FREE SAMPLE | Buy the complete pack at notesbazar.in | page 1 of 12

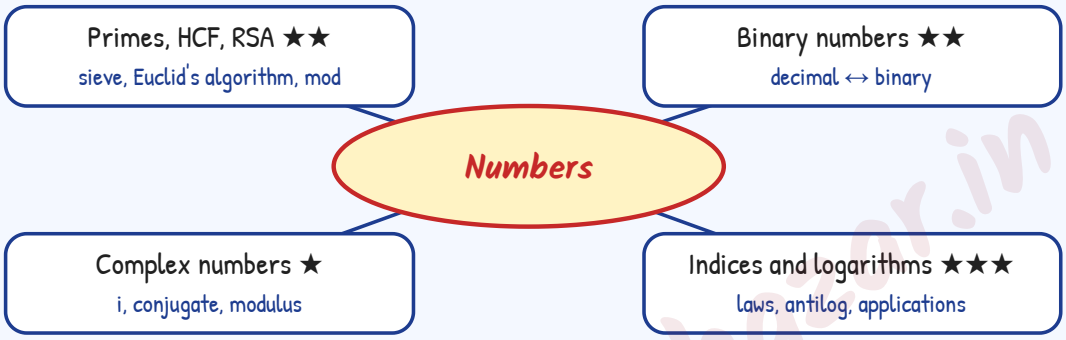
Chapter 1 Numbers and Quantification

101101

2, 3, 5, 7, 11 ...

CBSE Applied Mathematics Class XI support material, Chapter 1 · CBSE syllabus 2026-27

Chapter map (★ = asked often in school and annual exams)



What is inside

1. Concept notes with worked examples
2. CBSE support material exercises, fully solved
3. Important exam questions, fully solved
4. Quick-reference sheet; practice A–G, 20 MCQs, 6 A–R, answers, summary

Colour code used

red = key term green = definition

purple = sub-heading black = explanation

★ = high-frequency exam topic

1 = mark the examiner gives for that point

★ **Exam tip:** Logarithm laws carry the most marks: product → add, quotient → subtract, power → multiply. Practise converting between binary and decimal until it takes under a minute.

NB **Prepared by Notes Bazar** · Every answer written and checked by hand against NCERT and the CBSE marking schemes. Doubt or mistake? WhatsApp 88240 98091.

SAMPLE · notesbazar.in

1.2 Prime numbers ★★

Divisibility: $a \mid b$ (a divides b) if $b = ac$ for an integer c; e.g. $9 \mid 27$, $5 \nmid 13$. Then a is a **factor** (divisor) of b and b a **multiple** of a. ± 1 divide every integer; every non-zero integer divides 0.

A **prime** is an integer $p > 1$ whose only positive divisors are 1 and p (2, 3, 5, 7, 11, ...). An integer $n > 1$ that is not prime is **composite** (4, 6, 8, 9, ...). **1 is neither** prime nor composite.

Fundamental Theorem of Arithmetic: every integer $n > 1$ is a product of primes, unique apart from order: $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. E.g. $36 = 2^2 \cdot 3^2$, $105 = 3 \cdot 5 \cdot 7$, $104568 = 2^3 \cdot 3 \cdot 4357$.

Why 1 is not prime: if it were, $10 = 2 \cdot 5 = 1 \cdot 2 \cdot 5 = 1^2 \cdot 2 \cdot 5 = \ldots$ would have many factorisations, breaking uniqueness. 1 is not composite either, since it has no divisor other than itself.

Euclid's theorem: there are infinitely many primes. Proof: suppose $p_1, \ldots, p_r$ are all the primes. Let $N = p_1 p_2 \cdots p_r + 1 > 1$. N has a prime divisor p, so $p = p_i$ for some i. But dividing N by any p_i leaves remainder 1, so $p_i \nmid N$: a contradiction.

The largest known prime (found 2018) is the Mersenne prime $2^{82589933} - 1$ with 24 862 048 digits. (Mersenne primes have the form $2^p - 1$.)

Sieve of Eratosthenes

$n > 1$ is composite if and only if it has a prime divisor $p \leq \sqrt{n}$. For primes up to 100, $\sqrt{100} = 10$: cross out 1, then the multiples of 2, 3, 5 and 7 (keeping these four). What remains are the **25 primes up to 100**:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Testing a number: is 221 prime? $\sqrt{221} < 15$; try 2, 3, 5, 7, 11, 13: $221 = 13 \times 17$, so composite. Is 211 prime? None of 2, 3, 5, 7, 11, 13 divides it, so 211 is prime.

Ramanujan primes

The n-th Ramanujan prime R_n is the least integer such that there are at least n primes between $\frac{x}{2}$ and x for every $x \geq R_n$. They are all primes: $R_1 = 2$, $R_2 = 11$, $R_3 = 17$, $R_4 = 29$, $R_5 = 41$, $R_6 = 47$, $R_7 = 59$, $R_8 = 67$, $R_9 = 71$, $R_{10} = 97$.

