no solutions**

## WHERE MARKS GO · CHOOSE THE MODULUS

Pick the modulus where the power has the fewest remainders: 4 or 8 for squares, 7 or 9 for cubes, 16 for fourth powers. A badly chosen modulus gives a long table and no contradiction.

## 3.5 FERMAT'S LITTLE THEOREM

## THEOREM · FERMAT

If  $p$  is prime and  $p \nmid a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .  
For every integer  $a$ ,  $a^p \equiv a \pmod{p}$ .

Here is the idea of the proof. The numbers  $a, 2a, \dots, (p-1)a$  leave different remainders modulo  $p$  (if  $ia \equiv ja$ , cancel  $a$  to get  $i \equiv j$ ), and none of them is 0. So their remainders are  $1, 2, \dots, p-1$  in some order. Multiplying all of them,  $a^{p-1}(p-1)! \equiv (p-1)!$ , and cancelling  $(p-1)!$ , which is coprime to  $p$ , gives  $a^{p-1} \equiv 1$ .

In practice, when  $p \nmid a$ , the exponent of  $a$  may be reduced modulo  $p-1$ .

## EXAMPLE 3.5

Find the remainder when  $3^{100}$  is divided by 7.

7 is prime and  $7 \nmid 3$ , so by Fermat's little theorem

$$3^6 \equiv 1 \pmod{7}$$

(Check:  $3^6 = 729 = 104 \cdot 7 + 1$ .) So the exponent may be reduced modulo 6. As  $100 = 6 \cdot 16 + 4$ ,

$$3^{100} = (3^6)^{16} \cdot 3^4 \equiv 3^4 = 81$$

and  $81 = 11 \cdot 7 + 4$ .

ANSWER **4**

## WHERE MARKS GO · THE CONVERSE IS FALSE

$341 = 11 \cdot 31$  is composite, yet  $2^{340} \equiv 1 \pmod{341}$ .  
So  $a^{n-1} \equiv 1 \pmod{n}$  does not prove that  $n$  is prime.

## 3.6 EULER'S THEOREM

## DEFINITION AND THEOREM · EULER

$\varphi(n)$  counts the integers in  $1, \dots, n$  coprime to  $n$ , and

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

If  $\gcd(a, n) = 1$ , then  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

The proof is Fermat's, with the  $\varphi(n)$  residues coprime to  $n$  in place of  $1, \dots, p-1$ . Useful values:  $\varphi(p) = p-1$ ,  $\varphi(p^k) = p^k - p^{k-1}$ , and  $\varphi(mn) = \varphi(m)\varphi(n)$  for coprime  $m, n$ . Also  $\sum_{d|n} \varphi(d) = n$ .

$\varphi(n)$  is always a period of the powers of  $a$ , but not always the shortest:  $\varphi(100) = 40$ , while already  $7^4 = 2401 \equiv 1 \pmod{100}$ .

## EXAMPLE 3.6

Find the last two digits of  $7^{2026}$ .

We need  $7^{2026} \pmod{100}$ . Euler's theorem gives  $7^{40} \equiv 1 \pmod{100}$  ( $\varphi(100) = 40$ ), but already

$$7^4 = 49^2 = 2401 \equiv 1 \pmod{100}$$

So the last two digits of  $7, 7^2, 7^3, \dots$  repeat every 4: 07, 49, 43, 01. Now  $2026 = 4 \cdot 506 + 2$ , so

$$7^{2026} = (7^4)^{506} \cdot 7^2 \equiv 7^2 = 49$$

ANSWER **49**

## 3.7 WILSON'S THEOREM

## THEOREM · WILSON

For  $n \geq 2$ :  $n$  is prime exactly when  $(n-1)! \equiv -1 \pmod{n}$ .

For a prime  $p$ , each of  $2, 3, \dots, p-2$  pairs with its inverse, which is a different number in the same range, so their product is  $\equiv 1$ . Only 1 and  $p-1$  are their own inverses, which leaves  $(p-1)! \equiv 1 \cdot (p-1) \equiv -1$ . For composite  $n > 4$ ,  $(n-1)!$  is in fact  $\equiv 0 \pmod{n}$ ; for  $n = 4$  it is 2.

## EXAMPLE 3.7

Find the remainder when  $15!$  is divided by 17.

For  $p = 7$ :  $6! = 720 \equiv -1$  and  $5! = 120 \equiv 1 \pmod{7}$ .

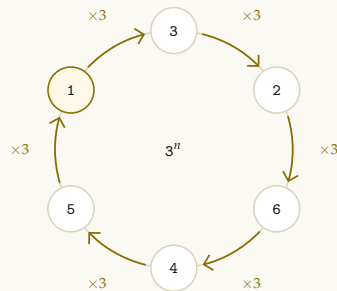
17 is prime, so by Wilson's theorem

$$16! \equiv -1 \pmod{17}$$

Also  $16! = 16 \cdot 15!$  and  $16 = 17 - 1 \equiv -1$ , so  $16! \equiv -15!$ .

Hence  $-15! \equiv -1$ , i.e.,  $15! \equiv 1 \pmod{17}$ .

ANSWER 1



order 6: every  
non-zero residue

## 3.8 ORDER, AND CYCLES OF POWERS

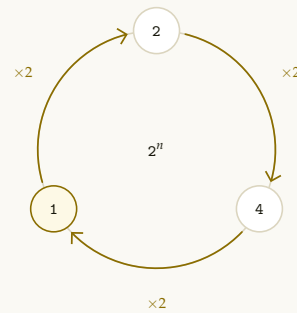
## DEFINITION · ORDER

For  $\gcd(a, m) = 1$ , the **order**  $\text{ord}_m(a)$  is the smallest  $d \geq 1$  with  $a^d \equiv 1 \pmod{m}$ . Then

$$a^n \equiv 1 \pmod{m} \iff \text{ord}_m(a) \mid n.$$

Divide  $n$  by the order  $d$ :  $n = dq + r$  with  $0 \leq r < d$ , so  $a^n \equiv a^r$ . This is 1 only if  $r = 0$ , because  $d$  is the smallest positive exponent that gives 1. So the powers of  $a$  repeat with period exactly  $d$ , and  $d$  divides  $\phi(m)$ , and  $p-1$  for a prime  $p$ . To find an order, test only the divisors of  $\phi(m)$ .

Two more facts: if  $d \mid n$  then  $a^d - 1 \mid a^n - 1$ ; and for a prime  $p \neq 2, 5$  the decimal period of  $1/p$  is  $\text{ord}_p(10)$ . For example  $10^3 \equiv -1 \pmod{13}$ , so  $1/13$  has period 6.



order 3, and  $3 \mid 6$

## EXAMPLE 3.8

Let  $n = \frac{4^{31} - 1}{3}$ . Find the remainder when  $2^{n-1}$  is divided by  $n$ . (IOQM 2026, Q29)

Putting  $4^5$  in place of  $4^{31}$ , we get  $n = 341$  and  $3n = 2^{10} - 1$ . So  $2^{10} \equiv 1 \pmod{341}$ , and  $10 \mid 340 = n-1$  gives  $2^{340} \equiv 1$ .

Now  $3n = 4^{31} - 1 = 2^{62} - 1$ , so  $n \mid 2^{62} - 1$ , i.e.,  $2^{62} \equiv 1 \pmod{n}$ . So it is enough to show  $62 \mid n-1$ .

$$n-1 = \frac{2^{62} - 4}{3} = 4 \cdot \frac{2^{60} - 1}{3}$$

$4^3 \equiv 1 \pmod{3}$ , so  $3 \mid 2^{60} - 1$ . Hence  $n-1$  is 4 times an integer, i.e., even.

$2^5 = 32 \equiv 1 \pmod{31}$  and  $60 = 5 \cdot 12$ , so  $31 \mid 2^{60} - 1$ .  
 As  $\gcd(31, 3) = 1$ ,  $31 \mid \frac{2^{60}-1}{3}$ , i.e.,  $31 \mid n - 1$ .  
 $\gcd(2, 31) = 1$ , so  $62 \mid n - 1$ . Putting  $n - 1 = 62k$ ,  
 $2^{n-1} = (2^{62})^k \equiv 1 \pmod{n}$ .

ANSWER 1

## 3.9 THE CHINESE REMAINDER THEOREM

## THEOREM · CHINESE REMAINDER THEOREM

If  $m_1, \dots, m_k$  are pairwise coprime, the system  
 $x \equiv a_i \pmod{m_i}$  has exactly one solution modulo  
 $m_1 m_2 \cdots m_k$ .

- (i) **Solve by listing:** list the numbers satisfying the largest modulus and take the first that fits the rest.
- (ii) **Use it in reverse:** to find  $N \pmod{100}$ , find  $N \pmod{4}$  and  $N \pmod{25}$  separately and combine them.
- (iii) For moduli that are not coprime, the system is solvable exactly when  $a_1 \equiv a_2 \pmod{\gcd(m_1, m_2)}$ , and then the solution is unique modulo the lcm.

