NumberTheory
과제

Square_Multi(x,a,n) x^a mod (|a|=k)

```
{
        z←1
        for  i ← k - 1 to 0 do
                z ←z² mod n
                if a_i==1 then z ←zx mod n
        return z
}
```

※참고
a 비트 수 구하기: BN_num_bits(a)
a의 i번째 비트가 1인지 확인: BN_is_bit_set(a, i)

If x = 1239 (decimal)
   a = 9 (decimal)
Then a = 1001(binary)
      |a|=4

$$1239^{9} = 1239^{1001_2}$$

(a_3 a_0)

입출력 예:

```
FAST Exponentiation (Square and Multiply)
////////////  x^(a) mod n = ?  ////////////////
x:256
a:80
n:2203
result = 1679
```

```
Ext-Euclid(a, b)
{
        if b==0 then return (a, 1, 0)
        else
                (d′, x', y′) ← Ext-Euclid(b,a mod b)
                (d, x, y) ←(d′, y′, x′ - ⌊a/b⌋y′)
                return (d, x, y)
}
```

⌊a/b⌋ = int(a / b) // 나눗셈 몫

입출력 예: