Congruences, primes and integers

Definitions

Let $a, b \in \mathbb{Z}$. We say a divides b if $b = ac$ for some $c \in \mathbb{Z}$. When a divides b, we write $a|b$.

Representation

$a \in \mathbb{Z}^+ \implies (\forall b \in \mathbb{Z}, \exists q, r \in \mathbb{Z} : b = qa + r \text{ and } 0 \le r < a)$

The integer q is called the quotient, and r is the remainder.

> Example: If $a = 17$ and $b = 183$, then the equation is $183 = 10 \cdot 17 + 13$.
>
> The quotient is 10 and the remainder 13.

> Example: Let $a, b, d \in \mathbb{Z}$ and suppose that $d|a$ and $d|b$. Then $d|(ma + nb)$ for any $m, n \in \mathbb{Z}$.
>
> Proof: Let $a = c_1 d$ and $b = c_2 d$ with $c_1, c_2 \in \mathbb{Z}$. Then for $m, n \in \mathbb{Z}$:
>
> $$ma + nb = mc_1 d + nc_2 d = (mc_1 + nc_2)d$$
>
> Hence, $d|(ma + nb)$.

Highest common factor

Let $a, b \in \mathbb{Z}$. A **common factor** of a and b is an integer that divides both a and b. The **highest common factor** of a and b, written $hcf(a, b)$, is the largest positive integer that divides both a and b.

> Example: $hcf(2, 3) = 1$ and $hcf(4, 6) = 1$.

Coprime integers

Two integers a and b are said to be coprime if their highest common factor is 1. For example, 2 and 3 are coprime.

Note that coprime integers need not be prime.

Euclidean algorithm

The **Euclidean algorithm** is a step-by-step method for calculating the common factors of two integers. Like most algorithms, the definition of the euclidean algorithm can be often displayed as pseudocode, but it may be easier to look at an example:

> Example: Find $hcf(5817, 1428)$.

> First, we write $a = 1428, b = 1428$, and let $d = hcf(a, b)$.
>
> 1. Divide a into b and get a quotient and remainder:
>
> $5817 = 4 \cdot 1428 + 105$
> 2. Divide 105 into 1428:
>
> $1428 = 13 \cdot 105 + 63$
> 3. Divide 63 into 105:
>
> $105 = 1 \cdot 63 + 42$
> 4. Divide 42 into 63:
>
> $63 = 1 \cdot 42 + 21$
> 5. Divide 21 into 42:
>
> $42 = 2 \cdot 21 + 0$
>
>   We stop here as we have reached a remainder of 0.
>
> ---
>
> We now claim that $d = hcf(5817, 1428) = 21$.
>
> To prove this, we work backwards. Step 5 shows that $21|42$, hence Step 4 shows that $21|63$, and so on, until Step 2 shows that $21|1428$ and Step 1 shows that $21|5817$.
>
> Therefore our claim that $hcf(5817, 1428) = 21$ was right.

Bézout's identity

$$(a, b \in \mathbb{Z}) \wedge \big(d = hcf(a, b)\big) \implies \exists s, t \in \mathbb{Z} : d = sa + tb$$

> Example: From the previous example, we know that $hcf(5817, 1428) = 21$, so by Bézout's identity $\exists s, t \in \mathbb{Z} : 21 = 5817s + 1428t$. To find such integers s and t, we use the steps from the Euclidean algorithm that we performed to find $hcf(5817, 1428)$ previously. We start from the penultimate step:
>
> Step 4: $21 = 63 - 1 \cdot 42$
>
> Step 3: $21 = 63 - 1(105 - 1 \cdot 63) = 2 \cdot 63 - 105$
>
> Step 2: $21 = 2(1428 - 13 \cdot 105) - 105 = 2 \cdot 1428 - 27 \cdot 105$
>
> Step 1: $21 = 2 \cdot 1428 - 27(5817 - 4 \cdot 1428) = 110 \cdot 1428 - 27 \cdot 5817$
>
> Thus, we have found our integers $s = -27$ and $t = 110$. Note that there will be many other values of s and t which will also work.

