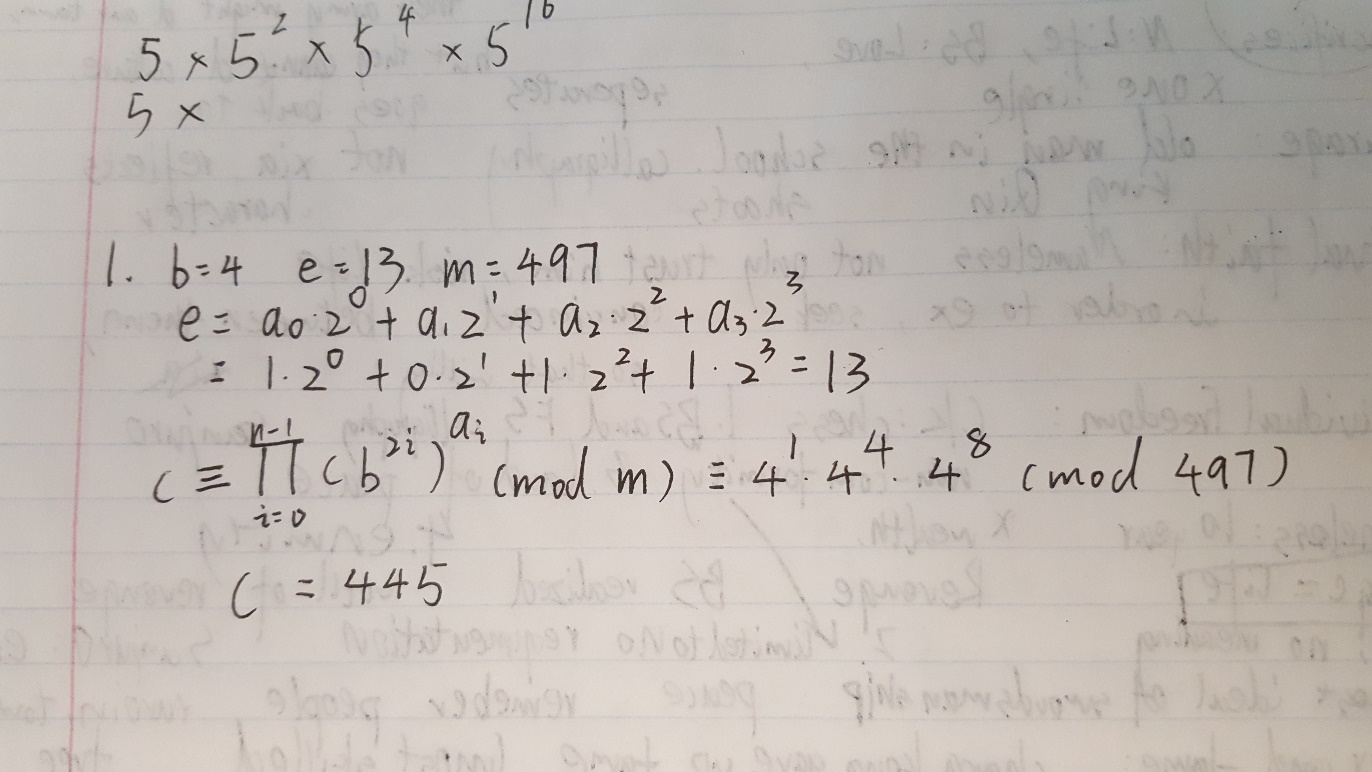
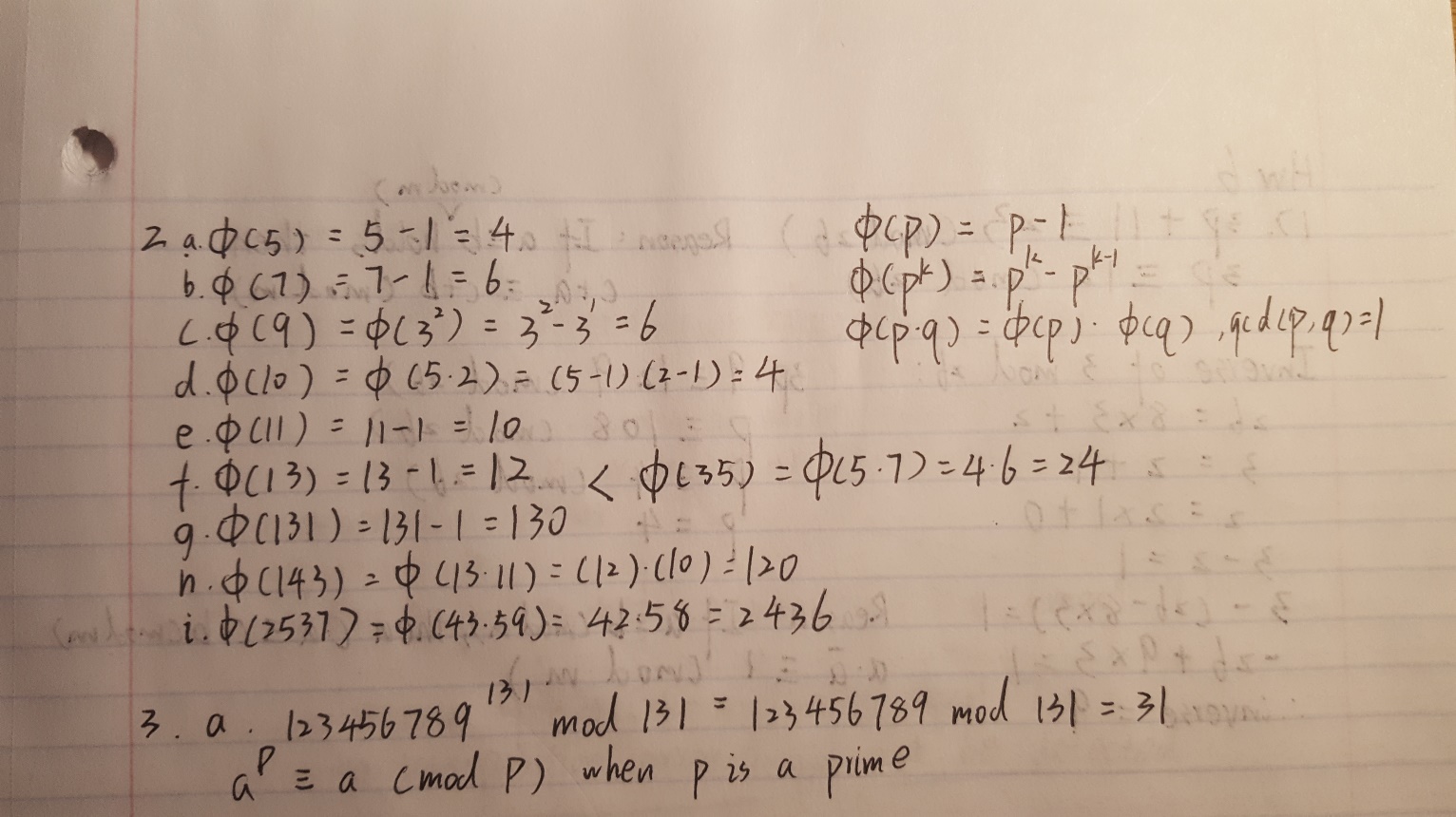
CS236 HW8 – Teng Xu

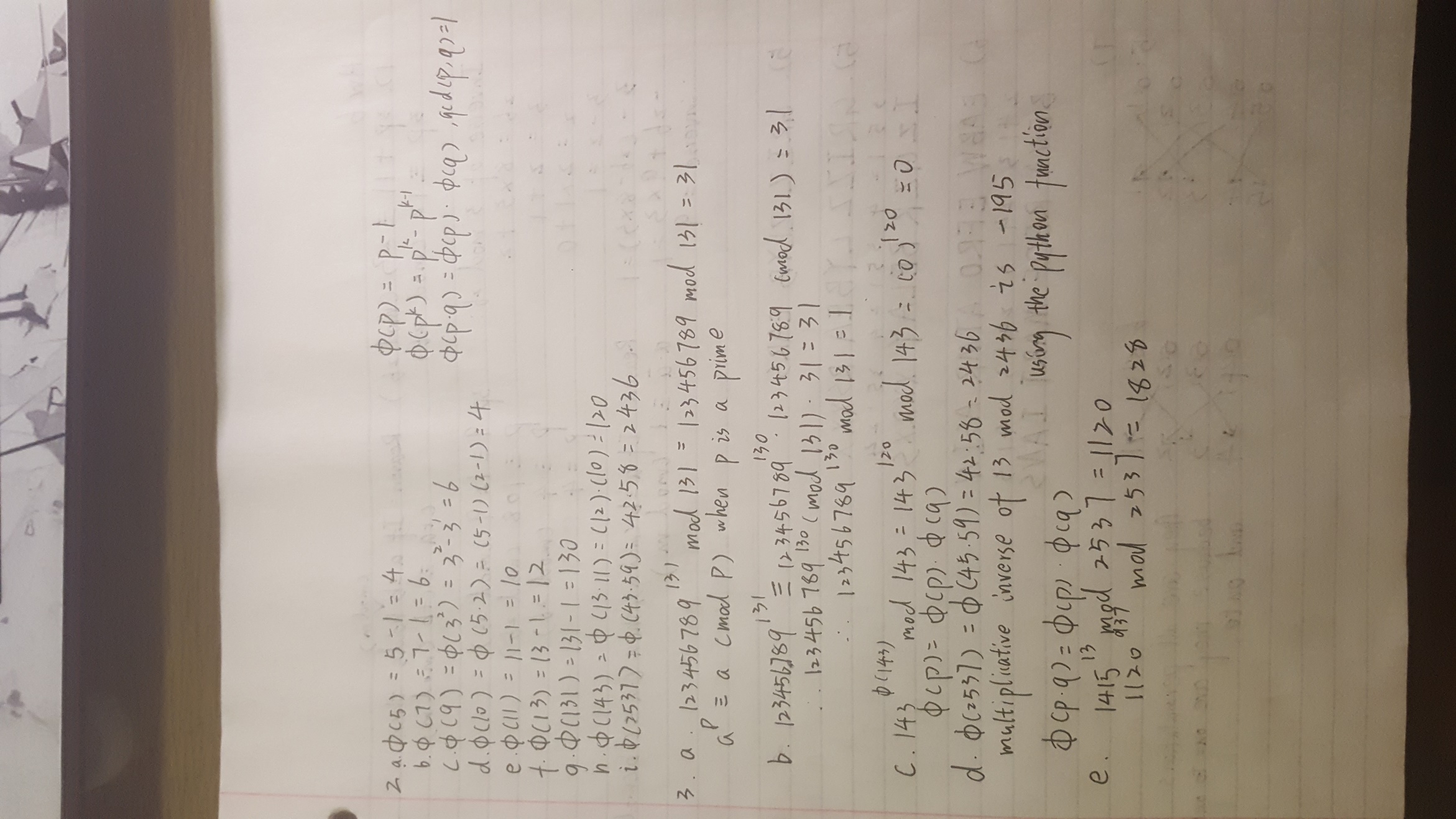
1. (2 pts) Compute the modular