

Math 453: Elementary Number Theory
Definitions and Theorems

Version 3/23/2008

Chapter 2

Congruences

2.1 Definitions and basic properties; applications

Definition (Congruences) Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$. We say that a is **congruent to b modulo m** , and write $a \equiv b \pmod{m}$, if $m \mid a - b$ (or, equivalently, if $a = b + mx$ for some $x \in \mathbf{Z}$). The integer m is called the **modulus** of the congruence.

Proposition 2.1 (Elementary properties of congruences) Let $a, b, c, d \in \mathbf{Z}$, $m \in \mathbf{N}$.

- (i) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
- (ii) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
- (iii) If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for any $n \in \mathbf{N}$.
- (iv) If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$ for any polynomial $f(n)$ with integer coefficients.
- (v) If $a \equiv b \pmod{m}$, then $a \equiv b \pmod{d}$ for any positive divisor d of m .

Proposition 2.2 (Congruences as equivalence relation) Let $m \in \mathbf{N}$. The congruence relation modulo m is an equivalence relation, i.e., satisfies the following properties, for any $a, b, c \in \mathbf{Z}$:

- (i) (*Reflexivity*) $a \equiv a \pmod{m}$.
- (ii) (*Symmetry*) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- (iii) (*Transitivity*) If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.

Definition (Residue classes) Let $m \in \mathbf{N}$. The equivalence classes defined by the congruence relation modulo m are called the **residue classes modulo m** . For any $a \in \mathbf{Z}$, $[a]$ denotes the equivalence class to which a belongs, i.e.,

$$[a] = \{n \in \mathbf{Z} : n \equiv a \pmod{m}\}.$$

Definition (Complete residue system) A set of integers r_1, \dots, r_m is called a **complete residue system modulo m** , if it contains exactly one integer from each equivalence class modulo m .

Definition (Least nonnegative residue) Let $m \in \mathbf{N}$. Given any integer n , the **least nonnegative residue of n modulo m** is the unique integer r such that $n \equiv r \pmod{m}$ and $0 \leq r < m$; i.e., r is the remainder upon division of n by m by the division algorithm.

2.2 Linear congruences in one variable

Theorem 2.3 (Solutions of linear congruences in one variable) Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$, and consider the congruence

$$(2.1) \quad ax \equiv b \pmod{m}.$$

Let $d = (a, m)$.

- (i) *(Existence of a solution)* The congruence (2.1) has a solution $x \in \mathbf{Z}$ if and only if $d \mid b$.
- (ii) *(Number of solutions)* Suppose $d \mid b$. Then $ax \equiv b \pmod{m}$ has exactly d pairwise incongruent solutions x modulo m . The solutions are of the form $x = x_0 + km/d$, $k = 0, 1, \dots, d-1$, where x_0 is a particular solution.
- (iii) *(Construction of a solution)* Suppose $d \mid b$. Then a particular solution can be constructed as follows: Apply the Euclidean algorithm to compute $d = (a, m)$, and, working backwards, obtain a representation of d as a linear combination of a and m . Multiply the resulting equation through with (b/d) . The new equation can be interpreted as a congruence of the desired type, (2.1), and reading off the coefficient of a gives a particular solution.

Corollary Let $a \in \mathbf{Z}$ and $m \in \mathbf{N}$. If $(a, m) = 1$, the congruence

$$(2.2) \quad ax \equiv 1 \pmod{m}$$

has a unique solution x modulo m ; if $(a, m) \neq 1$, the congruence has no solution.

Definition (Modular inverses) A solution x to the congruence (2.2), if it exists, is called a **modular inverse of a** (with respect to the modulus m) and denoted by \bar{a} .

Remark Note that \bar{a} is not uniquely defined. The definition depends implicitly on the modulus m . In addition, for a given modulus m , \bar{a} is only *unique modulo m* ; i.e., any $x \in \mathbf{Z}$ with $x \equiv \bar{a} \pmod{m}$ is also a modular inverse of a .

