LECTURE 3: CONGRUENCES

1. Basic properties of congruences

We begin by introducing some definitions and elementary properties.

Definition 1.1. Suppose that $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. We say that a is **congruent** to b modulo m, and write $a \equiv b \pmod{m}$, when $m \mid (a - b)$.
We say that a is **not congruent** to b modulo m, and write $a \not\equiv b \pmod{m}$, when $m \nmid (a - b)$.

Theorem 1.2. *Let a, b, c, d be integers. Then*
(i) $a \equiv b \pmod{m} \iff b \equiv a \pmod{m} \iff a - b \equiv 0 \pmod{m}$*;*
(ii) $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$*;*
(iii) $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$ *and* $ac \equiv bd \pmod{m}$*;*
(iv) If $a \equiv b \pmod{m}$ *and* $d \mid m$ *with* $d > 0$*, then* $a \equiv b \pmod{d}$*;*
(v) If $a \equiv b \pmod{m}$ *and* $c > 0$*, then* $ac \equiv bc \pmod{mc}$*.*

Proof. Verification of these properties is straightforward. For instance, we prove (iii). Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then $a - b = um$ and $c - d = vm$ for some integers u and v. Hence, $(a + c) - (b + d) = (u + v)m$, so that $a + c \equiv b + d \pmod{m}$. Also, $ac - bd = (b + um)(d + vm) - bd = (ud + bv + uvm)m$ which implies that $ac \equiv bd \pmod{m}$. □

Corollary 1.3. *When $p(t)$ is a polynomial with integral coefficients, it follows that whenever* $a \equiv b \pmod{m}$*, then* $p(a) \equiv p(b) \pmod{m}$*.*

Proof. Use induction to establish that whenever $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for each $n \in \mathbb{N}$. □

The above corollary also extends to polynomials in several variables. In particular, we see that if the polynomial equation $p(x_1, \ldots x_n) = 0$ has an integral solution, then the congruence $p(x_1, \ldots x_n) \equiv 0 \pmod{m}$ is also solvable for all $m \in \mathbb{N}$. This provides a useful test for solvability of equations in integers.

The next theorem indicates how factors may be cancelled through congruences.

Theorem 1.4. *Let $a, x, y \in \mathbb{Z}$ and $m \in \mathbb{N}$. Then*
(i) $ax \equiv ay \pmod{m} \iff x \equiv y \pmod{m/(a, m)}$*.*
In particular, if $ax \equiv ay \pmod{m}$ *and* $(a, m) = 1$*, then* $x \equiv y \pmod{m}$*;*
(ii) $x \equiv y \pmod{m_i}$ $(1 \leqslant i \leqslant r) \iff x \equiv y \pmod{[m_1, \ldots, m_r]}$*.*

Proof. Observe first that when $(a,m)=1$, then $m \mid a(x-y) \iff m \mid (x-y)$. Then the conclusion of whenever $(a,m)=1$. When $(a,m)>1$, on the other hand, one does at least have $(a/(a,m), m/(a,m))=1$, so that

$$m \mid a(x-y) \iff \frac{m}{(a,m)} \,\Big|\, \frac{a}{(a,m)}(x-y) \iff \frac{m}{(a,m)} \,\Big|\, (x-y).$$

This establishes the conclusion of part (i) of the theorem.

We now consider part (ii) of the theorem. Observe first that whenever $m_i \mid (x-y)$ for $(1 \leqslant i \leqslant r)$, then $[m_1,\dots,m_r] \mid (x-y)$. On the other hand, if $[m_1,\dots,m_r] \mid (x-y)$, then $m_i \mid (x-y)$ for $(1 \leqslant i \leqslant r)$. The conclusion of part (ii) is now immediate. □

We investigate existence of multiplicative inverse modulo m.

Theorem 1.5. *Suppose that $(a,m)=1$. Then there exists an integer x with the property that $ax \equiv 1 \pmod m$. If x_1 and x_2 are any two such integers, then $x_1 \equiv x_2 \pmod m$. Conversely, if $(a,m)>1$, then there is no integer x with $ax \equiv 1 \pmod m$.*

Proof. Suppose that $(a,m)=1$. Then by the Euclidean Algorithm, there exist integers x and y such that $ax+my=1$, whence $ax \equiv 1 \pmod m$. Meanwhile, if $ax_1 \equiv 1 \equiv ax_2 \pmod m$, then $a(x_1-x_2) \equiv 0 \pmod m$. But $(a,m)=1$, and thus $x_1-x_2 \equiv 0 \pmod m$. We have therefore established both existence and uniqueness of the multiplicative inverse for residues a with $(a,m)=1$. If $(a,m)>1$, then $(ax,m)>1$ for every integer x. But if one were to have $ax \equiv 1 \pmod m$, then $(ax,m)=(1,m)=1$, which yields a contradiction. This establishes the last part of the theorem. □

Now we examine the set of equivalence classes with respect to congruence modulo m.

