2. Congruences

We first recall the notion of congruence, then study how to solve linear congruence equations. The Chinese remainder theorem is important in solving simultaneous equations.

2.1. **Congruences and linear equations.**

We recall the following definition from Discrete Mathematics and Programming:

Definition 2.1. If $a, b, m \in \mathbb{Z}$ and $m \neq 0$, we say that a is *congruent to b modulo m* if m divides $b - a$. This relation is written as

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

For any $a \in \mathbb{Z}$, the set $\overline{a} = \{n \in \mathbb{Z} \mid n \equiv a \pmod{m}\}$ of integers congruent to a modulo m is called a *congruence class* modulo m. The set of congruence classes modulo m is denoted by $\mathbb{Z}_m$.

Remark 2.2. Although the notion of congruence is still well-defined for any non-zero integer m, we are usually only interested in positive values of m, as congruences modulo m and $-m$ coincide.

We have seen the following structure on $\mathbb{Z}_m$:

Proposition 2.3. *For any non-zero integer m, the set $\mathbb{Z}_m$ has the structure of a commutative ring with 1. In fact, it is the quotient ring $\mathbb{Z}/(m)$ where (m) is the principal ideal of $\mathbb{Z}$ generated by m.*

Proof. See Example (1) on Page 10 (2013) or Examples 1.20 and 1.35 (2014) in Algebra 2B. □

The cancellation law for congruences will be handy for solving congruence equations.

Proposition 2.4 (Cancellation Law). *For any $a, b, k, m \in \mathbb{Z}$, $k \neq 0$, $m \neq 0$, assume* $\mathrm{hcf}(k, m) = d$, *then* $ka \equiv kb \pmod{m}$ *iff* $a \equiv b \pmod{\frac{m}{d}}$.

Proof. See Exercise 2.3. □

Now we turn to look at congruence equations. In general a congruence equation has the form

$$f(x) \equiv 0 \pmod{m},$$

where $f(x)$ is a polynomial with integer coefficients and m is a non-zero integer. We are only interested in solutions modulo m; i.e. solutions in $\mathbb{Z}_m$. *The number of solutions* is the number of congruence classes in $\mathbb{Z}_m$ which satisfy the given equation.

Proposition 2.5. *For any $a, b, m \in \mathbb{Z}$, $a \neq 0$, $m \neq 0$, assume* $\operatorname{hcf}(a, m) = d$, *then the congruence equation $ax \equiv b \pmod{m}$ has solutions iff $d \mid b$. In this case there are exactly d solutions in $\mathbb{Z}_m$. If x_0 is a solution, then the complete set of solutions is given by the congruence classes of $x_0, x_0 + m', x_0 + 2m', \cdots, x_0 + (d-1)m'$, where $m' = \frac{m}{d}$.*

Proof. If x_0 is a solution, then $ax_0 - b = my_0$ for some integer y_0. Thus $ax_0 - my_0 = b$. Since d divides $ax_0 - my_0$, we must have $d \mid b$.

Conversely, suppose that $d \mid b$ then $b = cd$ for some $c \in \mathbb{Z}$. Since $\operatorname{hcf}(a, m) = d$, there exist integers x_0' and y_0' such that $ax_0' - my_0' = d$. Multiply both sides of the equation by c. Then $a(x_0'c) - m(y_0'c) = b$. Let $x_0 = x_0'c$. Then $ax_0 \equiv b \pmod{m}$.

We have shown that $ax \equiv b \pmod{m}$ has a solution iff $d \mid b$.

Suppose that x_0 and x_1 are solutions. $ax_0 \equiv b \pmod{m}$ and $ax_1 \equiv b \pmod{m}$ imply that $ax_1 \equiv ax_0 \pmod{m}$. By Proposotion 2.4, it is equivalent to $x_1 \equiv x_0 \pmod{m'}$, hence x_1 is a solution iff $x_1 = x_0 + km'$ for some integer k. Moreover, for each $k \in \mathbb{Z}$ there are integers r and s such that $k = rd + s$ and $0 \leqslant s < d$. Thus $x_1 = x_0 + sm' + rm$, or equivalently, $x_1 \equiv x_0 + sm' \pmod{m}$. These solutions are in d distinct congruence classes modulo m. This completes the proof. □

We immediately have the following corollary:

Corollary 2.6. *If* $\operatorname{hcf}(a, m) = 1$, *then $ax \equiv b \pmod{m}$ has exactly one solution. In particular, if p is a prime and $p \nmid a$, then $ax \equiv b \pmod{p}$ has exactly one solution.*

Proof. In this caes $d = 1$ so clearly $d \mid b$, and there is exactly $d = 1$ solution. □

In practice, we can solve such equations by cancellations and the Euclidean algorithm.

