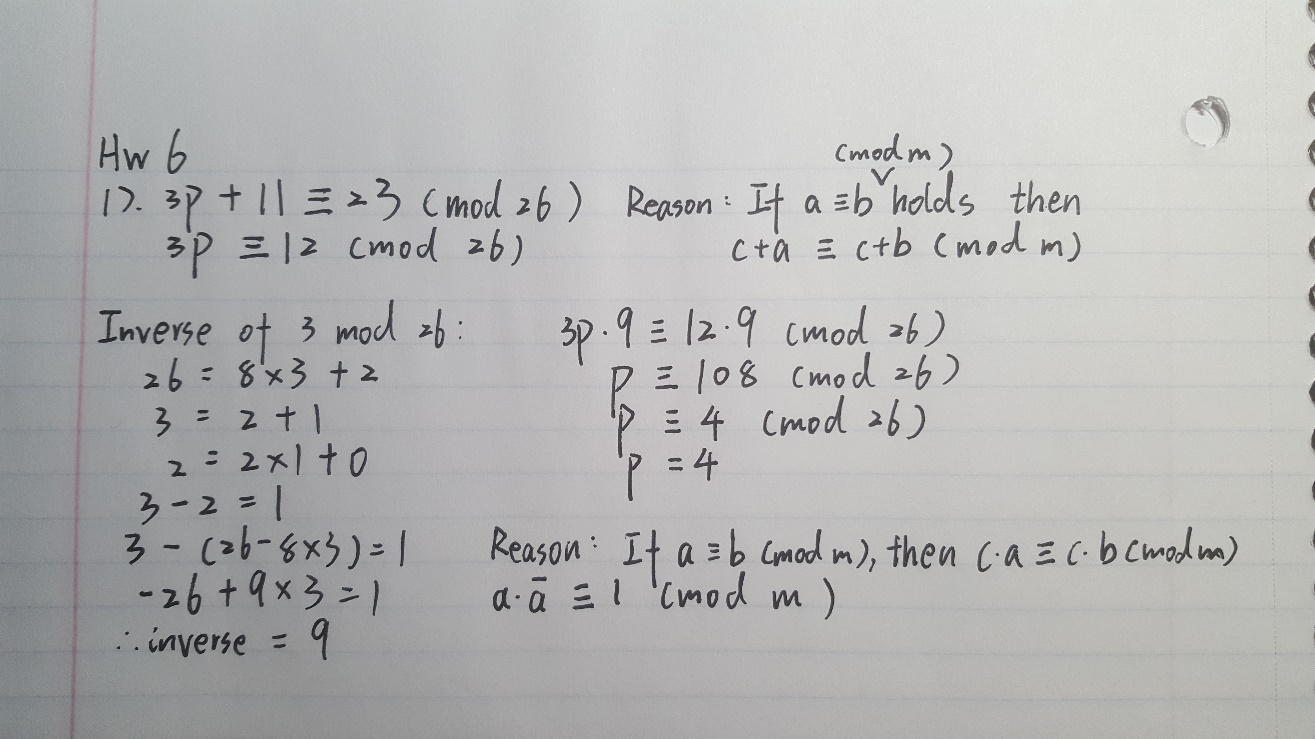
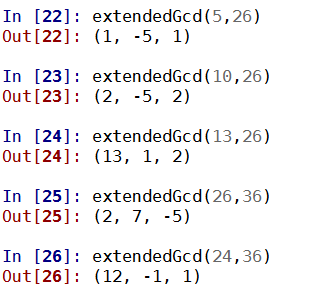
CS236 HW6 – Teng Xu

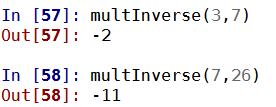
1. (2 pts) Solve 3p+11≡23 (mod 26) using subtraction and division of congruence by a number. Why are you allowed to do this?



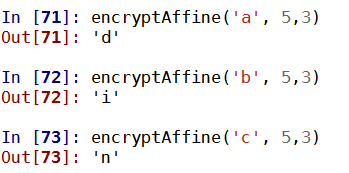
1. (2 pts) Write a function extendedGcd(a,b,) returning gcd and Bézout coefficients of a and b, using extended Euclidian algorithm outlined on slides 31, 34 of Lecture 5. Test it on gcd(5,26), gcd(10,26), gcd(13,26), gcd(26,36), gcd(24,36).

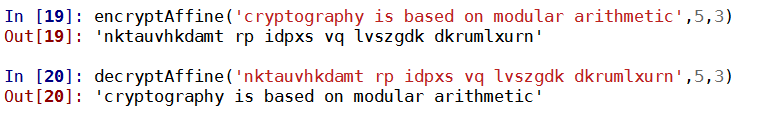


1. (2 pts) Is it possible for a multiplicative inverse modulo m to be 0? Under what condition does multiplicative inverse of *a* modulo m exist? Write a function returning multInverse(a,m) that checks existence of a multiplicative inverse of *a* modulo m, and if it exists - returns it (otherwise return 0 and print the message: “multiplicative inverse does not exist”).



1. (2 pts) Write a function encryptAffine(letter, a,b) that uses encryption function f(p)= ap+b (mod 26) and decryptAffine(letter, a,b) that uses corresponding decryption function. Check that encryption function is a bijection, otherwise – output error message. Test your functions on the results of problem 3 for HW5, and encrypting and decrypting back messages: “cryptography is based on modular arithmetic”





5.6.7 :

