Math 221 Winter 2023 (Darij Grinberg): homework set 4
due date: Sunday 2023-02-21 at 11:59PM on gradescope (`https://www.gradescope.com/courses/487830`).
Please solve only **4 of the 6 exercises**.

We begin with some exercises on greatest common divisors:

Exercise 1. Recall the `bezout_pair` function defined in §3.4.4 (Lecture 9). This function outputs a Bezout pair for any given pair (a, b) with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Tweak it so that it works for arbitrary $b \in \mathbb{Z}$ (not just for $b \in \mathbb{N}$).

[Feel free to use your favorite programming language instead of Python, but do not change the logic in the case when $b \geq 0$.]

Exercise 2. Prove that $\gcd(15n + 4,\ 12n + 5) = 1$ 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:** It is probably easiest to first prove this in the case when a and b are coprime. In this case, $g = 1$ and $a' = a$ and $b' = b$.]

Now, some exercises on primes:

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

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

(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 $p_0, p_1, p_2, \ldots$ are distinct.

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.]

And finally, here is a generalization of the $p \mid \dbinom{p}{k}$ divisibility (Theorem 3.6.3) from Lecture 10:

Exercise 6. Let p be a prime. Let $m \in \mathbb{N}$, and let $k \in \{1, 2, \ldots, p^m - 1\}$. Prove that $p \mid \dbinom{p^m}{k}$.