Definition 1.6. (i) If $x \equiv y \pmod m$, then y is called a **residue** of x modulo m;
(ii) We say that $\{x_1,\dots,x_m\}$ is a **complete residue system** modulo m if for each $y \in \mathbb{Z}$, there exists a unique x_i with $y \equiv x_i \pmod m$;
(iii) The set of integers x with $x \equiv a \pmod m$ is called the **residue class**, or **congruence class**, of a modulo m.

We also wish to consider residue classes containing integers coprime to the modulus, and this prompts the following observation.

Theorem 1.7. *Whenever $b \equiv c \pmod m$, one has $(b,m)=(c,m)$.*

Proof. If $b \equiv c \pmod m$, then $m \mid (b-c)$, whence there exists an integer x with $b=c+mx$. But then $(b,m)=(c+mx,m)=(c,m)$, as desired. □

Definition 1.8. A **reduced residue system** modulo m is a set of integers $r_1,\dots,r_\ell$ satisfying
(a) $(r_i,m)=1$ for $1 \leqslant i \leqslant \ell$,
(b) $r_i \not\equiv r_j \pmod m$ for $i \neq j$,

(c) whenever $(x, m) = 1$, then $x \equiv r_i \pmod{m}$ for some i with $1 \leqslant i \leqslant \ell$.

Theorem 1.9. *The number of elements in a reduced residue system is equal to the number of integers n satisfying $1 \leqslant n < m$ and $(n, m) = 1$.*

Proof. We observe that every integer x can be written as $x = qm + r$ with $0 \leqslant r < m$. Moreover, $(x, m) = (r, m)$. Hence, we see that

$$\{n \in \mathbb{N} : 1 \leqslant n < m,\ (n, m) = 1\}$$

is a reduced residue system modulo m.

Let $r_1, \dots, r_\ell$ and $s_1, \dots, s_k$ be reduced residue systems modulo m. Then for every $i = 1, \dots, \ell$, we have $r_i \equiv s_{\sigma(i)} \pmod{m}$ with some $\sigma(i) = 1, \dots, k$. Similarly, for every $j = 1, \dots, k$, we have $s_j \equiv r_{\theta(j)} \pmod{m}$ with some $\theta(j) = 1, \dots, \ell$. We deduce that $r_i \equiv r_{\theta(\sigma(i))} \pmod{m}$ and $s_j \equiv r_{\sigma(\theta(j))} \pmod{m}$. It follows from the properties of the reduced residue systems, that $\theta(\sigma(i)) = i$ and $\sigma(\theta(j)) = j$. Hence, the maps σ and θ define a bijection between $r_1, \dots, r_\ell$ and $s_1, \dots, s_k$. In particular, reduced residue systems have the same sizes. □

The number of elements in a reduced residue system modulo m is denoted by $\phi(m)$ (**Euler's totient**, or **Euler's ϕ-function**).

2. Euler and Fermat theorems

Theorem 2.1 (Euler, 1760)**.** *If $(a, m) = 1$ then*

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

In the proof we use the following lemma

Lemma 2.2. *Suppose that $(a, m) = 1$. Then whenever $\{r_1, \dots, r_\ell\}$ is a reduced residue system modulo m, the set $\{ar_1, \dots, ar_\ell\}$ is also a reduced residue system modulo m.*

Proof. Since $(a, m) = 1$, it follows that whenever $(r_i, m) = 1$ one has $(ar_i, m) = 1$. If $ar_i \equiv ar_j \pmod{m}$, then it follows from Theorem 1.4(i) that $r_i \equiv r_j \pmod{m}$. Hence we deduce that $ar_i \not\equiv ar_j \pmod{m}$ for $i \neq j$.

It remains to verify property (c). Take x with $(x, m) = 1$. By Theorem 1.5, there exists an integer a' such that $aa' \equiv 1 \pmod{m}$. Since $\{r_1, \dots, r_\ell\}$ is a reduced residue system modulo m, $a'x \equiv r_i \pmod{m}$ for some i. Then $ar_i \equiv (aa')x \equiv x \pmod{m}$. This shows that $\{ar_1, \dots, ar_\ell\}$ is a reduced residue system modulo m. □

Proof of Theorem 2.1. Let $\{r_1, r_2, \dots, r_{\phi(m)}\}$ be any reduced residue system modulo m, and suppose that $(a, m) = 1$. By Lemma 2.2, the system $\{ar_1, \dots, ar_{\phi(m)}\}$ is also a reduced residue system modulo m. Then there is a permutation σ of $\{1, 2, \dots, \phi(m)\}$ with the property that $r_i \equiv ar_{\sigma(i)} \pmod{m}$ for $1 \leqslant i \leqslant \phi(m)$. Consequently, one has

$$\prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} (ar_{\sigma(i)}) = \prod_{j=1}^{\phi(m)} (ar_j) = a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \pmod{m}.$$

