CHAPTER 4 THE INTEGERS

SECTION 4.1 DIVISIBILITY

DEFINITION:

Let $n, d \in \mathbb{Z}$ with $d \neq 0$. We say that

d **DIVIDES** n if $n = dk$ for some $k \in \mathbb{Z}$

or equivalently, $n/d \in \mathbb{Z}$.

DEFINITION:

Let $n, d \in \mathbb{Z}$ with $d \neq 0$. We say that

d **DIVIDES** n if $n = dk$ for some $k \in \mathbb{Z}$

or equivalently, $n/d \in \mathbb{Z}$.

Other ways of saying include:

n is **DIVISIBLE** by d, or

n is a **MULTIPLE** of d, or

d is a **FACTOR** of n, or

d is a **DIVISOR** of n.

DEFINITION:

Let $n, d \in \mathbb{Z}$ with $d \neq 0$. We say that

d **DIVIDES** n if $n = dk$ for some $k \in \mathbb{Z}$

or equivalently, $n/d \in \mathbb{Z}$.

We write $d \mid n$ if d divides n and

$d \nmid n$ if d does not divide n.

DEFINITION:

Let $n, d \in \mathbb{Z}$ with $d \neq 0$. We say that

d **DIVIDES** n if $n = dk$ for some $k \in \mathbb{Z}$

or equivalently, $n/d \in \mathbb{Z}$.

We write $d \mid n$ if d divides n and

$d \nmid n$ if d does not divide n.

Do not confuse this with $\frac{d}{n}$ or d/n.

For example, $2 \mid 4$ describes a relationship between the integers 2 and 4, namely, 2 is a factor of 4. But $2/4$ is a fraction.

Remarks

- $\forall n \in \mathbb{Z}, n \neq 0, n \mid 0.$

Remarks

- $\forall n \in \mathbb{Z}, n \neq 0, n \mid 0.$

PROOF: Since $\frac{0}{n} = 0 \in \mathbb{Z}$, therefore $n \mid 0$.

- If $d \mid n$, then $\pm d \mid \pm n$.

- If $d \mid n$, then $\pm d \mid \pm n$.

PROOF: It follows from:

$$\frac{n}{d} \in \mathbb{Z} \quad \Rightarrow \quad \frac{\pm n}{\pm d} \in \mathbb{Z}$$

- If $d \mid n$ and $n \neq 0$, then $|d| \leq |n|$.

- If $d \mid n$ and $n \neq 0$, then $|d| \leq |n|$.

PROOF: If $d \mid n$, then $|d| \mid |n|$.

- If $d \mid n$ and $n \neq 0$, then $|d| \leq |n|$.

PROOF: If $d \mid n$, then $|d| \mid |n|$.

Thus $\exists k \in \mathbb{Z}$ such that $|n| = |d|k$.

- If $d \mid n$ and $n \neq 0$, then $|d| \leq |n|$.

PROOF: If $d \mid n$, then $|d| \mid |n|$.

Thus $\exists k \in \mathbb{Z}$ such that $|n| = |d|k$.

Since $|n|, |d| > 0$, $k \geq 1$.

Thus $|n| = |d|k \geq |d|$.

- How many multiples of 3 are there in $[1, 1000]$?

ANS: $\lfloor 1000/3 \rfloor = 333$.

THEOREM:

Let $a, b, c \in \mathbb{Z}$. Then

(i) if $a \mid b$, $b \mid c$, then $a \mid c$. (**TRANSITIVE** property.)

(ii) $\forall m, n \in \mathbb{Z}$, if $a \mid b$, $a \mid c$, then $a \mid mb + nc$.

THEOREM:

Let $a, b, c \in \mathbb{Z}$. Then

(i) if $a \mid b$, $b \mid c$, then $a \mid c$. (**TRANSITIVE** property.)

(ii) $\forall m, n \in \mathbb{Z}$, if $a \mid b$, $a \mid c$, then $a \mid mb + nc$.

PROOF: (i) Since $a \mid b$ and $b \mid c$,

THEOREM:

Let $a, b, c \in \mathbb{Z}$. Then

(i) if $a \mid b$, $b \mid c$, then $a \mid c$. (**TRANSITIVE** property.)

(ii) $\forall m, n \in \mathbb{Z}$, if $a \mid b$, $a \mid c$, then $a \mid mb + nc$.

PROOF: (i) Since $a \mid b$ and $b \mid c$,

$\exists\ k, \ell \in \mathbb{Z}$, $b = ak$ and $c = b\ell$.

THEOREM:

Let $a, b, c \in \mathbb{Z}$. Then

(i) if $a \mid b$, $b \mid c$, then $a \mid c$. (**TRANSITIVE** property.)

(ii) $\forall m, n \in \mathbb{Z}$, if $a \mid b$, $a \mid c$, then $a \mid mb + nc$.

PROOF: (i) Since $a \mid b$ and $b \mid c$,

$\exists\ k, \ell \in \mathbb{Z}$, $b = ak$ and $c = b\ell$.

Therefore $c = (ak)\ell = a(k\ell)$.

Since $k\ell \in \mathbb{Z}$, $a \mid c$.

The proof of (ii) is similar.

THEOREM:

DIVISION ALGORITHM

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$.

Then there are unique integers q and r, with $0 \leq r < d$ such that $n = dq + r$.

REMARK

- q is called the **QUOTIENT** and r the **REMAINDER**.

Notations:

$$q = n \textbf{ div } d \quad \text{and} \quad r = n \textbf{ mod } d.$$

Thus $2 = 7 \textbf{ div } 3$ and $1 = 7 \textbf{ mod } 3$.

REMARK

- q is called the **QUOTIENT** and r the **REMAINDER**.

Notations:

$$q = n \textbf{ div } d \quad \text{and} \quad r = n \textbf{ mod } d.$$

Thus $2 = 7$ **div** 3 and $1 = 7$ **mod** 3.

- Remainder is **NEVER NEGATIVE**.
- This is really not an algorithm.

THEOREM:

DIVISION ALGORITHM

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$.

Then there are unique integers q and r, with $0 \leq r < d$ such that $n = dq + r$.

PROOF: Let $q = \lfloor a/d \rfloor$ and $r = a - qd$. Then

THEOREM:

DIVISION ALGORITHM

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$.

Then there are unique integers q and r, with $0 \leq r < d$ such that $n = dq + r$.

PROOF: Let $q = \lfloor a/d \rfloor$ and $r = a - qd$. Then

$$q \leq \frac{a}{d} < q + 1$$

THEOREM:

DIVISION ALGORITHM

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$.

Then there are unique integers q and r, with $0 \leq r < d$ such that $n = dq + r$.

PROOF: Let $q = \lfloor a/d \rfloor$ and $r = a - qd$. Then

$$q \leq \frac{a}{d} < q + 1$$

Thus

$$0 \leq a - qd < d$$

and

$$0 \leq r < d$$

Hence q and r exist.

For uniqueness, suppose that p, s are integers satisfying

$$a = pd + s \quad \text{with} \quad 0 \leq s < d.$$

For uniqueness, suppose that p, s are integers satisfying

$$a = pd + s \quad \text{with} \quad 0 \leq s < d.$$

Then

$$0 \leq a - pd < d \quad \Rightarrow$$

For uniqueness, suppose that p, s are integers satisfying

$$a = pd + s \quad \text{with} \quad 0 \leq s < d.$$

Then

$$0 \leq a - pd < d \quad \Rightarrow \quad 0 \leq \frac{a}{d} - p < 1$$

For uniqueness, suppose that p, s are integers satisfying

$$a = pd + s \quad \text{with} \quad 0 \leq s < d.$$

Then

$$\begin{aligned} 0 \leq a - pd < d \quad &\Rightarrow \quad 0 \leq \frac{a}{d} - p < 1 \\ &\Rightarrow \quad p \leq \frac{a}{d} < p + 1 \end{aligned}$$

For uniqueness, suppose that p, s are integers satisfying

$$a = pd + s \quad \text{with} \quad 0 \leq s < d.$$

Then

$$\begin{aligned} 0 \leq a - pd < d \quad &\Rightarrow \quad 0 \leq \frac{a}{d} - p < 1 \\ &\Rightarrow \quad p \leq \frac{a}{d} < p + 1 \\ &\Rightarrow \quad p = \lfloor a/d \rfloor = q \end{aligned}$$

For uniqueness, suppose that p, s are integers satisfying

$$a = pd + s \quad \text{with} \quad 0 \leq s < d.$$

Then

$$\begin{aligned} 0 \leq a - pd < d \quad &\Rightarrow \quad 0 \leq \frac{a}{d} - p < 1 \\ &\Rightarrow \quad p \leq \frac{a}{d} < p + 1 \\ &\Rightarrow \quad p = \lfloor a/d \rfloor = q \end{aligned}$$

It then follows that $s = r$. This proves uniqueness.

EXAMPLE

- What are the quotient and remainder when
    * 0 is divided by 5?

EXAMPLE

- What are the quotient and remainder when
  - * 0 is divided by 5?

$$0 = 0 \times 5 + 0$$

* -11 is divided by 5?

* -11 is divided by 5?

$$-11 = -3 \times 5 + 4$$

* -1 is divided by 10?

* -1 is divided by 10?

$$-1 = -1 \times 10 + 9$$

- Every integer is either odd or even.

