CS235 HW5 –Teng Xu

1) (2 pts) Write a function for gcd(a,b,) using Euclidian algorithm. Test it on gcd(5,26), gcd(10,26), gcd(13,26), gcd(26,36), gcd(24,36).

```
In [4]: gcd(5,26)
Out[4]: 1

In [5]: gcd(10,26)
Out[5]: 2

In [6]: gcd(13,26)
Out[6]: 13

In [7]: gcd(26,36)
Out[7]: 2

In [8]: gcd(24,36)
Out[8]: 12
```

2) (3 pts) Which of the following functions $f(p)$ could be used for affine cypher encryption? Explain.
   a. $f(p) = (9p + \mathrm{b})$ **mod** 26
      gcd(9,26) = 1 could be used for affine cypher encryption
   b. $f(p) = (10p + \mathrm{b})$ **mod** 26
      gcd(10,26) = 2 could not be used for affine cypher encryption
   c. $f(p) = (11p + \mathrm{b})$ **mod** 26
      gcd(11,26) = 1 could be used for affine cypher encryption
   d. $f(p) = (12p + \mathrm{b})$ **mod** 26
      gcd(12,26) = 2 could not be used for affine cypher encryption
   e. $f(p) = (13p + \mathrm{b})$ **mod** 26
      gcd(13,26) = 13 could not be used for affine cypher encryption
   f. $f(p) = (14p + \mathrm{b})$ **mod** 26
      gcd(14,26) = 2 could not be used for affine cypher encryption

3) (5 pts) The function $f(p) = (5p + 3)$ **mod** 26 is used for encryption.

a. Encrypt letters: A,B,C.

A: f(0) = 3 mod 26 = 3 -> D

B: f(1) = 8 mod 26 = 8 -> I

C: f(2) = 13 mod 26 = 0 -> N

b. Get multiplicative inverse of 5 mod 26, via extended Euclidian algorithm.

$5 \bmod 26 = 5$

$26 = 5 \times 5 + 1$

$5 = 5 \times 1 + 0$

$1 = 26 - 5 \times 5$

so inverse of 5 mod 26 is -5

The inverse is -5 == 21.

c. Write a decryption function p=f(e).

f(e) = ((e*21) - 63) % 26

d. Decrypt encrypted letters obtained in a (you should get A,B,C).

```
In [3]: f(3)
Out[3]: 0

In [4]: f(8)
Out[4]: 1

In [5]: f(13)
Out[5]: 2
```

e. Decrypt letters X,Y,Z.

```
In [6]: f(23)
Out[6]: 4

In [7]: f(24)
Out[7]: 25

In [8]: f(25)
Out[8]: 20
```

X -> E Y -> Z Z -> U