

Congruence.

Definition. Let a and b be integers and m be a natural number. Then a is *congruent to b modulo m* :

$$a \equiv b \pmod{m}$$

if $m \mid (a - b)$.

The number m is called the *modulus* of the congruence. Congruence modulo m divides the set \mathbb{Z} of all integers into m subsets called *residue classes*. For example, if $m = 2$, then the two residue classes are the *even integers* and the *odd integers*. Integers a and b are in the same class if and only if $a \equiv b \pmod{m}$. The following basic properties follow from the definition of congruence.

Property 1. Congruence is *reflexive*, i.e., $a \equiv a \pmod{m}$ for every integer a and natural number m .

Property 2. Congruence is *symmetric*, i.e., if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

Property 3. Congruence is *transitive*, i.e., if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Property 4. Congruences may be added: if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + b \equiv c + d \pmod{m}$.

Property 5. Congruences may be multiplied: if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ab \equiv cd \pmod{m}$.

Property 6. Both sides of a congruence may be divided by a number relatively prime to m : if $ab \equiv ac \pmod{m}$ and $(a, m) = 1$, then $b \equiv c \pmod{m}$.

An important concept related to residue classes is that of the field \mathbb{Z}_p of integers mod p where p is prime.

Definition. \mathbb{Z}_p is the set $\{0, 1, \dots, p - 1\}$ with addition and multiplication mod p .

Exercise. Check that \mathbb{Z}_p is a finite *field*, i.e., that its addition and multiplication are commutative and associative, that the distributive law holds, that there exists a element neutral under addition and an element neutral under multiplication, that each element has an inverse under addition and that each element except for the one neutral under addition has an inverse under multiplication.

Two important theorems about congruences are *Fermat's little theorem* and *Euler's theorem*, the latter being a generalization of the former.

Fermat's little theorem. If p is prime and a is not divisible by p , then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Euler's theorem. If $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Here, to recall, ϕ is Euler's totient function

$$\phi(m) := \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

Finally, an important fact about simultaneous congruences:

Chinese remainder theorem. Suppose that m_1, m_2, \dots, m_k are pairwise relatively prime and a_1, a_2, \dots, a_k are arbitrary integers. Then there exist solutions x to the simultaneous congruences

$$x \equiv a_j \pmod{m_j}, \quad j = 1, \dots, k.$$

Any two solutions are congruent modulo $M := m_1 m_2 \cdots m_k$.

Examples.

1. Prove that $36^{36} + 41^{41}$ is divisible by 77.
2. Find the last three digits of 7^{9999} .
3. Show that, for any fixed integer $n \geq 1$, the sequence

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \dots \pmod{n}$$

is eventually constant.

4. Prove that there is no integer $n > 1$ for which $n|(2^n - 1)$.
5. Prove that, for every n , there exists a sequence of n consecutive natural numbers none of which is square-free. (A *square-free* integer has no repeated prime factor.)
6. Prove that there is a positive integer k such that $k \cdot 2^n + 1$ is composite for every nonnegative integer n .

Further reading. ANALOGY BETWEEN THE CHINESE REMAINDER THEOREM AND LAGRANGE'S INTERPOLATION FORMULA by William Kahan, available at <http://www.cs.berkeley.edu/~wkahan/MathH90/>.