Divisibility of common factors

$$a, b \in \mathbb{Z} \implies \text{any common factor of } a \text{ and } b \text{ also divides } hcf(a, b).$$

> Proof: Let $d = hcf(a, b)$. By Bézout's identity, $\exists s, t \in \mathbb{Z} : d = sa + tb$. If m is a common factor of a and b, then m divides $sa + tb$ (any linear combination of a and b. By the same idea as the second example in the Representation section above), and hence m divides d.

Lowest common multiple

Let $a, b \in \mathbb{Z}$. A **common multiple** of a and b is an integer which is a multiple of both a and b. The **lowest common multiple** of a and b, written $lcm(a, b)$, is the smallest positive integer that is a multiple of both a and b.

Prime factorisation

Fundamental Theorem of Arithmetic

Let n be an integer with $n \geq 2$. Then:

- n is equal to a product of prime numbers:

$$n = \prod_{i=1}^{k} p_i$$

  where p_i is a prime and $p_1 \leq p_2 \leq \ldots \leq p_k$.
- This prime factorisation of n is unique. In other words, if:

$$n = \prod_{i=1}^{k} p_i = \prod_{i=1}^{l} q_i$$

  where the p_is and q_is are all primes such that $p_1 \leq p_2 \leq \ldots \leq p_k$ and $q_1 \leq q_2 \leq \ldots \leq q_l$, then

$$k = l \quad \text{and} \quad p_i = q_i \ \ \forall i = 1, \ldots k$$

Alternatively, it may be the case that some of the p_is are equal to each other. If we collect these up, we obtain a prime factorisation of form:

$$n = \prod_{i=1}^{k} p_i^{a_i}$$

Where $p_1 < p_2 < \ldots < p_k$ and $a_i \in \mathbb{Z}^+$.

Divisors of an integer

Let $n = \prod_{i=1}^{m} p_i^{a_i}$ where p_is are prime, and $p_1 < p_2 < \ldots < p_m$ and the a_is are positive integers. If m divides n, then:

$$m = \prod_{i=1}^{m} p_i^{b_i}$$

with $0 \leq b_1 \leq a_i \quad \forall i$.

> Example: The only divisors of $2^{100} 3^2$ are the numbers $2^a 2^b$, where $0 \leq a \leq 100$ and $0 \leq b \leq 2$.

Finding the hcf and lcm of two numbers (in prime representation)

Let $a, b \geq 2$ be integers with prime factorisatißons:

$$a = \prod_{i=1}^{m} p_i^{r_i} \quad b = \prod_{i=1}^{m} p_i^{s_i}$$

where the p_i are distinct primes and all $r_i, s_i \geq 0$. Note that some of the r_i and s_i can be 0. Then:

- $hcf(a, b) = \prod_{i=1}^{m} p_i^{min(r_1, s_1)}$
- $hcf(a, b) = \prod_{i=1}^{m} p_i^{max(r_1, s_1)}$

Congruence of integers

Definition

Let $m \in \mathbb{Z}^+$. For $a, b \in \mathbb{Z}$, if m divides $b - a$ we write $a \equiv b \pmod{m}$ and say a is congruent to b modulo m.

> Example: $5 \equiv 1 \pmod{2}$ and $12 \equiv 17 \pmod{5}$

Identities

Let m be a positive integer. The following are true $\forall a, b, c \in \mathbb{Z}$:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$
- $\big(a \equiv b \pmod{m}\big) \wedge \big(b \equiv c \pmod{m}\big) \implies a \equiv c \pmod{m}$

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then:

- $a + c \equiv b + d \pmod{m}$
- $ac \equiv bc \pmod{m}$

If $a \equiv b \pmod{m}$ and n is a positive integer, then $a^n \equiv b^n \pmod{m}$.

> Example: Find the remainder when 6^{82} is divided by 7.
>
> $$6 \equiv -1 \pmod{7}$$
> $$6^{82} \equiv (-1)^{82} \pmod{7}$$
> $$6^{82} \equiv 1 \pmod{7}$$
>
> The remainder is 1.