exponentiation: *c* ≡ *be* (mod *m*) for *b* = 4, *e* = 13, and *m* = 497, via binary method described at slide 15 of Lecture 8.

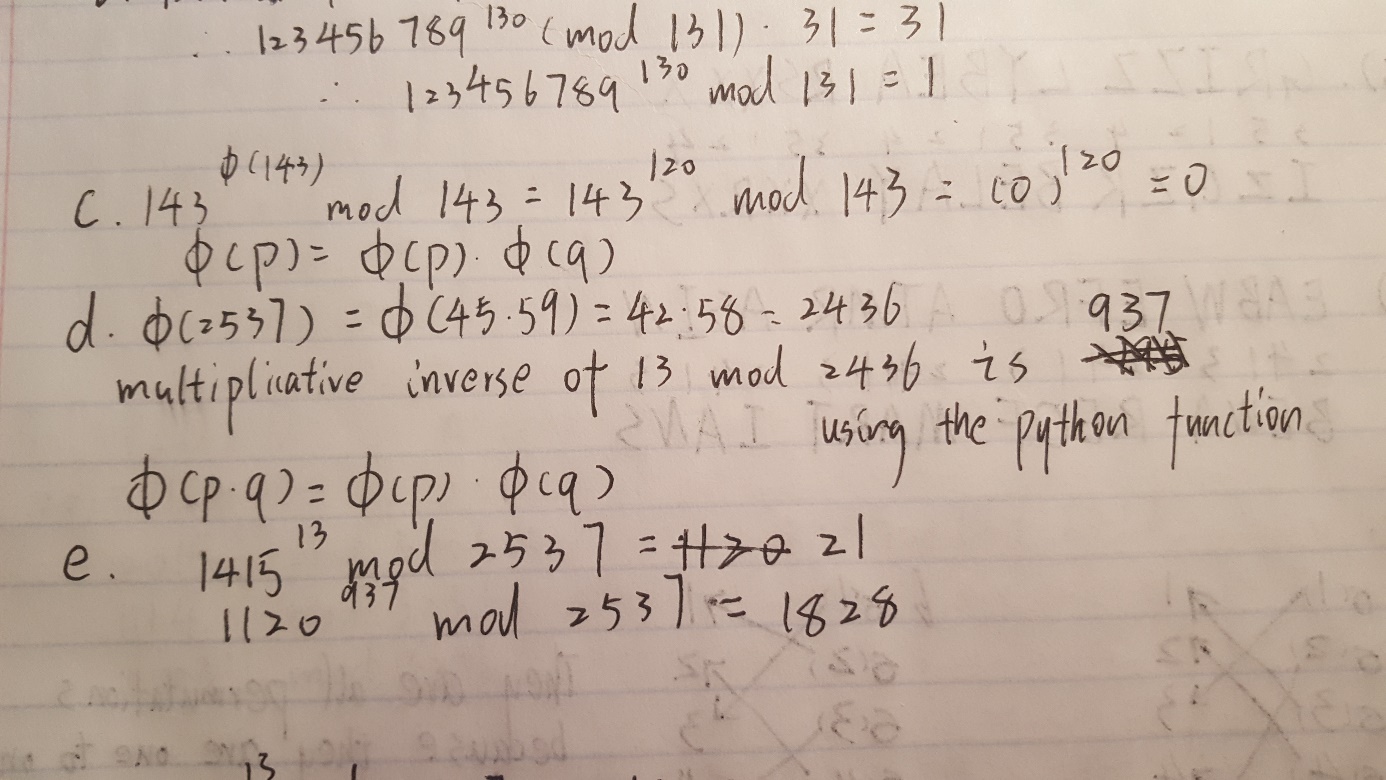
