Lecture 32, Nov. 8

32.1 Example. Determine whether 125 is a unit in $\mathbb{Z}_{471}$ and, if so, find 125^{-1}.

Solution. We use EA with BS.

EA:

$$471 = 3 \cdot 125 + 96$$
$$125 = 1 \cdot 96 + 29$$
$$96 = 3 \cdot 29 + 9$$
$$29 = 3 \cdot 9 + 2$$
$$9 = 4 \cdot 2 + 1$$

BS:

$$1, -4, 13, -43, 56, -211$$

So we have $471 \cdot 56 - 125 \cdot 211 = 1$

Thus $125^{-1} = -211 = 260$ in $\mathbb{Z}_{471}$.

32.2 Definition (Group)**.** A group is a set G with an element e (called the identity element) and one binary operation $*\colon G \times G \to G$ such that

1. $*$ is associative. For all $a, b, c \in G$ we have
$$a * (b * c) = (a * b) * c$$
2. e is an identity for all $a \in G$
$$a * e = e * a = a$$
3. every $a \in G$ has a inverse. For all $a \in G$ there exists $b \in G$ such that
$$a * b = b * a = e$$

32.3 Definition (Abelian Group)**.** A group G is called abelian (or commutative) when

4 $*$ is commutative. For all $a, b \in G$ we have
$$a * b = b * a$$

Note.

1. the identity element $e \in G$ is unique. For all $a, u \in G$, if ($a * u = a$ or $u * a = a$) then $e = u$
2. the inverse of $a \in G$ is unique. For all $a, b, c \in G$, if ($a * b = e$ and $c * a = e$) then $b = c$

32.4 Example. When R is a ring, R is also an abelian group under its addition operation $+$ (which we can call the additive group of R).

32.5 Example. Also when R is a ring, the set of all invertible elements in R under multiplication is a group, which we call the group of units of R, and denoted by R^* or $R^\times$

Remark. A product of two units is a unit.

32.6 Example. When F is a field, all non zero elements in F are invertible, so $F^* = F \backslash \{0\}$

32.7 Example. $(\mathbb{Z}[\sqrt{2}])^* = \{\pm u^k \mid k \in \mathbb{Z}\}$

32.8 Definition. The group of units in $\mathbb{Z}_n$ is called the group of units modulo n and it is denoted by U_n

$$\begin{aligned} U_n = \mathbb{Z}_n^* =& \{a \in \mathbb{Z}_n \mid a \text{ is invertible } \} \\ =& \{a \in \{1, 2, 3, \cdots, n\} \mid gcd(a, n) = 1\} \end{aligned}$$

Remark. The reason we can write $gcd(a, n)$ is because $gcd(a, n) = gcd([a], n)$

Remark. For $n \in \mathbb{Z}$ with $n \geq 2$ and $a, b \in \mathbb{Z}$, we <u>cannot</u> define

$$gcd([a], [b]) = gcd(a, b)$$

because for $a, b, c, d \in \mathbb{Z}$, $a = c \mod n$ and $b = d \mod n$ do not imply that $gcd(a, b) = gcd(c, d)$.

32.9 Definition (Euler phi function)**.** The map $\varphi \colon \mathbb{Z}^+ \to \mathbb{Z}^+$ denoted by $\varphi(n) = |U_n|$ for $n \geq 2$, (where for a finite set S, $|S|$ denotes the number of elements in S), is called the Euler phi function.

So we have

$$\begin{aligned} \varphi(n) =& |U_n| = |\{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}| \\ =& \text{the number of integers } a \text{ with } 1 \leq a \leq n \text{ such that } gcd(a, n) = 1 \end{aligned}$$

32.10 Example. $\varphi(20) = 8$.

32.11 Example. When p is prime and $k \in \mathbb{Z}^+$,

$$\varphi(p^k) = p^k - p^{k-1}$$

32.12 Theorem. *For*

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

where p_i are distinct primes and $k_i \in \mathbb{Z}^+$

$$\begin{aligned} \varphi(n) =& \varphi(\prod_{i=1}^{l} p_i^{k_i}) \\ =& \prod_{i=1}^{l} \varphi(p_i)^{k_i} \\ =& \prod_{i=1}^{l} p_i^{k_i}(1 - \frac{1}{p_i}) \\ =& n \prod_{i=1}^{l} (1 - \frac{1}{p_i}) \\ =& n \prod_{p \mid n} (1 - \frac{1}{p}) \end{aligned}$$

Powers Modulo n

32.13 Example. What day will it be in 2^{100} days?