Other useful facts

1. 2 is the only even prime.
2. Every prime greater than 3 has the form $6k \pm 1$.
3. Twin primes differ by 2: (3, 5), (11, 13), (17, 19).
4. Coprime numbers have HCF 1: (8, 15).

★ ***Exam tip:*** Suggested project (book): list all primes up to 10 000 with the sieve; you need to sieve by primes up to $\sqrt{10000} = 100$.

1.3 Encryption using prime numbers ★★

Cryptography: using mathematics to encrypt and decrypt data. **Cryptanalysis**: analysing and breaking secure communication. **Cryptology** = both. **Plaintext** → (encryption with a key) → **ciphertext** → (decryption) → plaintext. A **cryptosystem** = algorithm + all keys + protocols. Requirements: **authentication**, **confidentiality**, **non-repudiation**, **integrity**. Systems: RSA (1978: Rivest, Shamir, Adleman), Diffie-Hellman, ElGamal, elliptic curve.

SAMPLE · notesbazar.in

HCF (GCD)

$d = \gcd(a, b)$ is the largest positive common divisor. $\gcd(10, 25) = 5$, $\gcd(3, 17) = 1$ (coprime). From factorisations, take the smaller power of each prime: $4680 = 2^3 \cdot 3^2 \cdot 5 \cdot 13$, $15708 = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \Rightarrow \gcd = 2^2 \cdot 3 = 12$.

Euclid's algorithm (no factorising): $\gcd(a, b) = \gcd(a, b - aq)$. Divide repeatedly; the last non-zero remainder is the HCF.

step	division
1	$15708 = 3 \times 4680 + 1668$
2	$4680 = 2 \times 1668 + 1344$
3	$1668 = 1 \times 1344 + 324$
4	$1344 = 4 \times 324 + 48$
5	$324 = 6 \times 48 + 36$
6	$48 = 1 \times 36 + 12$
7	$36 = 3 \times 12 + 0 \Rightarrow$ HCF $= 12$

Modular arithmetic

$a \equiv b \pmod{m}$ if $m \mid (a - b)$: a and b leave the same remainder on division by m. $17 \equiv 2 \pmod{5}$. If $a \equiv b$ then $a^t \equiv b^t \pmod{m}$.

Euler's theorem: if $\gcd(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$ counts numbers up to m coprime to m. $\phi(35) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$, so $3^{24} \equiv 1 \pmod{35}$. For $m = pq$: $\phi(pq) = (p - 1)(q - 1)$.

RSA: (1) choose primes p, q, $n = pq$ (public), keep p, q secret; (2) choose e with $1 < e < \phi(n)$, $\gcd(e, \phi(n)) = 1$; public key (n, e); (3) private key d: $ed \equiv 1 \pmod{\phi(n)}$. Encrypt $C \equiv M^e \pmod{n}$; decrypt $M \equiv C^d \pmod{n}$ (works by Euler's theorem).

Book example: $p = 71$, $q = 101$, $n = 7171$, $\phi = 7000$, $e = 37$, $d = 3973$ ($37 \times 3973 = 147001 = 21 \times 7000 + 1$). $M = 117$: $C = 117^{37} \equiv 227$; $227^{3973} \equiv 117 \pmod{7171}$.

Small example: $p = 5$, $q = 11$: $n = 55$, $\phi = 40$, $e = 3$; $3d \equiv 1 \pmod{40} \Rightarrow d = 27$. $M = 8$: $C = 8^3 = 512 = 9 \times 55 + 17$, so $C = 17$; and $17^{27} \equiv 8 \pmod{55}$.

★ **Exam tip:** Security: to find d an attacker must factor n; for primes with hundreds of digits this is practically impossible.

1.4–1.5 Binary numbers; complex numbers ★★

Binary (base 2) numbers use only the digits 0 and 1; computers store everything this way. $(x_n x_{n-1} \ldots x_1 x_0)_2 = x_0 + 2x_1 + 2^2 x_2 + \cdots + 2^n x_n$.

Binary → decimal: add the powers of 2 where the digit is 1. $(1010101010)_2 = 2^1 + 2^3 + 2^5 + 2^7 + 2^9 = 682$.

Decimal → binary: divide by 2 repeatedly and read the remainders from bottom to top.

÷ 2	quotient	remainder
45	22	1
22	11	0

SAMPLE - notesbazar.in

11	5	1
5	2	1
2	1	0
1	0	1

Reading upwards: $45 = (101101)_2$. Book example: $23456 = 2^5 + 2^7 + 2^8 + 2^9 + 2^{11} + 2^{12} + 2^{14} = (101101110100000)_2$. The number of zeros at the right end is the power of 2 dividing the number ($2^5 \mid 23456$). (The book says the highest power is written "on the right"; it is written on the left.)

Binary addition: $0+0=0, 0+1=1, 1+1=10$ (write 0, carry 1), $1+1+1=11$. E.g. $(1011)_2 + (110)_2 = (10001)_2$ ($11+6=17$).