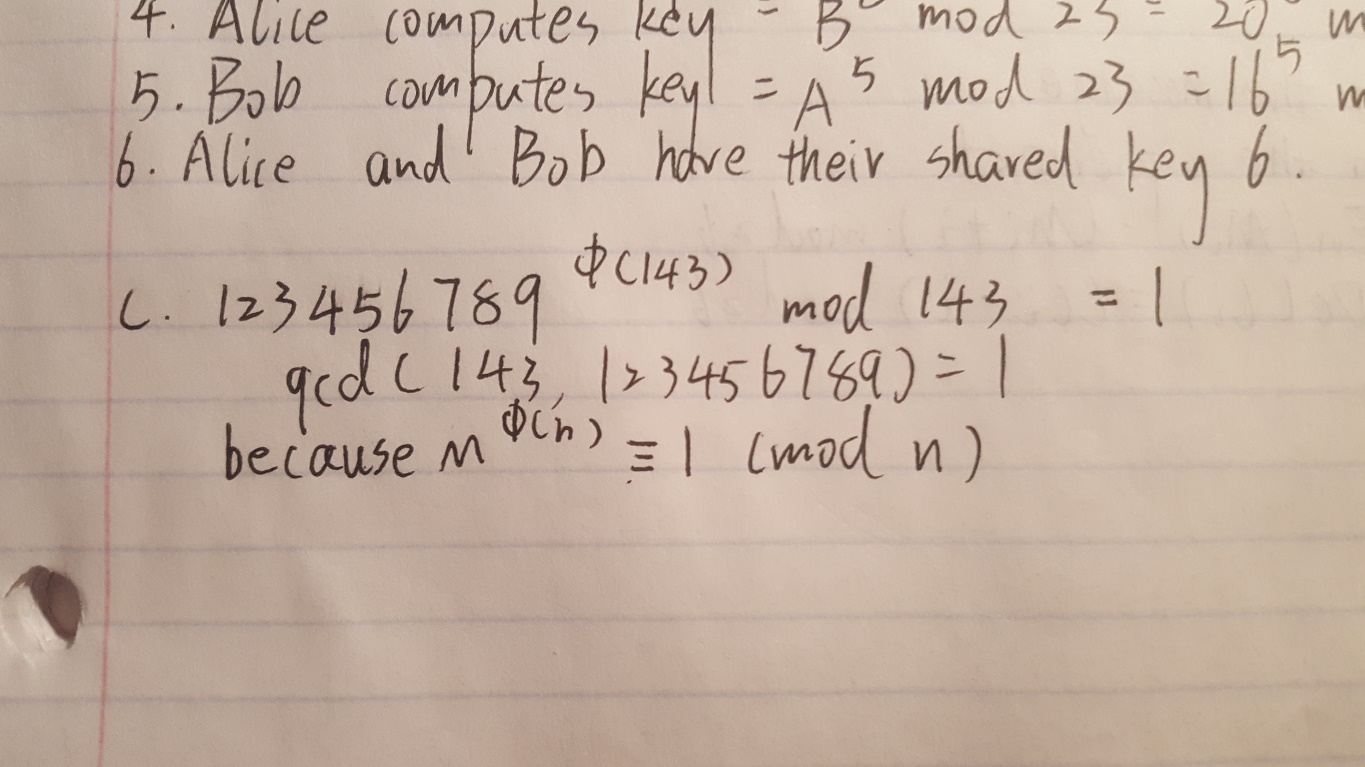


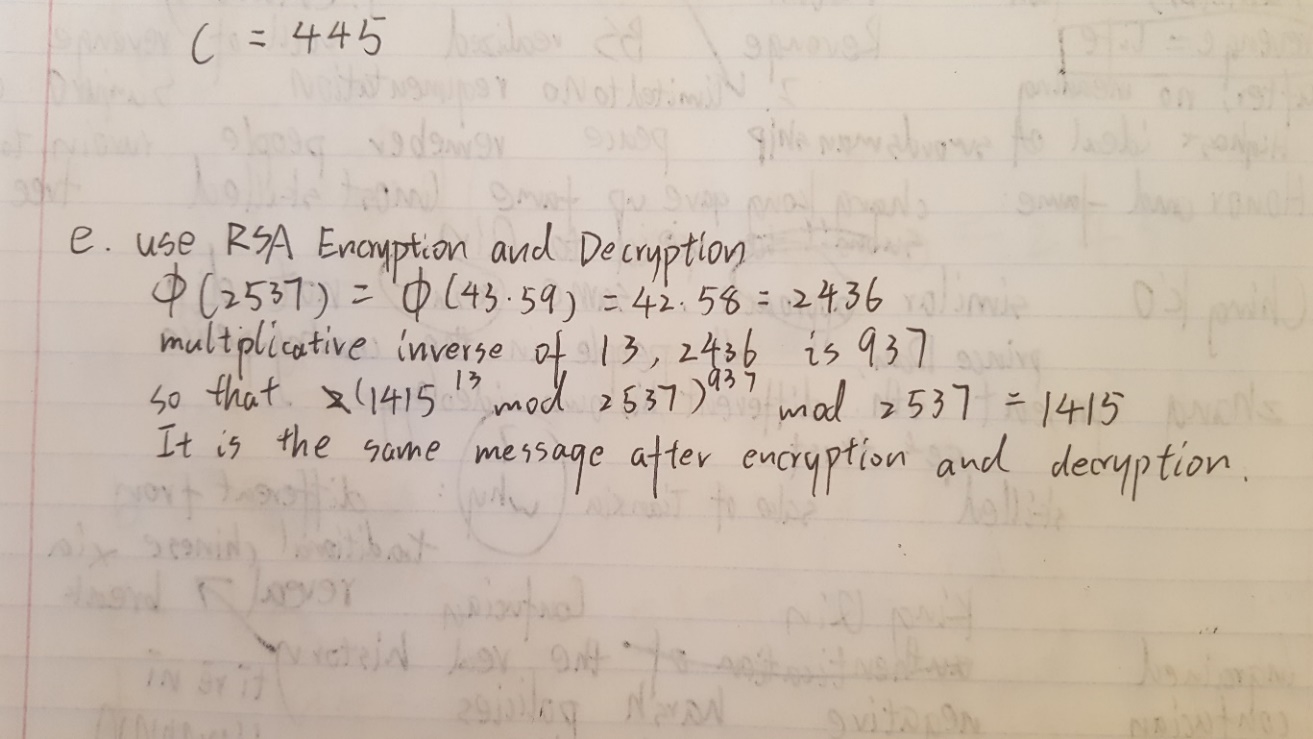
1. (10 pts) Calculate Euler’s totient function Φ(n) (defined at Lecture 9) for the following n:



