

12.1 Congruences, divisibility and arithmetic functions

Name: _____ Class: _____ Date: _____

Total: 10 marks

KEY WORDS congruence • totient

Objective

Solve linear congruences using gcd conditions; Combine coprime congruences with the Chinese remainder theorem; Apply Euler's theorem only to invertible residues; Use prime-exponent divisibility to find least admissible integers.

Original public practice. Marking guidance is authored locally. Use the topic reference for prerequisites and full theorem statements.

1 Key knowledge and worked examples

congruence : Equality of residues because the modulus divides their difference.

totient : The count of residues coprime to the positive integer modulus.

The equation $ax \equiv b \pmod{n}$ has a solution exactly when $d = \gcd(a, n)$ divides b . If it does, divide a, b, n by d to obtain an equation with an invertible coefficient. It has one residue solution modulo n/d and d distinct solutions modulo n . Dividing the coefficient but leaving the original modulus generally loses solutions. Prime factorisation gives another divisibility tool: if n^k must be divisible by a product of prime powers p^a , each prime exponent in n must be at least $\lceil a/k \rceil$. These minimum exponents independently produce the least positive admissible n . For n^4 divisible by $2^7 \cdot 3^5$, n must contain 2^2 and 3^2 , so the least value is 36. This is a prime-exponent condition, not a congruence solved by modular division.

Solve $6x \equiv 9 \pmod{15}$. The gcd is 3 and divides 9. Divide all three quantities to get $2x \equiv 3 \pmod{5}$; the inverse of 2 is 3, so $x \equiv 9 \equiv 4 \pmod{5}$. The original solutions modulo 15 are 4, 9, 14. For $x \equiv 2 \pmod{4}$ and $x \equiv 3 \pmod{7}$, write $x = 2 + 4k$; then $4k \equiv 1 \pmod{7}$, giving $k \equiv 2$. Hence $x \equiv 10 \pmod{28}$.

$6x \equiv 9 \pmod{15}$: lift the reduced solution $x \equiv 4 \pmod{5}$

x modulo 15	6x modulo 15	Valid solution?
4	9	Yes
9	9	Yes
14	9	Yes

Solve $2x \equiv 3 \pmod{5}$ to get $x \equiv 4$, then lift to three solutions modulo 15

2 Practice

2.1 How many distinct solutions modulo 18 satisfy $6x \equiv 12$?

[1]

- A 0
- B 1
- C 3
- D 6
- E 12

2.2 What is the least nonnegative x with $x \equiv 1$ modulo 3 and $x \equiv 2$ modulo 5?

[1]

- A 2
- B 4
- C 5
- D 7
- E 11

2.3 Solve $8x \equiv 12 \pmod{20}$ completely. Find an inverse of 7 modulo 20. Explain why Euler's theorem cannot be used to replace 2^8 by 1 modulo 20. [4]

3 Exam-style questions

3.1 Solve $x \equiv 2 \pmod{6}$, $x \equiv 5 \pmod{9}$, or prove inconsistency. State the modulus for uniqueness. Find the least positive n such that $2^5 \cdot 3^7$ divides n^3 . [4]