Complex numbers (preliminary idea)

$x^2+1=0$ has no real root. Let i (iota) satisfy $i^2=-1$. Then $i^{4n}=1, i^{4n+1}=i, i^{4n+2}=-1, i^{4n+3}=-i$.

$\mathbb{C} = \{z = a+bi : a, b \in \mathbb{R}\}$; $a = \operatorname{Re} z$, $b = \operatorname{Im} z$. Every real $r = r + 0i$, so $\mathbb{R} \subset \mathbb{C}$.

Sum: $(a_1+b_1i)+(a_2+b_2i) = (a_1+a_2)+(b_1+b_2)i$. Product: $(a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i$. E.g. $(1+i)(2+3i) = -1+5i$.

Conjugate $\bar{z} = a - bi$; $\overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2$, $\overline{z_1 z_2} = \bar{z}_1\bar{z}_2$. **Modulus** $|z| = \sqrt{z\bar{z}} = \sqrt{a^2+b^2}$; $|1+i| = \sqrt{2}$.

Properties: $|z| = |-z| = |\bar{z}| \geq 0$; $|z| = 0 \iff z = 0$; $|z_1 z_2| = |z_1||z_2|$; triangle inequality $|z_1+z_2| \leq |z_1| + |z_2|$.

Inverse and division: $z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{a-bi}{a^2+b^2}$; $\frac{z_1}{z_2} = \frac{z_1\bar{z}_2}{|z_2|^2}$. E.g. $(2+3i)^{-1} = \frac{2}{13} - \frac{3}{13}i$; $\frac{2+3i}{4-5i} = \frac{(2+3i)(4+5i)}{41} = -\frac{7}{41} + \frac{22}{41}i$.

Polar (Euler) form: $z = |z|(\cos\theta + i\sin\theta) = |z|e^{i\theta}$ with $\cos\theta = \frac{a}{\sqrt{a^2+b^2}}$, $\sin\theta = \frac{b}{\sqrt{a^2+b^2}}$ (the book omits the square roots). $1+i = \sqrt{2}e^{i\pi/4}$.

1.6–1.8 Indices, logarithms and antilogarithms ★★★

In 5^9, 5 is the **base** and 9 the **index** (exponent). $a^0 = 1$ ($a \neq 0$; 0^0 is not defined), $a^{-n} = \frac{1}{a^n}$, $a^{1/n} = \sqrt[n]{a}$ ($9^{1/2} = 3, 8^{1/3} = 2$).

law	example
$a^m a^n = a^{m+n}$	$2^3 \cdot 2^2 = 32$
$\frac{a^m}{a^n} = a^{m-n}$	$\frac{2^2}{2^3} = 2^{-1} = \frac{1}{2}$
$(a^m)^n = a^{mn}$	$(2^2)^3 = 64$
$(ab)^m = a^m b^m$	$3^2 \cdot 4^2 = 12^2 = 144$
$\left(\frac{a}{b}\right)^m = \frac{a^m}{b^m}$	$\frac{6^2}{2^2} = 3^2 = 9$

If $b^x = N$ ($N>0, b>0, b\neq 1$), then $x = \log_b N$: the **logarithm** of N to base b. $\log_3 81 = 4$; $\log_{10} 0.01 = -2$; $\log_2 \sqrt{2} = \frac{1}{2}$; $\log_b b = 1$; $\log_b 1 = 0$; $\log_b b^n = n$; $b^{\log_b a} = a$.

Systems: natural logs (Napier) to base $e \approx 2.718$, written $\ln x$; common logs to base 10. Facts: logs exist only for positive numbers and positive bases $\neq 1$; the value of a log can be negative; $\log_b a = \log_b c \Rightarrow a = c$.

Laws of logarithms

1. $\log_b(MN) = \log_b M + \log_b N$: $\log_2(4\times 8) = 2+3 = 5$.
2. $\log_b \frac{M}{N} = \log_b M - \log_b N$: $\log_3 \frac{81}{8} = 4 - 3\log_3 2$.

SAMPLE · notesbazar.in

3. $\log_b M^n = n \log_b M$: $\log_2 3^{100} = 100 \log_2 3$.

4. Change of base: $\log_a N = \frac{\log_b N}{\log_b a}$; $\log_{10} N = 0.4343 \ln N$, $\ln N = 2.303 \log_{10} N$.

Antilogarithm: if $\log_b y = x$ then $y = \text{antilog}\, x = b^x$. $\text{antilog}_{10} 2.5 = 10^{2.5} \approx 316.2$. Using tables: $\log N$ = characteristic (integer part) + mantissa (decimal part from the table); antilog table gives the digits, the characteristic places the decimal point.

Applications

Richter scale: $R = \log_{10} \frac{A}{A_0}$ (A = wave amplitude, A_0 = standard wave). Up to 4.9: no damage; 6–6.9 and above: major damage; Chile 1960: 9.5. Each unit = 10 times the amplitude. Example 1: $A = 2020 A_0$: $R = \log 2020 = 3.31$ (book: 3.3).

