Number Theory

By Purvi Tandel

Topics included:

- Modular arithmetic
- Prime and relative prime numbers
- Euler's Theorem
- Euclidean algorithm
- Finite field of the form GF(p)
- Polynomial arithmetic
- Finite field of the form GF(2^n)

Topics included:

- Modular arithmetic
- Prime and relative prime numbers
- Euler's Theorem
- Euclidean algorithm
- Finite field of the form GF(p)
- Polynomial arithmetic
- Finite field of the form GF(2^n)

Modular Arithmetic

Classical math problem:

Samantha says she will be home by 10:00, and she’s 13 hours late, what time does she get home?

$(10+13) \bmod 12 = 23 \bmod 12 = 11 \bmod 12 = 11$

Another way of writing the same is:

$23 \equiv 11 \pmod{12}$

Typical solution:

10:00 AM suppose to reach home (add 13 hours)

11:00 PM she will reach home

Modular Arithmetic

$23 \equiv 11 \pmod{12}$ (here $\equiv$ denotes congruence)

Basically, $a \equiv b \pmod{n}$ if $a = b + kn$ for some integer k.

Where, a is non negative and b is between 0 to n.

Sometimes, b is reminder of a when divided by n.

Sometimes, b is called the residue of a, modulo n.

Sometimes, a is called **Congruent** to b, modulo n.

Modular Arithmetic

Some examples of a = b + kn:

- For a = 11, n = 7,

  11 = 1 * 7 + 4; Residue b = 4, k =1.

- For a = -11, n = 7,

  -11 = -2 * 7 + 3; Residue b = 3, k = -2.

- $73 \equiv 4 \pmod{23}$

  73 = 3 * 23 + 4; Residue b = 4, k = 3.

- $21 \equiv -9 \pmod{10}$

  21 = 3 * 10 + (-9); Residue b = -9, k = 3.

- $21 \equiv 1 \pmod{10}$

  21 = 2 * 10 + 1; Residue b = 1, k = 2.

Modular Arithmetic

Properties of Congruence:

1. $a \equiv b \pmod{n}$ if $n|(a-b)$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

To demonstrate first point if $n|(a-b)$, then $(a-b) = kn$ for some k.

$23 \equiv 8 \pmod{5}$ because $23 - 8 = 15 = 5 * 3$

$-11 \equiv 5 \pmod{8}$ because $- 11 - 5 = -16 = 8 * (-2)$

$81 \equiv 0 \pmod{27}$ because $81 - 0 = 81 = 27 * 3$

Modular Arithmetic

Modular Arithmetic operations:

1. (a + b) mod n = ((a mod n) + (b mod n)) mod n
2. (a - b) mod n = ((a mod n) - (b mod n)) mod n
3. (a * b) mod n = ((a mod n) * (b mod n)) mod n

Now calculating the power of some number modulo some number,

a^x mod n,

is just a series of multiplications and divisions, but there are speedups.

Speedup aims minimize the number of multiplications.

Modular Arithmetic

$a^8 \bmod n = (a*a*a*a*a*a*a*a) \bmod n$

Speedup aims minimize the number of multiplications.

How???

To find $11^7 \bmod 13$, we can proceed as follows:

$11^2 \bmod 13 = 121 \bmod 13 = 4 \pmod{13} = 4$ (Because 13*9 + 4)

$11^4 \bmod 13 = (11^2 \bmod 13)^2 \bmod 13 = (4)^2 \bmod 13 = 16 \bmod 13 = 3 \pmod{13} = 3$

$11^7 \bmod 13 = (11^4 \bmod 13 * 11^2 \bmod 13 * 11 \bmod 13) \bmod 13 = (3*4*11) \bmod 13 = 132 \bmod 13 = 2 \pmod{13} = 2$ (Because 13*10 + 2)

So, $11^7 \bmod 13 = 2$.

Modular Arithmetic

In modular arithmetic mod 8, the additive inverse of x is the integer y such that (x + y) mod 8 = 0 mod 8.

Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Modular Arithmetic

In modular arithmetic mod 8, the multiplicative inverse of x is the integer y such that (x * y) mod 8 = 1 mod 8.

Multiplication Modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Modular Arithmetic

Additive and Multiplicative Inverses Modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

Modular Arithmetic

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{ 0 , 1 , \ldots\ldots\ldots , (n-1)\}$$

In ordinary arithmetic, the following statement is true only with the attached condition:

if (a x b) = (a x c) (mod n) then b = c (mod n)   if a is relatively prime to n

In general, an integer has a multiplicative inverse in Z_n if that integer is relatively prime to n.

Table shows that the integers 1, 3, 5, and 7 have a multiplicative inverse in Z_8, but 2, 4, and 6 do not.

Topics included:

- Modular arithmetic
- Prime and relative prime numbers
- Euler's Theorem
- Euclidean algorithm
- Finite field of the form GF(p)
- Polynomial arithmetic
- Finite field of the form GF(2^n)

Prime & Relative prime numbers

An integer $p>1$ is a **prime number** if and only if its only divisors are ± 1 and $\pm p$.

Any integer $a > 1$ can be factored in a unique way as

$$a = p_1^{a1} * p_2^{a2} \ldots p_t^{at}$$

Where $p_1 < p_2 < \ldots.. < p_t$ are prime numbers and where each a_i is a positive integer.

