Chapter 3

Congruence

3.1 Congruent Integers

In this section n denotes a positive integer.

Definition 3.1.1. Let n, a and b be integers. If n divides $a - b$, we say that a and b are *congruent modulo* n, and we write

$$a \equiv b \pmod{n} \ .$$

Example 3.1.2. From the definition: $17 \equiv 2 \pmod{5}$ and $-17 \equiv 3 \pmod{5}$.

Proposition 3.1.3.[*] Let a and b be integers. Then $a \equiv b \pmod{n}$ if, and only if, a and b leave the same remainder when divided by n.

Proposition 3.1.4. Let a, b and c be integers. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proposition 3.1.5. Let a, b, c and d be integers. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n} \ .$$

Proposition 3.1.6. Let a, b, c and d be integers. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$ac \equiv bd \pmod{n} \ .$$

Proposition 3.1.7. Let a and b be integers. If $a \equiv b \pmod{n}$, then

$$\gcd(a, n) \equiv \gcd(b, n) \pmod{n} \ .$$

Proposition 3.1.8.[*] Let $a_1, a_2, \ldots, a_r$ and $b_1, b_2, \ldots, b_r$ be integers, with $r > 1$. Suppose that

$$a_i \equiv b_i \pmod{n}$$

for each value of i. Then

$$a_1 + a_2 + \cdots + a_r \equiv b_1 + b_2 + \cdots + b_r \pmod{n},$$
$$a_1 a_2 \cdots a_r \equiv b_1 b_2 \cdots b_r \pmod{n} \ .$$

3.2 Decimal Representation

Definition 3.2.1. We assume in this section that every positive integer has a unique decimal representation. Let a be a positive integer with *decimal representation*

$$a = d_r d_{r-1} \cdots d_1 d_0 \ .$$

That is, r is a non-negative integer, for each i the integer d_i is between 0 and 9, $d_r \neq 0$, and

$$a = d_0 + d_1 10 + d_2 10^2 + \cdots + d_r 10^r \ .$$

The *digit sum* s, the *alternating digit sum* t, and the *units digit* u are given by:

$$\begin{aligned} s &= d_0 + d_1 + \cdots + d_r, \\ t &= d_0 - d_1 + \cdots + (-1)^r d_r, \\ u &= d_0 \ . \end{aligned}$$

Proposition 3.2.2 (Strong Rule of 10).* In Definition 3.2.1, $a \equiv u \pmod{10}$.

Proposition 3.2.3 (Strong Rule of 9). In Definition 3.2.1, $a \equiv s \pmod{9}$.

Proposition 3.2.4 (Strong Rule of 11). In Definition 3.2.1, $a \equiv t \pmod{11}$.

Proposition 3.2.5 (Strong Rule of 6). In Definition 3.2.1, $a \equiv 4s - 3u \pmod{6}$.

3.3 Solving Congruences

In this section n denotes a positive integer.

Definition 3.3.1. Let a and b be integers. We say that a and b are *multiplicative inverses modulo* n if $ab \equiv 1 \pmod{n}$.

Proposition 3.3.2. Let a be an integer that is relatively prime to n. Then there exists an inverse for a modulo n.

Definition 3.3.3. Two congruences in one or more variables are *equivalent*, which will be indicated by the symbol $\Leftrightarrow$, if they are both true for exactly the same values of the variables.

Proposition 3.3.4.* Let h be a positive integer. Then

$$x \equiv y \pmod{n} \quad \Leftrightarrow \quad hx \equiv hy \pmod{hn} \ .$$

Proposition 3.3.5. Let n and h be relatively prime integers. Then

$$x \equiv y \pmod{n} \quad \Leftrightarrow \quad hx \equiv hy \pmod{n} \ .$$

Definition 3.3.6. By solving a congruence of the form $ax \equiv b \pmod{n}$ we mean to find integers c and m such that $0 \leq c \leq m-1$ and

$$ax \equiv b \pmod{n} \quad \Leftrightarrow \quad x \equiv c \pmod{m} \ .$$

Example 3.3.7. Consider the congruence:

$$46x \equiv 106 \pmod{36} \ .$$

The congruences below are equivalent to each other:

(a) $46x \equiv 106 \pmod{36}$

(b) $10x \equiv 34 \pmod{36}$ by the results of Section 3.1.

