6. Modular Arithmetic and Chinese Remainder Theorem

Definition 6.1. *Let a, b, n be integers with $n \geq 1$. We say a* **is congruent to** b **modulo** n *and write $a \equiv b \mod n$, if $n \mid (a - b)$.*

Example 6.2. *(1)* $16 \equiv 5 \mod 11$*, since* $11 \mid (16 - 5)$.
(2) $23 \not\equiv 17 \mod 5$*, since* $5 \nmid 23 - 17 = 6$.
(3) $a \equiv b \mod 1$*, for all* $a, b \in \mathbb{Z}$*, since* $1 \mid (a - b)$.
(4) $a \equiv b \mod 2$*, if and only if both a and b are even or both are odd.*

Lemma 6.3. *Let a, n be integers, with $n \geq 1$. Then there exists a unique $r \in \{0, \dots, n-1\}$ such that $a \equiv r \mod n$. We call r* **residue of** a **modulo** n

Proof: Observe that $a \equiv r \mod n$ if and only if $n \mid (a - r)$ if and only if there is some $q \in \mathbb{Z}$ such that $a - r = qn$, that is, $a = qn + r$. In particular the existence and uniqueness of $r \in \{0, 1, \dots, n-1\}$ follows from the Division algorithm.

□

Lemma 6.4. *Let a, b, c, d, n be integers, with $n \geq 1$. Suppose $a \equiv b \mod n$ and $c \equiv d \mod n$. Then*

1. $a + c \equiv b + d \mod n$
2. $ac \equiv bd \mod n$
3. $a^k \equiv b^k \mod n$*, for all integers* $k \geq 0$

Proof: By assumption $n \mid (a - b)$ and $n \mid (c - d)$. Then, by Lemma 3.3 (7), we have $n \mid (a - b + c - d) = ((a + c) - (b + d)$. This gives (1). Also, by Lemma 3.3 (7), we have $n \mid (a - b)c + (c - d)b = ac - db$. This gives (2). Finally part (3) follows from (2).

□

Example 6.5. *(1) What is* $3^{20} \mod 41$*? We have*

$$3^2 = 9 \equiv 9 \mod 41$$
$$3^4 = (3^2)^2 \equiv 9^2 = 81 \equiv -1 \mod 41$$
$$3^8 = (3^4)^2 \equiv (-1)^2 = 1 \equiv 1 \mod 41$$
$$3^{16} = (3^8)^2 \equiv= 1^2 = 1 \equiv 1 \mod 41$$

Now $3^{20} = 3^{16} \cdot 3^4 \equiv 1 \cdot (-1) = -1 \mod 41$*, or in other words* $41 \mid 3^{20} + 1$.

Alternatively we have $3^{20} = (3^4)^5 = 81^5 \equiv (-1)^5 = -1 \mod 41$. *Thus again we get* $3^{20} \equiv -1 \mod 41$.
(2) What is the the remainder of $1! + 2! + 3! + 4! + \ldots + 100!$ *upon division by* 12*? Observe that* $12 = 3 \cdot 4$ *divides* $k!$ *for all* $k \geq 4$. *Hence* $k! \equiv 0 \mod 12$, *for all* $k \geq 4$. *Now*

$$1!+2!+3!+4!+\ldots+100! \equiv 1!+2!+3!+0+\ldots+0 = 1!+2!+3! = 9 \mod 12.$$

Remark 6.6. *Let* $a \geq 1$ *be an integer. Furthermore suppose that, read from the left, the digits of* a *are* $d_n, d_{n-1}, \ldots, d_1$, *that is,*

$$a = \sum_{k=1}^{n} d_k \cdot 10^{k-1}.$$

For instance $a = 12375 = 1 \cdot 10000 + 2 \cdot 1000 + 3 \cdot 100 + 7 \cdot 10 + 5 \cdot 10^0$.

(1) Divisibility by 2*: We have* $10^0 = 1 \equiv 1 \mod 2$, *and* $10 \equiv 0 \mod 2$. *By Lemma 6.4 (3) we now have* $10^k \equiv 0^k = 0 \mod 2$, *for all* $k \geq 1$. *Then*

$$a \equiv \sum_{k=1}^{n} d_k \cdot 10^{k-1} \equiv d_1 \mod 2.$$

Hence $a \equiv 0 \mod 2$ *iff* $d_1 \equiv 0 \mod 2$, *or in other words*

$$2 \mid a \text{ iff } 2 \mid d_1.$$

For instance, since $2 \nmid 5$ *we have* $2 \nmid 12375$.

