COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
New York, 2023/05/01

Mock Exam

Exercise 1. Prove Bernoulli's inequality, which states that if $x \in \mathbb{R}, x > 0$ and $n \in \mathbb{Z}, n > 1$, then

$$(1+x)^n > 1 + nx\,.$$

(Hint:) you can try by induction.

Exercise 2. Given integers a, b, c, show that if $a^2 + b^2 = c^2$, then $3|ab$.
(Hint:) use modular arithmetic.

Exercise 3. Prove that $19 \mid 2^{2^{6k+2}} + 3$ for every integer $k \geq 0$.

Exercise 4. Solve the following system of congruences.

$$\begin{cases} 11x \equiv 7 & (\text{mod } 12) \\ 3x \equiv 3 & (\text{mod } 20) \\ 2x \equiv 22 & (\text{mod } 30) \end{cases}$$

Exercise 5. Show that for every positive integer n, the number $n^7 - n$ is divisible by 42.

Exercise 6. Prove that, if $n > 1$ is odd, $\varphi(n)$ does not divide n.