

# Math 235: Mathematical Problem Solving, Fall 2024: Homework 6

---

Darij Grinberg

November 14, 2024

**Please solve 5 of the 10 exercises!**

**Deadline:** November 20, 2024

---

## 1 EXERCISE 1

### 1.1 PROBLEM

Let  $(a_0, a_1, a_2, \dots)$  be a sequence of positive integers such that

$$a_n = (a_{n-1}^2 \% a_{n-2}) + 1 \quad \text{for each } n \geq 2.$$

Prove that this sequence is eventually 2-periodic (i.e., there exists some  $m \in \mathbb{N}$  such that the subsequence  $(a_m, a_{m+1}, a_{m+2}, \dots)$  is 2-periodic).

### 1.2 SOLUTION

...

---

## 2 EXERCISE 2

### 2.1 PROBLEM

Find all pairs  $(x, y)$  of nonnegative integers such that  $|x^2 - xy - y^2| = 5$ . (Recall the Lucas sequence from Example 4.9.3 in the notes.)

### 2.2 SOLUTION

...

---

## 3 EXERCISE 3

### 3.1 PROBLEM

Let  $n$  be a positive integer. Let  $a$  be any integer. Prove that there exist  $i \in \mathbb{N}$  and  $x \in \mathbb{Z}$  such that  $a^{i+1}x \equiv a^i \pmod{n}$ .

### 3.2 REMARK

This  $x$  can be viewed as a weak version of a modular inverse of  $a$  modulo  $n$ . An actual modular inverse would satisfy the congruence  $ax \equiv 1 \pmod{n}$  (that is,  $a^{i+1}x \equiv a^i \pmod{n}$  for  $i = 0$ ), but it only exists when  $a \perp n$  (see Theorem 3.5.9 in the notes), whereas the weak version always exists according to this exercise.

### 3.3 SOLUTION

...

---

## 4 EXERCISE 4

### 4.1 PROBLEM

Let  $n$  be a positive integer. Let  $x_1, x_2, \dots, x_{n+2}$  be  $n+2$  integers. Prove that there exist two distinct elements  $i$  and  $j$  of  $\{1, 2, \dots, n+2\}$  such that  $x_i - x_j$  or  $x_i + x_j$  (or both) is divisible by  $2n$ .

### 4.2 SOLUTION

...

---

## 5 EXERCISE 5

## 5.1 PROBLEM

Inside a regular hexagon with sidelength 1, you have marked 7 points. Show that there are two marked points whose distance to each other is at most 1.

## 5.2 SOLUTION

...

---

## 6 EXERCISE 6

## 6.1 PROBLEM

Let  $a \in \mathbb{Z}$  be such that  $a \equiv 1 \pmod{3}$ . Let  $k$  be a positive integer.

- (a) Prove that there exists a unique  $x \in \{0, 1, \dots, 3^k - 1\}$  such that  $x \equiv 1 \pmod{3}$  and  $x^2 \equiv a \pmod{3^k}$ .
- (b) Prove that for each  $i \in \mathbb{N}$ , there exists a unique  $x_i \in \{0, 1, \dots, 3^k - 1\}$  such that  $x_i \equiv 1 \pmod{3}$  and  $x_i^{2^i} \equiv a \pmod{3^k}$ .
- (c) Consider the sequence  $(x_0, x_1, x_2, \dots)$  of these unique  $x_i$ 's. Is this sequence periodic?

## 6.2 REMARK

The  $x$  in part (a) can be regarded as the “canonical” square root of  $a$  modulo  $3^k$ . In general, square roots modulo  $n$  neither necessarily exist nor are always unique, just like square roots of real numbers; thus the claim of part (a) is rather remarkable.

## 6.3 SOLUTION

...

---

## 7 EXERCISE 7

## 7.1 PROBLEM

Let  $a_1, a_2, \dots, a_m$  be  $m$  integers, and let  $n$  be a positive integer such that  $n < 2^m$ . Prove that we can find  $m$  numbers  $x_1, x_2, \dots, x_m \in \{0, 1, -1\}$  such that not all these numbers  $x_1, x_2, \dots, x_m$  are zero and such that  $n \mid \sum_{i=1}^m x_i a_i$ . (In other words, prove that we can make the sum  $a_1 + a_2 + \dots + a_m$  divisible by  $n$  if we are allowed to throw some (not all) of the

addends away and replace some (possibly none, possibly all) of the remaining addends by their negatives.)

**[Example:** Let  $m = 4$  and  $n = 13$  and  $(a_1, a_2, \dots, a_m) = (4, 7, 19, 40)$ . Then, the four numbers  $0, -1, 1, 1$  are  $m$  numbers  $x_1, x_2, \dots, x_m$  that satisfy  $n \mid \sum_{i=1}^m x_i a_i$ , since  $13 \mid 0 \cdot 4 + (-1) \cdot 7 + 1 \cdot 19 + 1 \cdot 40$ .]

## 7.2 SOLUTION

...

---

## 8 EXERCISE 8

### 8.1 PROBLEM

Let  $a_1, a_2, \dots, a_k$  be  $k$  real numbers. Let  $(x_0, x_1, x_2, \dots)$  be a sequence of real numbers that is  $(a_1, a_2, \dots, a_k)$ -recurrent (see Definition 4.9.24 in the notes). Assume that this sequence has only finitely many distinct entries (i.e., the set  $\{x_0, x_1, x_2, \dots\}$  is finite). Show the following:

- (a) The sequence  $(x_0, x_1, x_2, \dots)$  is eventually periodic (i.e., there exists some  $m \in \mathbb{N}$  such that the sequence  $(x_m, x_{m+1}, x_{m+2}, \dots)$  is periodic).
- (b) If  $a_k \neq 0$ , then the sequence  $(x_0, x_1, x_2, \dots)$  is periodic.

### 8.2 SOLUTION

...

---

## 9 EXERCISE 9

### 9.1 PROBLEM

Let  $n > 1$ . Let  $A$  be an  $n \times n$ -matrix whose entries are the  $n^2$  integers  $1, 2, \dots, n^2$  in some arbitrary order.

- (a) Prove that we can find two entries  $i$  and  $j$  of  $A$  that lie in the same row and satisfy  $\frac{n-1}{n} \leq \frac{i}{j} < 1$ .
- (b) Prove that we can find two entries  $i$  and  $j$  of  $A$  that lie in the same row or the same column and satisfy  $\frac{n}{n+1} \leq \frac{i}{j} < 1$ .

## 9.2 SOLUTION

...

---

## 10 EXERCISE 10

## 10.1 PROBLEM

Let  $a$  and  $n$  be two integers such that  $n > 0$ . Let  $u$  and  $v$  be two positive integers such that  $uv > n$  and  $v > 1$ . Prove that there exist two integers  $x$  and  $y$  with  $|x| < u$  and  $0 < y < v$  and  $ay \equiv x \pmod{n}$ .

## 10.2 SOLUTION

...

---

## REFERENCES