CS 70 Discrete Mathematics and Probability Theory
Fall 2019 Alistair Sinclair and Yun S. Song

Quiz 4

1. [True/False]: For all $a, b \in \mathbb{Z}$, determine if the following statements are TRUE or FALSE.

(a) [ ] $(a+b)^3 \equiv a^3 + b^3 \pmod 3$, $[(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3]$.

(b) [ ] $(a+b)^4 \equiv a^4 + b^4 \pmod 4$, $[(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4]$.

(c) [ ] $(a+b)^5 \equiv a^5 + b^5 \pmod 5$, $[(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5]$.

2. [Modular Arithmetic]:

(a) Compute $11^{13} \pmod{100}$ using repeated squaring. Show your intermediate results.

(b) State Fermat's Little Theorem, and then use it to give a careful proof of the following claim.

Claim: If p is prime and b, c are positive integers such that $b = c \pmod{p-1}$, then $a^b = a^c \pmod p$ for any integer a.

(c) Find $8^{(321^{49})} \pmod{11}$.

NOTE: You should use part (b). It is possible to figure out this question in two lines. If you are doing a lot of calculations, you are probably on the wrong track. Write no more than five lines.

3. [Short Answer]: Bob runs a small business selling widgets over the Internet. Alice wants to buy one of Bob's widgets but is worried about the security of her credit card information, so she and Bob agree to use RSA encryption. Bob generates $p = 7$, $q = 3$ and $e = 5$.

(a) [ ] What does Bob need to send to Alice (i.e., what is Bob's public key)?

(b) [ ] What is Bob's private key?

(c) [ ] Suppose Alice's credit card number is $x = 4$. What is the encrypted message $E(x)$?