MATH 324 Summer 2010
Elementary Number Theory

Notes on Congruences

In this note we will discuss the congruence relation on the set of integers, in particular we will develop an arithmetic of remainders similar (but not identical) to the usual arithmetic on the set of integers. First the definitions.

Definition. Let $n \in \mathbb{Z}^+$, $n > 1$, for $a, b \in \mathbb{Z}$ we say that a is **congruent** to b **modulo** n, and we write $a \equiv b \pmod{n}$, or $a \equiv_n b$ if and only if $a - b$ is a multiple of n, that is, if and only if

$$a = b + k \cdot n$$

for some $k \in \mathbb{Z}$.

The first theorem shows that the relation $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

Theorem 1. If $n \in \mathbb{Z}^+$, $n > 1$, then

(a) $a \equiv a \pmod{n}$ for each $a \in \mathbb{Z}$. (reflexivity)

(b) $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$ for all $a, b \in \mathbb{Z}$. (symmetry)

(c) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$ for all $a, b, c \in \mathbb{Z}$. (transitivity)

Proof.

(a) If $a \in \mathbb{Z}$, then $a - a = 0 = 0 \cdot n$, so that $a \equiv a \pmod{n}$.

(b) If $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{n}$, then $a - b = k \cdot n$ for some $k \in \mathbb{Z}$, and so $b - a = (-k) \cdot n$, so that $b \equiv a \pmod{n}$ also.

(c) If $a, b, c \in \mathbb{Z}$, with $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a - b = k \cdot n$ and $b - c = \ell \cdot n$, for some $k, \ell \in \mathbb{Z}$, so that $a - c = a - b + b - c = (k + \ell) \cdot n$, and $a \equiv c \pmod{n}$.

□

The next result says that two integers a and b are congruent modulo n if and only if a and b leave the same remainder when the division algorithm is employed to divide them by n.

Theorem 2. If $n \in \mathbb{Z}^+$, $n > 1$, and $a, b \in \mathbb{Z}$, then $a \equiv b \pmod{n}$ if and only if a and b leave the same least nonnegative remainder when divided by n.

Proof. Suppose that a and b leave the same least nonnegative remainders when divided by n, then from the division algorithm we can write (uniquely)

$$a = k \cdot n + r \qquad \text{and} \qquad b = \ell \cdot n + r$$

where $k, \ell, r \in \mathbb{Z}$ and $0 \leq r < n$, so that

$$a - b = k \cdot n + r - (\ell \cdot n + r) = (k - \ell) \cdot n$$

and thus, $a \equiv b \pmod{n}$.

Conversely, suppose that $a \equiv b \pmod{n}$. From the division algorithm we can write (uniquely)

$$a = k \cdot n + r$$

where k, $r \in \mathbb{Z}$ and $0 \leq r < n$.

Since $a \equiv b \pmod{n}$, then $a - b = \ell \cdot n$ for some $\ell \in \mathbb{Z}$, so that

$$b = a - \ell \cdot n = k \cdot n - \ell \cdot n + r = (k - \ell) \cdot n + r$$

where $0 \leq r < n$, and therefore a and b leave the same least nonnegative remainder when divided by n.

□

From the division algorithm, when an integer a is divided by the positive integer $n > 1$, we have

$$a = k \cdot n + r$$

where $0 \leq r < n$.

Thus, the only possible least nonnegative remainders are

$$0,\ 1,\ 2,\ \ldots,\ n-1$$

and the congruence relation $\equiv_n$ partitions the set of integers $\mathbb{Z}$ into the union of n pairwise disjoints sets, called **congruence classes**

$$\mathbb{Z} = [\,0\,] \cup [\,1\,] \cup [\,2\,] \cup \cdots \cup [\,n-1\,],$$

where

$$\begin{aligned}
[\,0\,] &= \{\, 0 + n \cdot x \,|\, x \in \mathbb{Z} \,\} \\
[\,1\,] &= \{\, 1 + n \cdot x \,|\, x \in \mathbb{Z} \,\} \\
[\,2\,] &= \{\, 2 + n \cdot x \,|\, x \in \mathbb{Z} \,\} \\
&\vdots \\
[\,n-1\,] &= \{\, n - 1 + n \cdot x \,|\, x \in \mathbb{Z} \,\}
\end{aligned}$$

Note that for $0 \leq r \leq n-1$, the congruence class containing r, denoted by $[\,r\,]$, consists of precisely those integers x such that $x \equiv r \pmod{n}$; and each integer $x \in \mathbb{Z}$, is in exactly one of the congruence classes $[\,0\,]$, $[\,1\,]$, $[\,2\,]$, $\ldots$, $[\,n-1\,]$.