- Every integer is either odd or even.

PROOF: Let $n \in \mathbb{Z}$. Then $\exists q, r \in \mathbb{Z}$, $0 \leq r < 2$, such that

$$n = 2q + r$$

- Every integer is either odd or even.

PROOF: Let $n \in \mathbb{Z}$. Then $\exists q, r \in \mathbb{Z}$, $0 \leq r < 2$, such that

$$n = 2q + r$$

We have $r = 0$ or $r = 1$. Thus n is either even or odd.

MODULAR ARITHMETIC

DEFINITION:

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then

a is **CONGRUENT** to b modulo m

if $m \mid (a - b)$.

We write $a \equiv b \pmod{m}$.

EXAMPLE

- $5 \equiv 1 \pmod{2}$

because $2 \mid 5 - 1$.

- $-2 \equiv 4 \pmod 3$

because $3 \mid (-2) - 4$.

- $-4 \not\equiv 5 \pmod{7}$.

because $7 \nmid (-4) - 5$.

THEOREM:

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

Then $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$, i.e.,

a and b leave the same remainder when divided by m.

THEOREM:

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

Then $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$, i.e.,

a and b leave the same remainder when divided by m.

PROOF: $\exists q_i, r_i \in \mathbb{Z}$, with $0 \leq r_i < m$, $i = 1, 2$, such that

$$a = q_1 m + r_1 \quad \text{and} \quad b = q_2 m + r_2$$

THEOREM:

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

Then $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$, i.e.,

a and b leave the same remainder when divided by m.

PROOF: $\exists q_i, r_i \in \mathbb{Z}$, with $0 \leq r_i < m$, $i = 1, 2$, such that

$$a = q_1 m + r_1 \quad \text{and} \quad b = q_2 m + r_2$$

Therefore

$$a - b = m(q_1 - q_2) + (r_1 - r_2) \quad \text{with} \quad |r_1 - r_2| < m$$

$$a - b = m(q_1 - q_2) + (r_1 - r_2) \quad \text{with} \quad |r_1 - r_2| < m$$

Now

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid (a - b)$$

$$a - b = m(q_1 - q_2) + (r_1 - r_2) \quad \text{with} \quad |r_1 - r_2| < m$$

Now

$$\begin{aligned} a \equiv b \pmod{m} \quad &\Leftrightarrow \quad m \mid (a - b) \\ &\Leftrightarrow \quad m \mid r_1 - r_2 \end{aligned}$$

$$a - b = m(q_1 - q_2) + (r_1 - r_2) \quad \text{with} \quad |r_1 - r_2| < m$$

Now

$$\begin{aligned} a \equiv b \pmod{m} \quad &\Leftrightarrow \quad m \mid (a - b) \\ &\Leftrightarrow \quad m \mid r_1 - r_2 \\ &\Leftrightarrow \quad m \mid |r_1 - r_2| \end{aligned}$$

$$a - b = m(q_1 - q_2) + (r_1 - r_2) \quad \text{with} \quad |r_1 - r_2| < m$$

Now

$$\begin{aligned} a \equiv b \pmod{m} \quad &\Leftrightarrow \quad m \mid (a - b) \\ &\Leftrightarrow \quad m \mid r_1 - r_2 \\ &\Leftrightarrow \quad m \mid |r_1 - r_2| \\ &\Leftrightarrow \quad r_1 = r_2 \end{aligned}$$

THEOREM:

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

Then $a \equiv b \pmod{m}$

iff $\exists k \in \mathbb{Z}$ such that $a = b + km$.

THEOREM:

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

Then $a \equiv b \pmod{m}$

iff $\exists k \in \mathbb{Z}$ such that $a = b + km$.

PROOF:

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid (a - b)$$

THEOREM:

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

Then $a \equiv b \pmod{m}$

iff $\exists k \in \mathbb{Z}$ such that $a = b + km$.

PROOF:

$$\begin{aligned} a \equiv b \pmod{m} \quad &\Leftrightarrow \quad m \mid (a - b) \\ &\Leftrightarrow \quad \exists k \in \mathbb{Z}, a - b = km \end{aligned}$$

THEOREM:

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

Then $a \equiv b \pmod{m}$

iff $\exists k \in \mathbb{Z}$ such that $a = b + km$.

PROOF:

$$\begin{aligned} a \equiv b \pmod{m} &\Leftrightarrow m \mid (a - b) \\ &\Leftrightarrow \exists k \in \mathbb{Z}, a - b = km \\ &\Leftrightarrow \exists k \in \mathbb{Z}, a = b + km \end{aligned}$$

THEOREM:

Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}, \qquad ac \equiv bd \pmod{m}.$$

PROOF: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\exists p, q \in \mathbb{Z} \quad \text{s.t.} \quad a = b + pm,\ c = d + qm$$

PROOF: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\exists p, q \in \mathbb{Z} \quad \text{s.t.} \quad a = b + pm,\ c = d + qm$$

Thus

$$a + c = b + d + m(p + q)$$

PROOF: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\exists p, q \in \mathbb{Z} \quad \text{s.t.} \quad a = b + pm,\ c = d + qm$$

Thus

$$a + c = b + d + m(p + q)$$
$$ac = bd + m(bq + dp + mpq)$$

PROOF: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\exists p, q \in \mathbb{Z} \quad \text{s.t.} \quad a = b + pm,\ c = d + qm$$

Thus

$$a + c = b + d + m(p + q)$$
$$ac = bd + m(bq + dp + mpq)$$

Hence $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

PSEUDORANDOM NUMBERS

Randomly chosen numbers are often needed for computer simulation. Different methods have been devised for generating numbers that have properties of randomly chosen numbers. But such systematically chosen numbers are not truly random, they are called pseudorandom numbers.

LINEAR CONGRUENCE METHOD

In this method, we need 4 chosen integers:

- the **MODULUS** m,
- the **MULTIPLIER** a,
- the **INCREMENT** c, and
- the **SEED** x_0,

with $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.

We generate a sequence of numbers by starting with x_0 and

$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

With $m = 9$, $a = 7$, $c = 4$, $x_0 = 3$, we generate the sequence

$$3, 7, 8, 6, 1, 2, 0, 4, 5, \quad 3, 7, 8, 6, 1, 2, 0, 4, 5, \quad 3, \ldots$$

This sequence contains nine different integers before repeating, i.e., the period is 9.

(Note the period is at most m. Thus it is possible that it is less than m.)

Of course, such a short period is no good.

The common choice is

$$m = 2^{31} - 1, \quad a = 7^5, \quad c = 0$$

This can be proved to have a period of $p = 2^{31} - 2$.

This sequence of p numbers can be used as a sequence of random numbers.

SECTION 4.2 PRIME NUMBERS AND GCD

DEFINITION:

A positive integer is

- **PRIME** if it has exactly 2 positive divisors, 1 and itself;
- **COMPOSITE** if it has more than 2 positive divisors.

REMARK

- The number 1 is neither prime nor composite.
- 7 is prime because it has exactly 2 positive divisors.
- 9 is composite because $3 \mid 9$.

THEOREM:

Every positive integer n greater than 1 has a divisor which is prime.

THEOREM:

Every positive integer n greater than 1 has a divisor which is prime.

PROOF: If n is prime, then n is a prime divisor of n.

If n is composite, then it has divisor other than 1 and n.

If n is composite, then it has divisor other than 1 and n. Let a be the smallest among such divisors.

If n is composite, then it has divisor other than 1 and n.

Let a be the smallest among such divisors.

We prove that that a is prime by contradiction.

If n is composite, then it has divisor other than 1 and n.

Let a be the smallest among such divisors.

We prove that that a is prime by contradiction.

If a is composite, then it has a divisor b such that

$$1 < b < a$$

If n is composite, then it has divisor other than 1 and n.

Let a be the smallest among such divisors.

We prove that that a is prime by contradiction.

If a is composite, then it has a divisor b such that

$$1 < b < a$$

Since $b \mid a$ and $a \mid n$, we have $b \mid n$,

If n is composite, then it has divisor other than 1 and n.

Let a be the smallest among such divisors.

We prove that that a is prime by contradiction.

If a is composite, then it has a divisor b such that

$$1 < b < a$$

Since $b \mid a$ and $a \mid n$, we have $b \mid n$.

This contradicts the choice of a.

Thus a is a prime divisor.

THEOREM: (PRIME FACTORIZATION THEOREM)

Every positive integer greater than 1 can be written uniquely as a product of primes where the prime factors are written in order of nondecreasing size.

THEOREM: (PRIME FACTORIZATION THEOREM)

Every positive integer greater than 1 can be written uniquely as a product of primes where the prime factors are written in order of nondecreasing size.

- This is also known as the **FUNDAMENTAL THEOREM OF ARITHMETIC**.
- The proof is in the last part of the chapter.

EXAMPLE

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$,

$641 = 641$ (this is prime),

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 37$.

COROLLARY:

Let the prime factorization of a positive integer m be

$$m = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}.$$

Then its divisors are of the form

$$d = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

where $0 \leq b_i \leq a_i$ for $i = 1, \dots, n$.

EXAMPLE

Since $500 = 2^2 5^3$, all its divisors are of the form

$$2^x 5^y$$

where $0 \leq x \leq 2$ and $0 \leq y \leq 3$.

