Elementary Number Theory

Math 175, Section 30, Autumn 2010

Shmuel Weinberger (shmuel@math.uchicago.edu)

Tom Church (tchurch@math.uchicago.edu)

www.math.uchicago.edu/~tchurch/teaching/175/

Script 3: Congruence in the Integers

Definition 3.1. 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 3.2. Fix $n > 1$. Then congruence modulo 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 3.3. 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 3.4. If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{nc}$ for any $c > 0$.

Theorem 3.5. If $(a, n) = 1$, then there exists $b \in \mathbb{Z}$ such that $a \cdot b \equiv 1 \pmod{n}$.

Theorem 3.6. 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 3.7. Solve the following congruences for x:

a) $3x \equiv 1 \pmod 7$

b) $8x \equiv 11 \pmod{23}$

c) $25x + 1 \equiv 0 \pmod{126}$

d) $22x \equiv 2 \pmod{178}$

Theorem 3.8. If a and n are relatively prime, then

$$ax \equiv ay \pmod n \quad \text{if and only if} \quad x \equiv y \pmod n.$$

Theorem 3.9. If $m = (a, n)$, then

$$ax \equiv ay \pmod n \quad \text{if and only if} \quad x \equiv y \pmod{\frac{n}{m}}.$$

Definition 3.10. A number system (a collection of elements equipped with an addition operation and a multiplication operation) is called a *commutative ring with identity* (sometimes just called a *ring* if the context is clear) if it satisfies Axioms A1–A5, M1–M4, and D.

Definition 3.11. A number system is called a *field* if it satisfies Axioms A1–A5, M1–M4, and D (i.e. it is a ring), and in addition satisfies Axiom M5, which states that every nonzero element has a multiplicative inverse:

M5. (Multiplicative Inverses) For each nonzero element $a \neq 0$, there is a unique element a^{-1} such that $a \cdot a^{-1} = 1$ and $a^{-1} \cdot a = 1$.

Definition 3.12. Fix $n \in \mathbb{Z}$ with $n > 1$. For an integer $a \in \mathbb{Z}$, the *residue class of* a *modulo* n, or sometimes just the *residue class of* a, is the set of all integers congruent to $a \pmod n$:

$$[a] = \left\{ b \in \mathbb{Z} \;\middle|\; a \equiv b \pmod n \right\}$$

Exercise 3.13. Given $a, b \in \mathbb{Z}$, we have

$$[a] = [b] \quad \text{if and only if} \quad a \equiv b \pmod n$$

Theorem 3.14. The number of distinct residue classes modulo n is n.

Theorem 3.15. If $[a] = [b]$, then $(a, n) = (b, n)$.

Definition 3.16. Fix $n > 1$. We define the number system $\mathbb{Z}/n\mathbb{Z}$ to be the set of residue classes modulo n. We define addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ as follows:

$$[a] + [b] = [a + b] \qquad \text{for } a, b \in \mathbb{Z}$$
$$[a] \cdot [b] = [a \cdot b] \qquad \text{for } a, b \in \mathbb{Z}$$

Theorem 3.17. Show that addition and multiplication are well-defined in $\mathbb{Z}/n\mathbb{Z}$.

Exercise 3.18. Check that $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity for any $n > 1$.

Theorem 3.19. Show that $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is prime.

Theorem 3.20. If p is prime and $a, b \in \mathbb{Z}/p\mathbb{Z}$, then $a \neq 0$ and $b \neq 0$ implies $ab \neq 0$.

Definition 3.21. If R is a commutative ring with identity, then an element $x \in R$ is called a *unit* if x has a multiplicative inverse in R. We write $R^\times$ (pronounced "R-cross") for the set of invertible elements:

$$R^\times = \{x \in R \,|\, x \cdot y = 1 \text{ for some } y \in R\}$$

Theorem 3.22. For any ring R, the set $R^\times$ is closed under multiplication.

Theorem 3.23 (Wilson's Theorem)**.** If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.
(It may be helpful to consider $p = 2$ as a separate case.)

Exercise 3.24. If p is prime and $a \in \mathbb{Z}/p\mathbb{Z}$ is nonzero, the sets

$$\{x \,|\, x \in \mathbb{Z}/p\mathbb{Z}, x \neq 0\} \quad \text{and} \quad \{ax \,|\, x \in \mathbb{Z}/p\mathbb{Z}, x \neq 0\} \quad \text{are equal.}$$

Theorem 3.25. If p is prime and $a \in \mathbb{Z}$ with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 3.26 (Fermat's Little Theorem)**.** If p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

Theorem 3.27. Let p be prime. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

Theorem 3.28. Let p be an odd prime. Then the congruence $x^2 \equiv -1 \pmod{p}$ has solutions if and only if $p \equiv 1 \pmod{4}$.

Exercise 3.29. If q is prime and $q \equiv 3 \pmod{4}$, and $d \in \mathbb{Z}/q\mathbb{Z}$, then d and $-d$ cannot both be squares[1] in $\mathbb{Z}/q\mathbb{Z}$.

Theorem 3.30. Let q be a prime factor of $a^2 + b^2$. If $q \equiv 3 \pmod{4}$, then $q|a$ and $q|b$.

[1] As you would expect, an element of a ring is called a *square* if it is equal to y^2 for some element y.

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

Theorem 3.31. If p is a prime such that $p \equiv 1 \pmod 4$, there exist integers a, b such that

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

For Lemmas 3.32 through 3.35, 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 3.32. $|S \times S| > p$.

Lemma 3.33. 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 3.34. $a^2 + b^2 \equiv 0 \pmod p$.

Lemma 3.35. $0 < a^2 + b^2 < 2p$.

Theorem 3.31. $p = a^2 + b^2$.

Exercise 3.36. For any integers (or real numbers, for that matter),

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

Theorem 3.37. 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 prime factors 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 3.30, 3.31, and 3.36.)

Theorem 3.38 (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.