Example 2.7. As an example we consider the congruence $9x \equiv 6 \pmod{15}$. Since $d = \operatorname{hcf}(9, 15) = 3$ divides 6, the equation has 3 solutions modulo 15. By Proposition 2.4 we can cancel 3 on both sides and reduce the equation to $3x \equiv 2 \pmod{5}$. Euclidean algorithm shows that $\operatorname{hcf}(3, 5) = 1$ and $3 \times 2 + 5 \times (-1) = 1$, thus $3 \times 2 \equiv 1 \pmod{5}$. Then we multiply both sides by 2 and get $x \equiv 4 \pmod{5}$. Therefore the solutions to the original equation are $x \equiv 4, 9,$ or $14 \pmod{15}$.

From $3x \equiv 2 \pmod{5}$ we can also try to add multiples of 5 to 2 until we can cancel the coefficient 3. In this case we have $3x \equiv 2 + 5 \times 2 \pmod{5}$. By Proposition 2.4 we still get $x \equiv 4 \pmod{5}$. Hence the solutions to the original equation are $x \equiv 4, 9,$ or 14 (mod 15).

Proposition 2.5 can also be used to solve linear Diophantine equations of the form $ax+by = c$, where $a, b, c \in \mathbb{Z}$. We explain it by the following example.

Example 2.8. We want to find all integer solutions to the equation $9x + 15y = 6$. We solve it by considering the congruence equation $9x \equiv 6 \pmod{15}$. The computation above has showed that the solution is given by $x \equiv 4 \pmod{5}$, i.e. $x = 5k + 4$ for any $k \in \mathbb{Z}$. By substitution we have $9(5k + 4) + 15y = 6$, so $y = -3k - 2$. Therefore all solutions are given by $x = 5k + 4, y = -3k - 2$ where k is an arbitrary integer.

Now we apply Proposition 2.5 to study the group of units in the ring $\mathbb{Z}_m$.

Proposition 2.9. *Let m be a positive integer. An element $\overline{a} \in \mathbb{Z}_m$ is a unit iff* $\operatorname{hcf}(a, m) = 1$*. There are exactly $\phi(m)$ units in $\mathbb{Z}_m$. $\mathbb{Z}_m$ is a field iff m is a prime.*

Proof. $\overline{a} \in \mathbb{Z}_m$ is a unit iff $ax \equiv 1 \pmod{m}$ is solvable. By Proposition 2.5, this is equivalent to $\operatorname{hcf}(a, m) \mid 1$, hence equivalent to a and m being coprime.

The number of units is precisely the number of such a's with $1 \leqslant a \leqslant m$ and $\operatorname{hcf}(a, m) = 1$. By Definition 1.27, there are precisely $\phi(m)$ units in $\mathbb{Z}_m$.

If p is a prime and $\overline{a} \neq 0$ in $\mathbb{Z}_p$, then $\operatorname{hcf}(a, p) = 1$. Thus every non-zero element of $\mathbb{Z}_p$ is a unit, which shows that $\mathbb{Z}_p$ is a field.

If m is not a prime, then we can write $m = m_1 m_2$, where $1 < m_1, m_2 < m$. Thus $\overline{m_1} \neq \overline{0}$ and $\overline{m_2} \neq \overline{0}$, but $\overline{m_1} \cdot \overline{m_2} = \overline{m} = \overline{0}$. Therefore $\mathbb{Z}_m$ is not a field. □

We immediately obtain the following corollaries, both of which have their own names:

Corollary 2.10 (Euler's Theorem)**.** *If* $\operatorname{hcf}(a, m) = 1$*, then we have* $a^{\phi(m)} \equiv 1 \pmod{m}$*.*

Proof. The units in $\mathbb{Z}_m$ form a group of order $\phi(m)$. If a and m are coprime, $\overline{a}$ is a unit. Thus $\overline{a}^{\phi(m)} = \overline{1}$, or equivalently, $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Corollary 2.11 (Fermat's Little Theorem)**.** *If p is a prime and $p \nmid a$, then we have $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. If $p \nmid a$, then a are p are relatively prime. Thus $a^{\phi(p)} \equiv 1 \pmod{p}$. The result follows, since for a prime p, we have $\phi(p) = p - 1$. □