CHAPTER 3 THE INTEGERS

SECTION 3.1 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, $n/d \in \mathbb{Z}$.

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.

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

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

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

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

PROOF: It follows from: $\frac{n}{d} \in \mathbb{Z} \Rightarrow \frac{\pm n}{\pm d} \in \mathbb{Z}$.

- 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 $|n|, |d| > 0$, we have $k \geq 1$. 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 $a \mid mb + nc$.

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.

section 3.4 of text

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**. We use the following notations:

$$q = n \textbf{ Div } d \quad \text{and} \quad r = n \textbf{ Mod } d.$$

Thus $2 = 7 \textbf{ Div } 3$ and $1 = 7 \textbf{ Mod } 3$.

- Remainder is **NEVER NEGATIVE**.

PROOF: (Division algorithm) Let $q = \lfloor a/d \rfloor$ and $r = a - qd$. Then $q \leq a/d < q + 1$. Thus $0 \leq a - qd < d$. Thus $0 \leq r < d$. Hence q and r exist.

For uniqueness, suppose that p, s are integers satisfying

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

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?

  * -11 is divided by 5?

  * -1 is divided by 10?

- 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 **Mod** $m = b$ **Mod** m, i.e., a and b leave the same remainder when divided by m.

PROOF: By the division algorithm, $\exists q_i, r_i \in \mathbb{Z}$, with $0 \le r_i < m$, $i = 1, 2$, such that $a = q_1 m + r_1$, and $b = q_2 m + r_2$. Therefore $a - b = m(q_1 - q_2) + (r_1 - r_2)$, with $|r_1 - r_2| < m$. Now

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

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 $a = b + km$.

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 $\exists p, q \in \mathbb{Z}$ such that $a = b + pm$ and $c = d + qm$. Thus $a + c = b + d + m(p + q)$ and $ac = bd + m(bq + dp + mpq)$. Hence $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

SOME APPLICATIONS OF CONGRUENCE

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 $2 \le a < m$, $0 \le c < m$, $0 \le x_0 < m$. We generate a sequence of numbers by starting with x_0 and successively using the congruence

$$x_{n+1} = (ax_n + c) \ \mathbf{Mod} \ m.$$

EXAMPLE

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.

REMARK

The common choice is $m = 2^{31} - 1$, $a = 7^5$, $c = 0$. 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 3.2 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.

Section 3.5 in text

REMARK

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

SIEVE OF ERATOSTHENES

This is an algorithm to find all primes less than a given number n.

Step 1: 2 is prime. Delete all multiples of 2.

Step 2: The first number is now 3. It is prime. Delete all multiples of 3.

Step 3: The first number is now 5. It is prime. Delete all multiples of 5.

Continue this way until no numbers are left.

- Use this to find all primes < 50.

(1) List the numbers:

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

(2) Delete multiples of 2:

(2) 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49

(3) Delete multiples of 3:

(2 3) 5 7 11 13 17 19 23 25 29 31 35 37 41 43 47 49

(4) After a few more steps, the primes are:

2 3 5 7 11 13 17 19 23 25 29 31 37 41 43 47

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. Let a be the smallest among such divisors.

We'll 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.

- This is also known as the **FUNDAMENTAL THEOREM OF ARITHMETIC**.
- The uniqueness part is proved in section 3.7 while the existence part is in 4.2.

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

EXAMPLE

Since $500 = 2^2 5^3$, all its divisors are of the form $2^x 5^y$ where $0 \le x \le 2$ and $0 \le y \le 3$.

Some of the divisors are: $2^1 5^2$, $2^2 5^3$, $2^0 5^2$, $2^2 5^0$, etc.

THEOREM:

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

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 $\le \sqrt{n}$. This completes the proof since a is such a divisor.

The following is an easy corollary.

COROLLARY:

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

REMARK

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

EXAMPLE

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

THEOREM:

There are Infinitely Many Primes

PROOF: We will prove this by contradiction. 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 & LCM

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?
- The GCD can be found by the Euclidean Algorithm (Section 3.6.)

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.

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

- Since

$$120 = 2^3 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5 \cdot 7^0 \quad \text{and} \quad 700 = 2^2 \cdot 5^2 \cdot 7 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7,$$

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

DEFINITION:

The **LEAST COMMON MULTIPLE**, $\mathrm{lcm}(a, b)$, of the positive integers a and b is the smallest positive integer that is a multiple of both a and b.

With a and b as above,

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

Thus with $120 = 2^3 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5 \cdot 7^0$ and $700 = 2^2 \cdot 5^2 \cdot 7 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7$, $\mathrm{lcm}(120, 700) = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1 = 4200$.