The grid shows why the theorem holds for 3 and 4: the twelve numbers  $0, \dots, 11$  fill the twelve cells of remainder pairs exactly once each.

|              |   | $x \pmod{4}$ |   |    |    |
|--------------|---|--------------|---|----|----|
|              |   | 0            | 1 | 2  | 3  |
| $x \pmod{3}$ | 0 | 0            | 9 | 6  | 3  |
|              | 1 | 4            | 1 | 10 | 7  |
|              | 2 | 8            | 5 | 2  | 11 |

each of  $0, \dots, 11$  fills one cell;  $x \equiv$

$2 \pmod{3}$ ,  $x \equiv 3 \pmod{4}$  gives  $x \equiv 11 \pmod{12}$

## EXAMPLE 3.9

Find the smallest positive  $x$  with  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$  and  $x \equiv 2 \pmod{7}$ .

Taking the largest modulus first (Section 3.9), we test the numbers  $\equiv 2 \pmod{7}$  modulo 5 and 3:

| $x$ | $x \pmod{5}$ | $x \pmod{3}$ |
|-----|--------------|--------------|
| 2   | 2            | 2            |
| 9   | 4            | 0            |
| 16  | 1            | 1            |
| 23  | 3            | 2            |

23 is the first with remainders 3 and 2.

3, 5, 7 are pairwise coprime, so by the Chinese remainder theorem all solutions are  $23 + 105t$ . The smallest positive one is 23.

ANSWER 23

## 3.10 LAST DIGITS AND LAST TWO DIGITS

The last digit of a power cycles with period dividing 4.

| LAST DIGIT OF $a$ | LAST DIGITS OF $a, a^2, a^3, \dots$ |
|-------------------|-------------------------------------|
| 2                 | 2, 4, 8, 6                          |
| 3                 | 3, 9, 7, 1                          |
| 7                 | 7, 9, 3, 1                          |
| 8                 | 8, 4, 2, 6                          |
| 4, 9              | 4, 6 and 9, 1                       |
| 0, 1, 5, 6        | constant                            |

For the last two digits work modulo 4 and modulo 25 and combine by the Chinese remainder theorem. When  $\gcd(a, 10) = 1$ ,  $a^{20} \equiv 1 \pmod{100}$ .

## EXAMPLE 3.10

Find the last two digits of  $2^{2026}$ .

$\gcd(2, 100) \neq 1$ , so Euler's theorem cannot be used modulo 100. We work modulo 4 and modulo 25 instead.

Modulo 4:  $2^{2026} = 4 \cdot 2^{2024} \equiv 0$ .

Modulo 25:  $\gcd(2, 25) = 1$  and  $\phi(25) = 20$ , so by Euler's theorem  $2^{20} \equiv 1$ . As  $2026 = 20 \cdot 101 + 6$ ,

$$2^{2026} = (2^{20})^{101} \cdot 2^6 \equiv 64 \equiv 14$$

Combining by the Chinese remainder theorem ( $\gcd(4, 25) = 1$ ), we test the numbers below 100 that are  $\equiv 14 \pmod{25}$ :

|              |    |    |    |    |
|--------------|----|----|----|----|
| $x$          | 14 | 39 | 64 | 89 |
| $x \pmod{4}$ | 2  | 3  | 0  | 1  |

Only 64 is  $\equiv 0 \pmod{4}$ .

ANSWER 64

#### WHERE MARKS GO · REMAINDER ZERO IN A CYCLE

For  $n \geq 1$ , reduce  $n$  modulo the cycle length; a remainder of 0 means the **last** entry of the cycle, not the first.  $3^4$  ends in 1, not in 3.

### EXERCISES 3

3.1 Find the remainder when  $5^{100}$  is divided by 13.

3.2 Find the last digit of  $7^{2026}$ .

3.3 Find the last two digits of  $3^{2026}$ .

3.4 Find the remainder when  $2^{2026}$  is divided by 7.

3.5 Find the smallest positive integer that leaves remainders 3, 4, 5 on division by 4, 5, 6 respectively.

3.6 How many  $x$  in  $0, 1, \dots, 59$  satisfy  $x^2 \equiv 1 \pmod{60}$ ?

3.7 Find  $\varphi(360)$ .

3.8 Find the remainder when  $1! + 2! + 3! + \dots + 100!$  is divided by 12.

3.9 Find the remainder when  $10!$  is divided by 11.

3.10 Find the smallest positive integer  $n$  with  $2^n \equiv 1 \pmod{31}$ .

3.11 How many integers  $n$  with  $1 \leq n \leq 100$  make  $n^2 + 1$  a multiple of 5?

3.12 Find the remainder when  $2^{100} + 3^{100}$  is divided by 5.

3.13 Find the remainder when 123456789 is divided by 11.

## CHAPTER 04 DIGITS, SQUARES AND DIOPHANTINE METHODS

This chapter covers the methods that IOQM uses most often: the exponent of a prime in a factorial, the decimal digits of a number, the floor function in counting, perfect squares, sums of two squares and Pythagorean triples, and three methods for equations in integers when factorising does not work: bounding, congruences and descent. Five of the ten number theory questions of IOQM 2026 are solved here.

### 4.1 LEGENDRE'S FORMULA

How many times does a prime  $p$  divide  $n!$ ? For example,  $10!$  is divisible by  $2^8$  but not by  $2^9$ . Legendre's formula gives this exponent without multiplying anything out. First, a name for the exponent.

#### DEFINITION · EXPONENT OF A PRIME

For a prime  $p$  and an integer  $N \neq 0$ ,  $v_p(N)$  is the exponent of  $p$  in  $N$ :  $p^{v_p(N)} \mid N$  but  $p^{v_p(N)+1} \nmid N$ . Then

$$v_p(ab) = v_p(a) + v_p(b),$$

and if  $v_p(a) \neq v_p(b)$ , then  $v_p(a + b) = \min(v_p(a), v_p(b))$ .

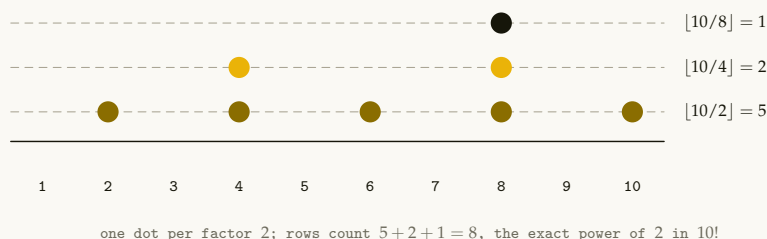
#### THEOREM · LEGENDRE

For a prime  $p$  and an integer  $n \geq 1$ ,

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

The sum stops at the first  $p^k > n$ .

Among  $1, 2, \dots, n$  there are  $\lfloor n/p \rfloor$  multiples of  $p$ , and each gives one factor  $p$ . The multiples of  $p^2$  give a second factor, and there are  $\lfloor n/p^2 \rfloor$  of them; and so on. A number divisible by exactly  $p^k$  is counted once in each of the first  $k$  terms, so  $k$  times in all, which is exactly its share of  $v_p(n!)$ .



Three applications are used often.

- (i) **Zeros at the end.**  $n!$  ends in  $v_5(n!)$  zeros, because  $v_2(n!) \geq v_5(n!)$ . So  $100!$  ends in  $20 + 4 = 24$  zeros.
- (ii) **Composite bases.** As  $12 = 2^2 \cdot 3$ , the largest power of 12 dividing  $n!$  is  $\min(\lfloor v_2(n!)/2 \rfloor, v_3(n!))$ .
- (iii) **Consecutive integers.**  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$  is an integer, so a product of  $k$  consecutive integers is a multiple of  $k!$ .

A quicker form, using the digits of  $n$  in base  $p$  (section 4.9):  $v_p(n!) = \frac{n - s_p(n)}{p-1}$ , where  $s_p(n)$  is the digit sum. For example  $100 = (1100100)_2$  has three 1s, so  $v_2(100!) = 100 - 3 = 97$ , the same as  $50 + 25 + 12 + 6 + 3 + 1$ .

#### EXAMPLE 4.1

Find the largest integer  $n$  for which  $12^n$  divides  $50!$ .

$12^n = 2^{2n} \cdot 3^n$ . By Legendre's formula,

$$v_2(50!) = 25 + 12 + 6 + 3 + 1 = 47$$

(multiples of 2, 4, 8, 16, 32 up to 50) and

$$v_3(50!) = 16 + 5 + 1 = 22$$

(multiples of 3, 9, 27 up to 50). So  $12^n \mid 50!$  exactly when  $2n \leq 47$  and  $n \leq 22$ , i.e.,  $n \leq 23$  and  $n \leq 22$ , so  $n \leq 22$ .

**ANSWER**  $n = 22$

## 4.2 DIGITS AND PLACE VALUE

A number written in digits is a polynomial in 10:

$$\overline{a_k a_{k-1} \dots a_1 a_0} = a_k 10^k + \dots + 10a_1 + a_0,$$

with every  $a_i \in \{0, 1, \dots, 9\}$  and the leading digit  $a_k \neq 0$ . Writing the number this way is the first step in every digit problem, and the conditions on the digits then complete the solution.

- (i)  $\overline{ab} + \overline{ba} = 11(a+b)$  and  $\overline{ab} - \overline{ba} = 9(a-b)$ .

