Drexel University, Department of Mathematics

Math 235: Mathematical Problem Solving, Fall 2021: Homework 3

Darij Grinberg

October 4, 2021

1 Exercise 1

1.1 Problem

Let p be a prime. Let $k \in \mathbb{N}$.

(a) Prove that

$$\binom{k}{p-1} \equiv \begin{cases} 1, & \text{if } k \equiv -1 \mod p; \\ 0, & \text{if } k \not\equiv -1 \mod p \end{cases} \mod p.$$

(b) Prove that

$$\binom{k}{p} \equiv \left\lfloor \frac{k}{p} \right\rfloor \mod p.$$

1.2 Solution

...

2 Exercise 2

2.1 Problem

A polynomial $p(x)$ with rational coefficients is called *integer-valued* if it has the property that $p(a) \in \mathbb{Z}$ for each $a \in \mathbb{Z}$.

An integer-valued polynomial $p(x)$ is called *congruence-preserving* if it has the following additional property: If n, a, b are three integers satisfying $a \equiv b \mod n$, then $p(a) \equiv p(b) \mod n$.

The substitution principle for congruences yields that every polynomial with integer coefficients is congruence-preserving.

On the other hand, the polynomial $p(x) = \dfrac{x(x-1)}{2} = \dbinom{x}{2}$ is integer-valued but not congruence-preserving (because $1 \equiv 3 \mod 2$ but $p(1) \not\equiv p(3) \mod 2$).

Prove that the polynomial

$$p(x) = \frac{x^2(x^2-1)}{2} = \binom{x^2}{2}$$

is integer-valued and congruence-preserving (despite not having integer coefficients). Thus, all inclusions in

$$\begin{aligned} &\{\text{polynomials with integer coefficients}\} \\ &\subseteq \{\text{congruence-preserving integer-valued polynomials}\} \\ &\subseteq \{\text{integer-valued polynomials}\} \end{aligned}$$

are strict.

2.2 Solution

...

---

3 Exercise 3

3.1 Problem

Let m and n be two coprime positive integers. Prove that

$$\sum_{k=0}^{m-1} \left\lfloor \frac{kn}{m} \right\rfloor = \frac{(m-1)(n-1)}{2}.$$

3.2 Solution

...

---

4 Exercise 4

4.1 Problem

Let $P(x)$ and $(s_0, s_1, s_2, \ldots)$ be as in Exercise 3.4.1. (That is, $P(x)$ is a polynomial with integer coefficients, and $(s_0, s_1, s_2, \ldots)$ is the integer sequence defined recursively by $s_0 = 0$ and $s_i = P(s_{i-1})$ for all $i \geq 1$.) Prove that

$$\gcd(s_a, s_b) = \left|s_{\gcd(a,b)}\right| \qquad \text{for any } a, b \in \mathbb{N}.$$

[**Hint:** Show that $\gcd(s_a, s_b) = \gcd(s_a, s_{b-a})$ whenever $a \leq b$; then argue by strong induction as in the proof of the Bezout theorem.]

4.2 Solution

...

---

5 Exercise 5

5.1 Problem

Let p be a prime such that $p \equiv 3 \mod 4$.

(a) Prove that there exists no $c \in \mathbb{Z}$ such that $c^2 \equiv -1 \mod p$.

(b) Prove that if $a, b \in \mathbb{Z}$ are two integers satisfying $a^2 + b^2 \equiv 0 \mod p$, then a and b are multiples of p.

(c) Prove that there exist no two rational numbers a and b such that $a^2 + b^2 = p$.

[**Hint:** For part **(a)**, apply Exercise 3.6.4 **(d)** and note that $(p-1)/2$ is odd. For part **(b)**, use modular inverses modulo p. Note that part **(c)** generalizes Exercise 3.6.1.]

5.2 Solution

...

---

6 Exercise 6

6.1 Problem

Prove that there exist infinitely many primes that are congruent to 1 modulo 4.

[**Hint:** You can use Exercise 5 **(a)**.]

6.2 Solution

...

References