(c) $5x \equiv 17 \pmod{18}$ by Proposition 3.3.4 with $h = 2$.

(d) $55x \equiv 187 \pmod{18}$ by Proposition 3.3.5 with $h = 11$, which is relatively prime to 18.

(e) $x \equiv 7 \pmod{18}$.

That is,

$$46x \equiv 106 \pmod{36} \quad \Leftrightarrow \quad x \equiv 7 \pmod{18} \ .$$

The inverse of 5 modulo 18 was found by trial and error. A general method exists and will be illustrated with an example after Section 3.5.

Exercise 3.3.8. If possible, solve the congruence $28x \equiv 35 \pmod{40}$.

Exercise 3.3.9. If possible, solve the congruence $28x \equiv 36 \pmod{40}$.

3.4 Prime Modulus

Proposition 3.4.1. Let p be a prime and let a be an integer not divisible by p. Then no two of the integers

$$a, 2a, 3a, \ldots, pa$$

are congruent modulo p.

Theorem 3.4.2 (Fermat's Little Theorem).* Let p be a prime and let a be an integer not divisible by p. Then

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

Proposition 3.4.3. Let p be a prime and let a be any integer. Then

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

Proposition 3.4.4. Let p be a prime greater than 3 and let a be an integer such that $1 < a < p-1$. Then there exists a unique integer b such that b is a multiplicative inverse for a modulo p and $1 < b < p-1$. Moreover, $b \neq a$.

Example 3.4.5. Here are the pairs of multiplicative inverses for the prime $p = 13$:

$$2 \text{ and } 7, \qquad 3 \text{ and } 9, \qquad 4 \text{ and } 10, \qquad 5 \text{ and } 8, \qquad 6 \text{ and } 11 \ .$$

Theorem 3.4.6 (Wilson's Theorem)**.** If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proposition 3.4.7.* Let k and m be positive integers and suppose that $p = k + m + 1$ is a prime. If k and m are both odd, then

$$k!m! \equiv 1 \pmod{p} \ .$$

If k and m are both even, then

$$k!m! \equiv -1 \pmod{p} \ .$$

Exercise 3.4.8. Use Theorem 3.4.2 to find the remainder left by 2^{100} when divided by 19.

Exercise 3.4.9. Use Proposition 3.4.7 and an inverse to reduce 97! modulo 101.

3.5 Systems of Congruences

Definition 3.5.1. Let $n_1, n_2, \ldots, n_r$ be positive integers and let $a_1, a_2, \ldots, a_r$ be integers. In this section, the expression

$$x \equiv a_1, a_2, \ldots, a_r \pmod{n_1, n_2, \ldots, n_r}$$

means that $x \equiv a_i \pmod{n_i}$ for $i = 1, 2, \ldots, r$.

Proposition 3.5.2. Let $n_1, n_2, \ldots, n_r$ be positive integers and let $m = n_1 n_2 \cdots n_r$. Suppose, for each i, that b_i is an inverse for $\frac{m}{n_i}$ modulo n_i. If $a_1, a_2, \ldots, a_r$ are integers and

$$c = a_1 b_1 \frac{m}{n_1} + a_2 b_2 \frac{m}{n_2} + \cdots + a_r b_r \frac{m}{n_r} \ ,$$

then

$$c \equiv a_1, a_2, \ldots, a_r \pmod{n_1, n_2, \ldots, n_r} \ .$$

Proposition 3.5.3. Let $r > 1$ and let $n_1, n_2, \ . \ . \ . \ , n_r$ be positive integers, each two of which are relatively prime. Let $m = n_1 n_2 \cdots n_r$. If b is an integer and b is divisible by each of the n_i, then b is divisible by m.