(2) Divisibility by 11*: We have* $10^0 = 1 \equiv 1 \mod 11$, *and* $10 \equiv -1 \mod 11$. *By Lemma 6.4 (3) we now have* $10^k \equiv 1 \mod 11$, *for all even* $k \geq 0$, *and* $10^k \equiv -1 \mod 11$, *for all odd* $k \geq 1$. *Then*

$$a \equiv \sum_{k=1}^{n} d_k \cdot 10^{k-1} \equiv (d_1 + d_3 + \ldots) - (d_2 + d_4 + \ldots) \mod 11$$

Hence $a \equiv 0 \mod 11$ *iff* $(d_1 + d_3 + \ldots) - (d_2 + d_4 + \ldots) \equiv 0 \mod 11$, *or in other words*

$$11 \mid a \text{ iff } 11 \mid (d_1 + d_3 + \ldots) - (d_2 + d_4 + \ldots).$$

For instance, since $11 \mid (5 + 3 + 1) - (7 + 2) = 0$ *we have* $11 \mid 12375$.

Lemma 6.7. *Let* $a, b, c, n \in \mathbb{Z}$ *and* $n \geq 1$ *such that* $ca \equiv cb \mod n$. *Then* $a \equiv b \mod n/d$, *where* $d = \gcd(c, n)$.

Proof: By assumption, there is some $r \in \mathbb{Z}$ such that $nr = (ac - bc) = (a-b)c$. Also $n = d \cdot (n/d)$ and $c = d \cdot (c/d)$. Thus $(n/d) \mid (a-b) \cdot (c/d)$. But $\gcd(n/d, c/d) = 1$, by Corollary 4.4 (2). Hence $(n/d) \mid (a-b)$, by Euclid's lemma. In particular $a \equiv b \mod (n/d)$.

$\square$

Definition 6.8. *Let $n \geq 1$ and a and b be integers. An equation of the form $ax \equiv b \mod n$ is called a* **linear congruence**. *A* **solution** *of such a linear congruence is any integer x_0 such that $ax_0 \equiv b \mod n$. We say two solutions x_1 and x_2 are* **congruent** *if $x_1 \equiv x_2 \mod n$.*

Example 6.9. *Consider the linear congruence $3x \equiv 9 \mod 12$. Clearly $x_1 = 3$ is a solution. Also note that $3 \cdot (-9) = -27 \equiv 9 \mod 12$. Hence $x_2 = -9$ is a solution too. But since $3 \equiv -9 \mod 12$, they are congruent solutions.*

Theorem 6.10. *The linear congruence $ax \equiv b \mod n$ has a solution if and only if $d \mid b$, where $d = \gcd(a, n)$. In this case there are exactly d incongruent solutions modulo n, which are given by*

$$x_0, x_0 + (n/d), x_0 + 2 \cdot (n/d), \ldots, x_0 + (d-1) \cdot (n/d).$$

Proof: omitted

$\square$

Example 6.11. *(1) Consider the linear congruence $9x \equiv 21 \mod 30$. Since $\gcd(9, 30) = 3$ and $3 \mid 21$, there are exactly 3 incongruent solutions modulo 30. As the $\gcd(3, 30) = 3$, it follows from Lemma 6.7 that $3x \equiv 7 \mod 10$. Since $\gcd(3, 10) = 1$ this linear congruence has a unique solution modulo 10. Note that if we multiply $3x \equiv 7 \mod 10$ by 7, we get $21x \equiv 49 \mod 10$, which implies that $x \equiv 9 \mod 10$.*

Now $x = 9$ is a solution of $9x \equiv 21 \mod 30$. Thus its three incongruent solutions are given by $9 + (n/d) \cdot t$, where $t = 1, 2, 3$. Hence the solutions modulo 30 are $9, 19, 29$.

