Multiplicative structure of integers mod n

Tuesday, June 29, 2021 3:29 PM

Here we want to investigate what elements of $\mathbb{Z}_n$ have multiplicative inverse.

<u>Def.</u> We say $[a]_n \in \mathbb{Z}_n$ has a multiplicative inverse if $[a]_n \cdot [a']_n = [1]_n$ for some $[a']_n \in \mathbb{Z}_n$. We say $[a]_n$ is a unit of $\mathbb{Z}_n$ if it has a multiplicative inverse. The set of all the units of $\mathbb{Z}_n$ is denoted by $\mathbb{Z}_n^{\times}$.

<u>Theorem</u>. Suppose $n \in \mathbb{Z}$ and $n \geq 2$. Then

$$\mathbb{Z}_n^{\times} = \{ [a]_n \mid \gcd(a,n) = 1 \}.$$

Moreover $|\mathbb{Z}_n^{\times}| = |\{ a \in \mathbb{Z} \mid 1 \leq a \leq n,\ \gcd(a,n)=1 \}|$.

(The left hand side of the above equality is denoted by $\phi(n)$ and it is called **Euler's phi function**.)

<u>Pf.</u> ($\subseteq$) Suppose $[a]_n \in \mathbb{Z}_n^{\times}$. Then $[a]_n [a']_n = [1]_n$ for some $a' \in \mathbb{Z}$. Hence $[aa']_n = [1]_n$ which implies that $aa' \overset{n}{\equiv} 1$.

(Earlier we proved that $b \overset{n}{\equiv} b'$ implies $\gcd(b,n) = \gcd(b',n)$.)

Hence $\gcd(aa', n) = \gcd(1, n) = 1$. Therefore $\gcd(a,n) = 1$.

($\supseteq$) Suppose $\gcd(a,n) = 1$. Then $1 = ra + sn$ for some

Multiplicative structure of integers mod n

Tuesday, June 29, 2021 3:29 PM

$r, s \in \mathbb{Z}$. Since $ra + sn = 1$, we obtain that

$$ra \overset{n}{\equiv} 1.$$

This implies that $[ra]_n = [1]_n$, and so $[r]_n [a]_n = [1]_n$.

Therefore $[a]_n \in \mathbb{Z}_n$.

- By the 1st part, we have

$$\{[a]_n \mid 1 \leq a \leq n,\ \gcd(a,n)=1\} \subseteq \mathbb{Z}_n^{\times}. \quad \text{(I)}$$

Next we show that the equality holds in (I). By the 1st part every element of $\mathbb{Z}_n^{\times}$ is of the form $[b]_n$ for some $b \in \mathbb{Z}$ such that $\gcd(b,n)$. Suppose r is the remainder of b divided by n. Then $b = nq + r$ for some integer q and $0 \leq r < n$. Hence $b \overset{n}{\equiv} r$. Therefore $\gcd(b,n) = \gcd(r,n)$, which implies that $\gcd(r,n) = 1$. Because $n \geq 2$ and $\gcd(r,n)=1$, $r \neq 0$. Altogether we have:

$$\left.\begin{array}{l} b \overset{n}{\equiv} r \Rightarrow [b]_n = [r]_n \\ 1 \leq r < n \text{ and } \gcd(r,n)=1 \end{array}\right\} \Rightarrow [b]_n \in \{[a]_n \mid 1 \leq a \leq n,\ \gcd(a,n)=1\}.$$

This completes the proof. ∎

Multiplicative structure of integers mod n

Tuesday, June 29, 2021 3:29 PM

Ex. List all the elements of $\mathbb{Z}_6^\times$.

Solution. $\mathbb{Z}_6^\times = \{[a]_6 \mid 1 \leq a \leq 6,\ \gcd(a,6)=1\}$

$$= \{[1]_6, [5]_6\}.$$

Ex. List all the elements of $\mathbb{Z}_8^\times$.

Solution. $\mathbb{Z}_8^\times = \{[a]_8 \mid 1 \leq a \leq 8,\ \gcd(a,8)=1\}$

Notice that all the divisors of 8 except 1 are even. So if a is odd, then $\gcd(a,8)=1$. Conversely if $\gcd(a,8)=1$, then a cannot be a multiple of 2. Hence

$$\gcd(a,8)=1 \iff a \text{ is odd.}$$

Thus $\mathbb{Z}_8^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$.