2.3 Simultaneous linear congruences. The Chinese Remainder Theorem

Theorem 2.5 (Chinese Remainder Theorem) Let $a_1, \dots, a_r \in \mathbf{Z}$ and let $m_1, m_2, \dots, m_r \in \mathbf{N}$ be given such that $(m_i, m_j) = 1$ for $i \neq j$. Then the system

$$(2.3) \quad x \equiv a_i \pmod{m_i} \quad (i = 1, \dots, r)$$

has a unique solution x modulo $m_1 \cdots m_r$.

Corollary (Structure of residue systems modulo $m_1 \cdots m_r$) Let $m_1, \dots, m_r \in \mathbf{N}$ with $(m_i, m_j) = 1$ for $i \neq j$ be given and let $m = m_1 \cdots m_r$. There exists a 1-1 correspondence between complete systems of residues modulo m and r -tuples of complete systems of residues modulo m_1, \dots, m_r . More precisely, if, for each i , a_i runs through a complete system of residues modulo m_i , then the corresponding solution x to the simultaneous congruence (2.3) runs through a complete system of residues modulo m .

2.4 Wilson's Theorem

Theorem 2.7 (Wilson's Theorem) Let p be a prime number. Then

$$(2.4) \quad (p-1)! \equiv -1 \pmod{p}.$$

Theorem 2.8 (Converse to Wilson's Theorem) If p is an integer ≥ 2 satisfying (2.4), then p is a prime number.

Remark The converse to Wilson's Theorem can be stated in contrapositive form as follows: If n is composite, then $(n-1)!$ is **not** congruent to -1 modulo n . In fact, the following much stronger statement holds: If $n > 4$ and n is composite, then $(n-1)! \equiv 0 \pmod{n}$. Thus, for $n > 4$, $(n-1)!$ is congruent to either -1 or 0 modulo n ; the first case occurs if and only if n is prime, and the second occurs if and only if n is composite.

2.5 Fermat's Theorem

Theorem 2.9 (Fermat's Little Theorem) Let p be a prime number. Then, for any integer a satisfying $(a, p) = 1$,

$$(2.5) \quad a^{p-1} \equiv 1 \pmod{p}.$$

Corollary (Fermat's Little Theorem, Variant) Let p be a prime number. Then, for any integer a ,

$$(2.6) \quad a^p \equiv a \pmod{p}.$$

Corollary (Inverses via Fermat's Theorem) Let p be a prime number, and let a be an integer such that $(p, a) = 1$. Then $\bar{a} = a^{p-2}$ is an inverse of a modulo p .

Remark In contrast to Wilson's Theorem, Fermat's Theorem does not have a corresponding converse; in fact, there exist numbers p that satisfy the congruence in Fermat's Theorem, but which are composite. Such "false positives" to the Fermat test are rare, but they do exist, motivating the following definition:

Definition (Pseudoprimes and Carmichael numbers) An integer $p \geq 2$ that is composite, but satisfies the Fermat congruence (2.5), is called a **pseudoprime to the base a** , or **a -pseudoprime**. A 2-pseudoprime is simply called a **pseudoprime**. An integer p that is a pseudoprime to all bases $a \in \mathbf{N}$ with $(a, p) = 1$ is called a **Carmichael number**.

2.6 Euler's Theorem

Definition (Reduced residue system) Let $m \in \mathbf{N}$. A set of integers is called a **reduced residue system modulo m** , if (i) its elements are pairwise incongruent modulo m , and (ii) every integer n with $(n, m) = 1$ is congruent to an element of the set. Equivalently, a reduced residue system modulo m is the subset of a complete residue system consisting of those elements that are relatively prime with m .

Definition (Euler phi-function) Let $m \in \mathbf{N}$. The **Euler phi-function**, denoted by $\varphi(m)$, is defined by

$$\varphi(m) = \#\{1 \leq n \leq m : (n, m) = 1\},$$

i.e., $\varphi(m)$ is the number of elements in a reduced system of residues modulo m .

Proposition 2.12 *If $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ is a reduced residue system modulo m , then so is the set $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$, for any integer a with $(a, m) = 1$.*

Theorem 2.13 (Euler's generalization of Fermat's theorem) *Let $m \in \mathbf{N}$. Then, for any integer a such that $(a, m) = 1$,*

$$(2.7) \quad a^{\varphi(m)} \equiv 1 \pmod{m}.$$