(2) What is $23^{91} \mod 33$? Let $23^{91} \equiv x \mod 33$. We have

$$\begin{aligned} 23^{91} \equiv x \mod 33 \Leftrightarrow 33 \mid 23^{91} - x &\Leftrightarrow 3 \text{ and } 11 \text{ divide } 23^{91} - x \\ &\Leftrightarrow 23^{91} \equiv x \mod 3 \text{ and } 23^{91} \equiv x \mod 11 \end{aligned}$$

As $23 \equiv -1 \mod 3$ we have $x \equiv 23^{91} \equiv (-1)^{91} = -1 \mod 3$. As $23 \equiv 1 \mod 11$ we have $x \equiv 23^{91} \equiv 1^{91} = 1 \mod 11$. This leads to the system of *linear congruences*

$$x \equiv -1 \mod 3$$
$$x \equiv 1 \mod 11$$

What is x?

Theorem 6.12. *(Chinese Remainder Theorem) Let $n_1, \ldots, n_r$ be positive, pairwise coprime integers, and let $a_1, \ldots, a_r$ be integers. Then the system of linear congruences*

$$x \equiv a_1 \mod n_1$$
$$\vdots$$
$$x \equiv a_r \mod n_r$$

has a simultaneous solution, which is unique modulo $n := n_1 \cdot \ldots \cdot n_r$. This solution is given by

$$\bar{x} = a_1 N_1 x_1 + \ldots + a_r N_r x_r,$$

where $N_k := \dfrac{n}{n_k} = n_1 \cdot n_{k-1} \cdot n_{k+1} \cdot n_r$ and x_k is a solution of $N_k x \equiv 1 \mod n_k$, for all $k = 1, \ldots, r$.

Proof: omitted.

$\square$

Example 6.13. *(1) Let us complete Example 6.11(2). We have the system*

$$x \equiv -1 \mod 3$$
$$x \equiv 1 \mod 11$$

Then $n_1 = 3$, $n_2 = 11$, $n = n_1 \cdot n_2 = 33$, $N_1 = \frac{n}{n_1} = 11$ and $N_2 = \frac{n}{n_2} = 3$.

As $11 \equiv -1 \mod 3$ we have $11x \equiv 1 \mod 3 \Leftrightarrow -x \equiv 1 \mod 3$. Thus $x \equiv -1 \mod 3$, and so $x_1 = -1$ is a solution of $11x \equiv 1 \mod 3$.

Next we look for a solution x_2 of $3x \equiv 1 \mod 11$. Since $4 \cdot 3 = 12 \equiv 1 \mod 11$ we multiply the congruence equation by 4. Then $x \equiv 12x \equiv 4(3x) \equiv 4 \mod 3$. Thus $x_2 = 4$ is a solution of $3x \equiv 1 \mod 11$.

Overall $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 = (-1) \cdot 11 \cdot (-1) + 1 \cdot 3 \cdot 4 = 11 + 12 = 23$ is a simultaneous solution to the given system. Finally this shows that $23^{91} \equiv 23 \mod 33$

(2) Which is the smallest positive number that leaves remainders $2, 3, 2$ when divided by $3, 5, 7$, respectively? That means we look for a solution of the system

$$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 2 \mod 7.$$

Note that $3, 5, 7$ are pairwise coprime. Hence we can expect a solution. We have $n = 3 \cdot 5 \cdot 7 = 105$ and $N_1 = 5 \cdot 7 = 35$, $N_2 = 3 \cdot 7 = 21$, $N_3 = 3 \cdot 5 = 15$. This leads to the linear congruences

$$35x \equiv 1 \mod 3, \quad 21x \equiv 1 \mod 5, \quad 15x \equiv 1 \mod 7,$$

which are equivalent to

$$2x \equiv 1 \mod 3, \quad x \equiv 1 \mod 5, \quad x \equiv 1 \mod 7.$$

So $x_1 = 2$, $x_2 = 1$ and $x_3 = 1$ are their respective solutions. Hence our system has the solution

$$\begin{aligned} \bar{x} &= a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \\ &= 140 + 63 + 30 = 233 \equiv 23 \mod 105. \end{aligned}$$

So all numbers of the form $23 + 105t$, for $t \in \mathbb{Z}$ solve our system, but 23 is the smallest positive such number.