Some of the divisors are:

$$2^1 5^2,\ 2^2 5^3,\ 2^0 5^2,\ 2^2 5^0, \text{ etc.}$$

THEOREM:

If n is composite, then it has a divisor d with $1 < d \leq \sqrt{n}$.

THEOREM:

If n is composite, then it has a divisor d with $1 < d \leq \sqrt{n}$.

PROOF: Since n is composite,

$\exists a$ such that $a \mid n$ and $1 < a < n$.

THEOREM:

If n is composite, then it has a divisor d with $1 < d \leq \sqrt{n}$.

PROOF: Since n is composite,

$\exists a$ such that $a \mid n$ and $1 < a < n$.

Thus $\exists b$ such that $n = ab$.

THEOREM:

If n is composite, then it has a divisor d with $1 < d \leq \sqrt{n}$.

PROOF: Since n is composite,

$\exists a$ such that $a \mid n$ and $1 < a < n$.

Thus $\exists b$ such that $n = ab$.

If a and b are both $> \sqrt{n}$, we get

$$n = ab > (\sqrt{n})^2 = n$$

a contradiction.

THEOREM:

If n is composite, then it has a divisor d with $1 < d \leq \sqrt{n}$.

PROOF: Since n is composite,

$\exists a$ such that $a \mid n$ and $1 < a < n$.

Thus $\exists b$ such that $n = ab$.

If a and b are both $> \sqrt{n}$, we get

$$n = ab > (\sqrt{n})^2 = n$$

a contradiction.

Thus the smaller of a, b, say a, is $\leq \sqrt{n}$.

This completes the proof since a is such a divisor.

COROLLARY:

If n does not have a divisor d with $1 < d \leq \sqrt{n}$, then n is prime.

COROLLARY:

If n does not have a divisor d with $1 < d \leq \sqrt{n}$, then n is prime.

REMARK

In the above theorem and corollary, we need only consider prime divisors.

EXAMPLE

- 101 is prime

EXAMPLE

• 101 is prime because the primes $\leq \sqrt{101}$ are 2, 3, 5, 7 and none of them divides 101.

THEOREM:

There are Infinitely Many Primes

THEOREM:

There are Infinitely Many Primes

PROOF: By contradiction.

Suppose there are only n primes:

$$p_1, p_2, \ldots, p_n.$$

Suppose there are only n primes:

$$p_1, p_2, \ldots, p_n.$$

Consider the integer

$$N = p_1 p_2 \ldots p_n + 1.$$

Suppose there are only n primes:

$$p_1, p_2, \ldots, p_n.$$

Consider the integer

$$N = p_1 p_2 \ldots p_n + 1.$$

Now N has a prime divisor d.

Suppose there are only n primes:

$$p_1, p_2, \ldots, p_n.$$

Consider the integer

$$N = p_1 p_2 \ldots p_n + 1.$$

Now N has a prime divisor d.

Then d must be one of $p_1, p_2, \ldots, p_n$, say $d = p_k$.

Suppose there are only n primes:

$$p_1, p_2, \ldots, p_n.$$

Consider the integer

$$N = p_1 p_2 \ldots p_n + 1.$$

Now N has a prime divisor d.

Then d must be one of $p_1, p_2, \ldots, p_n$, say $d = p_k$.

Since $p_k \mid N$, $p_k \mid p_1 p_2 \cdots p_n$,

Suppose there are only n primes:

$$p_1, p_2, \ldots, p_n.$$

Consider the integer

$$N = p_1 p_2 \ldots p_n + 1.$$

Now N has a prime divisor d.

Then d must be one of $p_1, p_2, \ldots, p_n$, say $d = p_k$.

Since $p_k \mid N$, $p_k \mid p_1 p_2 \cdots p_n$,

we conclude that $p_k \mid 1$, a contradiction.

Thus the number of primes is infinite.

GCD

DEFINITION:

Let a and b be integers, not both zero.

The **GREATEST COMMON DIVISOR** of a and b,

denoted by $\gcd(a, b)$,

is the largest integer d such that $d \mid a$ and $d \mid b$.

EXAMPLE

- $\gcd(72, 63) = 9$ since the common divisors are 1, 3 and 9.

- Why is $\gcd(0, 0)$ undefined?

DEFINITION:

The integers a, b are **RELATIVELY PRIME**

if $\gcd(a, b) = 1$

EXAMPLE

- 12 and 35 are relative prime since $\gcd(12, 35) = 1$.
- 0 and 1 are relatively prime since $\gcd(0, 1) = 1$.

- For any integer n, n and $n + 1$ are relatively prime.

- For any integer n, n and $n+1$ are relatively prime.

PROOF: Let $\gcd(n, n+1) = d$.

- For any integer n, n and $n+1$ are relatively prime.

PROOF: Let $\gcd(n, n+1) = d$.

Then $d \mid n \quad$ and $\quad d \mid n+1$.

- For any integer n, n and $n+1$ are relatively prime.

PROOF: Let $\gcd(n, n+1) = d$.

Then $d \mid n \quad$ and $\quad d \mid n+1$.

Therefore $d \mid 1$ implying that $d = 1$.

GCD VIA PRIME FACTORIZATION: Let the prime factorizations of a, b be

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

where $a_i, b_i \geq 0$ for $i = 1, \dots, n$. Then

$$\gcd(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \dots p_n^{\min\{a_n, b_n\}}.$$

Here $\min\{x, y\}$ represents the smaller of the two numbers x, y.

EXAMPLE

- $120 = 2^3 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5 \cdot 7^0.$

$700 = 2^2 \cdot 5^2 \cdot 7 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7,$

$\therefore \quad \gcd(120, 700) = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 20.$

SECTION 4.3 ALGORITHMS

In everyday life, we use decimal representation (base 10) of numbers. For example

$$1023 = 1 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$$

and we take the coefficients of the various powers of 10 as the digits. This can be generalize to other bases.

BASE b EXPANSION OF INTEGERS

THEOREM:

Let $b(>1)$ be an integer. If $n \in \mathbb{Z}^+$, then it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_0 b^0$$

where $k \in \mathbb{Z}^*$ and $0 \leq a_i < b$ for $i = 0, \ldots, k$ and $a_k \neq 0$.

REMARK

- The representation is called **BASE b EXPANSION OF** n and is denoted as

$$(a_k a_{k-1} \dots a_0)_b$$

- $(245)_8 = 2 \cdot 8^2 + 4 \cdot 8^1 + 5 \cdot 8^0 = 165.$

- $b = 2$: **BINARY EXPANSION**.

- $b = 16$: **HEXADECIMAL EXPANSION.**

Here we use A, B, C, D, E, F to represent the digits 10, 11, 12, 13, 14 ,15.

Thus $(E0B)_{16} = 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 3595$.

ALGORITHM FOR BASE b EXPANSION

procedure base b expansion of $n \in \mathbb{Z}^+$

$q := n \qquad k := 0$

while $q \neq 0$

begin

$a_k := q$ **mod** b

$q := \lfloor q/b \rfloor$

$k := k + 1$

end

the base b expansion of n is $(a_{k-1} \ldots a_1 a_0)_b$

The base 8 expansion of 250 can be computed as follows:

$$250 = 31 \cdot 8 + 2$$

The base 8 expansion of 250 can be computed as follows:

$$250 = 31 \cdot 8 + 2$$
$$(q = 31, a_0 = 2)$$

The base 8 expansion of 250 can be computed as follows:

$$\begin{aligned} 250 &= 31 \cdot 8 + 2 \\ &\quad (q = 31, a_0 = 2) \\ 31 &= 3 \cdot 8 + 7 \end{aligned}$$

The base 8 expansion of 250 can be computed as follows:

$$\begin{aligned} 250 &= 31 \cdot 8 + 2 \\ &\quad (q = 31, a_0 = 2) \\ 31 &= 3 \cdot 8 + 7 \\ &\quad (q = 3, a_1 = 7) \end{aligned}$$

The base 8 expansion of 250 can be computed as follows:

$$\begin{aligned} 250 &= 31 \cdot 8 + 2 \\ &\quad (q = 31, a_0 = 2) \\ 31 &= 3 \cdot 8 + 7 \\ &\quad (q = 3, a_1 = 7) \\ 3 &= 0 \cdot 8 + 3 \end{aligned}$$

The base 8 expansion of 250 can be computed as follows:

$$\begin{aligned} 250 &= 31 \cdot 8 + 2 \\ &\quad (q = 31, a_0 = 2) \\ 31 &= 3 \cdot 8 + 7 \\ &\quad (q = 3, a_1 = 7) \\ 3 &= 0 \cdot 8 + 3 \\ &\quad (q = 0, a_2 = 3) \end{aligned}$$

The base 8 expansion of 250 can be computed as follows:

$$\begin{aligned} 250 &= 31 \cdot 8 + 2 \\ &\quad (q = 31, a_0 = 2) \\ 31 &= 3 \cdot 8 + 7 \\ &\quad (q = 3, a_1 = 7) \\ 3 &= 0 \cdot 8 + 3 \\ &\quad (q = 0, a_2 = 3) \end{aligned}$$

Thus $250 = (372)_8$.

THE EUCLIDEAN ALGORITHM

This is an efficient algorithm for find the gcd of 2 integers. It is based on the following result.

