CS 70 Discrete Mathematics and Probability Theory
Summer 2022 Jingjia Chen, Michael Psenka and Tarang Srivastava
DIS 3A

1 Quick Computes

Simplify each expression using Fermat's Little Theorem.

(a) $3^{33} \pmod{11}$

(b) $10001^{10001} \pmod{17}$

(c) $10^{10} + 20^{20} + 30^{30} + 40^{40} \pmod{7}$

Solution:

(a) $3^{33} \pmod{11} \equiv 3^3 \cdot (3^{10})^3 \pmod{11} \equiv 27 \cdot 1^3 \pmod{11} \equiv 5 \pmod{11}$

(b) $10001^{10001} \pmod{17} \equiv 10001^1 \cdot (10001^{16})^{625} \pmod{17} \equiv 10001 \pmod{17} \equiv 5 \pmod{17}$

(c)

$$\begin{aligned} 10^{10} + 20^{20} + 30^{30} + 40^{40} \pmod{7} &\equiv 10^4 \cdot 10^6 + 20^2 \cdot 20^{18} \\ &\quad + 30^0 \cdot 30^{30} + 40^4 \cdot 40^{36} \pmod{7} \\ &\equiv 10^4 + 20^2 + 30^0 + 40^4 \pmod{7} \\ &\equiv 3^4 + 6^2 + 2^0 + 5^4 \pmod{7} \\ &\equiv 3^4 + (-1)^2 + 2^0 + (-2)^4 \pmod{7} \\ &\equiv 81 + 1 + 1 + 16 \pmod{7} \\ &\equiv 4 + 1 + 1 + 2 \pmod{7} \equiv 1 \pmod{7} \end{aligned}$$

2 Wilson's Theorem

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \ldots \cdot p-1$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?

Solution:

Direction 1: If p is prime, then the statement holds.

For the integers $1, \cdots, p-1$, every number has an inverse. However, it is not possible to pair a number off with its inverse when it is its own inverse. This happens when $x^2 \equiv 1 \pmod{p}$, or when $p \mid x^2 - 1 = (x-1)(x+1)$. Thus, $p \mid x-1$ or $p \mid x+1$, so $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. Thus, the only integers from 1 to $p-1$ inclusive whose inverse is the same as itself are 1 and $p-1$.

We reconsider the product $(p-1)! = 1 \cdot 2 \cdots p-1$. The product consists of 1, $p-1$, and pairs of numbers with their inverse, of which there are $\frac{p-1-2}{2} = \frac{p-3}{2}$. The product of the pairs is 1 (since the product of a number with its inverse is 1), so the product $(p-1)! \equiv 1 \cdot (p-1) \cdot 1 \equiv -1 \pmod{p}$, as desired.

Direction 2: The expression holds *only if* p is prime (contrapositive: if p isn't prime, then it doesn't hold).

We will prove by contradiction that if some number p is composite, then $(p-1)! \not\equiv -1 \pmod{p}$; Hypothetically assume that $(p-1)! \equiv -1 \pmod{p}$. Note that this means we can write $(p-1)!$ as $p \cdot k - 1$ for some integer k.

Since p isn't prime, it has some prime factor q where $2 \leq q \leq n-2$, and we can write $p = q \cdot r$. Plug this into the expression for $(p-1)!$ above, yielding us $(p-1)! = (q \cdot r)k - 1 = q(rk) - 1 \implies (p-1)! \equiv -1 \pmod{q}$. However, we know q is a term in $(p-1)!$, so $(p-1)! \equiv 0 \pmod{q}$. Since $0 \not\equiv 1 \pmod{q}$, we have reached our contradiction.

3 RSA Practice

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 $E(x)$?

(d) ☐ Will Bob correctly receive the message?

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.

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

(d) Yes. We can verify that $16^5 = 4 \pmod{21}$.