How to construct finite fields?

Ex: Construct a field of order 27.

Start with $\mathbb{F}_3$. Find an irreducible poly. of degree 3 in $\mathbb{F}_3[x]$:

Try #1:

x^3+1	x
1	0
2	1
0	2

Try #2:

x^3+x^2+x+1	x
1	0
1	1
0	2

Try #3:

x^3-x+1	x
1	0
1	1
1	2

✓

$f(x) = x^3 - x + 1$ is irred. over $\mathbb{F}_3$ b/c it is a degree poly. with no roots in $\mathbb{F}_3$.

Therefore, since $\mathbb{F}_3[x]$ is a PID, $(f(x))$ is a prime ideal, therefore maximal,

So $F = \mathbb{F}_3[x]/(f)$ is a field.

Representatives for F:

$\forall\, g(x) \in \mathbb{F}[x]$, $\exists\, q, r \in \mathbb{F}_3[x]$ s.t.

$g(x) = f(x)q(x) + r(x)$, and $r(x) = 0$ or $\deg r < \deg f$.

Then $g(x) = r(x)$ in F.

It follows that

$F = \{a_2x^2 + a_1x + a_0 : a_0, a_1, a_2 \in \mathbb{F}_3\}$,

so $|F| = 27$.

Follow up: find a generator for $F^\times$.

Since $|F^\times| = 26$, every element of $F^\times$ has order $1, 2, 13$, or 26.

Try #1: x

$f(x) = x^3 - x + 1$

$F = \mathbb{F}_3[x]/(f)$

$x^2 \neq 1$ in F

$$\begin{array}{r l}
 & x^{10} + x^8 - x^7 + x^6 \\
x^3 - x + 1 \,\big) & x^{13} \\
 & -(x^{13} - x^{11} + x^{10}) \\
\hline
 & x^{11} - x^{10} \\
 & -(x^{11} \quad - x^9 + x^8) \\
\hline
 & -x^{10} + x^9 - x^8 \\
 & -(-x^{10} \quad + x^8 - x^7) \\
\hline
 & x^9 + x^8 + x^7
\end{array}$$

⋮ (cont)

R1

$$x^3-x+1 \;\big)\; x^{13} \qquad \text{quotient: } x^{10}+x^8-x^7+x^6+x^5-x^4+x^2+x+1$$

$$\begin{array}{l}
x^{13} \\
-(x^{13}-x^{11}+x^{10}) \\
\hline
x^{11}-x^{10} \\
-(x^{11}-x^9+x^8) \\
\hline
-x^{10}+x^9-x^8 \\
-(-x^{10}+x^8-x^7) \\
\hline
x^9+x^8+x^7 \\
-(x^9-x^7+x^6) \\
\hline
x^8-x^7-x^6 \\
-(x^8-x^6+x^5) \\
\hline
-x^7-x^5 \\
-(-x^7+x^5-x^4) \\
\hline
x^5+x^4 \\
-(x^5-x^3+x^2) \\
\hline
x^4+x^3-x^2 \\
-(x^4-x^2+x) \\
\hline
x^3-x \\
-(x^3-x+1) \\
\hline
-1
\end{array}$$

So $x^{13}=-1$ in F $\Rightarrow$ $|x|=26$, so $F^\times=\langle x\rangle$.

Chinese Remainder Theorem

Assume R is a commutative ring with $1 \neq 0$.

Defs:

1) If R and S are rings then their direct product is $R \times S$ with ptwise add. and mult.
2) Ideals $A, B \subseteq R$ are comaximal (coprime) if $A + B = R$.

Chinese Remainder Thm (CRT): Suppose $A_1, \ldots, A_k$ are pairwise comaximal ideals in R. Then:

i) The map $\phi : R \to R/A_1 \times \cdots \times R/A_k$ defined by $\phi(x) = (x + A_1, \ldots, x + A_k)$ is a surjective ring homom.

ii) $\ker \phi = A_1 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$.

iii) $R/A_1 \cdots A_k \cong R/A_1 \times \cdots \times R/A_k$.

ring isom.

iv) $\left(R/A_1 \cdots A_k\right)^\times \cong \left(R/A_1\right)^\times \times \cdots \times \left(R/A_k\right)^\times$

gp-isom.

Pf: By induction, enough to prove this when $k=2$.

i) It is clear that ϕ is a ring homom. NTS that ϕ is surj.

Suppose A_1, A_2 are comaximal. Then $\exists x \in A_1$, $y \in A_2$ s.t. $x+y=1$.

Then $\phi(x) = (x+A_1, x+A_2) = (x+A_1, 1-y+A_2)$
$= (0,1)$,

and $\phi(y) = (y+A_1, y+A_2) = (1-x+A_1, y+A_2)$
$= (1,0)$.

So $\forall r,s \in R$, $\phi(rx+sy) = (s+A_1, r+A_2)$,
so the map is surjective.

ii) We already know that $A_1A_2 \subseteq A_1 \cap A_2$.
Also, it is clear from the def of ϕ that $\ker\phi = A_1 \cap A_2$.

NTS: $A_1 \cap A_2 \subseteq A_1A_2$. Let $x \in A_1, y \in A_2$, $x+y=1$. Let $a \in A_1 \cap A_2$. Then
$a = a(x+y) = ax+ay \in A_1A_2$.

iii) follows from i) + ii), plus the 1st Isom Thm. for rings.

iv) follows from the fact that an Isom. of rings maps units to units, so restricts to a group Isom. of the gp. of units. ∎

HW 9: due Monday, Dec 2, 9:59 pm

Final Exam:

Monday, Dec 9, 10am-12pm

Mainly over what we covered since midterm.

Details forthcoming.

Study: Lecture notes, examples, & hmwk probs.