

## Interesting Polynomials

Here we will look at polynomials with coefficients in the integers modulo a prime  $p$ . The notation for this collection of polynomials is  $\mathbb{Z}_p[X]$ .

Addition and multiplication of these polynomials is exactly the same as polynomials with real or rational coefficients.

Suppose  $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}_p[X]$  and  $a_n \neq 0$ . Then the *degree* of  $P(X)$  is  $n$ . The degree of 0 is defined to be  $-\infty$ . We write  $\deg(P(X))$  (or just  $\deg(P)$ ) for the degree of the polynomial  $P(X)$ .

**Lemma:** For any two polynomials  $P(X)$  and  $Q(X)$ ,

$$\deg(P \times Q) = \deg(P) + \deg(Q)$$

and

$$\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}.$$

**Lemma:** If  $P(X) \times Q(X) = 0$ , then either  $P(X) = 0$  or  $Q(X) = 0$ .

**NOTE:** These lemmas are true only because  $p$  is a prime. They are most definitely *not true* if we look at polynomials with coefficients in  $\mathbb{Z}_n$  for a composite  $n$ !

**Division Algorithm:** For any polynomials  $A(X)$  and  $B(X)$  with  $B(X) \neq 0$ , there are polynomials  $Q(X)$  and  $R(X)$  with

$$A(X) = Q(X) \times B(X) + R(X)$$

and  $\deg(R) < \deg(B)$ .

**Lemma:** Suppose  $P(X) \in \mathbb{Z}_p[X]$  and  $a \in \mathbb{Z}_p$ . Then  $a$  is a root of  $P(X)$ , i.e.,  $P(a) = 0$ , if and only if  $X - a \mid P(X)$ .

**Proof:** Use the division algorithm and divide  $P(X)$  by  $X - a$ . Since the degree of  $X - a$  is 1, the remainder must have degree 0 or  $-\infty$ . In other words,

$$P(X) = (X - a)Q(X) + b$$

for some  $b \in \mathbb{Z}_p$ . If  $X - a \mid P(X)$ , then  $b = 0$  and plugging in  $a$  for  $X$  shows that  $P(a) = 0$ . On the other hand, if  $P(a) = 0$ , then plugging in  $a$  for  $X$  shows that  $b = 0$ .

**Corollary 1:** If  $P(X) \in \mathbb{Z}_p[X]$  has degree  $n$ , then  $P$  has at most  $n$  roots in  $\mathbb{Z}_p$ .

**Corollary 2:** We have

$$X^p - X = \prod_{a \in \mathbb{Z}_p} X - a.$$

In particular,

$$\prod_{a \neq 0} a = -1,$$

in other words,

$$(p - 1)! \equiv -1 \pmod{p}$$

for any prime  $p$ .