Arithmetic modulo m

The set of integers modulo m is denoted as $\mathbb{Z}_m$:

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$$

Multiplicative inverses

The **multiplicative inverse** of an integer $x \pmod{m}$ is another integer $y \pmod{m}$ such that $xy \equiv 1 \pmod{m}$.

If $m, x \in \mathbb{Z}^+$ and $hcf(m, x) = 1$, then x has a multiplicative inverse $\mod m$ (and it is unique $\mod m$).

Chinese remainder theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise coprime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then the system:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = \prod_{i=1}^{n} m_i$.

> Example:
>
> $$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 1 \pmod{5} \end{aligned}$$
>
> We will work out the sum in three sections:
>
> | | $\pmod{3}$ | + | $\pmod{4}$ | + | $\pmod{5}$ |
> |---|---|---|---|---|---|
> | $x =$ | | + | | + | |
>
> Consider the first section, $\pmod{3}$. We want to ignore the other sections (when considering the first section), by making them congruent to $0 \pmod{3}$. We can do this by including 3 in their sections, since $3 \equiv 0 \pmod{3}$.
>
> | | $\pmod{3}$ | + | $\pmod{4}$ | + | $\pmod{5}$ |
> |---|---|---|---|---|---|
> | $x =$ | | + | 3 | + | 3 |
>
> Do the same for sections $\pmod{4}$ and $\pmod{5}$ (by multiplying):

	$\pmod 3$	+	$\pmod 4$	+	$\pmod 5$
$x =$	$4 \cdot 5$	+	$3 \cdot 5$	+	$3 \cdot 4$

	$\pmod 3$	+	$\pmod 4$	+	$\pmod 5$
$x =$	20	+	15	+	12

- In $\pmod 3$, we would have:

  $x = 20 + 0 + 0 \pmod 3 = 20 \pmod 3 = 2 \pmod 3$

Which is what we want, so we can leave the $\pmod 3$ section.

- In $\pmod 4$, we would have:

  $x = 0 + 15 + 0 \pmod 4 = 15 \pmod 4 = 3 \pmod 4$

  But we need $2 \pmod 4$. If we multiply $15 \pmod 4$ by $3 \pmod 4$, we get $3 \cdot 3 = 1 \pmod 4$. We can then multiply by 2 to get $2 \pmod 4$.

  So we need to add 3 and 2 to the middle section:

	$\pmod 3$	+	$\pmod 4$	+	$\pmod 5$
$x =$	20	+	$15 \cdot 3 \cdot 2$	+	12

- In $\pmod 5$, we would have:

  $x = 0 + 0 + 12 \pmod 5 = 2 \pmod 5$

  But we need $1 \pmod 5$. If we multiply $12 \pmod 5 = 2 \pmod 5$ by $3 \pmod 5$, we get $6 \pmod 5 = 1 \pmod 5$ as required, so we need to add a 3 to the last section in the table:

	$\pmod 3$	+	$\pmod 4$	+	$\pmod 5$
$x =$	20	+	$15 \cdot 3 \cdot 2$	+	$12 \cdot 3$

Giving us $x = 146$. Note that this isn't the only solution. We could have $x = 146 + (3 \cdot 4 \cdot 5)k$ where k is any positive or negative integer. A nicer looking solution would be when $k = 2$, we have $x = 26$.

Fermat's little theorem

Let p be a prime number, and let a be an integer that is not divisible by p. Then

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

> Example: $93^{16} \equiv 1 \pmod{17}$, $2^{16} \equiv 1 \pmod{17}$ and $72307892^{16} \equiv 1 \pmod{17}$.

> Example: Find $3^{972} \pmod{17}$.
>
> Fermat's Little Theorem tells us that $3^{16} \equiv 1 \pmod{17}$. Dividing 16 into 972, we get $972 = 16 \cdot 60 + 12$, so:

$$3^{972} = (3^{16})^{60} \cdot 3^{12} \equiv (1^{60}) \cdot 3^{12} \pmod{17}$$

So we only need to work out $3^{12} \pmod{17}$, which can be done by the method of successive squares.