Growth: bacteria double every 20 h from 200: $b = 200 \cdot 2^{t/20}$. For $b = 500$: $2^{t/20} = 2.5 \Rightarrow t = \frac{20 \log 2.5}{\log 2} = \frac{20 \times 0.3979}{0.3010} = 26.4$ h. (The book's working uses $(\sqrt{2})^{t/20}$, which would mean doubling every 40 h, and prints 22.96 h; with doubling every 20 h the answer is about 26.4 hours.)

Other uses: decibels, pH, star brightness, compound interest and population.

CBSE support material exercises, fully solved

Exercises on binary numbers (1.4)

Ex 1 Write in decimal notation: $(1010101100110)_2$, $(101011000110)_2$, $(101111100110)_2$, $(1000000000110)_2$.

> **Ans.** (i) $2^{12} + 2^{10} + 2^8 + 2^6 + 2^5 + 2^2 + 2^1 = 4096 + 1024 + 256 + 64 + 32 + 4 + 2 = 5478$.
> (ii) $2^{11} + 2^9 + 2^7 + 2^6 + 2^2 + 2 = 2048 + 512 + 128 + 64 + 4 + 2 = 2758$.
> (iii) $2048 + 512 + 256 + 128 + 64 + 32 + 4 + 2 = 3046$.
> (iv) $2^{12} + 2^2 + 2 = 4096 + 4 + 2 = 4102$.

Ex 2 Write in binary notation (the book prints "decimal"): 654321, 1000001, 56237801, 2468097531, 963258741.

> **Ans.** By repeated division by 2 (remainders read upwards):
> $654321 = (10011111101111110001)_2$
> $1000001 = (11110100001001000001)_2$
> $56237801 = (11010110100001111011101001)_2$
> $2468097531 = (10010011000111000010110111111011)_2$
> $963258741 = (11100101101010001010010111010 1)_2$
> Check (first): $2^{19} + 2^{16} + \cdots = 524288 + 65536 + 32768 + 16384 + 8192 + 4096 + 1024 + 512 + 256 + 128 + 64 + 32 + 16 + 1 = 654321$.

Ex 3 Simplify and write in decimal: $(1000101111100)_2 + (1100101000100)_2\ (11101100100)_2$.

> **Ans.** Convert each: $(1000101111100)_2 = 4096 + 256 + 64 + 32 + 16 + 8 + 4 = 4476$; $(1100101000100)_2 = 4096 + 2048 + 256 + 64 + 4 = 6468$; $(11101100100)_2 = 1024 + 512 + 256 + 64 + 32 + 4 = 1892$. The book omits the sign before the third number. Taking "+": $4476 + 6468 + 1892 = 12836$. Taking "×" (multiplication before addition): $4476 + 6468 \times 1892 = 4476 + 12237456 = 12241932$.

Ex 4 Simplify and write in binary: $(1111000110000)_2 \times 5642371$.

> **Ans.** $(1111000110000)_2 = 4096 + 2048 + 1024 + 512 + 32 + 16 = 7728$. $7728 \times 5642371 = 43604243088$. In binary: $(10100010011100000011111100101001 0000)_2$ (four zeros at the end, since $7728 = 2^4 \times 483$).

SAMPLE · notesbazar.in

Exercises on complex numbers (1.5)

Ex 1 Find the conjugate and modulus: $1-i$, $10+4i$, $(3+5i)(4+6i)$, $\frac{2+7i}{5+4i}$.

Ans. (i) $\bar{z}=1+i$, $|z|=\sqrt{2}$.

(ii) $\bar{z}=10-4i$, $|z|=\sqrt{116}=2\sqrt{29}$.

(iii) $z=12+18i+20i+30i^2=-18+38i$; $\bar{z}=-18-38i$; $|z|=\sqrt{324+1444}=\sqrt{1768}=2\sqrt{442}\approx 42.05$.

(iv) $z=\frac{(2+7i)(5-4i)}{25+16}=\frac{10-8i+35i+28}{41}=\frac{38+27i}{41}$; $\bar{z}=\frac{38-27i}{41}$; $|z|=\frac{|2+7i|}{|5+4i|}=\sqrt{\frac{53}{41}}\approx 1.137$.

Ex 2 Compute $\bar{z}$, z^2, z^3, z^{-1} for $1-i$, $3+i$, $4+6i$, $\frac{9+2i}{2+9i}$, $1+\pi i$, $\sqrt{3}+\sqrt{6}\,i$.

Ans. (i) $1-i$: $\bar{z}=1+i$; $z^2=-2i$; $z^3=-2-2i$; $z^{-1}=\frac{1+i}{2}$.

(ii) $3+i$: $\bar{z}=3-i$; $z^2=8+6i$; $z^3=18+26i$; $z^{-1}=\frac{3-i}{10}$.

