Practical 2

Note:

Division Relation

Assume I want to divide a by n. The quotient is q and remainder is r. Therefore, a=n*q+r.
Following are the constraints on values.

- a is Dividend--> It can be any valid Integer of set Z.
- n is Divisor--> Positive Integer n i.e. n>0.
- r is Remainder--> Non-negative Integer in the range 0 to (n-1).
- q is Quotient-->It can be any valid Integer i.e. 0 also.

But gcc is not giving answers in this manner, so refer "Sample.c" code to get the answer in the range specified above. Implement modulo according to it whenever required.

1. Implement Euclidean Algorithm to find Greatest Common Divisor.
   Hint: Implement following recurrence.
   GCD(A,B)= A if B=0
   = GCD(B, A MOD B) if B!=0
2. Implement Extended Euclidean Algorithm to find GCD of two numbers a,b such that a*s+b*t=d, where d=GCD(a,b).
   Input: a, b
   Output: d, s, t
   Verify whether above equation is satisfied or not. If not, answer is not correct, otherwise its correct.
3. Write a program to find Additive Inverse of some number a with respect to modulo n.
   Input: a, n
   Output: (-a) i.e. Additive Inverse of a with respect to Modulo n.
   A and B are called additive inverses of each other if A+B is congruent to 0 modulo n.

   If Mod 5 is assumed then, additive inverse of 0 is 5, 1 is 4, 2 is 3, 3 is 2, 4 is 1.

4. Implement modified version of Extended Euclidean algorithm to find multiplicative inverse of some number a with respect to modulo n.
   Input: a, n
   Output: I. (a^-1) i.e. Multiplicative Inverse of a with respect to Modulo n, if it exists
   II. Message, if it doesn't exist.

   A and B are called Multiplicative inverses of each other if A*B is congruent to 1 modulo n.
   Multiplicative inverse of a with respect to modulo n relation exists if a and n are relatively prime. Inverse of 2 in Z26 doesn't exist because GCD(2,26)=2 i.e. 2 and 26 are not relatively prime.