Proposition. Suppose p is prime. Then $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{[0]_p\}$.

Pf. By the previous theorem,

$$\mathbb{Z}_p^\times = \{[a]_p \mid 1 \leq a \leq p,\ \gcd(a,p)=1\}$$

Since p is prime, for every integer $1 \leq a < p$ we have $\gcd(a,p)=1$. Hence $\mathbb{Z}_p^\times = \{[a]_p \mid 1 \leq a < p\}$. Since $\mathbb{Z}_p = \{[0]_p, [1]_p, \ldots, [p-1]_p\}$, we obtain that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{[0]_p\}$. ∎

Multiplicative structure of integers mod n

Tuesday, June 29, 2021 3:29 PM

The converse of the previous proposition is essentially true:

- Suppose $n \in \mathbb{Z}, n \geq 2$. If $\mathbb{Z}_n^\times = \mathbb{Z}_n \setminus \{[0]_n\}$, then n is prime.

Pf. If $\mathbb{Z}_n^\times = \mathbb{Z}_n \setminus \{[0]_n\}$, then $\phi(n) = n-1$. This means

$$|\{a \in \mathbb{Z} \mid 1 \leq a \leq n, \ \gcd(a,n)=1\}| = n-1.$$

So n does not have any divisor in the interval $(1..n)$.

Since $n \geq 2$, we deduce that n is prime. ∎

Ex. Suppose p is prime and $k \in \mathbb{Z}^+$. Then $\phi(p^k) = p^k - p^{k-1}$.

Solution. We show that $\gcd(a, p^k) = 1 \iff p \nmid a$.

($\Rightarrow$) We show the contrapositive. If $p \mid a$, then p is a common divisor of a and p^k; and so $\gcd(a, p^k) \neq 1$.

($\Leftarrow$) We proceed by induction on k.

Base case. $k=1$.

Since $p \nmid a$, $\gcd(a,p) \neq p$. Since p has exactly two positive divisors 1 and p, we deduce that $\gcd(a,p)=1$.

Induction step. $\gcd(a, p^k)=1 \Rightarrow \gcd(a, p^{k+1}) = 1$.

By the base case, $\gcd(a,p)=1$. Then $\gcd(d,p)=1$ where

Multiplicative structure of integers mod n

Monday, August 7, 2017 3:29 PM

$d = \gcd(a, p^{k+1})$. Since $d \mid p^{k+1}$ and $\gcd(d,p)=1$, by Euclid's lemma, $d \mid p^k$. So d is a common divisor of a and p^k. Hence $d \le \gcd(a, p^k)$. By the induction hypothesis $\gcd(a, p^k)=1$, and so $d=1$. (Notice that $d \ge 1$).

This means $\gcd(a, p^{k+1})=1$, and claim follows.

By the above claim,

$$\phi(p^k) = |\{a \in \mathbb{Z} \mid 1 \le a \le p^k,\ \gcd(a,p^k)=1\}|$$
$$= |\{a \in \mathbb{Z} \mid 1 \le a \le p^k,\ p \nmid a\}|$$
$$= |[1..p^k] \setminus \{a \in \mathbb{Z} \mid 1 \le a \le p^k,\ p \mid a\}|$$
$$= p^k - |\{a \in \mathbb{Z} \mid 1 \le a \le p^k,\ p \mid a\}|.$$

$$1 \le a \le p^k,\ p \mid a \overset{(*)}{\iff} a = pa' \text{ and } 1 \le pa' \le p^k$$
$$\iff a = pa' \text{ and } 1 \le a' \le p^{k-1}$$

So there are p^{k-1} many a's that satisfy $(*)$. Hence

$$\phi(p^k) = p^k - p^{k-1}.$$ ∎

Next we show that $\mathbb{Z}_n^\times$ is closed under multiplication. This type of property plays an important role in group theory.

