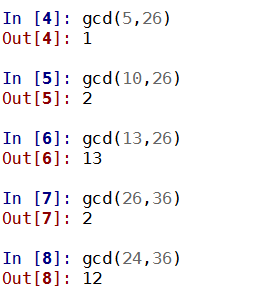
CS235 HW5 –Teng Xu

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).



1. (3 pts) Which of the following functions *f*(*p*)could be used for affine cypher encryption? Explain.
   1. *f*(*p*) *=* (9*p +* b)**mod** 26

**gcd(9,26) = 1 could be used for affine cypher encryption**

* 1. *f*(*p*) *=* (10*p +* b)**mod** 26

gcd(10,26) = 2 could not be used for affine cypher encryption

* 1. *f*(*p*) *=* (11*p +* b)**mod** 26

**gcd(11,26) = 1 could be used for affine cypher encryption**

* 1. *f*(*p*) *=* (12*p +* b)**mod** 26

gcd(12,26) = 2 could not be used for affine cypher encryption

* 1. *f*(*p*) *=* (13*p +* b)**mod** 26

gcd(13,26) = 13 could not be used for affine cypher encryption

* 1. *f*(*p*) *=* (14*p +* b)**mod** 26

gcd(14,26) = 2 could not be used for affine cypher encryption

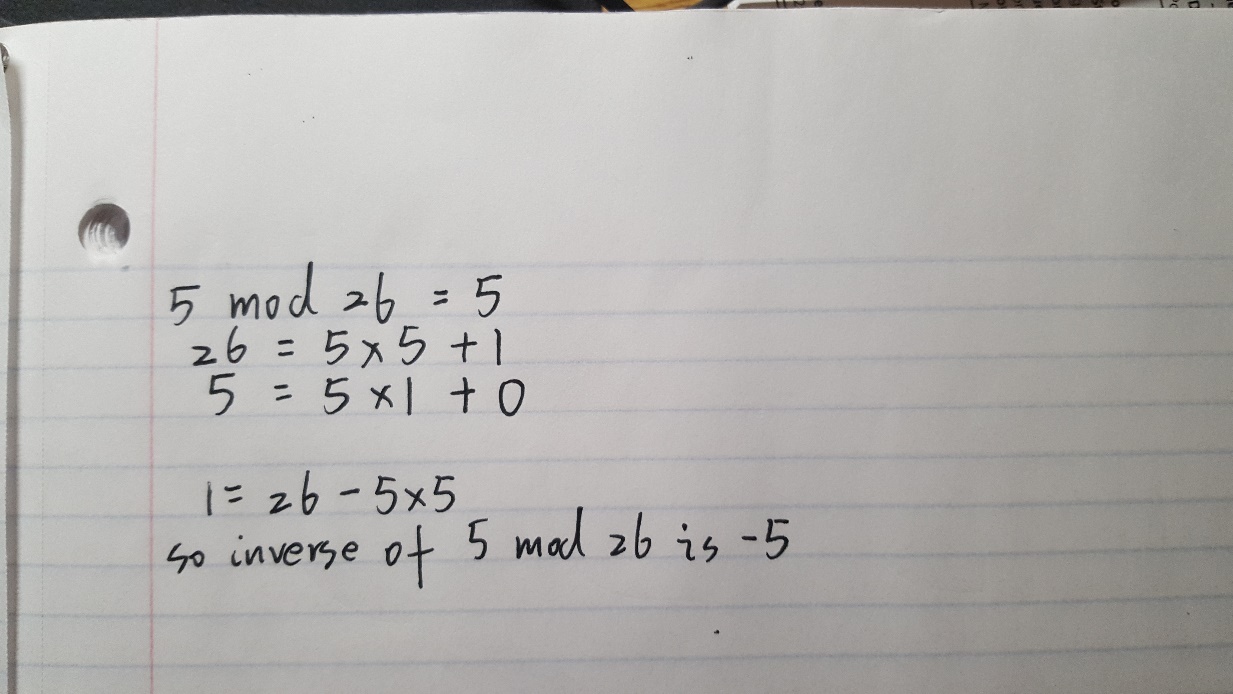
1. (5 pts) The function *f*(*p*) *=* (5*p +* 3)**mod** 26 is used for encryption.
   1. Encrypt letters: A,B,C.

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

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

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

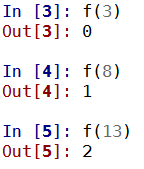
* 1. Get multiplicative inverse of 5 mod 26, via extended Euclidian algorithm.

 The inverse is -5 == 21.

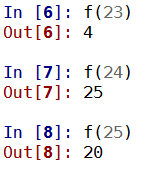
* 1. Write a decryption function p=f(e).

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

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



* 1. Decrypt letters X,Y,Z.

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