

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

Original course illustration; its values belong to the worked example, not the later practice.

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 $x \equiv 1 \pmod 3$ and $x \equiv 2 \pmod 5$? [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]

Solutions

2.1 D. $\gcd(6,18)=6$ divides 12, so there are six solutions; after dividing the modulus too, $x \equiv 2 \pmod{3}$. The six residues are 2,5,8,11,14,17. Zero, one, three and twelve are therefore incorrect counts; reducing the modulus does not leave only one residue modulo eighteen.

2.2 D. Among 1,4,7,10,13 modulo 15, only 7 has residue 2 modulo 5. Two fails the first congruence; four and eleven fail the second; five fails both. Seven has both required residues.

2.3 The gcd is four and divides 12. Dividing all three numbers gives $2x \equiv 3 \pmod{5}$, so $x \equiv 4 \pmod{5}$. Modulo 20 the four answers are 4, 9, 14, 19; substitution gives remainder 12 each time. Since $7 \cdot 3 = 21$, the inverse of 7 is 3. Although $\phi(20) = 8$, Euler's theorem requires a unit. The gcd of 2 and 20 is two, and $2^8 = 256 \equiv 16$, not 1.

3.1 The residues agree modulo the gcd three. Put $x = 2 + 6k$: then $6k \equiv 3 \pmod{9}$, hence $2k \equiv 1 \pmod{3}$ and $k \equiv 2 \pmod{3}$. Thus $x \equiv 14 \pmod{18}$. The modulus is the lcm, not 54. For the divisibility problem, write prime exponents in n . They must satisfy $3a \geq 5$, $3b \geq 7$, so $a \geq 2$, $b \geq 3$. The least n is $2^2 \cdot 3^3 = 108$; other prime factors can only increase it.

Local four-mark guidance for each written task: choose and justify the method; carry through the reasoning; give every requested result; check the relevant restriction, hypothesis or boundary case. These are classroom marks, not GRE scoring.