THEOREM:

Let a, b, q, r be integers such that

$$a = bq + r \quad \text{i.e.,} \quad a \ \mathbf{mod}\ b = r$$

Then

$$\gcd(a, b) = \gcd(b, r).$$

THEOREM:

Let a, b, q, r be integers such that

$$a = bq + r \quad \text{i.e.,} \quad a \ \mathbf{mod}\ b = r$$

Then

$$\gcd(a, b) = \gcd(b, r).$$

PROOF: Let $d = \gcd(a, b)$, $e = \gcd(b, r)$.

THEOREM:

Let a, b, q, r be integers such that

$$a = bq + r \quad \text{i.e.,} \quad a \ \mathbf{mod}\ b = r$$

Then

$$\gcd(a, b) = \gcd(b, r).$$

PROOF: Let $d = \gcd(a, b)$, $e = \gcd(b, r)$.

$$d = \gcd(a, b) \quad \Rightarrow \quad d \mid a \quad \text{and} \quad d \mid b.$$

THEOREM:

Let a, b, q, r be integers such that

$$a = bq + r \quad \text{i.e.,} \quad a \ \mathbf{mod}\ b = r$$

Then

$$\gcd(a, b) = \gcd(b, r).$$

PROOF: Let $d = \gcd(a, b)$, $e = \gcd(b, r)$.

$$d = \gcd(a, b) \quad \Rightarrow \quad d \mid a \quad \text{and} \quad d \mid b.$$

Thus $d \mid r$.

THEOREM:

Let a, b, q, r be integers such that

$$a = bq + r \quad \text{i.e.,} \quad a \ \mathbf{mod}\ b = r$$

Then

$$\gcd(a, b) = \gcd(b, r).$$

PROOF: Let $d = \gcd(a, b)$, $e = \gcd(b, r)$.

$$d = \gcd(a, b) \quad \Rightarrow \quad d \mid a \quad \text{and} \quad d \mid b.$$

Thus $d \mid r$.

Therefore d is a common divisor of b and r.

THEOREM:

Let a, b, q, r be integers such that

$$a = bq + r \quad \text{i.e.,} \quad a \ \mathbf{mod}\ b = r$$

Then

$$\gcd(a, b) = \gcd(b, r).$$

PROOF: Let $d = \gcd(a, b)$, $e = \gcd(b, r)$.

$$d = \gcd(a, b) \quad \Rightarrow \quad d \mid a \quad \text{and} \quad d \mid b.$$

Thus $d \mid r$.

Therefore d is a common divisor of b and r.

Thus $d \leq e$.

THEOREM:

Let a, b, q, r be integers such that

$$a = bq + r \quad \text{i.e.,} \quad a \ \mathbf{mod}\ b = r$$

Then

$$\gcd(a, b) = \gcd(b, r).$$

PROOF: Let $d = \gcd(a, b)$, $e = \gcd(b, r)$.

$$d = \gcd(a, b) \quad \Rightarrow \quad d \mid a \quad \text{and} \quad d \mid b.$$

Thus $d \mid r$.

Therefore d is a common divisor of b and r.

Thus $d \leq e$.

Similarly, we have $e \leq d$. Therefore $e = d$.

EUCLIDEAN ALGORITHM

To find $\gcd(a, b)$ **with** $a > b$**.**

$x := a$

$y := b$

while $y \neq 0$

begin

$r := x$ **mod** y

$x := y$

$y := r$

end $\{\gcd(a, b) = x\}$

EUCLIDEAN ALGORITHM

To find $\gcd(a, b)$ **with** $a > b$**.**

$x := a$

$y := b$

while $y \neq 0$

begin

$r := x$ **mod** y

$x := y$

$y := r$

end $\{\gcd(a, b) = x\}$

First divide a by b to get the remainder r.

Then divide b by r to get a new remainder.

Continue until the remainder is 0.

The last nonzero remainder the the gcd.

EXAMPLE

- Find $\gcd(414, 1076)$.

SOLN:

$$1076 \textbf{ mod } 414 = 248,$$

EXAMPLE

- Find $\gcd(414, 1076)$.

SOLN:

$$1076 \textbf{ mod } 414 = 248,$$
$$414 \textbf{ mod } 248 = 166,$$

EXAMPLE

- Find $\gcd(414, 1076)$.

SOLN:

$$1076 \textbf{ mod } 414 = 248,$$
$$414 \textbf{ mod } 248 = 166,$$
$$248 \textbf{ mod } 166 = 82,$$

EXAMPLE

- Find $\gcd(414, 1076)$.

SOLN:

$$1076 \textbf{ mod } 414 = 248,$$
$$414 \textbf{ mod } 248 = 166,$$
$$248 \textbf{ mod } 166 = 82,$$
$$166 \textbf{ mod } 82 = 2,$$

EXAMPLE

- Find $\gcd(414, 1076)$.

SOLN:

$$1076 \textbf{ mod } 414 = 248,$$
$$414 \textbf{ mod } 248 = 166,$$
$$248 \textbf{ mod } 166 = 82,$$
$$166 \textbf{ mod } 82 = 2,$$
$$82 \textbf{ mod } 2 = 0$$

Thus $\gcd(414, 1076) = 2$.

SECTION 4.4 APPLICATIONS

We shall discuss one application of number theory to cryptology.

SOME RESULTS

THEOREM:

Let $a, b \in \mathbb{Z}^+$ and $d = \gcd(a, b)$.

Then $\exists s, t \in \mathbb{Z}$ such that $d = as + bt$.

This is a consequence of the Euclidean algorithm.

EXAMPLE

$\gcd(414, 1076) = 2$: Work backwards. We have

$$166 \textbf{ mod } 82 = 2 \quad \therefore 2 = 166 - 82 \cdot 2$$

EXAMPLE

$\gcd(414, 1076) = 2$: Work backwards. We have

$$\begin{aligned} 166 \textbf{ mod } 82 = 2 \quad &\therefore 2 = 166 - 82 \cdot 2 \\ 248 \textbf{ mod } 166 = 82 \quad &\therefore 82 = 248 - 166 \cdot 1 \end{aligned}$$

EXAMPLE

$\gcd(414, 1076) = 2$: Work backwards. We have

$$\begin{aligned} 166 \textbf{ mod } 82 = 2 \quad & \therefore 2 = 166 - 82 \cdot 2 \\ 248 \textbf{ mod } 166 = 82 \quad & \therefore 82 = 248 - 166 \cdot 1 \\ 414 \textbf{ mod } 248 = 166 \quad & \therefore 166 = 414 - 248 \cdot 1 \end{aligned}$$

EXAMPLE

$\gcd(414, 1076) = 2$: Work backwards. We have

$$\begin{aligned} 166 \textbf{ mod } 82 = 2 \quad & \therefore 2 = 166 - 82 \cdot 2 \\ 248 \textbf{ mod } 166 = 82 \quad & \therefore 82 = 248 - 166 \cdot 1 \\ 414 \textbf{ mod } 248 = 166 \quad & \therefore 166 = 414 - 248 \cdot 1 \\ 1076 \textbf{ mod } 414 = 248 \quad & \therefore 248 = 1076 - 414 \cdot 2 \end{aligned}$$

$$
\begin{aligned}
166 \textbf{ mod } 82 = 2 \quad & \therefore 2 = 166 - 82 \cdot 2 \\
248 \textbf{ mod } 166 = 82 \quad & \therefore 82 = 248 - 166 \cdot 1 \\
414 \textbf{ mod } 248 = 166 \quad & \therefore 166 = 414 - 248 \cdot 1 \\
1076 \textbf{ mod } 414 = 248 \quad & \therefore 248 = 1076 - 414 \cdot 2
\end{aligned}
$$

Hence

$$2 = 166 - 82 \cdot 2$$

$$
\begin{aligned}
166 \bmod 82 = 2 \quad & \therefore 2 = 166 - 82 \cdot 2 \\
248 \bmod 166 = 82 \quad & \therefore 82 = 248 - 166 \cdot 1 \\
414 \bmod 248 = 166 \quad & \therefore 166 = 414 - 248 \cdot 1 \\
1076 \bmod 414 = 248 \quad & \therefore 248 = 1076 - 414 \cdot 2
\end{aligned}
$$

Hence

$$
\begin{aligned}
2 &= 166 - 82 \cdot 2 \\
&= 166 - (248 - 166 \cdot 1) \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
166 \bmod 82 = 2 \quad & \therefore 2 = 166 - 82 \cdot 2 \\
248 \bmod 166 = 82 \quad & \therefore 82 = 248 - 166 \cdot 1 \\
414 \bmod 248 = 166 \quad & \therefore 166 = 414 - 248 \cdot 1 \\
1076 \bmod 414 = 248 \quad & \therefore 248 = 1076 - 414 \cdot 2
\end{aligned}
$$

Hence

$$
\begin{aligned}
2 &= 166 - 82 \cdot 2 \\
&= 166 - (248 - 166 \cdot 1) \cdot 2 \\
&= -248 \cdot 2 + 166 \cdot 3
\end{aligned}
$$

$$
\begin{aligned}
166 \bmod 82 = 2 \quad & \therefore 2 = 166 - 82 \cdot 2 \\
248 \bmod 166 = 82 \quad & \therefore 82 = 248 - 166 \cdot 1 \\
414 \bmod 248 = 166 \quad & \therefore 166 = 414 - 248 \cdot 1 \\
1076 \bmod 414 = 248 \quad & \therefore 248 = 1076 - 414 \cdot 2
\end{aligned}
$$