But $(r_1 \cdots r_{\phi(m)}, m) = 1$, and thus $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Corollary 2.3 (Fermat's Little Theorem, 1640)**.** *Let p be a prime number, and suppose that $(a, p) = 1$. Then one has*

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

Moreover, for all integers a one has

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

Proof. Note that the set $\{1, 2, \ldots, p-1\}$ is a reduced residue system modulo p. Thus $\phi(p) = p-1$, and the first part of the theorem follows from Theorem 2.1. When $(a, p) = 1$, the second part of the theorem is immediate from the first part. Meanwhile, if $(a, p) > 1$, one has $p \mid a$, so that $a^p \equiv 0 \equiv a \pmod{p}$. This completes the proof of the theorem. □

Fermat's Little Theorem, and Euler's Theorem, ensure that the computation of powers is very efficient modulo p (or modulo m).

Example 2.4. Compute $5^{2016} \pmod{41}$. Observe first that $\phi(41) = 40$, and so it follows from Fermat's Little Theorem that $5^{40} \equiv 1 \pmod{41}$, and hence

$$5^{2016} = 5^{40 \cdot 50 + 16} = (5^{40})^{50} 5^{16} \equiv 5^{16} \pmod{41}.$$

Note next that powers which are themselves powers of 2 are easy to compute by repeated squaring (the "divide and conquer" algorithm). Thus one finds that

$$\begin{aligned} 5^2 &= 25 \equiv -16 \pmod{41}, \\ 5^4 &= (5^2)^2 \equiv (-16)^2 = 256 \equiv 10 \pmod{41}, \\ 5^8 &= (5^4)^2 \equiv (10)^2 = 100 \equiv 18 \pmod{41}, \\ 5^{16} &= (5^8)^2 \equiv (18)^2 = 324 \equiv 37 \pmod{41}. \end{aligned}$$

Thus $5^{2016} \equiv 37 \pmod{41}$.

Theorem 2.5 (Wilson's Theorem; Waring, Lagrange, 1771)**.** *For each prime number p, one has*

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

Proof. The proof for $p = 2$ and 3 is immediate, so suppose henceforth that p is a prime number with $p \geqslant 5$. Observe that when $1 \leqslant a \leqslant p-1$, one has $(a, p) = 1$, so there exists an integer $\overline{a}$ unique modulo p with $a\overline{a} \equiv 1 \pmod{p}$. Moreover, there is no loss in supposing that $\overline{a}$ satisfies $1 \leqslant \overline{a} \leqslant p-1$, and then $\overline{a}$ is a uniquely defined integer. We may now pair off the integers a with $1 \leqslant a \leqslant p-1$ with their counterparts $\overline{a}$ with $1 \leqslant \overline{a} \leqslant p-1$, so that $a\overline{a} \equiv 1 \pmod{p}$ for each pair. Note that $a \neq \overline{a}$ so long as $a^2 \not\equiv 1 \pmod{p}$. But $a^2 \equiv 1 \pmod{p}$ if and only if $(a-1)(a+1) \equiv 0 \pmod{p}$, and the latter is possible only when $a \equiv \pm 1 \pmod{p}$. Thus we find that

$$\prod_{a=2}^{p-2} a = \prod_{a} (a\overline{a}) \equiv 1 \pmod{p},$$

whence

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

□

The proof of Wilson's Theorem motivates a proof of a criterion for the solubility of the congruence $x^2 \equiv -1 \pmod{p}$.

Theorem 2.6. *When $p = 2$, or when p is a prime number with $p \equiv 1 \pmod{4}$, the congruence*

$$x^2 \equiv -1 \pmod{p}$$

is soluble.

When $p \equiv 3 \pmod{4}$, the latter congruence is not soluble.

Proof. When $p = 2$, $x = 1$ provides a solution. Assume next that $p \equiv 1 \pmod{4}$, and write $r = (p-1)/2$, $x = r!$. Then since r is even, one has

$$\begin{aligned} x^2 &= r! \cdot (-1)^r r! = (1 \cdot 2 \cdots r)((-1) \cdot (-2) \cdots (-r)) \\ &\equiv (1 \cdot 2 \cdots r)((p-1) \cdot (p-2) \cdots (p-r)) = (p-1)! \equiv -1 \pmod{p}. \end{aligned}$$

Thus, when $p \equiv 1 \pmod{4}$, the congruence $x^2 \equiv -1 \pmod{p}$ is indeed soluble.

Suppose then that $p \equiv 3 \pmod{4}$. If it were possible that an integer x exists with $x^2 \equiv -1 \pmod{p}$, then one finds that

$$(x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv -1 \pmod{p},$$

yet by Fermat's Little Theorem, one has

$$(x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \pmod{p}$$

whenever $(x, p) = 1$. We therefore arrive at a contradiction, and this completes the proof of the theorem. □