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

# 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 $(p-1)! \pmod{q}$?

## 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?