- (ii)  $\overline{abc} - \overline{cba} = 99(a-c)$ .

- (iii) A  $k$ -digit number with every digit  $a$  is  $a \cdot \frac{10^k - 1}{9}$ .

- (iv)  $N$  has exactly  $k$  digits when  $10^{k-1} \leq N < 10^k$ .

#### KEY IDEA · MOVING A DIGIT

Write  $M = d \cdot 10^k + m$  with  $0 \leq m < 10^k$ , where  $d$  is the leading digit. Moving  $d$  to the units place gives  $10m + d$ . Both numbers now have the same unknown  $m$ .

#### EXAMPLE 4.2

Let  $A$  be a three-digit number with distinct non-zero digits, and let  $B$  be the number obtained by reversing the digits of  $A$ . Find the largest possible prime factor of  $|A - B|$ . (IOQM 2026, Q14)

For  $A = 213$ :  $B = 312$  and

$$|A - B| = 99 = 3^2 \cdot 11$$

In general,  $A = 100a + 10b + c$  and  $B = 100c + 10b + a$ . On subtracting (the tens digits cancel),

$$A - B = 99a - 99c = 99(a - c)$$

$$|A - B| = 3^2 \cdot 11 \cdot |a - c|$$

$a \neq c$  and  $a, c \in \{1, \dots, 9\}$ , so  $1 \leq |a - c| \leq 8$ . A number from 1 to 8 has no prime factor above 7. Hence the largest prime factor of  $|A - B|$  is always 11.

**ANSWER** 11

#### EXAMPLE 4.3

$M$  is the smallest positive integer whose leading digit is 3 and such that moving this 3 to the units place gives the number  $M/4$ . Find the sum of the digits of  $M$ . (IOQM 2026, Q20)

Let  $M$  have  $k+1$  digits and let  $m$  be the number formed by the digits after the leading 3 (key idea above):

$$M = 3 \cdot 10^k + m, \quad 0 \leq m < 10^k$$

Moving the 3 to the units place gives  $10m + 3 = M/4$ , so

$$4(10m + 3) = 3 \cdot 10^k + m$$

$$39m = 3 \cdot 10^k - 12$$

$$13m = 10^k - 4$$

$\therefore 10^k \equiv 4 \pmod{13}$ . Each remainder is 10 times the one before, reduced modulo 13:

|                  |    |   |    |   |   |
|------------------|----|---|----|---|---|
| $k$              | 1  | 2 | 3  | 4 | 5 |
| $10^k \pmod{13}$ | 10 | 9 | 12 | 3 | 4 |

Fewer digits give a smaller  $M$ , so we take the least  $k$ , i.e.,  $k = 5$ :

$$m = \frac{99996}{13} = 7692, \quad M = 307692$$

Check: moving the 3 gives  $076923 = 76923$ , and  $4 \cdot 76923 = 307692$ .

Digit sum  $= 3 + 0 + 7 + 6 + 9 + 2 = 27$ .

ANSWER 27

#### 4.3 DIGIT SUMS

Write  $S(n)$  for the sum of the digits of  $n$ .

## RULES · DIGIT SUMS

$$S(n) \equiv n \pmod{9}, \text{ so } 9 \mid n - S(n).$$

$S(a+b) = S(a) + S(b) - 9c$ , where  $c$  is the number of carries in the addition  $a+b$ .

The first rule is the test for 9 from section 1.3. For the second, each carry replaces 10 in one place by 1 in the next place, which lowers the total of the digits by 9. So  $S(a+b) \leq S(a) + S(b)$ , with equality exactly when there is no carry.

**Smallest number with a given digit sum.** A number with  $k$  digits has digit sum at most  $9k$ . So the smallest number with digit sum  $s$  has  $\lceil s/9 \rceil$  digits, the smallest possible leading digit, and 9 in every other place. For example, the smallest number with digit sum 30 is 3999.

#### EXAMPLE 4.4

Let  $N$  be the smallest positive integer whose digits add up to 2026. What is the leading digit of  $N+1$ ? (IOQM 2026, Q9)

For digit sum 10: the smallest number is 19, and  $19+1=20$ .

For digit sum 2026: a  $k$ -digit number has digit sum at most  $9k$ , and

$$9 \cdot 225 = 2025 < 2026$$

So  $N$  has at least 226 digits, and exactly 226, as fewer digits give a smaller number.

A smaller leading digit gives a smaller number, so we take 1. The other 225 digits then add up to  $2025 = 9 \cdot 225$ , so all of them are 9:

$$N = \underbrace{199 \dots 9}_{225}$$

On adding 1, every 9 becomes 0 and the leading 1 becomes 2:

$$N+1 = \underbrace{200 \dots 0}_{225}$$

ANSWER 2

#### EXAMPLE 4.5

The digits of a positive integer  $n$  strictly increase from left to right. Find the sum of the digits of  $9n$ . (Russia 1999)

For  $n = 1357$ :  $9n = 10n - n$ ,

$$\begin{array}{r} 13570 \\ - 1357 \\ \hline 12213 \end{array}$$

and the digit sum of 12213 is  $1+2+2+1+3=9$ .

In general, let  $n = \overline{a_1 a_2 \dots a_k}$  with  $k \geq 2$  and  $a_1 < a_2 < \dots < a_k$ . On subtracting  $n$  from  $10n$  place by place,

| place   | digit of $9n$       |
|---------|---------------------|
| units   | $10 - a_k$          |
| tens    | $a_k - a_{k-1} - 1$ |
| higher  | $a_{i+1} - a_i$     |
| leading | $a_1$               |

The units place needs a borrow, as  $0 < a_k$ . The tens digit is  $a_k - a_{k-1} - 1 \geq 0$ , as  $a_k > a_{k-1}$ , and each

higher digit  $a_{i+1} - a_i$  is positive, so no other borrow is needed.

On adding the column (the  $a_i$  cancel in pairs),

$$S(9n) = a_1 + (a_2 - a_1) + \cdots + (a_k - a_{k-1}) - 1 + (10 - a_k) = 9$$

For a one-digit  $n$ ,  $9n = 10a_1 - a_1$  has digits  $a_1 - 1$  and  $10 - a_1$ , sum 9 again.

ANSWER 9

#### 4.4 THE FLOOR FUNCTION IN COUNTING

##### DEFINITION · FLOOR

$\lfloor x \rfloor$  is the greatest integer not exceeding  $x$ , and  $\{x\} = x - \lfloor x \rfloor$ , so  $0 \leq \{x\} < 1$ . For an integer  $n$ ,

$$\lfloor x \rfloor = n \iff n \leq x < n + 1.$$

- (i) The multiples of  $k$  in  $1, \dots, n$  number  $\lfloor n/k \rfloor$ ; in  $a, \dots, b$  they number  $\lfloor b/k \rfloor - \lfloor (a-1)/k \rfloor$ .
- (ii) With inclusion and exclusion: the integers from 1 to 100 divisible by 2, 3 or 5 number  $50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$ .
- (iii)  $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$  for every positive integer  $n$ .
- (iv) **Hermite:**  $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = \lfloor 2x \rfloor$ .
- (v)  $\tau(1) + \tau(2) + \cdots + \tau(n) = \sum_{k=1}^n \lfloor n/k \rfloor$ , since both sides count the pairs  $(k, m)$  of positive integers with  $km \leq n$ .

##### KEY IDEA · FLOORS IN AN EQUATION

First estimate the value of each floor term. On the interval where these values do not change, the equation becomes an ordinary equation.

##### EXAMPLE 4.6

A positive integer  $n$  satisfies  $n + \lfloor \sqrt{n} \rfloor + \lfloor \sqrt[4]{n} \rfloor = 2017$ . Find  $2017 - n$ . (CMIMC 2017)

First we estimate the floor terms (key idea above). They are at least 1, so  $n < 2017 < 2025 = 45^2$ , i.e.,  $\lfloor \sqrt{n} \rfloor \leq 44$ . Also  $n < 2017 < 2401 = 7^4$ , so  $\lfloor \sqrt[4]{n} \rfloor \leq 6$ .  $\therefore$  the floor terms add up to at most 50, and

$$n \geq 2017 - 44 - 6 = 1967$$

For  $1967 \leq n < 2017$ ,

$$44^2 = 1936 \leq n < 45^2$$

$$6^4 = 1296 \leq n < 7^4$$

So  $\lfloor \sqrt{n} \rfloor = 44$  and  $\lfloor \sqrt[4]{n} \rfloor = 6$ , and the equation becomes

$$n + 44 + 6 = 2017, \quad n = 1967$$

ANSWER 2017 - n = 50

#### 4.5 PERFECT SQUARES

- (i) A square ends in 0, 1, 4, 5, 6 or 9, and a square ending in 5 ends in 25.
- (ii) Squares leave remainder 0 or 1 on division by 3 and by 4, and 0, 1 or 4 on division by 8 (table in section 3.4).
- (iii)  $1, 2, \dots, N$  contains  $\lfloor \sqrt{N} \rfloor$  squares.
- (iv)  $n(n+1)(n+2)(n+3) + 1 = (n^2 + 3n + 1)^2$ .

