COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
New York, 2023/02/08

Exercise Sheet 4

Factorization

Exercise 1 (8 points)**.** Prove that for all $n \in \mathbb{N}$,

$$5|(11^n - 6)\,.$$

(Hint: you can try by induction.)

Exercise 2 (8 points)**.** Assume $d = p_1^{a_1} \dots p_k^{a_k}$ and $n = p_1^{b_1} \dots p_k^{b_k}$, where $p_1, \dots, p_k$ are distinct primes and $a_1, \dots, a_k, b_1, \dots, b_k \geq 0$. Prove that $d \mid n$ if and only if for every i, $a_i \leq b_i$.

Exercise 3 (8 points)**.** Assume $m = p_1^{a_1} \dots p_k^{a_k}$ and $n = p_1^{b_1} \dots p_k^{b_k}$, where $p_1, \dots, p_k$ are distinct primes and $a_1, \dots, a_k, b_1, \dots, b_k \geq 0$. Express $\gcd(m, n)$ as $p_1^{c_1} \dots p_k^{c_k}$ by describing the c_i's in terms of the a_i's and b_i's.

Exercise 4 (8 points)**.** Define the least common multiple of positive integers m, n to be

$$\operatorname{lcm}(m,n) = \min\{\ v \in \mathbb{N} \setminus \{0\} \quad | \quad m \mid v \quad \text{AND} \quad n \mid v\ \}\,.$$

Express $\operatorname{lcm}(m, n)$ in terms of the factorization of m and n given in Exercise 3, and prove that

$$\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)}\,.$$

Exercise 5 (8 points)**.** If p is a prime, prove that one cannot find non-zero integers a, b such that

$$a^2 = pb^2\,.$$

Then, prove that $\sqrt{p} \notin \mathbb{Q}$.

Exercise 6 (12 points)**.** Prove the following statements.

(a) Every odd natural number is either of the form $4n+1$ or of the form $4n+3$, for some $n \in \mathbb{N}$.

(b) Every odd number of the form $4n+3$ has at least a prime factor of the form $4n+3$.

(c) There is an infinite number of primes of the form $4n+3$.

Exercise 7 (8 points)**.** The numbers 3992003 and 1340939 are each products of two close primes. Find the primes.