(iii) $4+6i$: $\bar{z}=4-6i$; $z^2=-20+48i$; $z^3=-368+72i$; $z^{-1}=\frac{4-6i}{52}=\frac{2-3i}{26}$.

(iv) $z=\frac{(9+2i)(2-9i)}{85}=\frac{36-77i}{85}$ ($|z|=1$): $\bar{z}=\frac{36+77i}{85}=z^{-1}$; $z^2=\frac{-4633-5544i}{7225}\approx -0.641-0.767i$; $z^3\approx -0.967+0.256i$.

(v) $1+\pi i$: $\bar{z}=1-\pi i$; $z^2=(1-\pi^2)+2\pi i\approx -8.87+6.28i$; $z^3=(1-3\pi^2)+(3\pi-\pi^3)i\approx -28.61-21.58i$; $z^{-1}=\frac{1-\pi i}{1+\pi^2}$.

(vi) $\sqrt{3}+\sqrt{6}\,i$: $\bar{z}=\sqrt{3}-\sqrt{6}\,i$; $z^2=3-6+2\sqrt{18}\,i=-3+6\sqrt{2}\,i$; $z^3=-15\sqrt{3}+3\sqrt{6}\,i$; $z^{-1}=\frac{\sqrt{3}-\sqrt{6}\,i}{9}$.

Exercises on indices (1.6)

Ex 1 Simplify $a=x^{1/3}\cdot x^{4/3}$.

Ans. Add indices: $a=x^{\frac{1}{3}+\frac{4}{3}}=x^{5/3}$.

Ex 2 Simplify $a=x^2\div x^{3/2}$.

Ans. Subtract: $a=x^{2-\frac{3}{2}}=x^{1/2}=\sqrt{x}$.

Ex 3 Simplify $a=\left(x^{5/3}\right)^6$.

Ans. Multiply: $a=x^{\frac{5}{3}\times 6}=x^{10}$.

Ex 4 Simplify $a=\frac{x^3y^4}{x^5y^2}$.

Ans. $a=x^{3-5}y^{4-2}=x^{-2}y^2=\frac{y^2}{x^2}$.

Exercises on logarithms (1.7)

Ex 1 Expand $\log_b\left(\frac{a^ab^b}{c^cd^d}\right)$.

Ans. $=\log_b a^a+\log_b b^b-\log_b c^c-\log_b d^d=a\log_b a+b\log_b b-c\log_b c-d\log_b d=a\log_b a+b-c\log_b c-d\log_b d$ (since $\log_b b=1$).

Ex 2 Expand $\log_b\left(\frac{4x^6}{9y^7}\right)$.

Ans. $=\log_b 4+6\log_b x-\log_b 9-7\log_b y=2\log_b 2+6\log_b x-2\log_b 3-7\log_b y$.

Ex 3 Simplify $\log_{10} a+\log_{10} b^2+\log_{10} c^3$.

Ans. Product law: $=\log_{10}(ab^2c^3)$.

Ex 4 Simplify $\log_a a-\log_b b^2+\log_c c^3-\log_d d^4$.

Ans. $\log_k k^n=n$: $=1-2+3-4=-2$.

SAMPLE · notesbazar.in

Exercise on applications (1.8)

Ex 1 World population t years after 2010 is $P = 4.7(1.02)^t$ billion. (i) Find the population in 2029 to the nearest million. (ii) Find the year in which the population will be double that of 2020.

> **Ans.** (i) $t = 19$: $\log P = \log 4.7 + 19\log 1.02 = 0.6721 + 19(0.0086) = 0.6721 + 0.1634 = 0.8355$; $P = \text{antilog}\, 0.8355 \approx 6.847$ billion $\approx$ **6847 million**.
> (ii) 2020 ($t = 10$): $P_{2020} = 4.7(1.02)^{10}$. Double: $4.7(1.02)^t = 2 \times 4.7(1.02)^{10} \Rightarrow (1.02)^{t-10} = 2 \Rightarrow t - 10 = \frac{\log 2}{\log 1.02} = \frac{0.3010}{0.0086} = 35.0$. So $t = 45$: the year **2055**.

> ★ **Exam tip:** With log tables, $\log 1.02 = 0.0086$ and $\log 4.7 = 0.6721$. Rounding $\log 1.02$ affects the last digits; calculators give 6.847 billion and 35.0 years.

Book Ex (sieve project) How many primes are there up to 100, and which primes are needed to sieve them?

> **Ans.** 25 primes; sieve with 2, 3, 5, 7 (the primes up to $\sqrt{100} = 10$).

Important exam questions, fully solved

Questions of the kind set in school and annual exams, with complete solutions and mark steps.

