# A.6 · Congruences, divisibility and arithmetic functions

Original classroom teaching; not an official form or score predictor

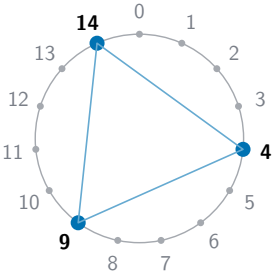
# Congruences, divisibility and arithmetic functions

- Solve linear congruences and find inverses modulo $n$.
- Use the Chinese remainder theorem.
- Apply Fermat's and Euler's theorems, and Wilson's theorem.
- Compute arithmetic functions such as $\varphi$, $\tau$ and $\sigma$.

# Congruences

- $ax \equiv b \pmod{n}$ has a solution exactly when $d = \gcd(a, n)$ divides $b$. Then it has $d$ solutions modulo $n$, spaced $n/d$ apart.
- To solve, divide $a$, $b$ and $n$ by $d$, solve the smaller congruence, and list the lifts.
- $a$ has an inverse modulo $n$ exactly when $\gcd(a, n) = 1$; find it with the Euclidean algorithm.

# Figure: Congruences




$6x \equiv 9 \pmod{15}$
$d = \gcd(6, 15) = 3$ divides 9
$d = 3$ solutions, spaced $15/3 = 5$ apart: 4, 9, 14

- d = gcd(a, n) solutions, n/d apart.
- Match each part of the diagram to the text.

# The Chinese remainder theorem

- Equivalently, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
- If $m$ and $n$ share a factor, a solution exists only when $a \equiv b$ modulo $\gcd(m, n)$.

# Fermat, Euler and Wilson

- Euler: if $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$. For a prime $p$ this is Fermat's little theorem, $a^{p-1} \equiv 1$.
- Wilson: $p$ is prime exactly when $(p-1)! \equiv -1 \pmod{p}$.
- These theorems need their conditions: Euler's needs $a$ to be a unit.

# Arithmetic functions

- $\varphi$ counts residues coprime to $n$; $\tau$ counts divisors; $\sigma$ adds them.
- All three are multiplicative: $f(mn) = f(m)f(n)$ when $\gcd(m, n) = 1$.

$$\varphi(n) = n\prod\left(1 - \frac{1}{p_i}\right), \qquad \tau(n) = \prod(a_i + 1), \qquad \sigma(n) = \prod\frac{p_i^{a_i+1} - 1}{p_i - 1}$$

# Worked example: a congruence with several solutions

- $\gcd(8, 20) = 4$, which divides 12, so there are 4 solutions.
- Divide by 4: $2x \equiv 3 \pmod 5$, so $x \equiv 4 \pmod 5$ (since $2 \times 4 = 8 \equiv 3$).
- Modulo 20: $x = 4, 9, 14, 19$. Check: $8 \times 9 = 72 = 60 + 12$.

# Figure: Worked example: a congruence with several solutions

$6x \equiv 9 \pmod{15}$: 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
- Match each part of the diagram to the text.

# Worked example: inverses and Euler

- The inverse of 7 modulo 20 is 3, since $21 \equiv 1$.
- $\varphi(20) = 20 \times \frac{1}{2} \times \frac{4}{5} = 8$, so $7^8 \equiv 1 \pmod{20}$.
- But $2^8 = 256 \equiv 16 \pmod{20}$, not 1: Euler's theorem does not apply, because $\gcd(2, 20) = 2$.
- CRT: $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$ give $x \equiv 8 \pmod{15}$.

# Common errors

- Dividing a congruence by a number that shares a factor with the modulus, without dividing the modulus.
- Giving one solution when there are $\gcd(a, n)$ of them.
- Using Euler's theorem for a non-unit.

# Common errors (2)

- Using the Chinese remainder theorem with moduli that are not coprime.
- Forgetting that $\varphi$ is multiplicative only for coprime factors.

# Key terms

- **congruence**: The relation $a \equiv b \pmod{n}$, meaning $n$ divides $a - b$.
- **totient**: Euler's function $\varphi(n)$, the number of residues from 1 to $n$ that are coprime to $n$.

# Check yourself

- What is $\varphi(36)$?
- What is $6! \bmod 7$?
- How many positive divisors does 72 have?