

**Math 221 Winter 2025 (Darij Grinberg): homework set 4**

due date: Thursday 2025-02-13 at 11:59PM on gradescope (

<https://www.gradescope.com/courses/930212> ).Please solve only **3 of the 6 exercises**.

**Exercise 1.** Let  $a$  and  $b$  be two coprime integers. Let  $i, j \in \mathbb{N}$  be arbitrary. Prove that  $a^i$  and  $b^j$  are again coprime.

**Exercise 2.** Prove that  $\gcd(2n + 3, 3n + 4) = 1$  for each  $n \in \mathbb{Z}$ .

**Exercise 3.** Let  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}$  be nonzero integers. Let  $(x, y)$  be some Bezout pair for  $(a, b)$ .

Let  $g = \gcd(a, b)$ . Let  $a' = a/g$  and  $b' = b/g$ .

Prove that each Bezout pair for  $(a, b)$  can be written in the form  $(x + kb', y - ka')$  for some  $k \in \mathbb{Z}$ .

[Hint: If  $(u, v)$  is a Bezout pair for  $(a, b)$ , then what is  $(u - x)a - (y - v)b$  ?]

Now, some exercises on primes:

**Exercise 4.** Let  $(a_0, a_1, a_2, \dots)$  be a sequence of integers defined recursively by

$$a_n = 1 + a_0 a_1 \cdots a_{n-1} \quad \text{for all } n \geq 0.$$

(This sequence has been studied in Exercise 5 on midterm 1.)

(a) Prove that  $\gcd(a_n, a_m) = 1$  for any two distinct integers  $n, m \in \mathbb{N}$ .

For each  $n \in \mathbb{N}$ , let  $p_n$  be a prime that divides  $a_n$ . (Such a prime exists, since  $a_n = 1 + \underbrace{a_0 a_1 \cdots a_{n-1}}_{\geq 1} \geq 1 + 1 > 1$ . Of course, there will often be several choices.

In this case, just choose one.)

(b) Prove that the primes  $p_0, p_1, p_2, \dots$  are distinct.

[Hint: Can two coprime integers share a prime divisor?]

**Remark 0.1.** This shows that there are infinitely many primes.

Two primes that differ by 2 are called **twin primes**. (For instance, 17 and 19 are twin primes.) To this day, no one knows whether there are infinitely many twin primes (this is the infamous “twin prime conjecture”). A much easier variant of this question asks how many “double-twin primes” (i.e., primes  $p$  such that both  $p - 2$  and  $p + 2$  are primes, so that  $p$  belongs to two twin-primes pairs) exist. The answer is, there is exactly one:

**Exercise 5.** Let  $p$  be a prime such that  $p - 2$  and  $p + 2$  are also prime. Prove that  $p = 5$ .

[**Hint:** Consider the remainders upon division by 6.]

**Exercise 6.** Let  $p$  be a prime such that  $p \equiv 3 \pmod{4}$ . Let  $n \in \mathbb{Z}$ . Prove that  $p \nmid n^2 + 1$ .

[**Hint:** In other words, prove that the congruence  $n^2 \equiv -1 \pmod{p}$  cannot hold. What happens if you take this congruence to the  $(p - 1) / 2$ -th power?]

---