Outline

Unique prime factorizations

greatest common divisors

Euclidean algorithm

Extended Euclidean algorithm

multiplicative inverse

Observations

① $\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n \mid \underline{\gcd(a,n) = 1} \}$

forms a group under multiplication

② $\mathbb{Z}_n \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ when $\underline{\gcd(m_1, m_2) = 1}$

Chinearse Remaindor Theorem

Unique Prime Factorization

has an essentially unique factorization as a product of primes.

Theorem 1.20 (The Fundamental Theorem of Arithmetic)**.** *Let $a \geq 2$ be an integer. Then a can be factored as a product of prime numbers*

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_r^{e_r}.$$

Further, other than rearranging the order of the primes, this factorization into prime powers is unique.

Greatest common divisors

Definition: Given two integers a, b

If d divides a and divides b then

d is a common divisor of a and b

The largest such value of d is called

the greatest common divisor of a, b.

$\gcd(a, b)$

Examples: $\gcd(12, 18) = 6$

Compute gcd

(1)

$$\gcd(748, 2024) = 44.$$

One way to check that this is correct is to make lists of all of the positive divisors of 748 and of 2024.

$$\text{Divisors of } 748 = \{1, 2, 4, 11, 17, 22, 34, 44, 68, 187, 374, 748\},$$
$$\text{Divisors of } 2024 = \{1, 2, 4, 8, 11, 22, 23, 44, 46, 88, 92, 184, 253, 506, 1012, 2024\}.$$

(2) Observe the following: Assume $b \geq a$.

Case 1: a is a divisor of b

$\gcd(a,b) = a$

Case 2: b is not a divisor of a.

$b = aq + r \quad 0 < r < a$

$r = b - aq$

Observe that a common divisor of a and b is also a common divisor of r and b

A common divisor of r and b is also a common divisor of a and b. Hence,

$\gcd(b,a) = \gcd(a, r) \quad 0 < r < a.$

Euclidean Algorithm

$a = 2024,\ b = 748$

$$\begin{aligned} 2024 &= 748 \cdot 2 + 528 \\ 748 &= 528 \cdot 1 + 220 \\ 528 &= 220 \cdot 2 + \ \ 88 \\ 220 &= \ \ 88 \cdot 2 + \ \ 44 \quad \leftarrow \\ 88 &= \ \ 44 \cdot 2 + \ \ \ \ 0 \end{aligned}$$

$$\begin{aligned} a &= bq + r \\ b &= r q_1 + r_1 \\ r_0 &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_2 &= r_3 q_4 + 0 \end{aligned}$$

$$\begin{aligned} \gcd(a,b) = \gcd(b,r) = \gcd(r,r_1) &= \gcd(r_1,r_2) \cdots\cdots \\ &= \gcd(r_k, 0) \\ &= r_3 \end{aligned}$$

Theorem 1.7 (The Euclidean Algorithm)**.** *Let a and b be positive integers with $a \geq b$. The following algorithm computes $\gcd(a,b)$ in a finite number of steps.*

(1) *Let $r_0 = a$ and $r_1 = b$.*

(2) *Set $i = 1$.*

(3) *Divide r_{i-1} by r_i to get a quotient q_i and remainder r_{i+1},*

$$r_{i-1} = r_i \cdot q_i + r_{i+1} \qquad \textit{with} \quad 0 \leq r_{i+1} < r_i.$$

(4) *If the remainder $r_{i+1} = 0$, then $r_i = \gcd(a,b)$ and the algorithm terminates.*

(5) *Otherwise, $r_{i+1} > 0$, so set $i = i + 1$ and go to Step 3.*

Extended Euclidean Algorithm (Homework)

Given two integers a, b, $\exists$ integer u, v s.t.

$$au + bv = \gcd(a, b)$$

Application of Extended Euclidean Algorithm

$\mathbb{Z}_n^* = \{ a \mid \gcd(a,n) = 1 \}$ forms a group under multiplication

① closure : $a, b \in \mathbb{Z}_n^*$, $a*b \in \mathbb{Z}_n^*$ because $\gcd(a*b, n) = 1$

② identity : $1 * a = a * 1 = a$, $1 \in \mathbb{Z}_n^*$

③ inverse :

④ associativity : (by associativity of multiplication over integers)

③ We need to show that

$\forall a \in \mathbb{Z}_n^*$, $\exists\, b$ s.t. $a*b = b*a = 1 \bmod n$

See next page.

Theorem: Given integers a, n, $\exists\, b$ s.t.

$a \cdot b \equiv 1 \mod n$ iff $\gcd(a, n) = 1$

– If $a \cdot c \equiv 1 \mod n$, then $c \equiv b \mod n$

Proof:

$\leftarrow$ If $\gcd(a, n) = 1$, then $ab \equiv 1 \mod n$ for some b.

proof: By extended euclidean algorithm, since $\gcd(a, n) = 1$

$ab + nc = 1$ for some b, c

Take mod n

$ab = 1 \mod n$

$\rightarrow$ If $a \cdot b \equiv 1 \mod n$ then $\gcd(a, n) = 1$

proof: $ab - 1 = nc$ for some integer c

$ab - nc = 1$

If $d = \gcd(a, n)$, then $d \mid a$ and $d \mid n$ then, $d \mid 1$. So, $d = 1$.

To show that if $ab \equiv 1 \mod n$ and $ac \equiv 1 \mod n$ then $b \equiv c \mod n$:

$$b = b \cdot 1 = b \cdot a \cdot c = (b \cdot a) \cdot c = 1 \cdot c = c \mod n$$