

A.6 · Congruences, divisibility and arithmetic functions

GRE · GRE Subject Test · GRE Mathematics

Scope and prerequisites

Undergraduate GRE preparation. Local objectives within the reviewed ETS scope; this is original teaching, not an official test or score predictor.

Prerequisites: Euclidean algorithm, prime factors and modular arithmetic.

- 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

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

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

Choose and justify a method

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 $\text{ceil}(a/k)$. 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.

The extended Euclidean algorithm expresses $\gcd(a, n)$ as $ua + vn$. When the gcd is 1, u is an inverse of a modulo n . Choose a representative in the required range after reduction. For 7 and 26, $1 = 15 \cdot 7 - 4 \cdot 26$, so 15 is the inverse of 7 modulo 26; verify the product to catch a sign error.

For coprime positive moduli m, n , the Chinese remainder theorem gives exactly one solution modulo mn for each pair of residue conditions. Substitute $x = r + mk$ into the second congruence and solve for k . If the moduli are not coprime, their residue values must agree modulo $\gcd(m, n)$; when consistent, uniqueness is modulo the least common multiple, not the product.

Euler's totient $\phi(n)$ counts residues coprime to n . For distinct prime divisors p , $\phi(n) = n$ times the product of $(1 - 1/p)$. Euler's theorem gives $a^{\phi(n)} \equiv 1 \pmod{n}$ only when $\gcd(a, n) = 1$. The prime case is Fermat's little theorem. Reduce exponents only after checking this condition; a nonunit can become zero under repeated powers instead.

Worked reasoning

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.

Conditions and counterexamples

The expression $a^{\phi(n)} \equiv 1$ is false for arbitrary a . For example 2 is not invertible modulo 8 and 2^4 is zero modulo 8.

Guided application

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.

■ Worked solution

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 $2^8 = 256 \equiv 16 \pmod{20}$, not 1.

Independent transfer

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 .

■ Check after attempting

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.