Elementary Number Theory
Math 17500, Section 30
Autumn Quarter 2008
John Boller, e-mail: boller@math.uchicago.edu
website: http://www.math.uchicago.edu/∼boller/M175

Congruence in the Integers

Definition 0.0.1 Fix $n \in \mathbb{Z}$ with $n > 1$. We say that two integers a and b are *congruent modulo* n and write $a \equiv b \pmod{n}$ provided that $n \mid (b - a)$.

Theorem 0.0.2 Fix $n > 1$. Then congruence (mod n) is an equivalence relation on $\mathbb{Z}$. That is:

(i) If $a \in \mathbb{Z}$, then $a \equiv a \pmod{n}$.

(ii) If $a, b \in \mathbb{Z}$, then $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$.

(iii) If $a, b, c \in \mathbb{Z}$ and $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Theorem 0.0.3 If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

(i) $a + c \equiv b + d \pmod{n}$

(ii) $a \cdot c \equiv b \cdot d \pmod{n}$

Theorem 0.0.4 If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{nc}$ for any $c > 0$.

Theorem 0.0.5 If $(a, n) = 1$, then there exists $b \in \mathbb{Z}$ such that $a \cdot b \equiv 1 \pmod{n}$.

Theorem 0.0.6 Given $c \in \mathbb{Z}$, if $(a, n) = 1$, then the congruence $ax \equiv c \pmod{n}$ has a solution for x in the integers.

Exercise 0.0.7 Solve the following congruences for x:

i. $3x \equiv 1 \pmod{7}$

ii. $8x \equiv 11 \pmod{19}$

iii. $25x + 1 \equiv 0 \pmod{127}$

iv. $22x \equiv 4 \pmod{94}$

Theorem 0.0.8 If $m = (a, n)$, then $ax \equiv ay \pmod{n}$ if and only if $x \equiv y \pmod{\frac{n}{m}}$.

Definition 0.0.9 If $a \equiv x \pmod{n}$, then x is called a *residue of a (mod n).*

Definition 0.0.10 A set of integers $\{x_1, \ldots, x_n\}$ is called a *complete residue system (mod n)* if, for every $a \in \mathbb{Z}$, there is exactly one x_i such that $a \equiv x_i \pmod{n}$.

Exercise 0.0.11 Show that a complete residue system (mod n) must, in fact, have n elements.

Definition 0.0.12 A set of integers $\{x_1, \ldots, x_j\}$ is called a *reduced residue system (mod n)* if, for every $a \in \mathbb{Z}$ such that $(a, n) = 1$, there is exactly one x_i such that $a \equiv x_i \pmod{n}$.

Exercise 0.0.13 Find a reduced residue system (mod n) for $n = 8, 10, 12, 20$.

Definition 0.0.14 If $n \in \mathbb{Z}$ and $n > 0$, then *Euler's ϕ-function* is denoted $\phi(n)$ and represents the number of elements of a reduced residue system (mod n).

Exercise 0.0.15 Show that $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

Theorem 0.0.16 Let $n > 0$ and suppose $(a, n) = 1$. Suppose $\{x_1, \ldots, x_{\phi(n)}\}$ is a reduced residue system (mod n). Then $\{ax_1, \ldots, ax_{\phi(n)}\}$ is also a reduced residue system (mod n).

Theorem 0.0.17 If $n = ab$ and $(a, b) = 1$, then $\phi(n) = \phi(a)\phi(b)$.

Exercise 0.0.18 Show that if p is prime, then $\phi(p^n) = (p-1)p^{n-1}$.