Theorem 3.5.4 (The Chinese Remainder Theorem)**.** Let $r > 1$ and let $n_1, n_2, \ldots, n_r$ be positive integers, each two of which are relatively prime. Set $m = n_1 n_2 \cdots n_r$. If $a_1, a_2, \ldots, a_r$ are any integers, then there exists an integer c such that

$$x \equiv a_1, a_2, \ldots, a_r \pmod{n_1, n_2, \ldots, n_r} \quad \Leftrightarrow \quad x \equiv c \pmod{m} \ .$$

Exercise 3.5.5. Use Proposition 3.5.2 and Theorem 3.5.4 to find c and m such that $0 < c < m$ and

$$x \equiv 2, 5, 6 \pmod{5, 7, 9} \quad \Leftrightarrow \quad x \equiv c \pmod{m} \ .$$

3.6 Several Examples

Example 3.6.1. The object is to find an inverse for 55 modulo 127. We construct a Euclidean array, related to the one in Chapter 2

$$\begin{array}{ccccc} 127 & 55 & 17 & 4 & 1 \\ & 2 & 3 & 4 & \\ 30 & 13 & 4 & 1 & 0 \end{array} .$$

Hence, $127 \cdot 13 - 55 \cdot 30 = 1$. This can be written as $55(-30) \equiv 1 \pmod{127}$. Thus, -30 is a multiplicative inverse for 55 modulo 127. So is $-30 + 127 = 97$. That is,

$$55 \cdot 97 \equiv 1 \pmod{127} .$$

Example 3.6.2. Consider the congruence

$$550x \equiv 130 \pmod{635} .$$

The congruences below are equivalent to each other:

(a) $550x \equiv 130 \pmod{635}$

(b) $110x \equiv 26 \pmod{127}$ dividing through by 5.

(c) $55x \equiv 13 \pmod{127}$ dividing on the left by 2.

(d) $97 \cdot 55x \equiv 97 \cdot 13 \pmod{127}$ using the result in Example 3.6.1.

(e) $x \equiv 118 \pmod{127}$.

The conclusion is:

$$550x \equiv 130 \pmod{635} \quad \Leftrightarrow \quad x \equiv 118 \pmod{127} .$$

Example 3.6.3. Consider the system

$$x \equiv 4, 5, 6 \pmod{7, 8, 9} .$$

Since $7, 8$ and 9 are pairwise relatively prime, Proposition 3.5.2 can be used to solve the system. We have:

$$n_1 = 7,\ n_2 = 8,\ n_3 = 9, \quad m = 7 \cdot 8 \cdot 9 = 504 .$$

The quotients specified in Proposition 3.5.2 are:

$$\frac{m}{7} = 8 \cdot 9 = 72, \quad \frac{m}{8} = 63, \quad \frac{m}{9} = 56 .$$

Before looking for inverses, it helps to reduce each $\dfrac{m}{n_i}$ modulo n_i:

$$72 \equiv 2 \pmod{7}, \qquad 63 \equiv 7 \pmod{8}, \qquad 56 \equiv 2 \pmod{9} .$$

By inspection, the least positive inverses are:

$$4 \text{ modulo } 7, \quad 7 \text{ modulo } 8, \quad 5 \text{ modulo } 9 .$$

By Proposition 3.5.3, one solution of the system is given by

$$c = 4 \cdot 4 \cdot 72 + 5 \cdot 7 \cdot 63 + 6 \cdot 5 \cdot 56 = 5037 .$$

This reduces to 501 modulo 504. By the Chinese Remainder Theorem,

$$x \equiv 4, 5, 6 \pmod{7, 8, 9} \quad \Leftrightarrow \quad x \equiv 501 \pmod{504} .$$

Example 3.6.4. Again consider the system in Example 3.6.3. One easily sees that $x = -3$ is a solution. By the Chinese Remainder Theorem,

$$x \equiv 4, 5, 6 \pmod{7, 8, 9} \quad \Leftrightarrow \quad x \equiv -3 \pmod{504} .$$

3.7 Problems

Problem 3.7.1. Find a multiplicative inverse for 1488 modulo 3409.

