Finite fields

- You also know other examples of fields: Z_p for p a prime is a field. We saw that Z_n has a well-defined $+$ and $\cdot$ coming from the integers. If n is prime then we also know that if $ax \equiv 1 \bmod n$ has a solution as long as $\gcd(a, n) = 1$ which happens as long as $a \neq 0$ in Z_n.
- As we will see, there are many other finite fields other than Z_p. Sometimes one writes $GF(k)$ for the finite field with k elements or other sources write F_k for the finite field with k elements. Your book uses GF except when talking about Z_p for primes p.

Finite fields, cont'd

- We define the characteristic of a field F to be the least number n such that

$$\underbrace{1 + 1 + 1 + \ldots + 1}_{n \text{ times}} = 0$$

  if such an n exists and we say that the characteristic is 0 otherwise.
- R, C and the rationals have characteristic 0; Z_p has characteristic p for any prime p.

Lemma

Any finite field has characteristic p for some prime p and size p^n for some positive integer n.

Finite fields, cont'd

- Some calculations are very simple in a finite field of characteristic p; for instance, in such a field

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}.$$

- In order to find all the finite fields, we start by studying the polynomials with coefficients from Z_p, $Z_p[x]$.
- The order or degree of a polynomial where $a_i \in Z_p$ for all i

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

  is n if $a_n \neq 0$. That is, $deg(f) = n$.
- Two polynomials in $Z_p[x]$ are said to be equal if all of their coefficients are equal. To add polynomials in $Z_p[x]$ one just add their coefficients.

Finite fields, cont'd

- Multiplication of two polynomials in $Z_p[x]$ is defined in the usual way: if

$$f(x) = a_0 + \ldots a_n x^n \text{ and } g(x) = b_0 + \ldots + b_m x^m$$

then

$$(fg)(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \ldots$$
$$(\sum_{j=0}^{i} a_j b_{i-j})x^i + \ldots + a_n b_m x^{m+n}.$$

Euclidean algorithm

Lemma

For $f, g, h \in Z_p[x]$

1. $deg(f+g) \leq \max(deg(f), deg(g))$.
2. *If* $f, g \neq 0$ *then* $deg(fg) = deg(f) + deg(g)$.
3. *If* $fg = 0$ *then* $f = 0$ *or* $g = 0$.
4. *If* $fh = gh$ *and* $h \neq 0$ *then* $f = g$.
5. *If* $f \neq 0$ *then there exists* g *with* $fg = 1$ *iff* $deg(f) = 0$.

Theorem (Euclidean algorithm)

For $f, g \in Z_p[x]$ *with* $deg(g) \neq 0$ *there exist unique* $q, r \in Z_p[x]$ *where* $deg(r) < deg(g)$ *and*

$$f = qg + r.$$

Irreducible polynomials

- For polynomials, we say that g divides f if there is some h, $f = gh$.
- We say that f is irreducible if whenever g divides f then either $deg(g) = deg(f)$ or $deg(g) = 0$.
- Notice that $a_1x + a_0$ is irreducible for any $a_1 \neq 0$.
- Polynomials can also be thought of as functions on the underlying field but you must be careful. If $f \in Z_p[x]$ and $Z_p \subseteq F$ for some field F then for any $c \in F$, $f(c)$ makes sense by direct substitution.
- On the other hand, it is possible for two polynomials to agree on all $c \in F$ but not to be equal as polynomials.

Irreducible polynomials, cont'd

Lemma

Suppose $f \in F[x]$.

1. *If* $f(c) = 0$ *for some* $c \in F$ *then* $x - c$ *divides* f.
2. *If* f *has degree* n *then* f *has at most* n *roots.*
3. *If* $deg(f) = 2, 3$ *then* f *is irreducible iff* f *has no root in* F.