1. Prove that $G.C.D(m, n)$, the greatest common divisor of two integers, is the minimal positive integer representable as their linear combination $am + bn$.

**Definition.** Call two integers congruent modulo $n$ (write: $a \equiv b \mod n$), if $a - b$ is divisible by $n$. Denote $\mathbb{Z}$ the set of all integers (positive, zero, and negative), $n\mathbb{Z}$ integers divisible by $n$, and $\mathbb{Z}/n\mathbb{Z}$ the set of classes of congruence of integers modulo $n$.

2. Show that $\mathbb{Z}/n\mathbb{Z}$ inherits from $\mathbb{Z}$ operations of addition and multiplication, and moreover, that the natural map $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ that associates to an integer $a$ its congruence class $\bar{a}$, respects both operations: $a + b = \bar{a} + \bar{b}$ and $a \cdot b = \bar{a} \cdot \bar{b}$ for all $a, b \in \mathbb{Z}$.

**Remark.** In algebraic terminology, $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are rings (more precisely, commutative rings with unity), and the map $a \mapsto \bar{a}$ is a homomorphism of rings.

**Definition.** Given a ring $R$ with unity $1$, one denotes by $R^*$ the set of all those elements which have multiplicative inverses, $R^* := \{x \in R | \exists y : xy = 1 = yx\}$. Then $R^*$ is a group with respect to multiplication, called the group of units of the ring $R$.

3. Show that $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is invertible if and only if $G.C.D.(a, n) = 1$. (Hint: Use Problem 1.)

4. Let $p$ be prime. Prove that $|\mathbb{Z}/p^k\mathbb{Z}| = (p^k - p^{k-1})$.

5. Given two integers $m$ and $n$, define map $\pi : \mathbb{Z}/mn\mathbb{Z} \rightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ that to a congruence class of $a \mod mn$ assigns the ordered pair of congruence classes $(a \mod m, a \mod n)$. Show that $\pi$ is a homomorphism of rings, and that it is a isomorphism (= 1-1-and-onto) if and only if $G.C.D.(m, n) = 1$.

**Hint:** Show that $\pi(\bar{a}) = \pi(\bar{b})$ if and only if $a - b$ is divisible by $L.C.M.(m, n)$ (the least common multiple of $m$ and $n$).

**Remark.** The last statement is called the Chinese Remainder Theorem; it implies that for any given $a, b$, the system of equations $x \equiv a \mod m, x \equiv b \mod n$ has a solution $x$ (unique mod $mn$) provided that $m$ and $n$ are relatively prime — a fact known in ancient China.

6. Prove that when $m$ and $n$ are relatively prime, $\pi$ defines an isomorphism of groups: $(\mathbb{Z}/mn\mathbb{Z})^* \rightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$.

7. Let $n$ have prime factorization $\phi(p_1^{k_1} \cdots p_r^{k_r})$. Show that $|(\mathbb{Z}/n\mathbb{Z})^*| = (p_1 - 1) \cdots (p_r - 1)p_1^{k_1 - 1} \cdots p_r^{k_r - 1}$.

**Remark.** This number, denoted $\phi(n)$, is called Euler’s function (of $n$), defined as the number of remainders modulo $n$ relatively prime to
The following two problems express Euler’s Theorem, and its special case Fermat’s Little Theorem.

8. Prove that $G.C.D.(a, n) = 1$ implies $a^{\phi(n)} \equiv 1 \mod n$.

**Hint:** In the group $(\mathbb{Z}/n\mathbb{Z})^*$ consider the cyclic subgroup formed by all powers (positive, zero, and negative) of $\bar{a}$, and then apply a general fact about finite groups (Lagrange’s Theorem), according to which the number of elements in a finite group is divisible by the number of elements of any subgroup.

9. Prove that if $a$ is not divisible by a prime $p$ then $a^{p-1} \equiv 1 \mod p$.

**Hint:** For an elementary proof, show that $\binom{p}{k}$ is divisible by $p$ when $0 < k < p$, and apply induction on $a = 1, 2, ..., p - 1$.

10. Prove Lagrange’s Theorem: For any subgroup $H$ of a finite group $G$, the order $|G|$ of $G$ is divisible by $|H|$. **Hint:** Partition $G$ into classes of congruence modulo $H$ defined by: $x \equiv y \mod H$ if $xy^{-1} \in H$.

11. Use Problem 10 to show that for every $x \in G$ the minimal positive $n$ such that $x^n = 1$ is a divisor of $|G|$.

12. Show that the commutative ring with unity $\mathbb{Z}/n\mathbb{Z}$ is a field (i.e. has all non-zero elements invertible) if and only if $n$ is prime.

13. Let $F$ be a field, and $F[x]$ denote the ring of polynomials in one indeterminate $x$ with coefficients in $F$. Prove Bezout’s Theorem: $a \in F$ is a root of a polynomial $f \in F[x]$ if and only if $f$ is divisible by $x - a$. **Hint:** The Long Division algorithm for polynomials still works in $F[x]$.

14. Prove that when $p$ is prime, the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic (i.e. consists of powers of a single element). **Hint:** The polynomial $x^m - 1$ cannot have more than $m$ roots in the field $\mathbb{Z}/p\mathbb{Z}$.

**Remark.** The argument works for any finite field $F$ to show that the group $F^*$ is cyclic.

15. For $n \leq 16$, find out which of the groups $(\mathbb{Z}/n\mathbb{Z})^*$ are cyclic.

16. Prove that for prime $p > 2$ and any $k > 0$, the group $(\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic. **Hint:** Study powers of $(1 + p)$ modulo $p^k$.

17. For $p = 2$, which of the groups $(\mathbb{Z}/p^k\mathbb{Z})^*$ are cyclic?

18. Find all $n$ for which the group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic.

19. Study the structure of the group $(\mathbb{Z}/100\mathbb{Z})^*$ and find the order of the cyclic subgroup generated by $3$.

20. How many different 2-digit numbers occur as pairs of rightmost digits of powers of 3?