Exercise 0.0.19 Let $n > 1$, and let $P = \{p \in \mathbb{Z} \mid p \text{ is prime and } p|n\}$. Show that

$$\phi(n) = n \cdot \prod_{p \in P} \left(1 - \frac{1}{p}\right).$$

Definition 0.0.20 Fix $n > 1$. Let $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$. (Note that $\mathbb{Z}/n\mathbb{Z}$ is a complete residue system mod n.) Define addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ as follows:

$$a + b = x \text{ where } x \text{ is the unique element of } \mathbb{Z}/n\mathbb{Z} \text{ such that } a + b \equiv x \pmod{n}$$

$$ab = x \text{ where } x \text{ is the unique element of } \mathbb{Z}/n\mathbb{Z} \text{ such that } ab \equiv x \pmod{n}$$

Exercise 0.0.21 Show that addition and multiplication are well-defined in $\mathbb{Z}/n\mathbb{Z}$.

Exercise 0.0.22 Show that $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity for any $n > 1$.

Exercise 0.0.23 Show that $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is prime.

Exercise 0.0.24 Fix $n > 1$. Show that if $R = \{x_1, \ldots, x_{\phi(n)}\}$ is a reduced residue system (mod n), then R is a group under the law of composition:

$$x_i * x_j = x_k \text{ provided that } x_k \text{ is the unique element of } R \text{ such that } x_i x_j \equiv x_k \pmod{n}$$

Theorem 0.0.25 (Fermat's Little Theorem) If p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

Exercise 0.0.26 If p is prime and $a \in \mathbb{Z}$ with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 0.0.27 (Euler's Generalization) If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Theorem 0.0.28 Let p be prime. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

Theorem 0.0.29 (Wilson's Theorem) If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.
(Hint: It may be helpful to consider small primes such as $p = 2$ and $p = 3$ separately.)

Theorem 0.0.30 Let p be prime. Then the congruence $x^2 \equiv -1 \pmod{p}$ has solutions if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Theorem 0.0.31 Let q be a prime factor of $a^2 + b^2$. If $q \equiv 3 \pmod{4}$, then $q|a$ and $q|b$.

We state the next theorem before giving a sequence of lemmas that leads to its proof.

Theorem 0.0.32 Let p be a prime such that $p \equiv 1 \pmod 4$. Then there exist integers a, b such that

$$p = a^2 + b^2.$$

For the following lemmas through Lemma 37, assume the following:

Let p be prime such that $p \equiv 1 \pmod 4$.
Let k be the greatest integer less than $\sqrt{p}$, and let $S = \{0, 1, \ldots, k\}$.
Let x be an integer such that $x^2 \equiv -1 \pmod p$ (as per Thm. 30).

Lemma 0.0.33 $|S \times S| > p$.

Lemma 0.0.34 There exist two distinct pairs $(u_1, v_1), (u_2, v_2) \in S \times S$ such that

$$u_1 + xv_1 \equiv u_2 + xv_2 \pmod p.$$

With u_1, u_2, v_1, v_2 from the preceding lemma, let $a = u_1 - u_2$ and $b = v_1 - v_2$.

Lemma 0.0.35 $a^2 + b^2 \equiv 0 \pmod p$.

Lemma 0.0.36 $0 < a^2 + b^2 < 2p$.

Lemma 0.0.37 $p = a^2 + b^2$.

Theorem 0.0.38 For any integers (or real numbers, for that matter),

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Theorem 0.0.39 Let n be an integer greater than 1. Suppose $n = 2^\alpha \cdot p_1^{\beta_1} \cdots p_k^{\beta_k} \cdot q_1^{\gamma_1} \cdots q_\ell^{\gamma_\ell}$, where the p_i are the primes that are congruent to 1 (mod 4) and the q_j are the primes congruent to 3 (mod 4). Then n may be written as the sum of two squares (of integers, of course) if and only if all of the exponents $\gamma_1, \ldots, \gamma_\ell$ are even.
(Hint: Combine Theorems 31, 32, and 38.)

Theorem 0.0.40 (The Chinese Remainder Theorem)
Let $m_1, \ldots, m_r$ denote r integers that are pairwise relatively prime, and let $a_1, \ldots, a_r$ be any integers. Then the set of r simultaneous congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a solution for x in the integers. Moreover, if x_0 is one solution, then every solution is of the form $x = x_0 + k(m_1 \cdots m_r)$ for some integer k.