THEOREM:

Let a, b be positive integers. Then $ab = \gcd(a, b)\mathrm{lcm}(a, b)$.

PROOF: The proof follows from the fact that $\max\{x, y\} + \min\{x, y\} = x + y$.

SECTION 3.3 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.

Section 3.6 in text

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 proof can be constructed using mathematical induction, a proof method to be discussed in chapter 4.

- The representation in the theorem is called **BASE b EXPANSION OF n** and is denoted as $(a_k a_{k-1} \ldots a_0)_b$.

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

- When $b = 2$, the representation is called **BINARY EXPANSION**. When $b = 16$, the expansion is called **HEXADECIMAL EXPANSION**. Here we use A, B, C, D, E, F to represent the digits 10, 11, 12, 13, 14 ,15. These are the representations commonly used in computer science. 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 $n \in \mathbb{Z}^+$
$q := n$
$k := 0$
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:

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

Thus $250 = (372)_8$.

MODULAR EXPONENTIATION

$\boxed{\text{Find } b^n \textbf{ Mod } m}$

(1) compute $n = (a_k \dots a_1 a_0)_2$.

(2) Compute $r_0 = b, r_1 = b^2, r_2 = b^4, \dots, r_k = b^{2^k}$ **Mod** m.

(3) b^n **Mod** $m = r_0^{a_0} r_1^{a_1} \cdots r_k^{a_k}$ **Mod** m.

EXAMPLE: Find 3^{101} **Mod** 100.

Step (1). $101 = (1100101)_2 = 2^6 + 2^5 + 2^2 + 2^0 = 64 + 32 + 4 + 1$. So $3^{101} = 3^{64}3^{32}3^4 3^1$.

Step (2) all congruences modulo 100:

$$\begin{aligned} 3^2 &\equiv 9 \\ 3^4 &\equiv 9^2 \equiv 81 \\ 3^8 &\equiv 81^2 \equiv 61 \\ 3^{16} &\equiv 61^2 \equiv 21 \\ 3^{32} &\equiv 21^2 \equiv 41 \\ 3^{64} &\equiv 41^2 \equiv 81. \end{aligned}$$

Step (3) Finally

$$3^{101} \equiv 3^{64}3^{32}3^4 3^1 \equiv 81 \cdot 41 \cdot 81 \cdot 3 \equiv 3 \pmod{100}.$$

- In general, if $n = (a_k \dots a_1 a_0)_2$, then $2^k \leq n < 2^{k+1}$. From here we deduce that $k = \lfloor \log_2 n \rfloor$. Thus we need to perform the squaring operation k times to obtain $r_0, r_1, \dots r_k$ and perform another $k+1$ multiplication operations to obtain the final result. Thus the total number of operations is roughly $2\lfloor \log_2 n \rfloor$. This is much lower than the n operations that you'd need if you were to perform the calculation by brute force.

