GCD & Euclidean Algorithms

- Ankita Dhar

Starting with basic problems before solving bigger ones…

1. Modulus

   Given integers:

   a = 7
   n = 2

   To find: a mod n; i.e. 7 mod 2

   - Integer n (=2) is called the modulus
   - When, $7 \div 2$, we get
     quotient = 3,
     remainder = 1
   - Remainder = a mod n
   - Therefore, 7 mod 2 = 1

2. Additive Inverse

   Given integers:

   x = 2
   n = 8

   To find: Additive inverse of x for Z_8 (Modulo 8)

   - Additive Inverse y is a number, which fits the following expression:
     $(x + y)\, mod\, n = 0$
   - Substituting values, we get, $(2 + y)\, mod\, 8 = 0$
     From this, we can say that when
     - y = 6,
       $(2 + 6)\, mod\, 8 = 0$
     - y = 14,
       $(2 + 14)\, mod\, 8 = 0$

3. Multiplicative Inverse

   Given integers:

   x = 3
   n = 8

To find: Multiplicative inverse of x(=3) for Z_8 (Modulo 8)

- Multiplicative Inverse y is a number, which fits the following expression:
  $(x \times y) \; mod \; n = 1$
- Substituting values, we get, $(3 \times y) \; mod \; 8 = 1$
  From this, we can say that when
  - $y = 3$,
    $(3 \times 3) \; mod \; 8 = 1$
  - $y = 11$
    $(3 \times 11) \; mod \; 8 = 1$

Finding GCD using Euclidean Algorithm

Algorithm:

Euclid(a,b)
// Inputs: Two integer values a & b
// Output: Greatest Common Divisor of both the numbers

if (b=0) **then return** a;
else return Euclid(b, a mod b);

Let us now solve a problem.

1. Given:
   a = 42
   b = 30

Solution:
Let us solve it using table format.
Let $r_1 = a$ & $r_2 = b$

	r_1	r_2	r $r = r_1 \text{mod } r_2$
Step1: take the larger among number a & b as r_1, and the other number as r_2	42	30	12
Step2: Shift r_2 value to r_1, r value to r_2	30	12	6
Step3: Repeat Step2	12	6	0
Step4: Repeat Step2	6	0	Since $r_2 = 0$ 6 cannot be divided by 0 At this point we can say gcd = r_1

Therefore, gcd (42, 30) = 6

Extended Euclidean Algorithm

> Extended Euclidean algorithm says that for given integer a and b, there exists x & y, such that $ax + by = d$, where d is the greatest common divisor of a and b

Now let us solve a problem using table format
At each step calculate

x as $x = x_1 - x_2 \times q$ AND y as $y = y_1 - y_2 \times q$ WHERE q is the quotient

	q	r_1	r_2	r $r = r_1 mod\, r_2$	x_1	x_2	x	y_1	y_2	y
Step1: as in previous table	1	42	30	12	Initialize $x_1 = 1$	Initialize $x_2 = 0$	1	Initialize $y_1 = 0$	Initialize $y_2 = 1$	-1
Step2: Shift r_2 value to r_1, r value to r_2, x_2 value to x_1, x value to x_2 & y_2 value to y_1, y value to y_2	2	30	12	6	0	1	-2	1	-1	3
Step3: Repeat Step2	2	12	6	0	1	-2	5	-1	3	-7
Step4: Repeat Step2		6	0	Stop when $r_2 = 0$ gcd = r_1	-2 $x = x_1$	5		3 $y = y_1$	-7	

Finally, we infer $x = x_1$ AND $y = y_1$, therefore $x = -2 \ AND \ y = 3$
We can verify it by substituting in the formula : $ax + by = d$
$(42 \times -2) + (30 \times 3) = 6$, where 6 is the greatest common divisor of a and b

Now use this method to find Multiplicative inverse…

Let us solve the same problem from above:

Given integers:
x = 3
n = 8

To find: Multiplicative inverse of x(=3) for Z_8 (Modulo 8)

	q	r_1	r_2	r $r = r_1 mod\, r_2$	y_1	y_2	y
Step1: take the larger number among x & n as r_1, and the other number as r_2	2	8	3	2	Initialize $y_1 = 0$	Initialize $y_2 = 1$	-2
Step2: Shift r_2 value to r_1, r value to r_2, x_2 value to x_1, x value to x_2 & y_2 value to y_1, y value to y_2	1	3	2	1	1	-2	3
Step3: Repeat Step2	2	2	1	0	-2	3	-8
Step4: Repeat Step2	X	1	0	Stop when $r_2 = 0$ gcd = 1	3 $y = y_1$	-8	X

Finally, we infer $y = y_1$, where y is the multiplicative inverse of x.

Note:

1. There is only one unique inverse of a number from 0 to n-1 range, this method helps in finding the unique inverse. Outside this range there are infinitely many inverses possible.
2. This method cannot calculate inverse of all numbers for a given n.
   For example, finding inverse of x(=2) for Z_8 (Modulo 8) is not possible using this method.