##### KEY IDEA · BETWEEN CONSECUTIVE SQUARES

If  $m^2 < N < (m+1)^2$  for an integer  $m$ , then  $N$  is not a perfect square.

For “find all  $n$  for which this expression is a square”, put the expression between two consecutive squares for all large  $n$ , then check the few small  $n$  left over. The other method is factorising:  $N = k^2$  with  $N = m^2 - c$  becomes  $(m-k)(m+k) = c$ , a divisor list.

##### EXAMPLE 4.7

Find all positive integers  $n$  for which  $n^4 + n^3 + n^2 + n + 1$  is a perfect square.

Let  $N = n^4 + n^3 + n^2 + n + 1$ . For small  $n$ :

|     |   |    |     |
|-----|---|----|-----|
| $n$ | 1 | 2  | 3   |
| $N$ | 5 | 31 | 121 |

Only  $121 = 11^2$  is a square. Now let  $n \geq 4$ .

$N$  is a square exactly when  $4N$  is, since  $4 = 2^2$ . As  $(2n^2 + n)^2 = 4n^4 + 4n^3 + n^2$ ,

$$4N = (2n^2 + n)^2 + 3n^2 + 4n + 4$$

and the extra part is positive. For the next square,

$$(2n^2 + n + 1)^2 = 4N + (n-3)(n+1)$$

and for  $n \geq 4$  the last term is positive. So

$$(2n^2 + n)^2 < 4N < (2n^2 + n + 1)^2$$

By the key idea in Section 4.5,  $4N$  is not a square, so no  $n \geq 4$  works.

ANSWER  $n = 3$

#### EXAMPLE 4.8

Find all non-negative integers  $m, n$  with  $3 \cdot 2^m + 1 = n^2$ . (New Zealand 2011)

For small  $m$ :

| $m$               | 0 | 1 | 2  | 3  | 4  | 5  |
|-------------------|---|---|----|----|----|----|
| $3 \cdot 2^m + 1$ | 4 | 7 | 13 | 25 | 49 | 97 |

The squares are 4, 25, 49, so  $m = 0, 3, 4$  give  $n = 2, 5, 7$ . The table covers  $m = 0$  and  $m = 1$ , so let  $m \geq 2$ . Then

$$(n-1)(n+1) = 3 \cdot 2^m$$

The right side is even, so  $n$  is odd. Putting  $n = 2u + 1$ ,

$$(n-1)(n+1) = 2u(2u+2) = 4u(u+1)$$

$$u(u+1) = 3 \cdot 2^{m-2}$$

One of  $u, u+1$  is odd, and an odd divisor of  $3 \cdot 2^{m-2}$  is 1 or 3.

If the odd one is 1, then  $u(u+1)$  is 0 or 2, but  $3 \cdot 2^{m-2} \geq 3$ . So the odd one is 3, i.e.,  $u+1 = 3$  or  $u = 3$ :

| $(u, u+1)$ | $u(u+1)$           | $(m, n)$ |
|------------|--------------------|----------|
| (2, 3)     | $6 = 3 \cdot 2^1$  | (3, 5)   |
| (3, 4)     | $12 = 3 \cdot 2^2$ | (4, 7)   |

ANSWER  $(m, n) = (0, 2), (3, 5), (4, 7)$

## 4.6 SUMS OF TWO SQUARES

### THEOREM · FERMAT, TWO SQUARES

An odd prime  $p$  is a sum of two squares exactly when  $p \equiv 1 \pmod{4}$ . A positive integer is a sum of two squares exactly when every prime  $\equiv 3 \pmod{4}$  divides it to an **even** power.

One half for primes is already in Chapter 3: squares leave 0 or 1 on division by 4, so a sum of two squares never leaves 3. The rest depends on two facts.

- (i) **Product identity:**  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$ . So a product of sums of two squares is again one:  $5 \cdot 13 = 65 = 1^2 + 8^2 = 4^2 + 7^2$ .
- (ii) If a prime  $q \equiv 3 \pmod{4}$  divides  $x^2 + y^2$ , then  $q$  divides both  $x$  and  $y$ . So  $q$  divides  $x^2 + y^2$  to an even power.

The proof that every prime  $p \equiv 1 \pmod{4}$  is a sum of two squares is beyond IOQM; only the statement is needed.

#### EXAMPLE 4.9

How many integers in the set  $\{0, 1, \dots, 20\}$  can be written as the sum of two squares of integers? (IOQM 2026, Q10)

The squares up to 20 are 0, 1, 4, 9, 16. Adding them in pairs (sums up to 20 only),

| + | 0 | 1 | 4 | 9  | 16 |
|---|---|---|---|----|----|
| 0 | 0 | 1 | 4 | 9  | 16 |
| 1 |   | 2 | 5 | 10 | 17 |
| 4 |   |   | 8 | 13 | 20 |
| 9 |   |   |   | 18 |    |

The different sums are

$$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20$$

i.e., 13 numbers.

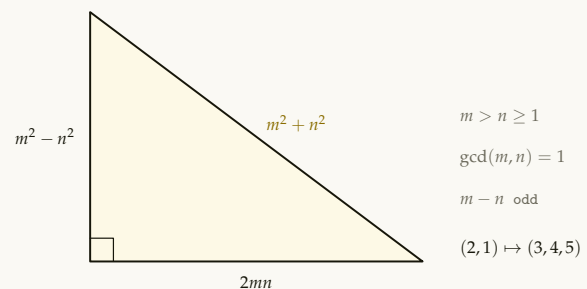
Check by Fermat's two-square theorem (Section 4.6): in  $1, \dots, 20$  the numbers with a prime  $\equiv 3 \pmod{4}$  to an odd power are

$$3, 6, 7, 11, 12, 14, 15, 19$$

That leaves  $21 - 8 = 13$ , counting  $0 = 0^2 + 0^2$ .

ANSWER 13

## 4.7 PYTHAGOREAN TRIPLES



## THEOREM · PRIMITIVE TRIPLES

Every solution of  $x^2 + y^2 = z^2$  in positive integers with  $\gcd(x, y, z) = 1$  is, with the legs possibly swapped,

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2,$$

where  $m > n \geq 1$ ,  $\gcd(m, n) = 1$  and  $m - n$  is odd.

Every triple is a multiple of a primitive one.

Why: in a primitive triple  $x$  and  $y$  are not both even, and not both odd either, since then  $z^2 \equiv 2 \pmod{4}$ . So one leg, say  $y$ , is even, and  $x, z$  are odd. Then

$$\left(\frac{y}{2}\right)^2 = \frac{z-x}{2} \cdot \frac{z+x}{2},$$

and the two factors on the right are coprime, because a common divisor divides their sum  $z$  and their difference  $x$ , and  $\gcd(x, z) = 1$ . So each is a perfect square,  $n^2$  and  $m^2$ , which gives the formula.

- (i) In a primitive triple the hypotenuse is odd and exactly one leg is even.
- (ii) In every triple one leg is a multiple of 3, one leg a multiple of 4, and one side a multiple of 5. So 12 divides the product of the legs and 60 divides  $xyz$ .
- (iii)  $(m, n) = (2, 1), (3, 2), (4, 1), (4, 3)$  give  $(3, 4, 5), (5, 12, 13), (15, 8, 17), (7, 24, 25)$ .
- (iv) With one leg  $x$  given:  $x^2 = (z - y)(z + y)$ , two factors of the same parity.

## EXAMPLE 4.10

How many right-angled triangles with integer sides have a leg of length 15?

Let the other leg be  $y$  and the hypotenuse  $z$ . Then

$$(z - y)(z + y) = z^2 - y^2 = 15^2 = 225$$

Both factors are odd, as 225 is odd. So  $z$  (half their sum) and  $y$  (half their difference) are whole numbers.

Factor pairs of 225, smaller factor first, as  $z - y < z + y$ :

| $z - y$ | $z + y$ | $y$ | $z$ |
|---------|---------|-----|-----|
| 1       | 225     | 112 | 113 |
| 3       | 75      | 36  | 39  |
| 5       | 45      | 20  | 25  |
| 9       | 25      | 8   | 17  |

The pair  $15 \cdot 15$  gives  $y = 0$ , so it is left out.

ANSWER 4 triangles

## 4.8 BOUNDING, PARITY AND DESCENT

When factorising does not solve an equation in integers, one of the following three methods usually does.

- (i) **Bound.** Order the variables and bound the smallest one. For  $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$  with  $x \leq y \leq z$ :  $1 \leq \frac{3}{x}$ , so  $x \leq 3$ , and each value of  $x$  leaves an equation in two unknowns.
- (ii) **Congruences.** Reduce both sides modulo a well-chosen  $m$  (section 3.4) and show the remainders cannot match, or use them to fix a variable.
- (iii) **Infinite descent.** Show that every solution gives a strictly smaller one. Positive integers cannot decrease for ever, so there is no solution.