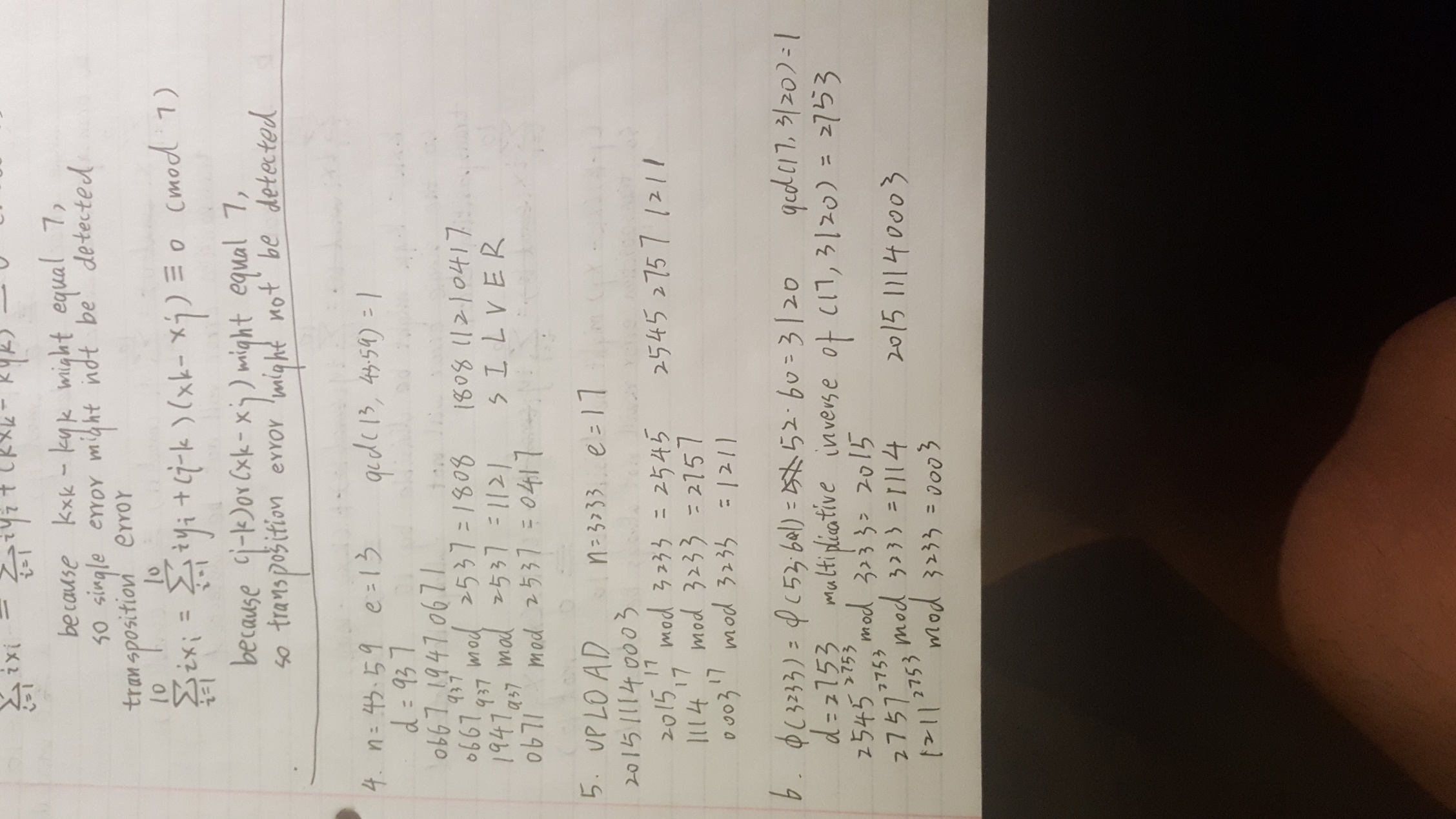
1. (5 pts) Use Fermat’s little theorem, Euler theorem (see Lecture 9), Python function computing multiplicative inverse (written for a previous