A. 1-mark questions

Exam-style The value of i^{2026} is: (A) 1 (B) i (C) -1 (D) $-i$ [1]

> **Ans.** $2026 = 4 \times 506 + 2$, so $i^{2026} = i^2 = -1$: **(C)**

Exam-style $(110101)_2$ in decimal is: (A) 51 (B) 53 (C) 45 (D) 55 [1]

> **Ans.** $32 + 16 + 4 + 1 = 53$: **(B)**

Exam-style Assertion (A): 1 is not a prime number. Reason (R): If 1 were prime, factorisation into primes would not be unique. [1]

> **Ans.** Both true; R explains A: **(A)**

B. 2-mark questions

Exam-style Find the HCF of 1071 and 462 by Euclid's algorithm. [2]

> **Ans.** $1071 = 2 \times 462 + 147$; $462 = 3 \times 147 + 21$; $147 = 7 \times 21 + 0$ (1). HCF $= 21$ (1).

Exam-style Find the modulus and inverse of $3 - 4i$. [2]

> **Ans.** $|z| = \sqrt{9 + 16} = 5$ (1); $z^{-1} = \frac{3+4i}{25}$ (1).

C. 3-mark questions

Exam-style If $\log 2 = 0.3010$ and $\log 3 = 0.4771$, find $\log \sqrt{72}$. [3]

> **Ans.** $72 = 2^3 \cdot 3^2$ (1); $\log \sqrt{72} = \frac{1}{2}(3\log 2 + 2\log 3)$ (1) $= \frac{1}{2}(0.9030 + 0.9542) = 0.9286$ (1).

Exam-style In RSA with $p = 5$, $q = 11$, $e = 3$, find d and encrypt $M = 8$. [3]

> **Ans.** $n = 55$, $\phi = 40$ (1); $3d \equiv 1 \pmod{40} \Rightarrow d = 27$ (1); $C = 8^3 = 512 \equiv 17 \pmod{55}$ (1).

SAMPLE · notesbazar.in

D. 5-mark question

Exam-style Two earthquakes measure 6.5 and 4.5 on the Richter scale. (a) How many times larger is the amplitude of the first? (b) Find the amplitude ratio $\frac{A}{A_0}$ of an earthquake of magnitude 5.3. (c) Solve $2^{x+1} = 24$ using logs. [5]

> **Ans.** (a) $\frac{A_1}{A_2} = 10^{6.5-4.5} = 10^2 = 100$ times (2). (b) $\frac{A}{A_0} = 10^{5.3} = \text{antilog}\,5.3 \approx 199500$ (1).
> (c) $(x+1)\log 2 = \log 24 \Rightarrow x+1 = \frac{1.3802}{0.3010} = 4.585 \Rightarrow x = 3.585$ (2).

Quick-reference sheet

topic	remember
prime test	try primes up to $\sqrt{n}$
primes ≤ 100	25
Euclid's algorithm	last non-zero remainder = HCF
$a \equiv b \pmod m$	$m \mid a-b$
$\phi(pq)$	$(p-1)(q-1)$
RSA	public (n,e), private d: $ed \equiv 1 \pmod\phi$; $C = M^e$, $M = C^d \pmod n$
binary → decimal	add powers of 2 under the 1s
decimal → binary	divide by 2; remainders upwards
powers of i	cycle $i, -1, -i, 1$
z^{-1}	$\frac{\bar z}{\lvert z\rvert^2}$
log laws	$\log MN = \log M + \log N$; $\log\frac{M}{N} = \log M - \log N$; $\log M^n = n\log M$
change of base	$\ln N = 2.303\log N$
Richter	$R = \log\frac{A}{A_0}$

Case study (practice): 'Secret messages' Riya and Aman use RSA with primes $p = 3$ and $q = 11$, and the public exponent $e = 7$. Aman wants to send the number $M = 4$.
(i) Find n and $\phi(n)$. (ii) Check that e is valid. (iii) Find Riya's private key d. (iv) Find the ciphertext C. (v) Write n in binary.

★ **Exam tip:** Always check $\gcd(e,\phi) = 1$ before finding d; find d by trying $d = 1, 2, 3, \ldots$ until ed leaves remainder 1.

Practice set: test yourself *Exam-style*

Try every question before looking at the answers at the end of the chapter. 56 or more out of 70 means you are ready for the exam.

A. Fill in the blanks (1 mark each)

1. The only even prime is ___.
2. $\gcd(a,b) = 1$ means a, b are ___.
3. $(1111)_2 =$ ___.
4. $i^{43} =$ ___.
5. The conjugate of $5 - 2i$ is ___.

6. $\log_5 125 = ___$.
7. $\log_b 1 = ___$.
8. Logarithms to base e are called ___ logarithms.

B. True or false? (1 mark each)

1. 1 is a composite number.
2. There are infinitely many primes.
3. $17 \equiv 5 \pmod 4$.
4. $|z_1 + z_2| \geq |z_1| + |z_2|$ always.
5. $\log(M + N) = \log M + \log N$.
6. $\log_{10} 0.001 = -3$.
7. $a^0 = 1$ for every $a \neq 0$.
8. In RSA the private key is made public.

