COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Intro to Modern Algebra I
Math GU4041
New York, 2021/01/20

EXERCISE SHEET 2

Primes

Exercise 1. Find (a, b) and express it as a linear combination of a, b (i.e. write $(a, b) = sa + tb$ with $s, t \in \mathbb{Z}$) for the following pairs of numbers.

(a) $a = 116, b = -84$.

(b) $a = 85, b = 65$.

(c) $a = 72, b = 26$.

(d) $a = 72, b = 25$.

Exercise 2. Show that if $a \mid m$, $b \mid m$ and $(a, b) = 1$, then

$$ab \mid m\,.$$

Exercise 3. To check that a given integer $n > 1$ is a prime, prove that it is enough to show that n is not divisible by any prime p with $p \leq \sqrt{n}$.

Exercise 4. Check if the following are prime.

(a) 301.

(b) 473.

(c) 1001.

Exercise 5. 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 (m, n) as $p_1^{c_1} \dots p_k^{c_k}$ by describing the c's in terms of the a's and b's.

Exercise 6. 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 5, and prove that

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

Exercise 7. If p is a prime, prove that one cannot find non-zero integers a, b such that

$$a^2 = pb^2.$$

Notice that this shows that $\sqrt{p} \notin \mathbb{Q}$.