homework), and math formulas for decrypting RSA encryption (at slide 13 of Lecture 9) to calculate the following:



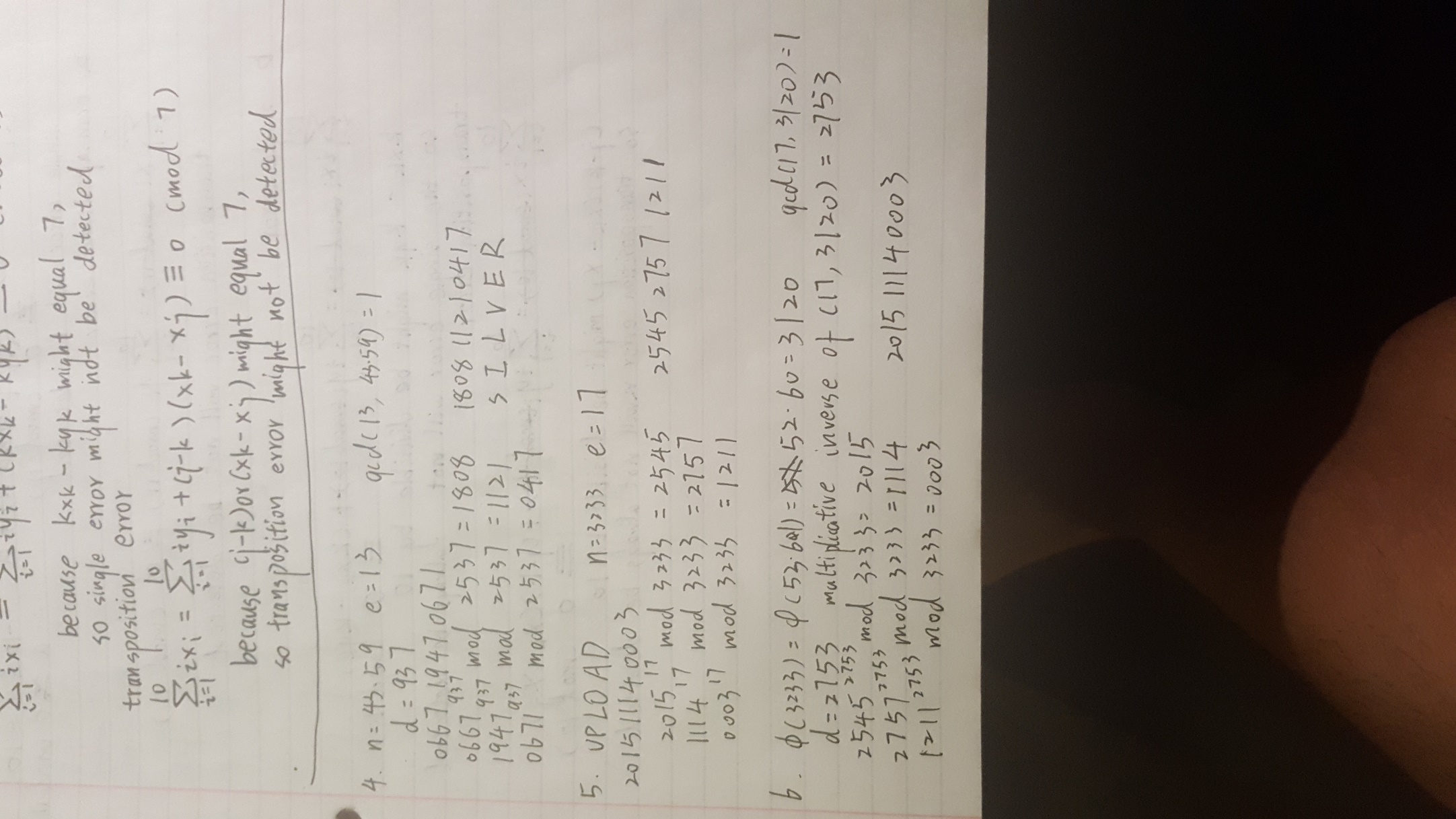




1. (2 pts) What is the original message encrypted using the RSA system with n =43·59 and e =13 if the encrypted message is 0667 1947 0671?



1. (2 pts) Encrypt the message UPLOAD using the RSA system with n =3233 and e =17.



1. (2 pts) Decrypt the encrypted message, obtained in the previous problem, showing all the steps of RSA decryption, using the factorization: n=53·61.