For example, take  $x^2 + y^2 = 3z^2$  in non-negative integers. Squares are 0 or 1 modulo 3, so  $x^2 + y^2 \equiv 0$  gives  $3 \mid x$  and  $3 \mid y$ . Then  $9 \mid 3z^2$ , so  $3 \mid z$ , and  $(x/3, y/3, z/3)$  is again a solution. If  $z > 0$ , repeating this makes  $z$  decrease for ever, which is not possible. So  $z = 0$ , then  $x = y = 0$ , and  $(0, 0, 0)$  is the only solution.

## KEY IDEA · BOUND FIRST, THEN CHECK

A bound reduces a “find all” question to a finite number of cases. A suitable congruence often shows in one line that there is no solution.

## EXAMPLE 4.11

Positive integers  $a, b, c, d$  satisfy  $a^2 + b^2 - cd^2 = 2026$ . Find the minimum possible value of  $a + b + c + d$ . (IOQM 2026, Q15)

Let  $s = a + b$ . We have

$$a^2 + b^2 = 2026 + cd^2 \geq 2027$$

**At least 51.** For a fixed  $s$ ,  $a^2 + b^2$  is largest when  $a$  or  $b$  is 1:

$$a^2 + b^2 = s^2 - 2ab \leq (s - 1)^2 + 1$$

as  $ab - (s - 1) = (a - 1)(b - 1) \geq 0$ . For  $s \leq 46$  this is at most  $45^2 + 1 = 2026 < 2027$ , which is not possible. So  $s \geq 47$ , and with  $c + d \geq 2$ ,

$$a + b + c + d \geq 49$$

Also  $a^2 + b^2$  and  $s$  have the same parity, as  $a^2 - a$  and  $b^2 - b$  are even.

All cases with  $a + b + c + d = 49$  or  $50$  ( $s \geq 47$ ,  $c, d \geq 1$ ):

| total | $s$ | $(c, d)$ | $a^2 + b^2$ |
|-------|-----|----------|-------------|
| 49    | 47  | (1, 1)   | 2027        |
| 50    | 48  | (1, 1)   | 2027        |
| 50    | 47  | (2, 1)   | 2028        |
| 50    | 47  | (1, 2)   | 2030        |

Row 1:  $2ab = 47^2 - 2027 = 182$ , so  $ab = 91$ . But  $91 = 1 \cdot 91 = 7 \cdot 13$ , and neither pair adds up to 47.

Rows 2 to 4:  $a^2 + b^2$  and  $s$  have different parity, which is not possible.

Hence  $a + b + c + d \geq 51$ .

**Example with 51.**  $a = 2, b = 45, c = 3, d = 1$ :

$$4 + 2025 - 3 = 2026$$

ANSWER 51

#### 4.9 OTHER BASES

##### DEFINITION · BASE $b$

For an integer  $b \geq 2$ , every positive integer  $n$  can be written in exactly one way as

$$n = a_k b^k + \cdots + a_1 b + a_0,$$

with  $0 \leq a_i \leq b - 1$  and  $a_k \neq 0$ , written  $n = (a_k \cdots a_1 a_0)_b$ .

The digits come from repeated division:  $a_0$  is the remainder of  $n$  on division by  $b$ ,  $a_1$  the remainder of the quotient, and so on.

- (i)  $n$  has exactly  $k$  digits in base  $b$  when  $b^{k-1} \leq n < b^k$ .
- (ii)  $n \equiv$  (its digit sum) modulo  $b - 1$ , and  $n \equiv$  (its alternating digit sum) modulo  $b + 1$ : the tests of section 1.3 with 10 replaced by  $b$ .
- (iii) **Base 2:** every positive integer is a sum of *distinct* powers of 2 in exactly one way.

##### EXAMPLE 4.12

Find all positive integers  $x, y, z$  with  $2^x + 2^y + 2^z = 2336$ . (Vietnam 1982)

Writing 2336 in base 2 (taking away the largest power of 2 each time),

$$2336 - 2048 = 288, \quad 288 - 256 = 32$$

So

$$2336 = 2^{11} + 2^8 + 2^5 = (100100100000)_2$$

If two of  $x, y, z$  are equal, say  $x = y$ , then

$$2^x + 2^y + 2^z = 2^{x+1} + 2^z$$

which has at most two 1s in base 2, but 2336 has three. So  $x, y, z$  are different.

Hence  $2^x + 2^y + 2^z$  is a sum of distinct powers of 2. By the base-2 fact in Section 4.9 this form is unique, so  $\{x, y, z\} = \{5, 8, 11\}$ .

ANSWER  $\{x, y, z\} = \{5, 8, 11\}$ , in any order

#### EXERCISES 4

- 4.1 Find the number of zeros at the end of  $2026!$ .
- 4.2 Find the largest integer  $k$  for which  $6^k$  divides  $100!$ .
- 4.3 Find the number of ordered triples  $(a, b, c)$  of positive integers with  $a! \cdot b! \cdot c! = 10!$ . (South Africa 2014)
- 4.4 Find the three-digit number  $n$  for which  $S(n) + 3n = 2020$ , where  $S(n)$  is the sum of the digits of  $n$ .
- 4.5 Writing the integers  $1, 2, \dots, 50$  one after another gives the number  $N = 1234 \cdots 4950$ . Find the remainder when  $N$  is divided by 9.
- 4.6 The smallest positive multiple of 225 whose digits are all 0 or 1 has how many digits?
- 4.7 How many integers from 1 to 1000 are divisible by none of 2, 3, 5?
- 4.8 Find the sum of all positive integers  $n$  for which  $n^2 - 19n + 99$  is a perfect square.
- 4.9 For how many positive integers  $n$  is  $n^2 + 2n + 2026$  a perfect square?
- 4.10 How many of the integers  $1, 2, \dots, 50$  are sums of two squares of integers? (0 is allowed as a square.)

4.11 How many right-angled triangles with integer sides have hypotenuse 65?

4.12 Find the largest integer that divides  $xyz$  for every triple of positive integers with  $x^2 + y^2 = z^2$ .

4.13 How many positive integers have the same number of digits in base 3 as in base 5? (ARML 2006)

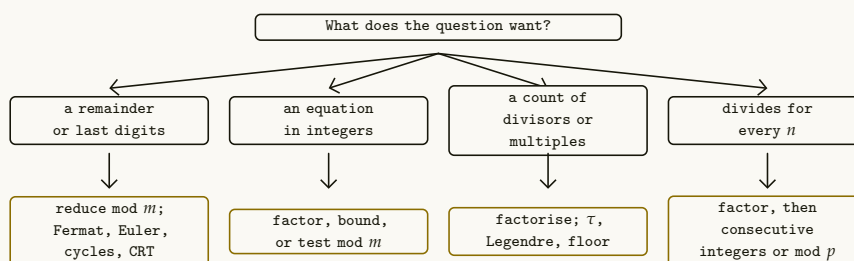
4.14 How many triples  $(x, y, z)$  of positive integers with  $x \leq y \leq z$  satisfy  $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$ ?

## CHAPTER 05 PROBLEM SOLVING IN NUMBER THEORY

Chapters 1 to 4 developed the methods of number theory. A question in the paper does not say which method to use: it asks for a remainder, or the solutions of an equation, or a count, and the first step is to decide which method suits it. This chapter helps with that choice. It has a table matching question types to methods, a list of standard results to remember, two further techniques (primes in equations and periodic

remainders), the ten number theory questions of IOQM 2026 with the examples that solve them, a list of common mistakes, and a mixed problem set in which, as in the paper, the chapter is not given.

### 5.1 CHOOSING THE METHOD



| THE QUESTION ASKS FOR    | METHOD TO TRY FIRST                                                                | SECTION       |
|--------------------------|------------------------------------------------------------------------------------|---------------|
| a remainder, last digits | reduce the base, find the cycle, combine the moduli                                | 3.1, 3.8, 3.9 |
| an equation in integers  | factorise, bound, or reduce modulo a well-chosen $m$                               | 2.7, 4.8, 3.4 |
| a count                  | factorise, then $\tau$ , Legendre's formula, or floor with inclusion and exclusion | 1.6, 4.1, 4.4 |
| "divides for every $n$ " | factor into consecutive integers, or test each prime power                         | 1.7, 1.8      |
| digits                   | place value, digit sum modulo 9                                                    | 4.2, 4.3      |
| primes in an equation    | test 2 and 3, then parity and remainders modulo 3                                  | 5.3           |
| a perfect square         | put it between consecutive squares, or use a difference of squares                 | 4.5           |

#### KEY IDEA · TRY SMALL CASES

Work out the first few cases by hand before choosing a method. Remainders that repeat are a period (section 5.4); answers that follow a pattern are a guess to be proved.

$x$ , and Legendre's formula then gives two different values of  $y$ .

Some questions need two methods together. In the next example a congruence shows that 3 and 7 divide

**EXAMPLE 5.1**

Find all pairs  $(x, y)$  of positive integers with  $x^{2008} + 2008! = 21^y$ . (Iberoamerican 2008)

$21^y = 3^y \cdot 7^y$ , so the left side must also have 3 and 7 to the same power  $y$ .

$3 \mid 2008!$  and  $3 \mid 21^y$ , so 3 divides

$$x^{2008} = 21^y - 2008!$$

$\therefore 3 \mid x$  (Euclid's lemma, Section 1.5). Similarly,  $7 \mid x$ .