Hence

$$
\begin{aligned}
2 &= 166 - 82 \cdot 2 \\
&= 166 - (248 - 166 \cdot 1) \cdot 2 \\
&= -248 \cdot 2 + 166 \cdot 3 \\
&= -248 \cdot 2 + (414 - 248 \cdot 1) \cdot 3
\end{aligned}
$$

$$
\begin{aligned}
166 \bmod 82 = 2 \quad & \therefore 2 = 166 - 82 \cdot 2 \\
248 \bmod 166 = 82 \quad & \therefore 82 = 248 - 166 \cdot 1 \\
414 \bmod 248 = 166 \quad & \therefore 166 = 414 - 248 \cdot 1 \\
1076 \bmod 414 = 248 \quad & \therefore 248 = 1076 - 414 \cdot 2
\end{aligned}
$$

Hence

$$
\begin{aligned}
2 &= 166 - 82 \cdot 2 \\
&= 166 - (248 - 166 \cdot 1) \cdot 2 \\
&= -248 \cdot 2 + 166 \cdot 3 \\
&= -248 \cdot 2 + (414 - 248 \cdot 1) \cdot 3 \\
&= 414 \cdot 3 - 248 \cdot 5
\end{aligned}
$$

$$
\begin{aligned}
166 \bmod 82 = 2 \quad & \therefore 2 = 166 - 82 \cdot 2 \\
248 \bmod 166 = 82 \quad & \therefore 82 = 248 - 166 \cdot 1 \\
414 \bmod 248 = 166 \quad & \therefore 166 = 414 - 248 \cdot 1 \\
1076 \bmod 414 = 248 \quad & \therefore 248 = 1076 - 414 \cdot 2
\end{aligned}
$$

Hence

$$
\begin{aligned}
2 &= 166 - 82 \cdot 2 \\
&= 166 - (248 - 166 \cdot 1) \cdot 2 \\
&= -248 \cdot 2 + 166 \cdot 3 \\
&= -248 \cdot 2 + (414 - 248 \cdot 1) \cdot 3 \\
&= 414 \cdot 3 - 248 \cdot 5 \\
&= 414 \cdot 3 - (1076 - 414 \cdot 2) \cdot 5
\end{aligned}
$$

$$
\begin{aligned}
166 \bmod 82 = 2 \quad & \therefore 2 = 166 - 82 \cdot 2 \\
248 \bmod 166 = 82 \quad & \therefore 82 = 248 - 166 \cdot 1 \\
414 \bmod 248 = 166 \quad & \therefore 166 = 414 - 248 \cdot 1 \\
1076 \bmod 414 = 248 \quad & \therefore 248 = 1076 - 414 \cdot 2
\end{aligned}
$$

Hence

$$
\begin{aligned}
2 &= 166 - 82 \cdot 2 \\
&= 166 - (248 - 166 \cdot 1) \cdot 2 \\
&= -248 \cdot 2 + 166 \cdot 3 \\
&= -248 \cdot 2 + (414 - 248 \cdot 1) \cdot 3 \\
&= 414 \cdot 3 - 248 \cdot 5 \\
&= 414 \cdot 3 - (1076 - 414 \cdot 2) \cdot 5 \\
&= 414 \cdot 13 - 1076 \cdot 5
\end{aligned}
$$

THEOREM:

If $a, b, c \in \mathbb{Z}^+$ such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

THEOREM:

If $a, b, c \in \mathbb{Z}^+$ such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

PROOF: There exist integers s, t, k such that

$$as + bt = 1 \quad \text{and} \quad bc = ak$$

THEOREM:

If $a, b, c \in \mathbb{Z}^+$ such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

PROOF: There exist integers s, t, k such that

$$as + bt = 1 \quad \text{and} \quad bc = ak$$

Multiple the first by c and then substitute for bc, we have

$$acs + bct = c \quad \Rightarrow \quad a(cs + kt) = c$$

THEOREM:

If $a, b, c \in \mathbb{Z}^+$ such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

PROOF: There exist integers s, t, k such that

$$as + bt = 1 \quad \text{and} \quad bc = ak$$

Multiple the first by c and then substitute for bc, we have

$$acs + bct = c \quad \Rightarrow \quad a(cs + kt) = c$$

Thus $a \mid c$ as required.

THEOREM:

If p is a prime and $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_k$ for some k.

The proof is by mathematical induction and is omitted.

THEOREM: CANCELLATION

Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. Then

$$ac \equiv bc \pmod{m} \quad \& \quad \gcd(c, m) = 1 \quad \Rightarrow \quad a \equiv b \pmod{m}.$$

THEOREM: CANCELLATION

Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. Then

$$ac \equiv bc \pmod{m} \quad \& \quad \gcd(c, m) = 1 \quad \Rightarrow \quad a \equiv b \pmod{m}.$$

PROOF: $ac \equiv bc \pmod{m} \quad \Rightarrow \quad m \mid c(a - b)$.

THEOREM: CANCELLATION

Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. Then

$$ac \equiv bc \pmod{m} \quad \& \quad \gcd(c, m) = 1 \quad \Rightarrow \quad a \equiv b \pmod{m}.$$

PROOF: $ac \equiv bc \pmod{m} \quad \Rightarrow \quad m \mid c(a - b)$.

Since $\gcd(c, m) = 1$, $m \mid a - b$.

THEOREM: CANCELLATION

Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. Then

$$ac \equiv bc \pmod{m} \quad \& \quad \gcd(c, m) = 1 \quad \Rightarrow \quad a \equiv b \pmod{m}.$$

PROOF: $ac \equiv bc \pmod{m} \quad \Rightarrow \quad m \mid c(a - b)$.

Since $\gcd(c, m) = 1$, $m \mid a - b$.

Therefore $a \equiv b \pmod{m}$.

DEFINITION:

Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$.

An integer $\overline{a}$ such that

$$\overline{a}a \equiv 1 \pmod{m}$$

is called a **MULTIPLICATIVE INVERSE OF** a **MODULO** m.

REMARK

• Multiplicative inverses are not unique. For example, 2, 7, 12, etc are all inverses of 3 modulo 5. since

$$2 \cdot 3 \equiv 1, \quad 7 \cdot 3 \equiv 1 \quad 12 \cdot 3 \equiv 1 \pmod{5}.$$

REMARK

• Multiplicative inverses are not unique. For example, 2, 7, 12, etc are all inverses of 3 modulo 5 since

$$2 \cdot 3 \equiv 1, \quad 7 \cdot 3 \equiv 1 \quad 12 \cdot 3 \equiv 1 \pmod{5}.$$

However, there is only one between 0 and m. We usually take this as the inverse.

• Multiplicative inverses may not exist. For example, 2 does not have an inverse modulo 6 since

$$2 \cdot 1, 2 \cdot 2, 2 \cdot 3, 2 \cdot 4, 2 \cdot 5$$

are all ALL $\not\equiv 1 \pmod 6$.

THEOREM:

Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$.

Then the inverse of a modulo m exists iff $\gcd(a, m) = 1$.

The inverse, if exists, is unique modulo m, i.e., if c, d are inverses, then

$$c \equiv d \pmod{m}$$

PROOF: Suppose a has an inverse, say b. Then

$$ab \equiv 1 \pmod{m}$$

PROOF: Suppose a has an inverse, say b. Then

$$\begin{aligned} & ab \equiv 1 \pmod{m} \\ \Rightarrow \quad & ab - 1 = mt \quad \text{for some } t \in \mathbb{Z} \end{aligned}$$

PROOF: Suppose a has an inverse, say b. Then

$$\begin{aligned} & ab \equiv 1 \pmod{m} \\ \Rightarrow \quad & ab - 1 = mt \quad \text{for some } t \in \mathbb{Z} \\ \Rightarrow \quad & ab - mt = 1 \end{aligned}$$

PROOF: Suppose a has an inverse, say b. Then

$$\begin{aligned} & ab \equiv 1 \pmod{m} \\ \Rightarrow \quad & ab - 1 = mt \quad \text{for some } t \in \mathbb{Z} \\ \Rightarrow \quad & ab - mt = 1 \end{aligned}$$

If $\gcd(a, m) = d$, then $d \mid a$, $d \mid m$.

PROOF: Suppose a has an inverse, say b. Then

$$\begin{aligned} & ab \equiv 1 \pmod{m} \\ \Rightarrow \quad & ab - 1 = mt \quad \text{for some } t \in \mathbb{Z} \\ \Rightarrow \quad & ab - mt = 1 \end{aligned}$$

If $\gcd(a, m) = d$, then $d \mid a$, $d \mid m$.

Therefore $d \mid 1$ which implies that $d = 1$.

Suppose $\gcd(a, m) = 1$.

Suppose $\gcd(a, m) = 1$.

Then there exists integers s, t such that

$$\gcd(a, m) = 1 = as + mt$$

Suppose $\gcd(a, m) = 1$.

Then there exists integers s, t such that

$$\gcd(a, m) = 1 = as + mt$$

Thus $as \equiv 1 \pmod{m}$. Hence s is an inverse of a.

Suppose w is another inverse.