Multiplicative structure of integers mod n

Tuesday, June 29, 2021 3:29 PM

<u>Theorem</u>. Suppose $n \in \mathbb{Z}$ and $n \geq 2$. Then

(Operator) For every $[a]_n, [b]_n \in \mathbb{Z}_n^\times$, $[a]_n \cdot [b]_n \in \mathbb{Z}_n^\times$.

(Associative) For every $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n^\times$,

$$([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$$

(Neutral element) For every $[a]_n \in \mathbb{Z}_n^\times$, $[a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [a]_n$.

(Inverse) For every $[a]_n \in \mathbb{Z}_n^\times$, there is $[a']_n \in \mathbb{Z}_n^\times$ such that

$$[a]_n \cdot [a']_n = [a']_n \cdot [a]_n = [1]_n .$$

<u>Pf.</u> We have already proved that multiplication in $\mathbb{Z}_n$ is associative, and $[1]_n$ is a neutral element of multiplication. Next we show that $\mathbb{Z}_n^\times$ is closed under multiplication. Suppose $[a]_n, [b]_n \in \mathbb{Z}_n^\times$. Then there are $[a']_n, [b']_n \in \mathbb{Z}_n$ such that $[a]_n [a']_n = [1]_n$ and $[b]_n [b']_n = [1]_n$.

Hence $([a]_n [b]_n)([b']_n [a']_n) = [a]_n ([b]_n [b']_n) [a']_n$

$$= ([a]_n [1]_n) [a']_n$$

$$= [a]_n [a']_n = [1]_n .$$

This means $[a]_n [b]_n \in \mathbb{Z}_n^\times$. Finally let's discuss why

Multiplicative structure of integers mod n

Tuesday, June 29, 2021 3:29 PM

every element of $\mathbb{Z}_n^\times$ has an inverse in $\mathbb{Z}_n^\times$.

Since $[a]_n \in \mathbb{Z}_n^\times$, there is $[a']_n$ in $\mathbb{Z}_n$ such that

$$[a]_n [a']_n = [1]_n. \qquad \text{(I)}$$

(I) implies that $[a']_n [a]_n = [1]_n$, and so $[a']_n \in \mathbb{Z}_n^\times$.

This completes the proof. $\blacksquare$

Ex. Find a multiplicative inverse of $[20]_{47}$.

Solution. We have to find $x \in \mathbb{Z}$ such that

$$[20]_{47} [x]_{47} = [1]_{47}. \qquad \text{(II)}$$

Notice that (II) holds if and only if $20\, x \overset{47}{\equiv} 1$. (III)

(III) means $20\, x - 1 = 47\, y$ for some $y \in \mathbb{Z}$.

Hence we need to find an integer solution for

$$-47\, y + 20\, x = 1. \qquad \text{(IV)}$$

Earlier we have discussed that using Euclid's algorithm we can find an integer solution for (IV). Let $a_0 = 47$, $a_1 = 20$.

$47 = 20 \times 2 + 7$, $q_1 = 2$, $a_2 = 7$

$20 = 7 \times 2 + 6$, $q_2 = 2$, $a_3 = 6$

Multiplicative structure of integers mod n

Tuesday, June 29, 2021 3:29 PM

$7 = 6 \times 1 + 1, \quad q_3 = 1, \quad a_4 = 1$

$6 = 1 \times 6 + 0, \quad q_4 = 6, \quad a_5 = 0$

Then $\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \begin{bmatrix} 47 \\ 20 \end{bmatrix}$

$$\begin{bmatrix} 0 & 1 \\ 1 & -6 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 1 \\ 1 & -6 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 1 \\ 1 & -6 \end{bmatrix} \begin{bmatrix} -2 & 5 \\ 3 & -7 \end{bmatrix} = \begin{bmatrix} 3 & -7 \\ * & * \end{bmatrix}$$

So $\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 & -7 \\ * & * \end{bmatrix} \begin{bmatrix} 47 \\ 20 \end{bmatrix}$, which implies that

$$1 = (47)(3) + (20)(-7).$$

Hence $[20]_{47} \, [-7]_{47} = [1]_{47}$. (If you prefer a representative in the interval $[0 .. 46]$, notice that $[-7]_{47} = [40]_{7}$.) ∎