Examples:

$91 = 7 * 13$

$3600 = 2^4 * 3^2 * 5^2$

$11011 = 7 * 11^2 * 13$

Prime & Relative prime numbers

If P is the set of all prime numbers, then any positive integer a can be written uniquely in the following form:

$$a = \prod_{p \in P} pap \qquad \text{where each } a_p \geq 0$$

If gcd (p , q) = 1 then, p & q both are **relative prime numbers** to each other.

Examples:

1. p = 3, q = 5 then gcd (3 , 5) = 1 (Both Prime numbers)
2. p = 7, q = 13 then gcd (7 , 13) = 1 (Both Prime numbers)
3. p = 31, q = 84 then gcd (31 , 84) =1 (Both are not Prime numbers)

Prime & Relative prime numbers

Note:

- ✓ All prime numbers are relative to each other.
- ✓ Non prime number also can be relative to each other.

Topics included:

- Modular arithmetic
- Prime and relative prime numbers
- Euler’s Theorem
- Euclidean algorithm
- Finite field of the form GF(p)
- Polynomial arithmetic
- Finite field of the form GF(2^n)

Euler's Theorem:

Euler's theorem states that for every a and n that are relatively prime:

$$a^{ø(n)} \equiv 1 \pmod{n}$$

Examples:

- a=3; n=10;   ø(10)=4;

  hence $3^4 = 81 = 1 \bmod 10$

- a=2; n=11;   ø(11)=10;

  hence $2^{10} = 1024 = 1 \bmod 11$

Alternative form of the theorem is:

$$a^{ø(n)+1} \equiv a \pmod{n}$$

Euler's Theorem:

Euler's Totient function:

Euler's totient function, written as Ø(n), defined as the number of positive integers less than n and relatively prime to n.

If n is prime number, then Ø(n) = (n - 1).

Example: n = 37 (prime number)

So all the positive integers from 1 through 36 are relatively prime to 37.

Ø(n) = (n – 1) = 36 = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ………, 36}

Euler's Theorem:

If n is non-prime number, and whose factors are two prime numbers p and q, with $p \neq q$, then

$\varnothing(n) = \varnothing(pq) = \varnothing(p) * \varnothing(q) = (p - 1) * (q - 1)$.

Example: n = 35 (Non-prime number)

$n = 35 = 7 * 5$ (factors of 35, both prime and $p \neq q$)

$\varnothing(35) = (p - 1) * (q - 1) = (7 - 1) * (5 - 1) = 6 * 4 = 24$

$\varnothing(35) = \{ 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$

Topics included:

- Modular arithmetic
- Prime and relative prime numbers
- Euler's Theorem
- Euclidean algorithm
- Finite field of the form GF(p)
- Polynomial arithmetic
- Finite field of the form GF(2^n)

Euclidean algorithm:

One of the basic techniques of number theory is the Euclidean algorithm,

which is a simple procedure for determining the greatest common divisor of two positive integers.

Use the notation GCD(a , b) which is the greatest common divisor of a and b.

Example:

- ✓ GCD(60,24) = 12
- ✓ GCD(8,15) = 1 , hence 8 & 15 are relatively prime

Euclidean algorithm:

Finding the Greatest Common Divisor:

The Euclidean algorithm is based on the following theorem: For any nonnegative integer a and any positive integer b,

$$GCD(a, b) = GCD(b, a \bmod b)$$

Example:

GCD(55, 22) = GCD(22, 55 mod 22) = GCD(22, 11) = 11

GCD (18, 12) = GCD(12, 18 mod 12) = GCD(12, 6) = 6

Euclidean algorithm:

```
EUCLID(a,b)
1. A = a; B = b
2. if B = 0 return  A = gcd(a, b)
3. R = A mod B
4. A = B
5. B = R
6. goto 2
```

The algorithm has following progression:

$$A_1 = B_1 \times Q_1 + R_1$$

$$A_2 = B_2 \times Q_2 + R_2$$

$$A_3 = B_3 \times Q_3 + R_3$$

$$A_4 = B_4 \times Q_4 + R_4$$

Euclidean algorithm:

Example GCD(1970, 1066) = 2

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	gcd(2, 0)

Euclidean algorithm:

Example GCD(1160718174, 316258250) = 1078

Dividend	**Divisor**	**Quotient**	**Remainder**
a = 1160718174	b = 316258250	q1 = 3	r1 = 211943424
b = 316258250	r1 = 211943424	q2 = 1	r2 = 104314826
r1 = 211943424	r2 = 104314826	q3 = 2	r3 = 3313772
r2 = 104314826	r3 = 3313772	q4 = 31	r4 = 1587894
r3 = 3313772	r4 = 1587894	q5 = 2	r5 = 137984
r4 = 1587894	r5 = 137984	q6 = 11	r6 = 70070
r5 = 137984	r6 = 70070	q7 = 1	r7 = 67914
r6 = 70070	r7 = 67914	q8 = 1	r8 = 2516
r7 = 67914	r8 = 2516	q9 = 31	r9 = 1078
r8 = 2516	r9 = 1078	q10 = 2	r10 = 0

Topics included:

- Modular arithmetic
- Prime and relative prime numbers
- Euler's Theorem
- Euclidean algorithm
- Finite field of the form GF(p)
- Polynomial arithmetic
- Finite field of the form GF(2^n)