Example 1. If $n = 2$, then there are two congruence classes modulo 2, namely

$$[\,0\,] = \{\ldots,\ -4,\ -2,\ 0,\ 2,\ 4,\ \ldots\}$$

and

$$[\,1\,] = \{\ldots,\ -3,\ -1,\ 1,\ 3,\ \ldots\}$$

that is, the **even** integers, and the **odd** integers.

Since $\mathbb{Z} = [\,0\,] \cup [\,1\,]$ and $[\,0\,] \cap [\,1\,] = \emptyset$, we have another proof of the fact that every integer is either even or odd, and no integer is both even and odd.

□

Example 2. If $n = 3$, then there are three congruence classes modulo 3, namely

$$[\,0\,] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[\,1\,] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[\,2\,] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

since there are only three possible least nonnegative remainders when an integer is divided by 3.

Thus, every integer n has exactly one of the forms

$$n = 3k, \qquad \text{or} \qquad n = 3k + 1, \qquad \text{or} \qquad n = 3k + 2$$

for some integer k.

We can use this to prove the following result:

$$\forall n \in \mathbb{Z}^+ \left[(\text{prime}(n) \wedge \text{prime}(n^2 + 2)) \rightarrow \text{prime}(n^2 - 2)\right]$$

where the statement prime(n) has the intended meaning that n is a prime number.

To see that this is true, we note that

- if $n = 3$ then $n^2 + 2 = 11$, and $n^2 - 2 = 7$, and since 3, 7, 11 are all prime numbers, then the implication

  $$(\text{prime}(n) \wedge \text{prime}(n^2 + 2)) \rightarrow \text{prime}(n^2 - 2)$$

  is true for $n = 3$.
- if $n > 3$ and $n \equiv 0 \,(\text{mod}\, 3)$ then $n = 3k$ for some integer $k > 1$, and n is not prime, and thus prime$(n) \wedge$ prime$(n^2 + 2)$ is false, so the implication is true for $n \equiv 0 \,(\text{mod}\, 3)$, and $n > 3$.
- if $n \equiv 1 \,(\text{mod}\, 3)$ then $n = 3k + 1$ for some integer k, so that

  $$n^2 + 2 = (3k + 1)^2 + 2 = 9k^2 + 6k + 3 = 3(3k^2 + 2k + 1)$$

  and $n^2 + 2$ is not prime, thus, prime$(n) \wedge$ prime$(n^2 + 2)$ is false, so the implication is also true for $n \equiv 1 \,(\text{mod}\, 3)$.
- if $n \equiv 2 \,(\text{mod}\, 3)$ then $n = 3k + 2$ for some integer k, so that

  $$n^2 + 2 = (3k + 2)^2 + 2 = 9k^2 + 12k + 6 = 3(3k^2 + 4k + 2)$$

  and $n^2 + 2$ is not prime, thus, prime$(n) \wedge$ prime$(n^2 + 2)$ is false, so the implication is also true for $n \equiv 2 \,(\text{mod}\, 3)$.

Since this exhausts all possibilities, then

$$\forall n \in \mathbb{Z}^+ \left[(\text{prime}(n) \wedge \text{prime}(n^2 + 2)) \rightarrow \text{prime}(n^2 - 2)\right]$$

is a true statement.

