

## Homework 12: Due Wednesday, November 9

**Problem 1:** Let  $n \in \mathbb{N}^+$ .

a. Evaluate

$$\sum_{k=0}^n 3^k \cdot c(n, k).$$

b. Evaluate

$$\sum_{k=0}^n 3^k \cdot s(n, k).$$

*Note:* Simplify your answers as much as possible.

**Problem 2:** Let  $n \in \mathbb{N}$  with  $n \geq 2$ .

a. Show that

$$c(n, 2) = \frac{n!}{2} \sum_{k=1}^{n-1} \frac{1}{k(n-k)}.$$

b. Show that  $c(n, 2) = (n-1)! \cdot H_{n-1}$ , where  $H_{n-1}$  is as defined in the interlude on Homework 11.

**Problem 3:** Show that for all  $a \in \mathbb{Z}$ , either  $a^2 \equiv 0 \pmod{3}$  or  $a^2 \equiv 1 \pmod{3}$ .

*Note:* This problem is equivalent to Problem 1 on Homework 4. However, you should *not* just appeal to Problem 1 on Homework 4. Instead, use properties of congruences.

**Problem 4:** Let  $a, b \in \mathbb{Z}$  and  $m \in \mathbb{N}^+$  be such that  $a \equiv b \pmod{m}$ . Show that  $\gcd(a, m) = \gcd(b, m)$ .

**Problem 5:** Suppose that  $m, k \in \mathbb{N}^+$  and  $a, b \in \mathbb{Z}$  are such that  $ka \equiv kb \pmod{m}$ . Let  $d = \gcd(k, m)$ , and fix  $n \in \mathbb{N}^+$  with  $m = dn$ . Show that  $a \equiv b \pmod{n}$ .

**Problem 6:** Let  $p \in \mathbb{N}^+$  be prime and let  $a \in \mathbb{Z}$ . Show that  $a^2 \equiv 1 \pmod{p}$  if and only if either  $a \equiv 1 \pmod{p}$  or  $a \equiv -1 \pmod{p}$ .

**Problem 7:** Let  $p \in \mathbb{N}^+$  be prime. Define a function  $\text{ord}_p: \mathbb{N}^+ \rightarrow \mathbb{N}$  as follows. Given  $a \in \mathbb{N}^+$ , let  $\text{ord}_p(a)$  be the largest  $k \in \mathbb{N}$  such that  $p^k \mid a$ . For example, we have  $\text{ord}_3(45) = 2$  and  $\text{ord}_3(10) = 0$ . Without using the Fundamental Theorem of Arithmetic, prove that for all  $p, a, b \in \mathbb{N}^+$  with  $p$  prime, we have  $\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b)$ .

*Note:* Think carefully about what you need to do in order to prove that  $\text{ord}_p(c) = k$ . You need to show that  $p^k \mid c$ , but you also need to show that  $p^\ell \nmid c$  whenever  $\ell > k$ .