Suppose w is another inverse.

Then $as \equiv aw \pmod{m}$.

Suppose w is another inverse.

Then $as \equiv aw \pmod{m}$.

Since $\gcd(a, m) = 1$, we have $s \equiv w \pmod{m}$.

REMARK

• When m is small, multiplicative inverses can be found by trying numbers less than m.

If $m = 5$, the multiplicative inverse of 2 can be found by computing

$$2 \cdot 2, \quad 2 \cdot 3, \quad 2 \cdot 4$$

Since $2 \cdot 3 \equiv 1 \pmod 5$, $\overline{2} = 3$.

- When m is large, we can use the Euclidean algorithm.
- To find $\overline{207}$ modulo 331, we note that

$$\gcd(207, 331) = 1 = 207 \cdot 8 - 331 \cdot 5$$

Thus $\overline{207} = 8$

THEOREM:

Let $n \in \mathbb{Z}^+$. Suppose $a, b, c \in \mathbb{Z}$, where b is a multiplicative inverse of a modulo n. Then

$$ax \equiv c \textbf{ mod } n \Leftrightarrow x \equiv bc \pmod{n}.$$

PROOF: ($\Rightarrow$) If $ax \equiv c \bmod n$, then

$$x = 1 \cdot x \equiv (ab)x \bmod n$$

(as b is a multiplicative inverse of a modulo n;)

PROOF: ($\Rightarrow$) If $ax \equiv c \bmod n$, then

$$\begin{aligned} x = 1 \cdot x &\equiv (ab)x \bmod n \\ &\quad \text{(as } b \text{ is a multiplicative inverse of } a \text{ modulo } n\text{;)} \\ &= b(ax) \equiv bc \bmod n \\ &\quad \text{(as } ax \equiv c \bmod n\text{.)} \end{aligned}$$

($\Leftarrow$) If $x \equiv bc \bmod n$, then

$$\begin{aligned} ax &\equiv a(bc) \bmod n \\ &\qquad (\text{as } x \equiv bc \bmod n;) \end{aligned}$$

($\Leftarrow$) If $x \equiv bc \bmod n$, then

$$\begin{aligned} ax &\equiv a(bc) \bmod n \\ &\quad \text{(as } x \equiv bc \bmod n\text{;)} \\ &\equiv 1 \cdot c \bmod n \\ &\quad \text{(as } b \text{ is a multiplicative inverse of } a \text{ modulo } n\text{;)} \\ &= c. \end{aligned}$$

EXAMPLE

- Solve $5x \equiv 2 \textbf{ mod } 6$:

EXAMPLE

- Solve $5x \equiv 2 \textbf{ mod } 6$:

SOLN: $5 \cdot 5 \equiv 1 \textbf{ mod } 6$. Therefore, 5 is a multiplicative inverse of 5.

The solution is

$$\begin{aligned} x &\equiv 5 \times 2 \textbf{ mod } 6 \\ &= 10 \\ &\equiv 4 \textbf{ mod } 6. \end{aligned}$$

- Solve $26x \equiv 9 \textbf{ mod } 35$.

- Solve $26x \equiv 9$ **mod** 35.

SOLN:

Run the Euclidean Algorithm on 35 and 26:

$$35 = 26 \times 1 + 9$$

- Solve $26x \equiv 9$ **mod** 35.

SOLN:

Run the Euclidean Algorithm on 35 and 26:

$$35 = 26 \times 1 + 9$$
$$26 = 9 \times 2 + 8$$

- Solve $26x \equiv 9$ **mod** 35.

SOLN:

Run the Euclidean Algorithm on 35 and 26:

$$\begin{aligned} 35 &= 26 \times 1 + 9 \\ 26 &= 9 \times 2 + 8 \\ 9 &= 8 \times 1 + 1 \end{aligned}$$

- Solve $26x \equiv 9$ **mod** 35.

SOLN:

Run the Euclidean Algorithm on 35 and 26:

$$\begin{aligned} 35 &= 26 \times 1 + 9 \\ 26 &= 9 \times 2 + 8 \\ 9 &= 8 \times 1 + 1 \\ 8 &= 1 \times 8 + 0 \end{aligned}$$

- Solve $26x \equiv 9$ **mod** 35.

SOLN:

Run the Euclidean Algorithm on 35 and 26:

$$\begin{aligned} 35 &= 26 \times 1 + 9 \\ 26 &= 9 \times 2 + 8 \\ 9 &= 8 \times 1 + 1 \\ 8 &= 1 \times 8 + 0 \end{aligned}$$

So

$$1 = 9 - 8 \times 1$$

- Solve $26x \equiv 9$ **mod** 35.

SOLN:

Run the Euclidean Algorithm on 35 and 26:

$$\begin{aligned} 35 &= 26 \times 1 + 9 \\ 26 &= 9 \times 2 + 8 \\ 9 &= 8 \times 1 + 1 \\ 8 &= 1 \times 8 + 0 \end{aligned}$$

So

$$\begin{aligned} 1 &= 9 - 8 \times 1 \\ &= 9 - (26 - 9 \times 2) \times 1 = -26 + 3 \times 9 \end{aligned}$$

- Solve $26x \equiv 9$ **mod** 35.

SOLN:

Run the Euclidean Algorithm on 35 and 26:

$$\begin{aligned} 35 &= 26 \times 1 + 9 \\ 26 &= 9 \times 2 + 8 \\ 9 &= 8 \times 1 + 1 \\ 8 &= 1 \times 8 + 0 \end{aligned}$$

So

$$\begin{aligned} 1 &= 9 - 8 \times 1 \\ &= 9 - (26 - 9 \times 2) \times 1 = -26 + 3 \times 9 \\ &= -26 + 3 \times (35 - 26 \times 1) = 3 \times 35 - 4 \times 26 \end{aligned}$$

- Solve $26x \equiv 9 \textbf{ mod } 35$.

SOLN:

Run the Euclidean Algorithm on 35 and 26:

$$\begin{aligned} 35 &= 26 \times 1 + 9 \\ 26 &= 9 \times 2 + 8 \\ 9 &= 8 \times 1 + 1 \\ 8 &= 1 \times 8 + 0 \end{aligned}$$

So

$$\begin{aligned} 1 &= 9 - 8 \times 1 \\ &= 9 - (26 - 9 \times 2) \times 1 = -26 + 3 \times 9 \\ &= -26 + 3 \times (35 - 26 \times 1) = 3 \times 35 - 4 \times 26 \\ &\equiv -4 \times 26 \textbf{ mod } 35. \end{aligned}$$

Hence -4 is a multiplicative inverse of 26 modulo 35. Thus the solution to the congruence equation is

$$\begin{aligned} x &\equiv -4 \times 9 \textbf{ mod } 35 \\ &= -36 \\ &\equiv 34 \textbf{ mod } 35. \end{aligned}$$

THEOREM: FERMAT'S LITTLE THEOREM

If p is a prime and $a \in \mathbb{Z}$ such that $\gcd(p, a) = 1$,

then $a^{p-1} \equiv 1 \pmod{p}$.

THEOREM: FERMAT'S LITTLE THEOREM

If p is a prime and $a \in \mathbb{Z}$ such that $\gcd(p, a) = 1$,

then $a^{p-1} \equiv 1 \pmod{p}$.

EXAMPLE

- Let $p = 5$, $a = 2$, then $2^4 \equiv 1 \pmod{5}$.
- Let $p = 7$, $a = 3$, then $3^6 \equiv 1 \pmod{7}$.

PROOF: We first prove, by contradiction, that

$$ai \not\equiv aj \pmod{p} \quad \text{if } 1 \leq i < j \leq p-1.$$

PROOF: We first prove, by contradiction, that

$$ai \not\equiv aj \pmod{p} \quad \text{if } 1 \leq i < j \leq p-1.$$

Suppose there exist $i < j$ so that

$$ai \equiv aj \pmod{p}$$

PROOF: We first prove, by contradiction, that

$$ai \not\equiv aj \pmod{p} \quad \text{if } 1 \leq i < j \leq p-1.$$

Suppose there exist $i < j$ so that

$$\begin{aligned} & ai \equiv aj \pmod{p} \\ \Rightarrow \quad & i \equiv j \pmod{p} \quad (\text{since } \gcd(p, a) = 1) \end{aligned}$$

PROOF: We first prove, by contradiction, that

$$ai \not\equiv aj \pmod{p} \quad \text{if } 1 \leq i < j \leq p-1.$$

Suppose there exist $i < j$ so that

$$\begin{aligned} & ai \equiv aj \pmod{p} \\ \Rightarrow \quad & i \equiv j \pmod{p} \quad (\text{since } \gcd(p, a) = 1) \\ \Rightarrow \quad & j - i \equiv 0 \pmod{p} \end{aligned}$$

PROOF: We first prove, by contradiction, that

$$ai \not\equiv aj \pmod{p} \quad \text{if } 1 \leq i < j \leq p-1.$$

Suppose there exist $i < j$ so that

$$\begin{aligned} & ai \equiv aj \pmod{p} \\ \Rightarrow \quad & i \equiv j \pmod{p} \quad (\text{since } \gcd(p, a) = 1) \\ \Rightarrow \quad & j - i \equiv 0 \pmod{p} \\ \Rightarrow \quad & p \mid (j - i) \end{aligned}$$

PROOF: We first prove, by contradiction, that

$$ai \not\equiv aj \pmod{p} \quad \text{if } 1 \leq i < j \leq p-1.$$

Suppose there exist $i < j$ so that

$$\begin{aligned} & ai \equiv aj \pmod{p} \\ \Rightarrow \quad & i \equiv j \pmod{p} \quad (\text{since } \gcd(p, a) = 1) \\ \Rightarrow \quad & j - i \equiv 0 \pmod{p} \\ \Rightarrow \quad & p \mid (j - i) \end{aligned}$$

This leads to a contradiction as

p is prime and $0 < j - i < p$ and therefore

p cannot divide $j - i$.