□

If $n > 1$ is a positive integer, we use $\mathbb{Z}_n$ to denote the set

$$\mathbb{Z}_n = \{\, [0], [1], [2], \ldots, [n-1] \,\}$$

of distinct congruence classes modulo n. If there is no danger of ambiguity, we often write

$$\mathbb{Z}_n = \{\, 0, 1, 2, \ldots, n-1 \,\}.$$

Addition and multiplication of congruence classes can be defined as follows, for $a, b \in \mathbb{Z}$,

$$[a] + [b] = [a+b] \qquad \text{and} \qquad [a] \cdot [b] = [a \cdot b],$$

and we leave it as an exercise to show that these operations are well-defined. In fact, these definitions of addition and multiplication give the set $\mathbb{Z}_n$ the structure of a commutative ring with identity.

The next results show that congruence behaves the same way as equality with respect to addition and multiplication, and the first theorem shows when congruence of two integers modulo $n > 1$ implies that the integers are, in fact, equal.

Theorem 3. If $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$ with $0 \leq a, b < n$, and $a \equiv b \pmod{n}$, then $a = b$.

Proof. Since $a \equiv b \pmod{n}$ there exists an integer k such that $a - b = k \cdot n$, and since $0 \leq a, b \leq n-1$, then we have

$$0 \leq a \leq n-1 \qquad \text{and} \qquad -(n-1) \leq -b \leq 0,$$

and adding these two inequalities we get

$$-(n-1) \leq a - b \leq n-1.$$

But if $a - b$ is a multiple of n and $-(n-1) \leq a - b \leq n-1$, then we must have $a - b = 0$, since there is only one multiple of n between $-(n-1)$ and $n-1$, namely, $0 \cdot n$. Therefore, $a = b$.

□

Theorem 4. If $n > 1$ is a positive integer and $a, b, c, d, \in \mathbb{Z}$ with $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

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

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

Proof. Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ there exist integers k and ℓ such that

$$a - b = k \cdot n \qquad \text{and} \qquad c - d = \ell \cdot n,$$

and therefore

$$a + c - (b + d) = a - b + c - d = k \cdot n + \ell \cdot n = (k + \ell) \cdot n,$$

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

Also,

$$a \cdot c - b \cdot d = a \cdot c - b \cdot c + b \cdot c - b \cdot d = (a - b)d + b(c - d) = (k \cdot d + b \cdot \ell)n,$$

so that $a \cdot c \equiv b \cdot d \pmod{n}$.

□

Example 3. Find the least nonnegative remainder when 5^{110} is divided by 6.

Solution. First we note that $5 \equiv -1 \pmod 6$, and using the previous theorem, we have

$$\begin{aligned} 5^2 &\equiv (-1)^2 \pmod 6 \\ 5^3 &\equiv (-1)^3 \pmod 6 \\ 5^4 &\equiv (-1)^4 \pmod 6 \\ &\vdots \\ 5^{110} &\equiv (-1)^{110} \pmod 6 \end{aligned}$$

and therefore $5^{110} \equiv 1 \pmod 6$, and there exists an integer k such that $5^{110} = 6k + 1$.

□

Congruences may behave the same way with respect to addition and multiplication, but not with respect to division. The next example shows that the cancellation law, which held for the integers, is no longer true for congruences.

Example 4. Note that

$$5 \cdot 10 \equiv 2 \cdot 10 \pmod{15},$$

since

$$50 - 20 = 30 = 2 \cdot 15.$$

However, we cannot cancel the 10 in this congruence, since $5 - 2 = 3$ is not a multiple of 15, that is,

$$5 \not\equiv 2 \pmod{15}.$$

□

We do, however, have the following results.

Theorem 5. Let $n \in \mathbb{Z}^+$ and a, b, $c \in \mathbb{Z}$, with $d = \gcd(c, n)$, if $a \cdot c \equiv b \cdot c \pmod n$, then $a \equiv b \pmod{\frac{n}{d}}$.

Proof. If $a \cdot c \equiv b \cdot c \pmod n$ then there exists an integer k such that $a \cdot c - b \cdot c = k \cdot n$, that is, $c(a-b) = k \cdot n$, and therefore

$$\frac{c}{d}(a - b) = k \cdot \frac{n}{d}.$$

Since $\gcd\left(\frac{c}{d}, \frac{n}{d}\right) = 1$, then $\frac{n}{d} \mid a - b$, that is, $a \equiv b \pmod{\frac{n}{d}}$.

