Theory of Computation

Solutions to Homework 4

Problem 1. Let $a, b \in \mathbb{N}$ and p be a prime. Show that $(a+b)^p = a^p + b^p \bmod p$.

Proof. By the binomial expansion,

$$(a+b)^p = \sum_{r=0}^{p} \binom{p}{r} a^r\, b^{p-r}. \tag{1}$$

As p is a prime, $r!(p-r)!$ is not a multiple of p for $0 < r < p$. But $\binom{p}{r} = p!/(r!(p-r)!)$ is an integer and $p \,|\, p!$. Hence $\binom{p}{r}$ is a multiple of p for $0 < r < p$. Therefore, Eq. (1) gives $(a+b)^p = a^p + b^p \bmod p$. □

Problem 2. Let d be a positive integer. Show that

$$\left| \left\{ x \in \mathbb{R} \mid \exists a_0, \ldots, a_d \in \{1,2,3\}, \sum_{i=0}^{d} a_i x^i = 0 \right\} \right| \leq d\, 3^{d+1},$$

i.e., degree-d polynomials with coefficients in $\{1,2,3\}$ have at most $d\,3^{d+1}$ distinct roots altogether.

Proof. There are 3^{d+1} degree-d polynomials with coefficients in $\{1,2,3\}$. Each of them has at most d roots. □