Problem 3.7.2. Solve: $140x \equiv 126 \pmod{301}$.

Problem 3.7.3. Reduce 5^{6789} modulo 17.

Problem 3.7.4. Let $c = 2^{100}$. Reduce c modulo both 8 and 9, and then reduce c modulo 72.

Problem 3.7.5. Show that $a^{13} \equiv a \pmod{35}$ for all integers a.

Problem 3.7.6. By convention, 2^{3^4} equals 2^{81} and not 8^4. Reduce $2^{3^{4^{5^{6^{7^{8^9}}}}}}$ modulo 13.

Problem 3.7.7. Show that there does not exist an integer x such that $x \equiv 5, 7 \pmod{6, 15}$.

Problem 3.7.8. Seventeen pirates tried to divide a bag of gold coins into equal parts, but 3 coins were left over. After a discussion, 16 pirates tried to divide the coins equally, but 10 were left over. Further discussion allowed 15 pirates to divide the coins into equal parts. How many coins were in the bag?

3.8 Projects

Project 3.8.1. Devise a Strong Rule of 99, similar to the Strong Rule of 6, that uses a linear combination of s and t.

Project 3.8.2. Devise a Strong Rule of 37.

Project 3.8.3. For a composite integer n, reduce $(n-1)!$ modulo n.

Project 3.8.4. Let p be an odd prime. Reduce $(p-2)!$ and $(p-3)!$ modulo p.

Project 3.8.5. Devise a useful method for determining whether $ax \equiv b \pmod{n}$ has a solution.

Project 3.8.6. Devise a useful method for determining whether the system

$$x \equiv a, b \pmod{m, n}$$

has a solution.

3.9 Proofs and Suggestions

Proof of Proposition 3.1.3.

(1) Let n, a and b be integers.

(2) Let q_1, q_2, r_1 and r_2 be the integers specified in Proposition 1.4.1:

$$a = q_1 n + r_1,\ b = q_2 n + r_2,\ 0 \le r_1 \le n-1,\ 0 \le r_2 \le n-1.$$

(3) $a - b = (q_1 - q_2)n + (r_1 - r_2)$.

(4) By (3), $n|(a-b) \quad \Leftrightarrow \quad n|(r_1 - r_2)$.

(5) By (2) and (4), $a \equiv b \pmod{n} \quad \Leftrightarrow \quad r_1 = r_2$ □

Suggestion for Proposition 3.1.6. Notice that $ac - bd = (a-b)c + b(c-d)$.

Proof of Proposition 3.1.8*, Informal proof.* Let $a_1, a_2, \ldots, a_r$ and $b_1, b_2, \ldots, b_r$ be integers with $r > 1$ and $a_1 \equiv b_i \pmod{n}$ for all i. We shall deal with the sum first. By Proposition 3.1.5, $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$. If $r = 2$, we are done. If $r > 2$, then $a_1 + a_2 + a_3 = (a_1 + a_2) + a_3$ and $b_1 + b_2 + b_3 = (b_1 + b_2) + b_3$ and, by Proposition 3.1.5 again, $(a_1 + a_2) + a_3 \equiv (b_1 + b_2) + b_3 \pmod{n}$. This can continue until we have $a_1 + \cdots + a_r \equiv b_1 + \cdots + b_r \pmod{n}$. The argument for product is analogous, using Proposition 3.1.6. □

Proof of Proposition 3.2.2.

(1) Let a be as in Definition 3.2.1.

(2) $a = d_0 + d_1 10 + \cdots + d_r 10^r$.

