COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
New York, 2023/04/26

EXERCISE SHEET 14

Review exercises

Exercise 1. Prove that, for all $n \in \mathbb{Z}, n \geq 0$, we have

$$3 \mid 2^{2n+1} + 1\,.$$

Exercise 2. Solve the following equation

$$x^{21} \equiv 1 \pmod{31}$$

Exercise 3. Alice and Bob are exchanging a key using the Diffie-Helmann algorithm. Eve spies their communications. Assume they use $p = 47$, $g = 5$. They exchange the numbers $X = 38, Y = 3$. What is the key k?

Exercise 4. Use Shor's algorithm to factor the number 7097.
(Hint: 2 has order 345 modulo 7097. 3 has order 1150 modulo 7097.)

Exercise 5. Use Shor's algorithm to factor the number 3551.
(Hint: 2 has order 1716 modulo 3551, 3 has order 572 modulo 3551.)

Exercise 6. Show that, if $p > 3$ is a prime, then

$$p^2 \equiv 1 \pmod{24}.$$

(Hint: Use the Chinese remainder theorem, $24 = 2^3 3$.)

Exercise 7. Prove that there exists infinitely many positive integers n such that $4n^2 + 1$ is divisible both by 17 and 29.

(Hint:) use modular arithmetic.