□

In particular, we have the folllowing corollary:

Corollary 6. Let $n \in \mathbb{Z}^+$ and a, b, $c \in \mathbb{Z}$, with $\gcd(n, c) = 1$, that is, n and c are relatively prime.

If $a \cdot c \equiv b \cdot c \pmod n$, then $a \equiv b \pmod n$.

Given a positive integer $n > 1$, a **linear congruence** is a congruence of the form

$$ax \equiv b \,(\mathrm{mod}\, n) \qquad (*)$$

where a and b are integers. A **solution** to the linear congruence is an integer x_0 such that $ax_0 \equiv b \,(\mathrm{mod}\, n)$, that is, an integer that satisfies the congruence $(*)$.

For example, we have $3 \cdot 4 \equiv 2, (\mathrm{mod}\, 10)$, so that 4 is a solution to the congruence $3x \equiv 2 \,(\mathrm{mod}\, 10)$. However, the congruence $2x \equiv 1 \,(\mathrm{mod}\, 4)$ has no solution, since there does not exist an integer x such that $2x - 1$ is divisible by 4.

The next theorem gives a necessary and sufficient condition for the linear congruence $(*)$ to have a solution.

Theorem 7. If $n > 1$ is a positive integer and a, $b \in \mathbb{Z}$, then the linear congruence

$$ax \equiv b \,(\mathrm{mod}\, n)$$

has a solution if and only if $d \,|\, b$, where $d = \gcd(a, n)$. Moreover, if $d \,|\, b$, then the congruence has d incongruent solutions.

Proof. Let $d = \gcd(a, n)$, and suppose that $d \,|\, b$, then there exists an integer k such that $b = kd$. From the Euclidean algorithm, there exist integers x and y such that $d = ax + ny$, and therefore,

$$b = k(ax + ny) = a(kx) + n(ky)$$

and letting $x_0 = kx$, we have $ax_0 \equiv b \,(\mathrm{mod}\, n)$ and x_0 is a solution to the congruence.

Conversely, if x_0 is a solution to the congruence, then $ax_0 \equiv b \,(\mathrm{mod}\, n)$, so that $b = ax_0 + kn$ for some integer k, and therefore if $d = \gcd(a, n)$, then $d \,|\, b$.

Finally, suppose that $d \,|\, b$ and that x_0 is an arbitrary solution to the congruence $ax \equiv b \,(\mathrm{mod}\, n)$, then

$$x_0 + \left(\frac{n}{d}\right) k$$

is also a solution for $k = 0, 1, 2, \ldots, d - 1$, since $ax_0 + \left(\frac{n}{d}\right) ak \equiv ax_0 + \left(\frac{a}{d}\right) kn \equiv ax_0 \equiv b \,(\mathrm{mod}\, n)$.

If $x_1 = x_0 + \left(\frac{n}{d}\right) k_1$ and $x_2 = x_0 + \left(\frac{n}{d}\right) k_2$ are two solutions and $x_1 \equiv x_2 \,(\mathrm{mod}\, n)$, then

$$\left(\frac{n}{d}\right) k_1 \equiv \left(\frac{n}{d}\right) k_2 \,(\mathrm{mod}\, n),$$

and from Theorem 5, since $\frac{n}{d} \,|\, n$, then

$$k_1 \equiv k_2 \,(\mathrm{mod}\ d),$$

that is, x_1 and x_2 are congruent modulo n if and only if k_1 and k_2 are congruent modulo d, thus, x_1 and x_2 are incongruent modulo n if and only if they belong to distinct equivalence classes modulo d.

□

Note: The d incongruent (modulo n) solutions $x = x_0 + \left(\frac{n}{d}\right) k$, where $0 \leq k \leq d - 1$, make up what is called the **general solution** of the linear congruence $ax \equiv b \,(\mathrm{mod}\, n)$.

As a corollary to this theorem, we have a useful result.

