Recall $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

division by b: $a = qb + r$ where r is remainder $0 \leq r < |b|$
$b \neq 0$

$\gcd(a,b) = d$ greatest common divisor, $(d \geq 1)$

$\operatorname{lcm}(a,b) = m$ least common multiple

note $m = \frac{|ab|}{d}$

<u>Bezouts Identity</u>: If $\gcd(a,b) = d$ then $\exists\, x, y \in \mathbb{Z}$ s.t. $ax + by = d$

<u>Corollary 1.9</u>: Integers a and b are coprime $\Leftrightarrow$ $ax + by = 1$ for some $x, y \in \mathbb{Z}$

<u>Theorem 1.10 (FTA)</u>: Every positive integer $n > 1$ can be represented as the product of prime powers $n = p_1^{a_1} \cdots p_k^{a_k}$. where $p_1, \dots, p_k$ are primes and $a_1, \dots, a_k$ are positive integers.

Example: $4004 = 2^2 \times 7 \times 11 \times 13$

hence $k = 4$, $p_1 = 2$, $p_2 = 7$, $p_3 = 11$, $p_4 = 13$ and $a_1 = 2$, $a_2 = a_3 = a_4 = 1$.

<u>Theorem 1.11 (Euclid)</u>. There are infinitely many primes.

Proof: Assume there is only a finite number of primes: $p_1, \dots, p_k$.

Consider the number $A = p_1, \dots, p_k + 1$ note that p_i does not divides A, for any $i = 1, \dots, k$.

So A is not divisible by any prime, which contradicts to FTA.

Remark 1.12: FTA provides another algorithm for finding $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$. If

$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ $(\alpha_i \geq 0)$ and $p_1, p_2, p_3, \dots$ all primes
$p_1 = 2$, $p_2 = 3$, $p_3 = 5$

$b = p_1^{\beta_1} \dots p_k^{\beta_k}$ $(\beta_i \geq 0)$ and

Then $\gcd(a,b) = p_1^{\gamma_1} \dots p_k^{\gamma_k}$ where $\gamma_i = \min(\alpha_i, \beta_i)$

$\operatorname{lcm}(a,b) = p_1^{\delta_1} \dots p_k^{\delta_k}$ where $\delta_i = \max(\alpha_i, \beta_i)$

Example 1.13: $a = 77077 = 7^2 \times 11^2 \times 13 = 2^0 \times 3^0 \times 5^0 \times 7^2 \times 11^2 \times 13$

$b = 674817 = 3 \times 11^3 \times 13^2 = 2^0 \times 3 \times 5^0 \times 7^0 \times 11^3 \times 13^2$

then $\gcd(a,b) = 2^0 \times 3^0 \times 5^0 \times 7^0 \times 11^2 \times 13 = 11^2 \times 13 = 1573$

$\text{lcm}(a,b) = 3 \times 7^2 \times 11^3 \times 13^2 = 33066033$

note: on computer, Euclidean Algorithm is used to find gcd (factorization uses too many calculations)

---

2. Modular Arithmetics

"Truncated" version of $\mathbb{Z}$: the ring of integers mod n:

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

or simply $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$ (here $0, 1, \ldots, n-1$ are not normal integers)

Definition 2.1: Let $n > 0$, $n \in \mathbb{Z}$. Then integers a and b are congruent modulo n, written

$a \equiv b \mod n$ if $n \mid (a-b)$.

Recall that by Division Alg, $a = qn + r$ where $0 \leq r < n$ is the remainder (or residue) after division by n. Then $a - r = qn$ is divisible by n, so $a \equiv r \mod n$

Hence $a \equiv b \mod n \Leftrightarrow a$ and b have the same residue mod n.

Example: Let $n=5$. If we divide 19 by 5, we get residue 4: $19 = 3 \times 5 + 4$. But the same is true for

$14, 9, 4, -1$ ($-1 = (-1) \times 5 + 4$), so $19 \equiv 14 \equiv 9 \equiv 4 \equiv -1 \ldots$

Exercise: Properties of $\equiv \mod n$

(0) $a \equiv a$ (trivial)

(1) $a \equiv b \Rightarrow b \equiv a$ (symm.)

(2) $a \equiv b$ & $b \equiv c \Rightarrow a \equiv c$ (transitive)

so "$\equiv$" is an equivalence relation

(3) $a \equiv b$ & $a' \equiv b' \Rightarrow aa' \equiv bb'$ and $a + a' \equiv b + b'$

(but no division unless $n = p$ prime)

Definition 2.3: The residue class of a modulo n is $[a]_n = a + n\mathbb{Z} = \{a, a \pm n, a \pm 2n, a \pm 3n, \dots\} \subseteq \mathbb{Z}$ (subset)

(all integers with the same residue as a mod n).

Example: $[0]_n = 0 + n\mathbb{Z} = n\mathbb{Z} = \{$ all multiples of $n\}$

note: $a \equiv b \mod n \Leftrightarrow [a]_n = [b]_n \Leftrightarrow n \mid (a-b)$

Example: Since $19 \equiv 14 \equiv 9 \equiv 4 \equiv -1 \mod 5$,

$$[19]_5 = [14]_5 = [9]_5 = [4]_5 = \{-6, -1, 4, 9, 14, \dots\} = [-1]_5 = \cdots$$