It then follows that

$$1a \bmod p, \quad 2a \bmod p, \quad \ldots \quad , \quad (p-1)a \bmod p$$

are pairwise distinct.

It then follows that

$$1a \bmod p, \quad 2a \bmod p, \quad \ldots \quad , \quad (p-1)a \bmod p$$

are pairwise distinct.

Hence, they just rearrangement of

$$\{1, 2 \ldots, p-1\}.$$

It then follows that

$$1a \bmod p, \quad 2a \bmod p, \quad \ldots \quad , \quad (p-1)a \bmod p$$

are pairwise distinct.

Hence, they just rearrangement of

$$\{1, 2 \ldots, p-1\}.$$

Thus

$$(p-1)! \equiv (1a) \cdot (2a) \cdots ((p-1)a) = (p-1)! a^{p-1} \pmod{p}.$$

It then follows that

$$1a \bmod p, \quad 2a \bmod p, \quad \dots \quad , \quad (p-1)a \bmod p$$

are pairwise distinct.

Hence, they just rearrangement of

$$\{1, 2 \dots, p-1\}.$$

Thus

$$(p-1)! \equiv (1a) \cdot (2a) \cdots ((p-1)a) = (p-1)! a^{p-1} \pmod{p}.$$

Since $\gcd(p, (p-1)!) = 1$, we can cancel and have

$$a^{p-1} \equiv 1 \pmod{p}.$$

TWO THEOREMS' PROOF

THEOREM: (FUNDAMENTAL THEOREM OF ARITHMETIC, PRIME FACTORIZATION THEOREM)

Every positive integer greater than 1 can be written uniquely as a product of primes where the prime factors are written in order of nondecreasing size.

PROOF: (EXISTENCE)

We show this by Strong Mathematical Induction.

PROOF: (EXISTENCE)

We show this by Strong Mathematical Induction.

For each $n \in \mathbb{Z}_{\geq 2}$, let $P(n)$ be the proposition "n has a prime factorization".

PROOF: (EXISTENCE)

We show this by Strong Mathematical Induction.

For each $n \in \mathbb{Z}_{\geq 2}$, let $P(n)$ be the proposition "n has a prime factorization".

Base step: 2 is a prime factorization of 2 because 2 is prime. So $P(2)$ is true.

Induction step:

Let $k \in \mathbb{Z}_{\geq 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

Induction step:

Let $k \in \mathbb{Z}_{\geq 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

If $k+1$ is prime, then $k+1$ is a prime factorization of $k+1$.

Induction step:

Let $k \in \mathbb{Z}_{\geq 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

If $k+1$ is prime, then $k+1$ is a prime factorization of $k+1$.

So suppose $k+1$ is not prime.

Induction step:

Let $k \in \mathbb{Z}_{\geq 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

If $k+1$ is prime, then $k+1$ is a prime factorization of $k+1$.

So suppose $k+1$ is not prime.

Then $k+1$ is composite.

Induction step:

Let $k \in \mathbb{Z}_{\geq 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

If $k+1$ is prime, then $k+1$ is a prime factorization of $k+1$.

So suppose $k+1$ is not prime.

Then $k+1$ is composite.

Suppose $1 < d, e < k+1$ are such that $k+1 = de$.

Induction step:

Let $k \in \mathbb{Z}_{\geq 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

If $k+1$ is prime, then $k+1$ is a prime factorization of $k+1$.

So suppose $k+1$ is not prime.

Then $k+1$ is composite.

Suppose $1 < d, e < k+1$ are such that $k+1 = de$.

By inductive hypothesis, $P(d)$ and $P(k)$ are both true.

Induction step:

Let $k \in \mathbb{Z}_{\geq 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

If $k+1$ is prime, then $k+1$ is a prime factorization of $k+1$.

So suppose $k+1$ is not prime.

Then $k+1$ is composite.

Suppose $1 < d, e < k+1$ are such that $k+1 = de$.

By inductive hypothesis, $P(d)$ and $P(k)$ are both true.

Therefore, both d and e have prime factorizations.

Induction step:

Let $k \in \mathbb{Z}_{\geq 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

If $k+1$ is prime, then $k+1$ is a prime factorization of $k+1$.

So suppose $k+1$ is not prime.

Then $k+1$ is composite.

Suppose $1 < d, e < k+1$ are such that $k+1 = de$.

By inductive hypothesis, $P(d)$ and $P(k)$ are both true.

Therefore, both d and e have prime factorizations.

This implies $k+1$ has a prime factorization, because $k+1 = de$.

Induction step:

Let $k \in \mathbb{Z}_{\geq 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

If $k+1$ is prime, then $k+1$ is a prime factorization of $k+1$.

So suppose $k+1$ is not prime.

Then $k+1$ is composite.

Suppose $1 < d, e < k+1$ are such that $k+1 = de$.

By inductive hypothesis, $P(d)$ and $P(k)$ are both true.

Therefore, both d and e have prime factorizations.

This implies $k+1$ has a prime factorization, because $k+1 = de$.

So $P(k+1)$ is true.

(UNIQUENESS)

Suppose $n \in \mathbb{Z}_{\geq 2}$ with two different prime factorizations:

$$p_0 p_1 \dots p_k = n = q_0 q_1 \dots q_\ell.$$

(UNIQUENESS)

Suppose $n \in \mathbb{Z}_{\geq 2}$ with two different prime factorizations:

$$p_0 p_1 \dots p_k = n = q_0 q_1 \dots q_\ell.$$

Now we cancel all the primes that are common to both sides of the above equation.

(UNIQUENESS)

Suppose $n \in \mathbb{Z}_{\geq 2}$ with two different prime factorizations:

$$p_0 p_1 \dots p_k = n = q_0 q_1 \dots q_\ell.$$

Now we cancel all the primes that are common to both sides of the above equation.

We know that some primes are left on both sides because otherwise the two prime factorizations are the same when arranged in nondecreasing order.

(UNIQUENESS)

Suppose $n \in \mathbb{Z}_{\geq 2}$ with two different prime factorizations:

$$p_0 p_1 \dots p_k = n = q_0 q_1 \dots q_\ell.$$

Now we cancel all the primes that are common to both sides of the above equation.

We know that some primes are left on both sides because otherwise the two prime factorizations are the same when arranged in nondecreasing order.

Let the result of the cancellation be

$$p'_0 p'_1 \dots p'_{k'} = q'_0 q'_1 \dots q'_{\ell'}.$$

(UNIQUENESS)

Suppose $n \in \mathbb{Z}_{\geq 2}$ with two different prime factorizations:

$$p_0 p_1 \dots p_k = n = q_0 q_1 \dots q_\ell.$$

Now we cancel all the primes that are common to both sides of the above equation.

We know that some primes are left on both sides because otherwise the two prime factorizations are the same when arranged in nondecreasing order.

Let the result of the cancellation be

$$p'_0 p'_1 \dots p'_{k'} = q'_0 q'_1 \dots q'_{\ell'}.$$

No prime occurs on both sides of the above equation. since we cancelled out all of them.

(UNIQUENESS)

Suppose $n \in \mathbb{Z}_{\geq 2}$ with two different prime factorizations:

$$p_0 p_1 \dots p_k = n = q_0 q_1 \dots q_\ell.$$

Now we cancel all the primes that are common to both sides of the above equation.

We know that some primes are left on both sides because otherwise the two prime factorizations are the same when arranged in nondecreasing order.

Let the result of the cancellation be

$$p'_0 p'_1 \dots p'_{k'} = q'_0 q'_1 \dots q'_{\ell'}.$$

No prime occurs on both sides of the above equation. since we cancelled out all of them.

$\therefore p'_0 \mid q'_0 q'_1 \dots q'_{\ell'}.$

(UNIQUENESS)

Suppose $n \in \mathbb{Z}_{\geq 2}$ with two different prime factorizations:

$$p_0 p_1 \dots p_k = n = q_0 q_1 \dots q_\ell.$$

Now we cancel all the primes that are common to both sides of the above equation.

We know that some primes are left on both sides because otherwise the two prime factorizations are the same when arranged in nondecreasing order.

Let the result of the cancellation be

$$p'_0 p'_1 \dots p'_{k'} = q'_0 q'_1 \dots q'_{\ell'}.$$

No prime occurs on both sides of the above equation. since we cancelled out all of them.

$\therefore p'_0 \mid q'_0 q'_1 \dots q'_{\ell'}.$

Then there is an $i \in \{0, 1, \dots, \ell'\}$ such that $p'_0 \mid q'_i$.

