

## 1 Polynomial Practice

- (a) If  $f$  and  $g$  are non-zero real polynomials, how many roots do the following polynomials have at least? How many can they have at most? (Your answer may depend on the degrees of  $f$  and  $g$ .)

- (i)  $f + g$
- (ii)  $f \cdot g$
- (iii)  $f/g$ , assuming that  $f/g$  is a polynomial

- (b) Now let  $f$  and  $g$  be polynomials over  $\text{GF}(p)$ .

- (i) We say a polynomial  $f = 0$  if  $\forall x, f(x) = 0$ . If  $f \cdot g = 0$ , is it true that either  $f = 0$  or  $g = 0$ ?
- (ii) How many  $f$  of degree *exactly*  $d < p$  are there such that  $f(0) = a$  for some fixed  $a \in \{0, 1, \dots, p-1\}$ ?

- (c) Find a polynomial  $f$  over  $\text{GF}(5)$  that satisfies  $f(0) = 1, f(2) = 2, f(4) = 0$ . How many such polynomials are there?

## 2 Lagrange Interpolation in Finite Fields

Find a unique polynomial  $p(x)$  of degree at most 3 that passes through points  $(-1, 3)$ ,  $(0, 1)$ ,  $(1, 2)$ , and  $(2, 0)$  in modulo 5 arithmetic using the Lagrange interpolation.

- (a) Find  $p_{-1}(x)$  where  $p_{-1}(0) \equiv p_{-1}(1) \equiv p_{-1}(2) \equiv 0 \pmod{5}$  and  $p_{-1}(-1) \equiv 1 \pmod{5}$ .
- (b) Find  $p_0(x)$  where  $p_0(-1) \equiv p_0(1) \equiv p_0(2) \equiv 0 \pmod{5}$  and  $p_0(0) \equiv 1 \pmod{5}$ .
- (c) Find  $p_1(x)$  where  $p_1(-1) \equiv p_1(0) \equiv p_1(2) \equiv 0 \pmod{5}$  and  $p_1(1) \equiv 1 \pmod{5}$ .
- (d) Find  $p_2(x)$  where  $p_2(-1) \equiv p_2(0) \equiv p_2(1) \equiv 0 \pmod{5}$  and  $p_2(2) \equiv 1 \pmod{5}$ .
- (e) Construct  $p(x)$  using a linear combination of  $p_{-1}(x)$ ,  $p_0(x)$ ,  $p_1(x)$  and  $p_2(x)$ .

## 3 Secrets in the United Nations

A vault in the United Nations can be opened with a secret combination  $s \in \mathbb{Z}$ . In only two situations should this vault be opened: (i) all 193 member countries must agree, or (ii) at least 55 countries, plus the U.N. Secretary-General, must agree.

- (a) Propose a scheme that gives private information to the Secretary-General and all 193 member countries so that the secret combination  $s$  can only be recovered under either one of the two specified conditions.

- (b) The General Assembly of the UN decides to add an extra level of security: each of the 193 member countries has a delegation of 12 representatives, all of whom must agree in order for that country to help open the vault. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary-General and to each representative of each country.

## 4 To The Moon!

A secret number  $s$  is required to launch a rocket, and Alice distributed the values  $(1, p(1)), (2, p(2)), \dots, (n+1, p(n+1))$  of a degree  $n$  polynomial  $p$  to a group of \$GME holders  $\text{Bob}_1, \dots, \text{Bob}_{n+1}$ . As usual, she chose  $p$  such that  $p(0) = s$ .  $\text{Bob}_1$  through  $\text{Bob}_{n+1}$  now gather to jointly discover the secret. However,  $\text{Bob}_1$  is secretly a partner at Melvin Capital and already knows  $s$ , and wants to sabotage  $\text{Bob}_2, \dots, \text{Bob}_{n+1}$ , making them believe that the secret is in fact some fixed  $s' \neq s$ . How could he achieve this? In other words, what value should he report in order to make the others believe that the secret is  $s'$ ?