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 $a = bq + r$, i.e., a **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 $y$ ($r$ is the remainder when $x$ is divided by $y$.)
    $x := y$
    $y := r$
end $\{\gcd(a,b) = x\}$
```

This is what you do:

$$\begin{aligned} a \textbf{ Mod } b &= r_1 \\ b \textbf{ Mod } r_1 &= r_2 \\ r_1 \textbf{ Mod } r_2 &= r_3 \\ r_2 \textbf{ Mod } r_3 &= r_4 \\ &\cdots \\ r_{k-2} \textbf{ Mod } r_{k-1} &= r_k \\ r_{k-1} \textbf{ Mod } r_k &= 0 \end{aligned}$$

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

EXAMPLE

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

SOLN:

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

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

SECTION 3.4 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. We shall not provide a formal proof.

The integers s, t can be obtained by working backwards from the Euclidean algorithm.

EXAMPLE

$\gcd(414, 1076) = 2$: We have, backwards from the algorithm,

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

Hence

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

Section 3.7 in text

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 $p \mid a_1 a_2 \dots a_n$, 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 $a, b, c \in \mathbb{Z}$. Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. Then

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

PROOF: $ac \equiv bc \pmod{m}$ implies $m \mid c(a - b)$. 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 an **INVERSE OF** a **MODULO** m.

REMARK

- Inverses are not unique. For example, 2, 7, 12, etc are all inverses of 3 modulo 5

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

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

- Inverse 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. We want to prove that $\gcd(a, m) = 1$. Then

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

If $\gcd(a, m) = d$, then $d \mid a$, $d \mid m$. Therefore $d \mid 1$ which implies that $d = 1$. d l a*b + m*(-t)

Suppose $\gcd(a, m) = 1$. We want to prove that an inverse exists. 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.

mt multiple of m,

Finally, we prove the uniqueness of inverse. Suppose w is another inverse, then $as \equiv aw \pmod{m}$. Since $\gcd(a, m) = 1$, we have $s \equiv w \pmod{m}$. s is an inverse, w also inverse

cancellation

REMARK

- When m is small, inverses can be found by trying numbers less than m. If $m = 5$, the inverse of 2 can be found by computing $2 \cdot 2, 2 \cdot 3, 2 \cdot 4$. 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, by using the Euclidean Algorithm, we have

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

Taking mod 331, we have $1 \equiv 207 \cdot 8 \pmod{331}$. Thus $\overline{207} = 8$.

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 $3^6 \equiv 1 \pmod{7}$.

RSA CRYPTOSYSTEM

In the public key cryptography, the encryption key E to encode a message is known to the public but only the receiver has the decryption key D to decode the message. The sender has a message M and uses E to turn it into a coded message C. The receiver then uses D to recover M from C.

Thus for the system to work, it would have to be practically impossible for anyone to work out the decryption key from knowing the encryption key. In 1976 three researchers at MIT, Ronald Rivest, Adi Shamir and Leonard Adleman announced to the world the **RSA system** of public key cryptosystem based on modular arithmetic.

The system:

Initial step: Find two large primes p, q, say with 200 digits each and an exponent e such that $\gcd((p-1)(q-1), e) = 1$. Compute the product $n = pq$. Find the inverse d of e modulo $(p-1)(q-1)$, i.e.,

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

(The number $d(< (p-1)(q-1))$ exists because $\gcd((p-1)(q-1), e) = 1$.)

The Keys: The encryption key is n, e and is public knowledge. The decryption key is d and is known only to the receiver.

Encryption: Represent each of the alphabets, punctuation marks, spaces, etc, by an integer. These integers are grouped together to form a large integer I. If n has k digits, then I is broken up into blocks of size $k-1$, starting from the right so that each block is an integer less than n. Each such block of the plaintext is an integer M. This is encrypted into the ciphertext C using the formula

$$C = M^e \textbf{ Mod } n,$$

which is transmitted to the receiver.

Decryption The receiver uses the decryption key d and the formula:

$$M = C^d \textbf{ Mod } n$$

to recover the message.

Proof of the formula We have

$$C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}.$$

We may assume that $\gcd(M, p) = \gcd(M, q) = 1$. (This holds except in rare cases). Then, by FLT,

$$M^{p-1} \equiv 1 \pmod{p} \quad \text{and} \quad M^{q-1} \equiv 1 \pmod{q}.$$

Consequently,

$$C^d \equiv M(M^{p-1})^{k(q-1)} \equiv M \pmod{p}$$

and

$$C^d \equiv M(M^{q-1})^{k(p-1)} \equiv M \pmod{q}.$$

Because p, q are distinct primes, we have $C^d \equiv M \pmod{pq}$.

RSA system works because it is easy to find large primes p, q. To break the code, we need to factorize the large integer n. However, all known algorithms to factorize large integers are very slow. Thus the code cannot be broken unless a fast factorization algorithm is found.

EXAMPLE

Encrypt the message STOP using RSA with $p = 43$, $q = 59$ and $e = 13$.

SOLN:

We have $n = pq = 2537$. Note that $\gcd(e, (p-1)(q-1)) = \gcd(13, 2436) = 1$ so that the choice of $e = 13$ is alright.

Now translate STOP into its numerical equivalent, using 01 for a, 02 for b, etc. The message is translated into 19201516. Since n has 4 digits, we need to break it up into blocks of 3 digits so that each block is $< n$:

$$19 \quad 201 \quad 516.$$

We now encrypt using $C = M^{13}$ **Mod** 2537, we have

$$19^{13} \textbf{ Mod } 2537 = 2299, \quad 201^{13} \textbf{ Mod } 2537 = 1953, \quad 516^{13} \textbf{ Mod } 2537 = 1247$$

The encrypted message is

$$2299 \quad 1953 \quad 1247.$$

EXAMPLE

Decode the above message.

SOLN: It's not hard to find that the inverse of $e = 13$ mod $(p-1)(q-1) = 2436$ is $d = 937$. (Use the euclidean algorithm.) Thus we can decrypt using $M = C^{937}$ **Mod** 2537. We have

$$2299^{937} \textbf{ Mod } 2537 = 19, \quad 1953^{937} \textbf{ Mod } 2537 = 201, \quad 1247^{937} \textbf{ Mod } 2537 = 516$$

The message is 19201516 which translates back to STOP.

(Note: The message has 3 blocks. All the blocks, except the first, must have 3 digits each. You append digits at the left to achieve that.)