By Legendre's formula (Section 4.1),

$$v_3(2008!) = 669 + 223 + 74 + 24 + 8 + 2 = 1000$$

$$v_7(2008!) = 286 + 40 + 5 = 331$$

As  $3 \mid x$ ,

$$v_3(x^{2008}) \geq 2008 > 1000$$

and hence

$$v_3(x^{2008} + 2008!) = 1000, \text{ so } y = 1000$$

(the sum of two numbers with different powers of 3 has the smaller power, Section 4.1; for example  $v_3(81 + 18) = v_3(99) = 2$ ).

Similarly,  $v_7(x^{2008}) \geq 2008 > 331$  gives  $y = 331$ .

But  $y$  cannot be both 1000 and 331. Hence there is no such pair.

**ANSWER** no solutions

**5.2 STANDARD RESULTS TO REMEMBER**

Each of these has been proved in this part. Learn them well enough to use them directly.

- (i) A product of  $k$  consecutive integers is a multiple of  $k!$ . 4.1
- (ii)  $6 \mid n^3 - n$  and  $30 \mid n^5 - n$  for every integer  $n$ . 1.8
- (iii)  $24 \mid p^2 - 1$  for every prime  $p > 3$ , and  $8 \mid m^2 - 1$  for every odd  $m$ . 1.7
- (iv)  $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1$ . 2.4
- (v)  $n = x^2 - y^2$  has a solution exactly when  $n \not\equiv 2 \pmod{4}$ . 1.8
- (vi)  $1001 = 7 \cdot 11 \cdot 13$  and  $10^6 - 1 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$ .
- (vii)  $\tau(n)$  is odd exactly when  $n$  is a perfect square. 1.6
- (viii) For coprime  $a, b \geq 2$ ,  $ab - a - b$  is the largest number not of the form  $ax + by$  with  $x, y \geq 0$ . 2.6
- (ix) For a prime  $p$ :  $a^p \equiv a$  and  $(p-1)! \equiv -1$

$(\text{mod } p)$ . 3.5, 3.7

(x) Squares are  $0, 1 \pmod{3}$ ,  $0, 1 \pmod{4}$  and  $0, 1, 4 \pmod{8}$ . 3.4

(xi)  $n!$  ends in  $v_5(n!)$  zeros. 4.1

**5.3 PRIMES IN EQUATIONS**

When the unknowns are primes, two simple facts are used in most questions.

**KEY IDEA · TEST 2 AND 3 FIRST**

2 is the only even prime and 3 is the only prime divisible by 3. Check  $p = 2$  and  $p = 3$  by hand; every other prime is odd and leaves remainder 1 or 2 on division by 3.

- (i) If a sum or difference of two primes is odd, one of them is 2.
- (ii) Among  $p, p+2, p+4$  one is a multiple of 3, so all three are prime only for  $p = 3$ . The same works for any three numbers that cover the three remainders modulo 3.
- (iii) A product  $ab$  of positive integers is prime only if one factor is 1. So factorise first:  $p^2 + 2p - 8 = (p+4)(p-2)$  is prime only for  $p = 3$ .
- (iv) For  $p > 3$ :  $p^2 \equiv 1 \pmod{24}$ .

**EXAMPLE 5.2**

Find all primes  $p$  for which  $2p+1$  and  $4p+1$  are also prime. (Moldova 2002)

For  $p \leq 7$ :

| $p$ | $2p+1$ | $4p+1$ | all prime? |
|-----|--------|--------|------------|
| 2   | 5      | 9      | no         |
| 3   | 7      | 13     | yes        |
| 5   | 11     | 21     | no         |
| 7   | 15     | 29     | no         |

For  $p = 5$  and  $7$  the composite one, 21 or 15, is a multiple of 3.

A prime  $p > 3$  is not a multiple of 3, so  $p \equiv 1$  or  $2 \pmod{3}$ . Modulo 3,

$$p \equiv 1 \Rightarrow 2p+1 \equiv 3 \equiv 0$$

$$p \equiv 2 \Rightarrow 4p+1 \equiv 9 \equiv 0$$

So one of  $2p+1, 4p+1$  is a multiple of 3 greater than 3, hence not prime.

**ANSWER**  $p = 3$ **EXAMPLE 5.3**

Find all triples  $(p, q, r)$  of primes with  $pq = r + 1$  and  $2(p^2 + q^2) = r^2 + 1$ . (RMO 2013)

If  $p, q$  are both odd, then  $pq$  is odd, so  $r = pq - 1$  is even and prime, so  $r = 2$ . Then  $pq = 3$ , which is not a product of two primes. So  $p = 2$  or  $q = 2$ .

The equations are unchanged when  $p$  and  $q$  are swapped, so let  $p = 2$ ; the swap gives the second triple.

From  $pq = r + 1$ ,  $r = 2q - 1$ . Substituting in the second equation,

$$2(4 + q^2) = (2q - 1)^2 + 1$$

$$8 + 2q^2 = 4q^2 - 4q + 2$$

$$q^2 - 2q - 3 = 0$$

$\therefore (q - 3)(q + 1) = 0$ . As  $q > 0$ ,  $q = 3$  and  $r = 2 \cdot 3 - 1 = 5$ , a prime.

Check:  $2 \cdot 3 = 5 + 1$  and  $2(4 + 9) = 26 = 5^2 + 1$ .

**ANSWER**  $(2, 3, 5)$  and  $(3, 2, 5)$ **5.4 PERIODIC REMAINDERS**

If each term of a sequence is fixed by the one or two terms before it, its remainders modulo  $m$  can take only finitely many values, so a block of remainders must come back, and from there everything repeats. Powers repeat with period equal to the order (section 3.8). Two periodic quantities with periods  $r$  and  $s$  together repeat with period  $\text{lcm}(r, s)$ .

**KEY IDEA · REMAINDERS, NOT NUMBERS**

The terms grow fast, but their remainders never exceed  $m - 1$ . Write out the remainders until a block repeats, then count within one period.

**EXAMPLE 5.4**

How many positive integers  $x \leq 225$  make  $2^x - x^2$  divisible by 7? (Moscow 1940)

We need  $x^2 \equiv 2^x \pmod{7}$ .  $2^3 = 8 \equiv 1 \pmod{7}$ , so the powers of 2 repeat with period 3 (Section 3.8):

$$2^1, 2^2, 2^3, \dots \equiv 2, 4, 1, 2, 4, 1, \dots$$

So  $2^x$  depends only on  $x \pmod{3}$ , and  $x^2$  only on  $x \pmod{7}$ .  $x \equiv 0 \pmod{7}$  gives  $x^2 \equiv 0$ , which no power of 2 equals. For the rest,

$$1^2, 2^2, \dots, 6^2 \equiv 1, 4, 2, 2, 4, 1$$

Matching the two lists,

| $x \pmod{3}$ | $2^x$ | $x \pmod{7}$ | $x \pmod{21}$ |
|--------------|-------|--------------|---------------|
| 0            | 1     | 1, 6         | 15, 6         |
| 1            | 2     | 3, 4         | 10, 4         |
| 2            | 4     | 2, 5         | 2, 5          |

(last column by the Chinese remainder theorem, Section 3.9; for example 15 is a multiple of 3 and  $15 = 14 + 1$ ). Check:  $x = 10$  gives  $2^{10} - 10^2 = 924 = 7 \cdot 132$ .

So exactly 6 numbers work in every block of 21 consecutive numbers.

$225 = 21 \cdot 10 + 15$ . The 10 full blocks give 60. The last 15 numbers, 211 to 225, leave the same remainders modulo 21 as 1 to 15, which contain all of 2, 4, 5, 6, 10, 15.

**ANSWER**  $60 + 6 = 66$ **EXAMPLE 5.5**

A sequence has  $S_1 = 1$ ,  $S_2 = 2$  and  $S_{n+2} = S_{n+1}^2 + S_n^2$ . How many of  $S_1, S_2, \dots, S_{100}$  are multiples of 5? (AIMO 2016)

We take remainders modulo 5 only (Section 5.4); each remainder is fixed by the two before it:

| $n$ | $S_n \pmod{5}$ | from             |
|-----|----------------|------------------|
| 1   | 1              |                  |
| 2   | 2              |                  |
| 3   | 0              | $2^2 + 1^2 = 5$  |
| 4   | 4              | $0^2 + 2^2 = 4$  |
| 5   | 1              | $4^2 + 0^2 = 16$ |
| 6   | 2              | $1^2 + 4^2 = 17$ |

At  $n = 5, 6$  the pair  $(1, 2)$  comes again, so the remainders repeat with period 4:

$$1, 2, 0, 4, 1, 2, 0, 4, \dots$$

So  $5 \mid S_n$  exactly when  $n \equiv 3 \pmod{4}$ , i.e.,

$$n = 3, 7, 11, \dots, 99$$

These are  $3 + 4k$  for  $k = 0, 1, \dots, 24$ .