C. Very short answer (1 mark each)

1. Write 36 as a product of primes.
2. Find $\phi(15)$.
3. Write 13 in binary.
4. Find $|6 + 8i|$.
5. Simplify $(2 + i)(2 - i)$.
6. Evaluate $8^{2/3}$.
7. Evaluate $\log_2 \frac{1}{16}$.
8. Find x if $\log_x 49 = 2$.
9. Expand RSA.
10. Find the remainder of 47 mod 6.

D. Short answer I (2 marks each)

1. Find the HCF of 252 and 105 by Euclid's algorithm.
2. Convert $(10110110)_2$ to decimal.
3. Convert 100 to binary.
4. Find $\frac{1+2i}{3-i}$ in the form $a + bi$.
5. Simplify $\frac{(x^2y^{-3})^2}{x^{-1}y}$.
6. Show that $\log \frac{75}{16} - 2\log \frac{5}{9} + \log \frac{32}{243} = \log 2$.
7. Is 391 prime? Justify.
8. Find $\log_{10} 5$ if $\log_{10} 2 = 0.3010$.

My score (fill in after checking the answers)

Section	A /8	B /8	C /10	D /16	E /18	F /10	G (bonus)	Total /70
My marks								

Rough work

SAMPLE · notesbazar.in

E. Short answer II (3 marks each)

1. Prove that there are infinitely many primes.
2. Find z^2, z^3 and z^{-1} for $z = 2 - 3i$.
3. In RSA, $p = 7$, $q = 11$, $e = 7$: find d.
4. Solve $3^{2x-1} = 50$ using $\log 3 = 0.4771$, $\log 5 = 0.6990$, $\log 2 = 0.3010$.
5. Add $(110111)_2$ and $(10101)_2$ and check in decimal.
6. If $\log_a x = 2$ and $\log_a y = 3$, find $\log_a \frac{x^3}{\sqrt{y}}$.

F. Long answer (5 marks each)

1. A sum of ₹ 10 000 grows at 8% compound interest a year: $A = 10000(1.08)^n$. Using logs, find (i) the amount after 10 years (ii) the years needed to double ($\log 1.08 = 0.0334$, $\log 2.159 = 0.3342$).
2. Explain the RSA cryptosystem with $p = 3$, $q = 11$, $e = 3$ and encrypt $M = 5$, then decrypt it.

G. HOTS (higher-order thinking)

1. Why is it enough to test divisibility by primes up to $\sqrt{n}$?
2. Why does RSA become unsafe if n can be factorised?
3. Why do computers use binary rather than decimal?
4. Why is $\log_b 0$ not defined?

20 MCQs

1. Which is a prime?
   (a) 91 (b) 87 (c) 97 (d) 51
2. Number of primes up to 100:
   (a) 25 (b) 24 (c) 26 (d) 20
3. HCF of 4680 and 15708:
   (a) 6 (b) 36 (c) 24 (d) 12
4. $17 \equiv ___ \pmod 5$:
   (a) 3 (b) 2 (c) 1 (d) 4
5. $\phi(35)$ equals:
   (a) 34 (b) 24 (c) 12 (d) 30
6. In RSA, the public key is:
   (a) (p, q) (b) $\phi(n)$ (c) d (d) (n, e)
7. $(1010101010)_2$ in decimal:
   (a) 682 (b) 680 (c) 684 (d) 1365
8. 45 in binary:
   (a) 101011 (b) 110101 (c) 101101 (d) 100101
9. i^{4n+3} equals:
   (a) i (b) -1 (c) 1 (d) $-i$
10. $(1 + i)(2 + 3i)$ equals:
    (a) $5 + 5i$ (b) $-1 + 5i$ (c) $2 + 3i$ (d) $-1 - 5i$

SAMPLE · notesbazar.in

11. $|1+i|$ equals:
(a) 1 (b) 2 (c) $\sqrt{2}$ (d) 0

12. $(2+3i)^{-1}$ equals:
(a) $\frac{2-3i}{13}$ (b) $\frac{2+3i}{13}$ (c) $\frac{2-3i}{5}$ (d) $2-3i$

13. $\left(x^{5/3}\right)^{6}$ equals:
(a) $x^{5/18}$ (b) x^{10} (c) x^{11} (d) x^{8}

14. $\log_{10} 0.01$ equals:
(a) 2 (b) 0.2 (c) -2 (d) -0.2

15. $\log_2 \sqrt{2}$ equals:
(a) 2 (b) $\sqrt{2}$ (c) 1 (d) $\frac{1}{2}$

16. $\log_a a - \log_b b^2 + \log_c c^3 - \log_d d^4$ equals:
(a) -2 (b) 2 (c) 10 (d) 0

17. $\ln N$ equals:
(a) $2.303 \log N$ (b) $0.434 \log N$ (c) $\log N$
(d) $10 \log N$

18. $b^{\log_b a}$ equals:
(a) b (b) 1 (c) ab (d) a

19. An earthquake 1000 times the standard amplitude measures:
(a) 2 (b) 3 (c) 4 (d) 1000

20. $\log_3 81$ equals:
(a) 3 (b) 27 (c) 4 (d) 9

1 (c) · 2 (a) · 3 (d) · 4 (b) · 5 (b) · 6 (d) · 7 (a) · 8 (c) · 9 (d) · 10 (b) · 11 (c) · 12 (a) · 13 (b) · 14 (c) · 15 (d) · 16 (a) · 17 (a) · 18 (d) · 19 (b) · 20 (c)

Assertion–Reason (6)

(a) Both true, R explains A. (b) Both true, R does not explain A. (c) A true, R false. (d) A false, R true.

