CS 70
Fall 2019

Discrete Mathematics and Probability Theory
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) □ $(a+b)^5 \equiv a^5+b^5 \pmod 5$, $[(a+b)^5 = a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5]$.

Solution:

(a) **True.** To prove this, first notice that $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$. Also we have that $3a^2b+3ab^2 \equiv 0 \pmod 3$ because each term is a multiple of 3. Hence, taking the remainder of the division by 3 on both sides of $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$, we obtain

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 \equiv a^3+0+b^3 = a^3+b^3 \pmod 3.$$

(b) **False.** A counter example is obtained by setting $a=1$, $b=1$. In this case $a^4+b^4 = 1^4+1^4 = 1+1 = 2 \pmod 4$. On the other hand, $(a+b)^4 = (1+1)^4 = 2^4 = 16 \equiv 0 \pmod 4$)

(c) **True.** This can be shown using the same argument as in part (a). First notice that $5a^4b+10a^3b^2+10a^2b^3+5ab^4 \equiv 0 \pmod 5$ because each term is a multiple of 5. Now using the formula for $(a+b)^5$, we have

$$\begin{aligned}(a+b)^5 &= a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5 \pmod 5\\ &\equiv a^5+0+b^5 \pmod 5\\ &= a^5+b^5 \pmod 5.\end{aligned}$$

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.

Solution:

(a) By repeated squaring we compute:

$$11^2 = 121 \equiv 21 \pmod{100}$$

$$11^4 \equiv 21^2 \equiv 41 \pmod{100}$$
$$11^8 \equiv 41^2 \equiv 81 \pmod{100}$$

$$\begin{aligned}11^{13} &= 11^{1+4+8} \\ &= 11^1 \times 11^4 \times 11^8 \\ &\equiv 11 \times 41 \times 81 \\ &\equiv 51 \times 81 \\ &\equiv 31 \pmod{100}\end{aligned}$$

(b) Fermat's Little Theorem states that for any prime p, for any $a \in \{1,2,...,p-1\}$,

$$a^{p-1} = 1 \pmod p$$

. We prove by cases:

- Case 1: $a = 0 \pmod p$. Then $a^b = 0 = a^c \pmod p$ for any positive integers b and c.
- Case 2: $a \neq 0 \pmod p$. Since $b = c \pmod{p-1}$, we have $b = c + k(p-1)$ for some integer k, so

$$a^b = a^{c+k(p-1)} = a^c \times (a^{k(p-1)}) \underbrace{=}_{(*)} a^c \times 1^k = a^c \pmod p,$$

where the equality $(*)$ comes from Fermat's Little Theorem.

(c) Using part (b) with $p = 11$, the first step is to calculate:

$$321^{49} = (32 \times 10 + 1)^{49} \equiv 1^{49} = 1 \pmod{10}.$$

Then by part (b) we have

$$8^{(321^{49})} = 8^1 \equiv 8 \pmod{11}.$$

---

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 $E(x)$?

Solution:

(a) $(N,e) = (pq,e) = (21,5)$.

(b) 5.

$$d = e^{-1} \pmod{(p-1)(q-1)} \Rightarrow \quad d = 5^{-1} \pmod{12} \Rightarrow \quad d = 5 \pmod{12}$$

(c) 16.

$$\begin{aligned} E(x) = x^e \mod N \Rightarrow E(4) &= 4^5 \pmod{21} \\ &= 4^3 \cdot 4^2 \pmod{21} \\ &= 64 \cdot 4^2 \pmod{21} \\ &\equiv (1) \cdot 4^2 \pmod{21} \\ &= 16 \pmod{21} \end{aligned}$$