Corollary 8. If $n > 1$ is a positive integer and a, $b \in \mathbb{Z}$, then the linear congruence $ax \equiv b \pmod{n}$ has a unique solution if and only if $\gcd(a, n) = 1$, that is, if and only if a and n are relatively prime.

In particular, if $b = 1$, then we have

Corollary 9. If $n > 1$ is a positive integer and $a \in \mathbb{Z}$, then the linear congruence

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if $\gcd(a, n) = 1$, that is, if and only if a and n are relatively prime. In this case, the unique solution is called the **inverse** of a modulo n and is denoted by a^{-1}.

If $n > 1$ is a positive integer and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, the Euclidean algorithm gives an elementary method to find the inverse of a modulo n, namely, we use the algorithm to find integers x and y such that

$$ax + ny = 1,$$

and then $a^{-1} \equiv x \pmod{n}$.

Example 4. Find the inverse of 12 modulo 35.

Solution. Applying the Euclidean algorithm we have

$$\begin{aligned} 35 &= 2 \cdot 12 + 11 \\ 12 &= 1 \cdot 11 + 1 \\ 11 &= 11 \cdot 1 + 0 \end{aligned}$$

and the last nonzero remainder is 1, that is, $\gcd(35, 12) = 1$, so that 12 has an inverse modulo 35.

Working backwards, we write the greatest common divisor 1 as a linear combination of 35 and 12,

$$\begin{aligned} 1 &= 12 - 1 \cdot 11 \\ &= 12 - 1 \cdot (35 - 2 \cdot 12) \\ &= 3 \cdot 12 + 1 \cdot 35 \end{aligned}$$

so that

$$12 \cdot 3 \equiv 1 \pmod{35},$$

and the inverse of 12 modulo 35 is 3.

Our last result gives another method for finding the inverse of a modulo a prime p, provided p does not divide a.

Theorem 10. (Fermat's Little Theorem) If p is a prime then

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

so that $a^{-1} \equiv a^{p-2} \pmod{p}$ for any integer a such that p does not divide a,

Proof. Let a be an integer such that $\gcd(a, p) = 1$, then the only possible remainders when a is divided by p are

$$r_1 = 1,\ r_2 = 2,\ r_3 = 3,\ \ldots,\ r_{p-1} = p - 1.$$

Note that r_1, r_2, r_3, $\ldots$, r_{p-1} are all relatively prime to p, and since a is also relatively prime to p, then the integers

$$ar_1 = a,\ ar_2 = 2a,\ ar_3 = 3a,\ \ldots,\ ar_{p-1} = (p-1)a$$

are also all relatively prime to p.

Note also, that these integers are also mutually incongruent modulo p, since if

$$ar_i \equiv ar_j \pmod{p}$$

for some $i \neq j$, then since $\gcd(a, p) = 1$, Corollary 6 implies that

$$r_i \equiv r_j \pmod{p}$$

for some $i \neq j$, which is a condradiction.

Thus, each ar_i with $1 \leq i \leq p-1$ is congruent modulo p to exactly one r_j with $1 \leq j \leq p-1$, and conversely, each r_i is congruent modulo p to exactly one ar_j, so that

$$r_1 r_2 r_3 \cdots r_{p-1} \equiv ar_1 ar_2 ar_3 \cdots ar_{p-1} \pmod{p}.$$

If we let $R = r_1 r_2 r_3 \cdots r_{p-1}$, then this last congruence says that

$$R \equiv a^{p-1} R \pmod{p},$$

and since $\gcd(R, p) = 1$, then again by Corollary 6, we have $a^{p-1} \equiv 1 \pmod{p}$.

□

There is generalization of this theorem due to Euler in which the modulus does not have to be a prime.

Theorem 11. (Euler's Theorem) If m is a positive integer and a is any integer such that $\gcd(a, m) = 1$, then

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

where $\phi(m)$ is *Euler's Phi Function*, that is, $\phi(m)$ counts the number of positive integers k with $1 \leq k \leq m$ which are relatively prime to m.

The proof of Euler's Theorem is similar to the proof of Fermat's Little Theorem, and is left is an exercise.