Finite fields (12.2)

Recall $m \in \mathbb{N}$, $x, y \in \mathbb{Z}$ $x \equiv y \pmod m \overset{\text{def}}{\iff} x-y$ divisible by m.

$\rightsquigarrow$ Congruence classes $[x]_m = \{y \in \mathbb{Z} \mid x \equiv y \pmod m\}$

$\rightsquigarrow$ Ring of integers $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$, with addition & multiplication $[x]+[y]=[x+y]$, $[x][y]=[xy]$.

Not, in general, division, say $\mathbb{Z}_m$ is a field if $\forall x \in \mathbb{Z}_m \setminus \{0\}$, there is an inverse y s.t. $xy = 1 \ (=[1])$.

Thm $\mathbb{Z}_m$ is a field $\iff$ m is prime.

Other fields are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$... other finite ones?

Thm For every prime p & integer $n \geq 1$ there is a field of p^n elements, which is unique up to isomorphism. A finite field F must have $|F| = p^n$ for some prime p & $n \geq 1$.

Ex No field of 6 elements.

Rmk Unique up to isomorphism means: If F_1 & F_2 are fields with $p^n = |F_1| = |F_2|$, then there is a bijection $\phi : F_1 \to F_2$ such that $\phi(xy) = \phi(x)\phi(y)$ & $\phi(x+y) = \phi(x) + \phi(y)$ $\forall x, y \in F_1$.

Rmk The field of $q = p^n$ elements is called a Galois field, denoted $GF(q)$ or $\mathbb{F}_q$.

Construction of $GF(q)$ Let $q = p^n$.

Build $GF(q)$ from $\mathbb{Z}_p$ + a formal addition of an element α, satisfying some polynomial equation

$$f(\alpha) = 0$$

Analogy: Build $\mathbb{C}$ from $\mathbb{R}$ + formal addition of i, with $f(i)=0$ for $f(x) = x^2+1$.

Def $\mathbb{Z}_m[x] = \{ \sum_{i=0}^{n} a_i x^i \mid n \geq 0, a_i \in \mathbb{Z}_m \}$, the ring of polynomials with coefficients in $\mathbb{Z}_m$.
Addition & multiplication "as usual", but using + & × from $\mathbb{Z}_m$ on coefficients.

Ex In $\mathbb{Z}_3[x]$, $2x^2+x+1$, $2x^2+1 \in \mathbb{Z}_3[x]$,

$$(2x^2+x+1)+(2x^2+1) = (2+2)x^2+(1+0)x+(1+1)$$
$$= 4x^2+x+2 = x^2+x+2.$$

$$1+x \in \mathbb{Z}_2[x] \rightsquigarrow (1+x)(1+x) = x^2+(1\cdot 1+1\cdot 1)x+1\cdot 1$$
$$= x^2+2x+1 = x^2+1.$$

Exercise: $\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}_p[x] \rightsquigarrow \left(\sum_{i=0}^{n} a_i x^i\right)^p = \sum_{i=0}^{n} a_i x^{ip}$ (Needs Fermat) & $\binom{p}{i} \equiv 0 \pmod p$ for $0 < i < p$

Let $f(x) \in \mathbb{Z}_p[x]$. Say $g(x) \equiv h(x) \pmod{f(x)}$ if $f(x)$ divides $g(x)-h(x) \overset{\text{def}}{\iff} \exists\, q(x)$ s.t. $g(x)-h(x) = f(x)q(x)$.

$\equiv \pmod{f(x)}$ forms an equivalence relation

$\rightsquigarrow \mathbb{Z}_p[x]/\langle f(x)\rangle$ = set of equivalence classes.

$[g(x)] = \{ h(x) \mid h(x) \equiv g(x) \mod f(x) \}$

Elements of $\mathbb{Z}_p[x]/\langle f(x)\rangle$?

Let $g(x) \in \mathbb{Z}_p[x]$. Polynomial division by $f(x)$ gives

$$g(x) = f(x)q(x) + r(x) \quad \text{for some } r(x) \text{ with } \deg r(x) < \deg f(x) = n$$

$$\Updownarrow$$

$$g(x) - r(x) = f(x)q(x)$$

$$\Updownarrow$$

$$g(x) \equiv r(x) \mod f(x).$$

$\Longrightarrow$ Every equivalence class mod $f(x)$ is represented by a unique $r(x)$ of deg $r(x) < n$.

$$\mathbb{Z}_p[x]/\langle f(x)\rangle \longleftrightarrow \{ a_{n-1}x^{n-1} + \cdots + a_0 \mid a_i \in \mathbb{Z}_p \}$$

$$|\mathbb{Z}_p[x]/\langle f(x)\rangle| = p^n.$$

Ex $x^3 \in \mathbb{Z}_3[x]/\langle x^2+1\rangle$ $\quad x^3 = (x^2+1)x - x \Longrightarrow x^3 \equiv -x \equiv 2x \mod x^2+1.$

The set $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a ring, with operations defined by

$$[g(x)] + [h(x)] = [g(x) + h(x)]$$

$$[g(x)][h(x)] = [g(x)h(x)]$$

Ex $f(x) = x^2 + x \in \mathbb{Z}_2[x]$. Write $\alpha = [x] \in \mathbb{Z}_2[x]/\langle x^2+x\rangle$.

Then $\mathbb{Z}_2[x]/\langle x^2+x\rangle = \{0, 1, \alpha, \alpha+1\}$

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

x	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	α	0
$\alpha+1$	0	$\alpha+1$	0	$\alpha+1$

Ex $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ $\alpha = [x]$, addition table the same as in previous example,

x	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

$\alpha^2 = [x]^2 = [x^2] = [x+1] = \alpha+1$

$\alpha(1+\alpha) = \alpha^2+\alpha = [x^2+x] = [1] = 1$

2nd example a field, 1st not.

Def A polynomial $f(x) \in \mathbb{Z}_p[x]$ is irreducible if $\deg f \geq 1$ & there is no way to write $f(x) = g(x)h(x)$ with $1 \leq \deg g, \deg h < \deg f$.

Rmk Analogue in $\mathbb{Z}_p[x]$ of primes in $\mathbb{Z}$.

Ex $x^2+x = (x+1)x$, so x^2+x not irreducible

x^2+x+1 is irreducible: If $x^2+x+1 = g(x)h(x)$ with $1 \leq \deg g, \deg h < \deg x^2+x+1 = 2$

then $\deg g = \deg h = 1 \Rightarrow$ either $g(0) = 0$ or $g(1) = 0$.

But $0^2+0+1 = 1$ & $1^2+1+1 = 1$, so this is impossible.

Thm $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field $\iff$ $f(x)$ is irreducible

Pf of $\Rightarrow$: If $f(x) = g(x)h(x)$ with $\deg g(x), \deg h(x) < \deg f(x)$,

Then $[g(x)] \neq 0 \neq [h(x)]$ in $\mathbb{Z}_p[x]/\langle f(x)\rangle$.

But $[g(x)][h(x)] = [g(x)h(x)] = [f(x)] = 0$, so $\mathbb{Z}_p[x]/\langle f(x)\rangle$ not a field.

To define $GF(p^n)$, find some irreducible $f(x) \in \mathbb{Z}_p[x]$ of degree n ($\approx \frac{1}{n}$ of deg n pols are irreducible),

Then $GF(p^n) = \mathbb{Z}_p[x]/\langle f(x)\rangle$.