ANSWER 25

### 5.5 IOQM 2026 NUMBER THEORY QUESTIONS

Ten of the thirty questions of IOQM 2026 were number theory, more than any other area, and each of them needs one section of this part followed by a short check of cases. The table below gives, for each of them, the example that solves it. Nine are solved in the earlier chapters; the tenth, Q28, is solved after the table.

| Q  | QUESTION AND METHOD                    | EXAMPLE |
|----|----------------------------------------|---------|
| 2  | remainders mod 256: division algorithm | 1.2     |
| 6  | digit equation: isolate a quotient     | 2.8     |
| 9  | digit sum 2026: digit sums             | 4.4     |
| 10 | two squares: sums of two squares       | 4.9     |
| 14 | digit reversal: place value            | 4.2     |
| 15 | a minimum: bound, then cases           | 4.11    |
| 20 | digit shift: $10^k \bmod 13$           | 4.3     |
| 25 | universal divisor: $6k \pm 1$          | 1.6     |
| 28 | recurrences: inverse mod 21            | 5.6     |
| 29 | power mod $n$ : order divides 62       | 3.8     |

#### EXAMPLE 5.6

Let  $a_1, a_2, \dots$  and  $b_1, b_2, \dots$  be strictly increasing sequences of positive integers with  $a_{n+1} = a_n + a_{n-1}$  for  $n \geq 2$ ,  $b_n = 2b_{n-1}$  for  $n \geq 2$ , and  $a_{10} = b_{10} < 2026$ . Find the sum of all possible values of  $a_1 + b_1$ . (IOQM 2026, Q28)

In terms of  $a_1$  and  $a_2$ ,

$$a_3 = a_1 + a_2, \quad a_4 = a_1 + 2a_2, \dots$$

Each coefficient is the sum of the two before it  $(1, 1, 2, 3, 5, 8, \dots)$ , so

$$a_{10} = 21a_1 + 34a_2, \quad b_{10} = 2^9 b_1 = 512b_1$$

$512b_1 < 2026$ , so  $b_1 \leq 3$ . The sequence  $a$  is increasing, so  $a_2 > a_1 \geq 1$ . Also  $21a_1 + 34a_2 = 512b_1$  with  $a_1 \geq 1$  gives  $34a_2 < 512b_1$ .

Modulo 21:  $34 \equiv 13$  and  $512 = 24 \cdot 21 + 8 \equiv 8$ , so

$$13a_2 \equiv 8b_1 \pmod{21}$$

$13 \cdot 13 = 169 \equiv 1$  (Example 3.2), so multiplying both sides by 13,

$$a_2 \equiv 104b_1 \equiv -b_1 \pmod{21}$$

( $104 = 105 - 1$  and  $105 = 5 \cdot 21$ ).

$b_1 = 1$ :  $a_2 \equiv 20$ , so  $a_2 \geq 20$ ; but  $34 \cdot 20 = 680 > 512$ , not possible.

$b_1 = 2$ :  $a_2 \equiv 19$ ;  $34a_2 < 1024$  gives  $a_2 \leq 30$ . So  $a_2 = 19$ .

$b_1 = 3$ :  $a_2 \equiv 18$ ;  $34a_2 < 1536$  gives  $a_2 \leq 45$ . So  $a_2 = 18$  or 39.

Now  $a_1 = (512b_1 - 34a_2)/21$ :

| $b_1$ | $512b_1$ | $a_2$ | $34a_2$ | $a_1$ | $a_1 < a_2?$ |
|-------|----------|-------|---------|-------|--------------|
| 2     | 1024     | 19    | 646     | 18    | yes          |
| 3     | 1536     | 18    | 612     | 44    | no           |
| 3     | 1536     | 39    | 1326    | 10    | yes          |

So  $a_1 + b_1$  is  $18 + 2 = 20$  or  $10 + 3 = 13$ .

ANSWER 20 + 13 = 33

### 5.6 COMMON MISTAKES

Students often lose marks on these points.

- (i) A remainder is never negative:  $-17$  leaves 3 on division by 5.
- (ii) 1 is not prime, and 2 is the only even prime.
- (iii) Euclid's lemma needs a prime:  $6 \mid 4 \cdot 9$ , but 6 divides neither factor.
- (iv)  $a \mid n$  and  $b \mid n$  give  $ab \mid n$  only when  $\gcd(a, b) = 1$ .
- (v) Cancel a factor modulo  $m$  only if it is coprime to  $m$ ; otherwise divide the modulus by the gcd.
- (vi) Exponents reduce modulo the order,  $p-1$  or  $\varphi(m)$ , and only for a base coprime to  $m$ ; never modulo  $m$  itself.
- (vii) In a cycle of length 4, remainder 0 means the

fourth entry.

- (viii)  $\gcd \cdot \text{lcm} = \text{product}$  holds for two numbers; for three it needs them pairwise coprime.
- (ix) In digit problems the leading digit is not 0, and every digit is at most 9.
- (x) After factorising an equation, include the negative divisor pairs, then apply the sign and range conditions.
- (xi) “Largest number dividing every value” needs a proof that it divides, and two values whose gcd is exactly that number.

### 5.7 A MIXED PROBLEM SET

The exercises below are not arranged by chapter, as in the actual paper. Before solving, decide from the table in section 5.1 which method the question needs. Answers with one-line hints are at the end of this part.

#### EXERCISES 5

- 5.1 Find all primes  $p$  for which  $p^2 + 2007p - 1$  is also prime. (*Berkeley Math Circle 2008*)
- 5.2 Primes  $p$  and  $q$  satisfy  $p + q = (p - q)^3$ . Find  $pq$ . (*Russia 2003*)
- 5.3 Primes  $p, q, r$  satisfy  $p(q - r) = q + r$ . Find  $p + q + r$ . (*Australian MO 2003*)
- 5.4 For primes  $p$  and  $q$  the equation  $x^2 + px + q = 0$  has an integer root. Find  $p + q$ . (*Czech and Slovak 2018*)
- 5.5 Find the sum of all primes of the form  $n^4 - 3n^2 + 9$ , where  $n$  is an integer. (*Czech and Slovak 2012*)
- 5.6 Find the least positive integer  $n$  for which  $10n + 1$  and  $10n + 9$  are prime but  $10n + 3$  and  $10n + 7$  are composite. (*ARML 2020*)
- 5.7 How many nine-digit numbers end in 1996 and are divisible by 1996? (*Moldova 1996*)
- 5.8 Find the largest integer  $n$  with at most three digits such that  $n^2$  leaves remainder  $n$  on division by 1000. (*Australian Intermediate 2014*)
- 5.9 Find the smallest positive integer  $n$  with  $\text{lcm}(1, 2, \dots, 100 + n) = \text{lcm}(101, 102, \dots, 100 + n)$ . (*Hong Kong 2018*)
- 5.10 An infinite sequence  $a_1, a_2, \dots$  of positive integers has  $k \mid \gcd(a_{k-1}, a_k)$  for every  $k \geq 2$ . Find the smallest possible value of  $a_1 + a_2 + \dots + a_5$ . (*CMIMC 2016*)
- 5.11 Find the positive integer  $n$  for which  $\text{lcm}(36, n) - \gcd(36, n) = 500$ .
- 5.12 Let  $d_1 < d_2 < d_3 < d_4$  be the four smallest positive divisors of  $n$ , and suppose  $n = d_1^2 + d_2^2 + d_3^2 + d_4^2$ . Find  $n$ . (*Balkan 1989*)
- 5.13 Find the prime  $p$  for which  $p^2 + 11$  has exactly six positive divisors. (*Russia 1995*)
- 5.14  $n$  is a positive multiple of 24. Find the largest integer that always divides the sum of the positive divisors of  $n - 1$ . (*Putnam 1969*)
- 5.15 Positive integers  $x, y$  satisfy  $2x^2 + 5y^2 = 11(xy - 11)$ . Find  $x + y$ . (*Baltic Way 1998*)
- 5.16  $p$  and  $p^2 + 2$  are both prime. At most how many different prime divisors can  $p^3 + 3$  have? (*Turkey 2006*)
- 5.17 Find the remainder when  $2^{2026} + 3^{2026}$  is divided by 11.
- 5.18 How many pairs  $(p, q)$  of primes less than 100 make  $p^2 + q^2 + 2020$  prime? (*Kosovo 2020*)

## PART I ANSWERS TO THE EXERCISES

Every answer below was checked by computer, by direct search or exact calculation. The hint gives only the first step of the solution; if it is enough, complete the question yourself before reading further.

### CHAPTER 1 · DIVISIBILITY AND PRIMES

- 1.1 39  $n + 3 \mid 24$ , so  $n = 1, 3, 5, 9, 21$ .
- 1.2 9  $8 \mid \overline{89b}$  gives  $b = 6$ ;  $9 \mid a + 33$  gives  $a = 3$ .