1. A: 221 is composite. R: 221 is divisible by 13.
2. A: $\log(-10)$ is defined. R: Logarithms are defined only for positive numbers.
3. A: $i^{100} = 1$. R: $i^{4n} = 1$ for every whole number n.
4. A: $\gcd(12, 35) = 1$. R: 12 and 35 are both prime.
5. A: $\log_2 8 + \log_2 4 = 5$. R: $\log_b(MN) = \log_b M + \log_b N$.
6. A: $(10000)_2 = 16$. R: The number of zeros at the end gives the power of 2 dividing the number.

Key: 1 (a) · 2 (d) · 3 (a) · 4 (c) · 5 (a) · 6 (b)

Answers to the practice set

A. 1. 2 2. coprime 3. 15 4. $-i$ 5. $5+2i$ 6. 3 7. 0 8. natural

B. 1. F 2. T 3. T $(12 = 3 \times 4)$ 4. F 5. F 6. T 7. T 8. F

C. 1. $2^2 \cdot 3^2$ 2. 8 3. $(1101)_2$ 4. 10 5. 5 6. 4 7. -4 8. 7 9. Rivest-Shamir-Adleman 10. 5

SAMPLE · notesbazar.in

D. 1. $252 = 2 \times 105 + 42$, $105 = 2 \times 42 + 21$, $42 = 2 \times 21$: 21 2. $128 + 32 + 16 + 4 + 2 = 182$ 3. $(1100100)_2$ 4. $\frac{(1+2i)(3+i)}{10} = \frac{1+7i}{10}$ 5. $\frac{x^4y^{-6}}{x^{-1}y} = x^5y^{-7}$ 6. $\log\left(\frac{75}{16} \cdot \frac{81}{25} \cdot \frac{32}{243}\right) = \log 2$ 7. $391 = 17 \times 23$: composite 8. $\log \frac{10}{2} = 1 - 0.3010 = 0.6990$

E. 1. p. 2 2. $z^2 = -5 - 12i$; $z^3 = -46 - 9i$; $z^{-1} = \frac{2+3i}{13}$ 3. $\phi = 60$; $7d \equiv 1 \pmod{60}$: $d = 43$ 4. $(2x - 1)(0.4771) = \log 50 = 1.6990$: $2x - 1 = 3.561$, $x = 2.281$ 5. $(1001100)_2 = 76 = 55 + 21$ 6. $3(2) - \frac{1}{2}(3) = 4.5$

F. 1. (i) $\log A = 4 + 10(0.0334) = 4.334$: $A \approx$ ₹ 21 590 (ii) $(1.08)^n = 2$: $n = \frac{0.3010}{0.0334} = 9.01$, about 9 years 2. $n = 33$, $\phi = 20$, $e = 3$, $d = 7$ $(21 \equiv 1)$; $C = 5^3 = 125 \equiv 26 \pmod{33}$; $26^7 \equiv 5 \pmod{33}$

G. 1. if $n = ab$ with both factors greater than $\sqrt{n}$, then $ab > n$; so one factor is at most $\sqrt{n}$ 2. from p, q anyone can compute ϕ and then d 3. electronic switches have two states, on and off 4. no power of a positive base gives 0

Case. (i) $n = 33$, $\phi = 20$ (ii) $\gcd(7, 20) = 1$ (iii) $7d \equiv 1 \pmod{20}$: $d = 3$ (iv) $4^7 = 16384 = 496 \times 33 + 16$: $C = 16$ (v) $(100001)_2$

Last-night summary

- Primes: 1 is neither; FTA (unique factorisation); infinitely many primes; sieve up to $\sqrt{n}$; 25 primes up to 100.
- HCF by Euclid's algorithm; $a \equiv b \pmod{m}$; $\phi(pq) = (p-1)(q-1)$; RSA: $C = M^e$, $M = C^d \pmod{n}$.
- Binary: powers of 2 under the 1s; decimal → binary by dividing by 2.
- $i^2 = -1$; $\bar{z} = a - bi$; $|z| = \sqrt{a^2 + b^2}$; $z^{-1} = \frac{\bar{z}}{|z|^2}$.
- Index laws; $\log_b N = x \iff b^x = N$; product, quotient, power, change of base; antilog; Richter scale.

SAMPLE · notesbazar.in