Jin Young Park

May 25, 2020

TCSS 581A

Homework

1. Describe the extended Euclidean algorithm.

   The extended Euclidean algorithm is indeterminate equation. Let a and b be positive integer. The gcd(a,b) is the greatest common divisor of a and b. Using the greatest common divisor, we create the following indeterminate equation. $\gcd(a, b) = X * a + Y * b$. And we get X and Y.

   Ex) a=527, b=32

   gcd(527, 32)=1

   1=15-7*2

   1=15-7(32-2*15) =15*15-7*32

   1=15(527-32*16)-7*32=15*527-240*32-7*32=15*527-247*32

   X=15, Y=-247

2. Implement it in a programming language of your choice.

   EuclideanAlgorithm.exe can be executed from the command line. When two numbers are input, the first number is input as a and the second number is input as b to obtain the values of X and Y. EuclideanAlgorithm.cpp can see the code.

3. Explain how one can use the Euclidian algorithm for computing multiplicative inverses in modular arithmetic.

   Let b is $b^{-1} mod\ n$ and $\gcd(b, n) = 1 \Rightarrow 1 = X \cdot b + Y \cdot n.$

   Reduce the two sides of the equation modulo n

   $1\ mod\ n = (X \cdot b + Y \cdot n) mod\ n.$

   $1\ mod\ n = 1$ and $(Y \cdot n)\ mod\ n = 0$, so

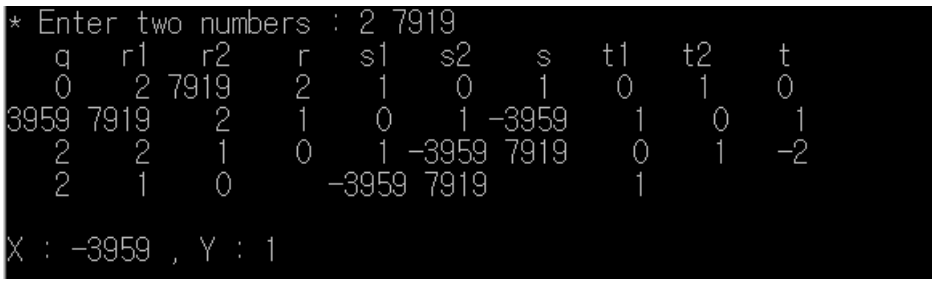
   $1\ = (X \cdot b) mod\ n.$

   The identity of multiplication is 1, so the inverse of $b\ mod\ n$ is $X\ mod\ n$

   $b^{-1} mod\ n = X\ mod\ n.$

   So, by using the extended Euclidian algorithm, $\gcd(a, b) = X * a' + Y * b'$ can be obtained X by putting b into a' and n into b'.

4. Use your implementation to compute the multiplicative inverse of 2 modulo 7919.



So, X is $-3959 mod\ 7919$. And $-3959\ mod\ 7919 = 3960\ mod\ 7919$. As a result, the multiplicative inverse of 2 modulo 7919 is $3960\ mod\ 7919$.