(3) $u = d_0$

(4) By Proposition 3.1.8, $a \equiv u + d_1 0 + \cdots + d_r 0^r \pmod{10}$.

(5) $a \equiv u \pmod{10}$. □

Proof of Proposition 3.3.4.

(1) Let h be positive integer.

(2) The following statements are equivalent:

  (i) $x \equiv y \pmod{n}$.
  (ii) $n|(x - y)$.

(iii) $hn|h(x-y)$.

(iv) $hn|(hx-hy)$.

(v) $hx \equiv hy \pmod{hn}$. □

Proof of Proposition 3.4.2, *Informal proof.* Let p be a prime and let a be an integer not divisible by p. Consider the integers $a, 2a, \ldots, (p-1)a$. By Proposition 3.4.1, they leave remainders, in some order, of $1, 2, \ldots, p-1$ when divided by p. By Proposition 3.1.8,

$$a \cdot 2a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod{p} .$$

That is,

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

But $(p-1)!$ and p are relatively prime. By Proposition 3.3.5

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

□

Suggestion for Proposition 3.4.3. Consider two cases: a is divisible by p, and a is not divisible by p.

Suggestion for Proposition 3.4.4. Use Definition 3.3.1 to get an inverse c for a modulo p. Let b be the remainder left by c when divided by p. Show that b does not equal 0, 1 or $p-1$. Then show that $b \neq a$.

Suggestion for Theorem 3.4.6. First, verify that the statement is true for p equal to 2 or 3. Then, suppose that $p \geq 5$. By Proposition 3.4.4, the numbers $2, 3, \ldots, p-2$ can be grouped in pairs of multiplicative inverses. Conclude that

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \pmod{p} .$$

Proof of Proposition 3.4.7. Let k and m be positive integers and set $p = k + m + 1$. Suppose that p is prime. Using the fact that $k + 1 = p - m$, we have:

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot \cdots \cdot k \cdot (k+1) \cdot (k+2) \cdots (k+m) \\ &= k!(p-m) \cdots (p-1) \\ &= k!(p-1)(p-2) \cdots (p-m) \\ &= (-1)^m k!(1-p)(2-p) \cdots (m-p) .\end{aligned}$$

Since $p \,\big|\, \big(m! - (1-p)(2-p) \cdots (m-p)\big)$ we have

$$(p-1)! \equiv (-1)^m k!m! \pmod{p} .$$

By Wilson's Theorem,

$$-1 \equiv (-1)^m k!m! \pmod{p} .$$

Therefore, $k!m!$ is congruent to 1 if m is odd and to -1 if m is even. Since p is a prime greater than 2, it is odd, and so $k + m$ is even, which implies that k and m have the same parity. □

Suggestion for Proposition 3.5.3. Let b be a common multiple of n_i. Use Proposition 2.2.10 to show that $n_1n_2|b$. If $r > 2$, use Proposition 2.2.9 to show that n_1n_2 and n_3 are relatively prime, and use Proposition 2.2.10 to show that $n_1n_2n_3|b$.

Suggestion for Theorem 3.5.4. Use Propositions 3.3.2, 3.5.2 and 3.5.3.

Comments

1. Most of the results in this chapter were known before 1800, but were not expressed in the notation of congruences. That notation was introduced by Gauss in 1801.

2. The Rule of 9 says that a is divisible by 9 if, and only if, s is divisible by 9. The Rule of 9 follows from Proposition 3.2.3, but does not imply Proposition 3.2.3.

3. Solving the congruence $ax \equiv b \pmod{n}$ is essentially the same as solving the Diophantine equation $ax + ny = b$.

4. There is such a thing as Fermat's Big (or Last) Theorem:

Let n be an integer greater than 2. Then there do not exist positive integers x, y and z such that

$$x^n + y^n = z^n \ .$$

5. Problems such as Theorem 3.5.4, though stated in a different way, were considered by both the Chinese and the Greeks nearly 2000 years ago.