(UNIQUENESS)

Suppose $n \in \mathbb{Z}_{\geq 2}$ with two different prime factorizations:

$$p_0 p_1 \dots p_k = n = q_0 q_1 \dots q_\ell.$$

Now we cancel all the primes that are common to both sides of the above equation.

We know that some primes are left on both sides because otherwise the two prime factorizations are the same when arranged in nondecreasing order.

Let the result of the cancellation be

$$p'_0 p'_1 \dots p'_{k'} = q'_0 q'_1 \dots q'_{\ell'}.$$

No prime occurs on both sides of the above equation. since we cancelled out all of them.

$\therefore p'_0 \mid q'_0 q'_1 \dots q'_{\ell'}.$

Then there is an $i \in \{0, 1, \dots, \ell'\}$ such that $p'_0 \mid q'_i$.

Since q'_i is prime, its only positive divisors are 1 and q'_i. So $p'_0 = q'_i$ as $p'_0 \neq 1$. (Contradiction.)

THEOREM: (BASE-b EXPANSION)

For any $n \in \mathbb{Z}^+$, there exist unique $k \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_k \in \{0, 1, \ldots, b-1\}$ such that

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_0 b^0, \qquad a_k \neq 0.$$

PROOF: **(EXISTENCE)** As we already saw, Algorithm for base b expansion gives a base-b representation of any positive integer.

(UNIQUENESS) We prove this by Strong Mathematical Induction.

(UNIQUENESS) We prove this by Strong Mathematical Induction.

For each $n \in \mathbb{Z}^+$, let $P(n)$ be the proposition "n has at most one base-b representation".

(UNIQUENESS) We prove this by Strong Mathematical Induction.

For each $n \in \mathbb{Z}^+$, let $P(n)$ be the proposition "n has at most one base-b representation".

Base step: Let $c \in \{1, 2, \ldots, b-1\}$.

Suppose

$$c = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0$$

and $a_\ell \neq 0$, where $\ell \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell \in \{0, 1, \ldots, b-1\}$.

(UNIQUENESS) We prove this by Strong Mathematical Induction.

For each $n \in \mathbb{Z}^+$, let $P(n)$ be the proposition "n has at most one base-b representation".

Base step: Let $c \in \{1, 2, \ldots, b-1\}$.

Suppose

$$c = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0$$

and $a_\ell \neq 0$, where $\ell \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell \in \{0, 1, \ldots, b-1\}$.

If we have $i \in \{1, 2, \ldots, \ell\}$ such that $a_i \geq 1$, then

$$c = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0 \geq a_i b^i \geq 1 \times b^1 = b,$$

which contradicts the choice of c.

(UNIQUENESS) We prove this by Strong Mathematical Induction.

For each $n \in \mathbb{Z}^+$, let $P(n)$ be the proposition "n has at most one base-b representation".

Base step: Let $c \in \{1, 2, \ldots, b-1\}$.

Suppose

$$c = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0$$

and $a_\ell \neq 0$, where $\ell \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell \in \{0, 1, \ldots, b-1\}$.

If we have $i \in \{1, 2, \ldots, \ell\}$ such that $a_i \geq 1$, then

$$c = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0 \geq a_i b^i \geq 1 \times b^1 = b,$$

which contradicts the choice of c.

This means $a_1 = a_2 = \ldots = a_\ell = 0$, and so $\ell = 0$. Thus $c = a_0 b^0 = a_0$.

(UNIQUENESS) We prove this by Strong Mathematical Induction.

For each $n \in \mathbb{Z}^+$, let $P(n)$ be the proposition "n has at most one base-b representation".

Base step: Let $c \in \{1, 2, \ldots, b-1\}$.

Suppose

$$c = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0$$

and $a_\ell \neq 0$, where $\ell \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell \in \{0, 1, \ldots, b-1\}$.

If we have $i \in \{1, 2, \ldots, \ell\}$ such that $a_i \geq 1$, then

$$c = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0 \geq a_i b^i \geq 1 \times b^1 = b,$$

which contradicts the choice of c.

This means $a_1 = a_2 = \ldots = a_\ell = 0$, and so $\ell = 0$. Thus $c = a_0 b^0 = a_0$.

Hence all base-b representations of c must be the same as $(c)_b$. So $P(c)$ is true.

Induction step:

Let $k \in \mathbb{Z}_{\geq b-1}$ such that

$$P(1), P(2), \ldots, P(k)$$

are all true.

Induction step:

Let $k \in \mathbb{Z}_{\geq b-1}$ such that

$$P(1), P(2), \ldots, P(k)$$

are all true.

Let $\ell, m \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell, d_0, d_1, \ldots, d_m \in \{0, 1, \ldots, b-1\}$ such that

$$a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0 = k+1 = d_m b^m + d_{m-1} b^{m-1} + \ldots + d_0 b^0$$

and $a_\ell > 0$ and $d_m > 0$.

Induction step:

Let $k \in \mathbb{Z}_{\geq b-1}$ such that

$$P(1), P(2), \ldots, P(k)$$

are all true.

Let $\ell, m \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell, d_0, d_1, \ldots, d_m \in \{0, 1, \ldots, b-1\}$ such that

$$a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0 = k+1 = d_m b^m + d_{m-1} b^{m-1} + \ldots + d_0 b^0$$

and $a_\ell > 0$ and $d_m > 0$.

The quotients one gets when these are divided by b are equal too, i.e.,

$$a_\ell b^{\ell-1} + a_{\ell-1} b^{\ell-2} + \ldots + a_1 b^0 = (k+1) \textbf{ div } b$$
$$= d_m b^{m-1} + d_{m-1} b^{m-2} + \ldots + d_1 b^0.$$

Induction step:

Let $k \in \mathbb{Z}_{\geq b-1}$ such that

$$P(1), P(2), \ldots, P(k)$$

are all true.

Let $\ell, m \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell, d_0, d_1, \ldots, d_m \in \{0, 1, \ldots, b-1\}$ such that

$$a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0 = k+1 = d_m b^m + d_{m-1} b^{m-1} + \ldots + d_0 b^0$$

and $a_\ell > 0$ and $d_m > 0$.

The quotients one gets when these are divided by b are equal too, i.e.,

$$a_\ell b^{\ell-1} + a_{\ell-1} b^{\ell-2} + \ldots + a_1 b^0 = (k+1) \textbf{ div } b$$

$$= d_m b^{m-1} + d_{m-1} b^{m-2} + \ldots + d_1 b^0.$$

Note that $1 \leq (k+1) \textbf{ div } b \leq (k+k) \textbf{ div } 2 = k$ because $k + 1 \geq b \geq 2$.

Induction step:

Let $k \in \mathbb{Z}_{\geq b-1}$ such that

$$P(1), P(2), \ldots, P(k)$$

are all true.

Let $\ell, m \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell, d_0, d_1, \ldots, d_m \in \{0, 1, \ldots, b-1\}$ such that

$$a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0 = k+1 = d_m b^m + d_{m-1} b^{m-1} + \ldots + d_0 b^0$$

and $a_\ell > 0$ and $d_m > 0$.

The quotients one gets when these are divided by b are equal too, i.e.,

$$a_\ell b^{\ell-1} + a_{\ell-1} b^{\ell-2} + \ldots + a_1 b^0 = (k+1) \textbf{ div } b$$

$$= d_m b^{m-1} + d_{m-1} b^{m-2} + \ldots + d_1 b^0.$$

Note that $1 \leq (k+1) \textbf{ div } b \leq (k+k) \textbf{ div } 2 = k$ because $k + 1 \geq b \geq 2$.

So $P((k+1) \textbf{ div } b)$ is true by the induction hypothesis, i.e., $(k+1) \textbf{ div } b$ has at most one base-b representation.

Induction step:

Let $k \in \mathbb{Z}_{\geq b-1}$ such that

$$P(1), P(2), \ldots, P(k)$$

are all true.

Let $\ell, m \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_\ell, d_0, d_1, \ldots, d_m \in \{0, 1, \ldots, b-1\}$ such that

$$a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_0 b^0 = k+1 = d_m b^m + d_{m-1} b^{m-1} + \ldots + d_0 b^0$$

and $a_\ell > 0$ and $d_m > 0$.

The quotients one gets when these are divided by b are equal too, i.e.,

$$a_\ell b^{\ell-1} + a_{\ell-1} b^{\ell-2} + \ldots + a_1 b^0 = (k+1) \textbf{ div } b$$

$$= d_m b^{m-1} + d_{m-1} b^{m-2} + \ldots + d_1 b^0.$$

Note that $1 \leq (k+1) \textbf{ div } b \leq (k+k) \textbf{ div } 2 = k$ because $k + 1 \geq b \geq 2$.

So $P((k+1) \textbf{ div } b)$ is true by the induction hypothesis, i.e., $(k+1) \textbf{ div } b$ has at most one base-b representation.

This implies $\ell = m$ and $a_i = d_i$ for all $i \in \{1, 2, \ldots, \ell\}$.

Substituting these back, it gives

$$\begin{aligned} & a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_1 b^1 + a_0 b^0 \\ &= d_m b^m + d_{m-1} b^{m-1} + \ldots + d_1 b^1 + d_0 b^0 \\ &= a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \ldots + a_1 b^1 + d_0 b^0. \end{aligned}$$

Thus $a_0 = a_0 b^0 = d_0 b^0 = d_0$. So $P(k+1)$ is true.