- 1.3 12  $7200 = 2^5 3^2 5^2$ ; even exponents:  $3 \cdot 2 \cdot 2$ .
- 1.4 60  $\tau = 12$ :  $2^2 \cdot 3 \cdot 5$ , against 72, 96,  $2^{11}$ .
- 1.5 1170  $\sigma(2^3 3^2 5) = 15 \cdot 13 \cdot 6$ .
- 1.6 9 product of divisors  $= 36^{\tau/2} = 36^{9/2} = 6^9$ .
- 1.7 1 for  $p \neq 3, 3 \mid p^2 + 2$ ;  $p = 3$  gives 11.
- 1.8 75 leave out  $n \equiv 2 \pmod{4}$ :  $100 - 25$ .
- 1.9 257  $2^{16} - 1 = 3 \cdot 5 \cdot 17 \cdot 257$ .

1.10 1  $(n^2 + n + 1)(n^2 - n + 1)$ ; prime only at  $n = 1$ .

1.11 6  $(n - 1)n(n + 1)$ ;  $n = 2$  gives exactly 6.

1.12 31  $\tau(n)$  odd iff  $n$  is a square;  $\lfloor \sqrt{1000} \rfloor = 31$ .

#### CHAPTER 2 · GCD, LCM AND LINEAR EQUATIONS

2.1 63  $2^{\gcd(30,18)} - 1 = 2^6 - 1$ .

2.2 8  $a = 6x, b = 6y, xy = 60 = 2^2 \cdot 3 \cdot 5$ , coprime:  $2^3$ .

2.3 42 the least positive value is  $\gcd(84, 126)$ .

2.4 6  $y \equiv 2 \pmod{3}$ :  $y = 2, 5, \dots, 17$ .

2.5 83  $8 \cdot 13 - 8 - 13$ .

2.6 9  $\frac{(4-1)(7-1)}{2}$ .

2.7 15  $(x - 12)(y - 12) = 144$ ;  $\tau(144) = 15$ .

2.8 4  $n + 2 \mid 18$  with  $n + 2 \geq 3$ : 3, 6, 9, 18.

2.9 33  $\gcd(n + 4, n + 1) = \gcd(3, n + 1)$ ;  $n \equiv 2 \pmod{3}$ .

2.10 6  $(x - 3)(y - 4) = 12$ ; negative pairs give  $x \leq 0$  or  $y \leq 0$ .

2.11 4 one way for each odd divisor of 1000: 1, 5, 25, 125.

2.12 610  $\gcd(F_{30}, F_{45}) = F_{15} = 610$ .

#### CHAPTER 3 · MODULAR ARITHMETIC

3.1 1  $5^2 \equiv -1$ , so  $5^4 \equiv 1 \pmod{13}$ , and  $4 \mid 100$ .

3.2 9 cycle 7, 9, 3, 1;  $2026 \equiv 2 \pmod{4}$ .

3.3 29  $3^{20} \equiv 1 \pmod{100}$ ;  $3^6 = 729$ .

3.4 2  $2^3 \equiv 1 \pmod{7}$ ;  $2026 \equiv 1 \pmod{3}$ .

3.5 59  $x \equiv -1$  modulo 4, 5, 6; lcm = 60.

3.6 8 two roots each modulo 4, 3, 5:  $2^3$  by CRT.

3.7 96  $360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$ .

3.8 9  $4!$  onwards are multiples of 12;  $1 + 2 + 6 = 9$ .

3.9 10 Wilson:  $10! \equiv -1 \pmod{11}$ .

3.10 5  $2^5 = 32 \equiv 1 \pmod{31}$ , and 5 is prime.

3.11 40  $n \equiv 2$  or  $3 \pmod{5}$ :  $20 + 20$ .

3.12 2  $2^4 \equiv 3^4 \equiv 1 \pmod{5}$ , so each term is 1.

3.13 5  $9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1$ .

#### CHAPTER 4 · DIGITS, SQUARES AND DIOPHANTINE METHODS

4.1 505  $v_5(2026!) = 405 + 81 + 16 + 3$ .

4.2 48  $v_2(100!) = 97, v_3(100!) = 48$ .

4.3 15  $v_7(10!) = 1$ ;  $10!1!1! = 7!6!1! = 7!5!3!$ :  $3 + 6 + 6$  orders.

4.4 667  $4n \equiv 2020$ , so  $n \equiv 1 \pmod{9}$ , and  $665 \leq n \leq 673$ .

4.5 6 same remainder as  $1 + 2 + \dots + 50 = 1275$ .

4.6 11 ends in 00, digit sum a multiple of 9: 11111111100.

4.7 266  $1000 - (500 + 333 + 200 - 166 - 100 - 66 + 33)$ .

4.8 38  $4k^2 = (2n - 19)^2 + 35$ ;  $n = 1, 9, 10, 18$ .

4.9 7  $k^2 - (n + 1)^2 = 2025$ : seven factor pairs  $d < e$ .

4.10 24 leave out  $n$  with a prime  $\equiv 3 \pmod{4}$  to an odd power.

4.11 4 legs (16, 63), (25, 60), (33, 56), (39, 52).

4.12 60 3, 4, 5 always divide (section 4.7); (3, 4, 5) gives 60.

4.13 8 1, 2; 5, 6, 7, 8; 25, 26.

4.14 3  $x \leq 3$ : (3, 3, 3), (2, 4, 4), (2, 3, 6).

#### CHAPTER 5 · PROBLEM SOLVING

5.1  $p = 3$  for  $p \neq 3$ ,  $p^2 + 2007p - 1 \equiv p^2 - 1 \equiv 0 \pmod{3}$ .

5.2 15  $d = p - q$ ;  $q = \frac{(d-1)d(d+1)}{2}$ , prime only at  $d = 2$ .

5.3 10  $q(p - 1) = r(p + 1)$ :  $p - 1 = kr$ ,  $p + 1 = kq$ ,  $k(q - r) = 2$ .

5.4 5 roots  $-1$  and  $-q$ , so  $p = q + 1$ :  $q = 2$ ,  $p = 3$ .

5.5 20  $(n^2 - 3n + 3)(n^2 + 3n + 3)$ ; primes 7 and 13.

5.6 40 401, 409 prime;  $403 = 13 \cdot 31$ ,  $407 = 11 \cdot 37$ .

5.7 180  $1996 = 4 \cdot 499$ : the first five digits form a multiple of 499.

5.8 625  $n \equiv 0$  or  $1$  modulo 8 and 125; combine by CRT.

5.9 94 97 needs its multiple 194;  $n = 94$  then works.

5.10 70  $k(k + 1) \mid a_k$ :  $2 + 6 + 12 + 20 + 30$ .

5.11 56  $g = \gcd$  divides 500 and 36; only  $g = 4$ , lcm = 504.

5.12 130  $n$  even,  $4 \nmid n$ :  $d_3 = p$ ,  $d_4 = 2p$ ,  $n = 5(1 + p^2)$ ,  $p = 5$ .

5.13  $p = 3$  20 has six divisors; for  $p > 3$ , 12 is a proper divisor of  $p^2 + 11$ .

5.14 24  $d + \frac{n-1}{d} \equiv 0 \pmod{24}$ ;  $n = 24$  gives  $\sigma(23) = 24$ .

5.15 41  $(2x - y)(x - 5y) = -121$ :  $x = 14$ ,  $y = 27$ .

5.16 3  $p = 3$ , as otherwise  $3 \mid p^2 + 2$ ;  $30 = 2 \cdot 3 \cdot 5$ .

5.17 1  $2^{10} \equiv 3^5 \equiv 1 \pmod{11}$ :  $2^6 + 3 = 67 \equiv 1$ .

5.18 0 no 3: a multiple of 3; one 3: even, or  $2033 = 19 \cdot 107$ .

[ A NOTE BEFORE YOU CLOSE IT ]

## Four things worth remembering

Every IOQM answer is an integer from 00 to 99, so it is tempting to guess. Do not guess. Almost every question in this part was solved by one idea followed by a short check of cases, and most marks are lost in that check. Write out every case, including the negative divisor pairs and the digit ranges.

Decide the method before you start. The table in section 5.1 sums up this part in seven rows: a remainder, an equation, a count, a divisibility statement, digits, primes, a perfect square. If you cannot say which row a question belongs to, read it again before calculating.

Revise this part three times. The first pass, a few weeks out, is slow and complete, with every exercise attempted. The second, a week out, is only the gold cards and the worked examples. The third, on the morning of the paper, is only the dark cards and the common mistakes of section 5.6, since these are the mistakes most likely to happen in the paper.

Finally, tell us when we are wrong. If a line here does not match what you work out, write to [ritesh@iitianforum.com](mailto:ritesh@iitianforum.com) or [academics@iitianforum.com](mailto:academics@iitianforum.com) with the page and the line. Corrections go into the next edition, and the student who finds one is credited in it.

IOQM HANDBOOK RELEASE

REF IITF-IOQM-2027-HANDBOOK-PART-I

STATUS PART I · EDITION 1

**Ritesh Raj**

IIT Delhi

Founder, IITian Forum

### COPYRIGHT

© 2026 IITian Forum. All rights reserved. This book is issued for the personal use of one student. No part of it may be copied, photographed, uploaded, sold or distributed, in print or electronically, without written permission. IITian Forum and doMath are marks of IITian Forum.

doMath · An IITian Forum initiative

## Want more practice?

Every chapter of this handbook has graded problems waiting on doMath, each one solved step by step.

**Practice with doMath** →

SCAN TO PRACTICE