Algorithms for finite fields

(by H. Lenstra)

<u>Theorem</u> (Galois, 1830, E.H. Moore, 1893):

The map $\{\text{finite fields}\}/\cong \longrightarrow \{\text{primes}\} \times \mathbb{Z}_{\geq 0}$ is bijective

$$k \longmapsto (p = \text{char } k, [k : \mathbb{F}_p])$$

We'll try to find a constructive version of this theorem.

<u>Construction of finite fields:</u>

<u>Open problem</u>: is there a poly'l-time algorithm that given (p, n), p prime, $n \in \mathbb{Z}_{\geq 0}$, constructs an explicit model for $\mathbb{F}_{p^n}$?

By <u>algorithm</u> we'll understand a <u>deterministic</u> <u>computer program</u>, with certain input and output, considered as a Turing machine.

By <u>polynomial time</u> we'll understand that $\exists c : \forall p, n$ the run-time of the algorithm is $\leq (n + \log p)^c$

By <u>explicit model for $\mathbb{F}_{p^n}$</u> we understand a system of n^3 numbers $(a_{ijk})_{1 \leq i,j,k \leq n}$, $a_{ijk} \in \mathbb{F}_p$, such that the additive group $\mathbb{F}_p^{\oplus n}$ is a field with multiplication $(x_i)_{1 \leq i \leq n} \circ (y_j)_{1 \leq j \leq n} = \left(\sum_{i,j} a_{ijk} x_i y_j\right)_{1 \leq k \leq n}$.

Alternatively we can construct $c_0, \ldots, c_{n-1} \in \mathbb{F}_p$ s.t. $X^n + \sum_{i=0}^{n-1} c_i X^i$ is irreducible in $\mathbb{F}_p[X]$.

<u>Partial result #1</u>: there is a probabilistic algorithm with polynomial expected runtime, that upon (p, n) constructs $\mathbb{F}_{p^n}$.

(i.e. $\exists c : \forall p, n$, $E\{\text{runtime}\} \leq (n + \log p)^c$)

<u>Partial result #2</u>: there is an algorithm that given (p, n) constructs $\mathbb{F}_{p^n}$ s.t.

$$\exists c : \forall p, n \quad \text{runtime} \leq (n + p)^c$$

(So, for instance, fields of characteristic 2 can be constructed in polynomial time).

Partial result #3: There is an algorithm that, given (p,n) constructs $\mathbb{F}_{p^n}$, s.t.

$$\text{GRH} \Rightarrow \exists c : \forall p,n : \text{runtime} \leq (n+\log p)^c.$$

(we need to ensure that $\forall$ number field K, and each $s \in \mathbb{C}$, $\text{Re}\, s > \frac{1}{2}$, $\zeta_K(s) \neq 0$)

(where $\zeta_K(s) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \text{nonzero ideal}}} (\# \mathcal{O}_K/\mathfrak{a})^{-s}$ for $\text{Re}(s) > 0$)

Uniqueness of finite fields

Theorem: There is a polynomial-time algorithm that, given two models for $\mathbb{F}_{p^n}$ (with same p,n), finds a field isomorphism between them. (represented by an $n \times n$ matrix $/\mathbb{F}_p$).

Finite rings

Prime ring: $\mathbb{Z}/m\mathbb{Z}$, $m > 1$

Proposition: There are poly'l time algorithms that, given $m > 1$, and $a, b \in \mathbb{Z}/m\mathbb{Z}$, compute $a+b$, $a-b$, $a \cdot b$, and <u>either</u> an element $d \in \mathbb{Z}/m\mathbb{Z}$ s.t. $ad = b$ or an element d' with $ad' = 0 \neq bd'$

Pf ($\%$): for $b = 1$, want to find $ad = 1$ or $ad' = 0 \neq d'$

Using Euclid's algorithm, $xa + ym = \gcd(a,m)$ $x, y \in \mathbb{Z}$.

If $\gcd(a,m) = 1$, then $d = x$.

If $\gcd(a,m) \neq 1$, then $d' := \left(\frac{m}{\gcd(a,m)} \bmod m\right)$

Linear algebra on $\mathbb{Z}/m\mathbb{Z}$:

There are polynomial algorithms that solve any linear algebra problem over $\mathbb{Z}/m\mathbb{Z}$, or find $a, b \in \mathbb{Z}/m\mathbb{Z}$, $a \neq 0$, $b \neq 0$ with $ab = 0$.

Example:
- Solve or decide unsolvability of a system of linear equations $AX = B$.
- Find a $\mathbb{Z}/m\mathbb{Z}$-basis for Ker, Coker, Img, of any group homomorphism from a free rank-s module to a rank-t free module, given by a $t \times s$-matrix $f : (\mathbb{Z}/m\mathbb{Z})^s \to (\mathbb{Z}/m\mathbb{Z})^s$

For a general ring$^{\text{finite}}$ R, we have that $\mathbb{Z}/m\mathbb{Z} \subset R$ where $m = \operatorname{char} R \geq 1$.

The only R's that we'll look at satisfy $R^{\oplus} \cong (\mathbb{Z}/m\mathbb{Z})^n$ for some n.

(remember that finding a 0 divisor is fine).

Such rings will be represented by a multiplication tensor $(a_{ijk})_{1 \leq i,j,k \leq n}$ $a_{ijk} \in \mathbb{Z}/m\mathbb{Z}$

<u>Fact</u>: There are poly'l time algorithms for finding 1, for doing $+, -, \times$ in R (R is not fixed, is part of the input), and for finding upon being given $a \in R$, an element c with $ac = 1$ or $ac = 0 \neq c$; or find a pair of zero divisors in $\mathbb{Z}/m\mathbb{Z}$, hence in R.

Likewise, we can do linear algebra over R in poly'l time, or find $a, b \in R$, $\neq 0$ with $ab = 0$.

<u>Finite Commutative $\mathbb{F}_p$-algebras</u>

Let R be any commutative ring, and $\sqrt{0} = \sqrt{0_R} = \{x \in R : \exists n \in \mathbb{Z}_{\geq n} : x^n = 0\}$

Recall $\sqrt{0_R} = \bigcap_{\mathfrak{p} \text{ prime ideal} \subset R} \mathfrak{p} \underset{R \text{ finite}}{=} \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m} = \prod_{\mathfrak{m} \text{ maximal}} \mathfrak{m} = \ker \left[R \longrightarrow \prod_{\mathfrak{m} \text{ maximal}} R/\mathfrak{m} \right]$

So the following is true:

"If R is a finite commutative ring, then $R/\sqrt{0} \overset{\text{as rings}}{\cong}$ finite product of finite fields.

<u>Exercise</u>: $R \xrightarrow{\sim} \prod_{\mathfrak{m} \text{ maximal}} R_{\mathfrak{m}}$ (localization)

Note that if $R = \mathbb{Z}/m\mathbb{Z}$, $\sqrt{0} = R \cdot \prod_{p \mid m} p$ so it is hopeless to try to find it, as we are dealing with factorization of m (prime).

<u>Assumptions</u>:

R finite, commutative ring of prime characteristic p, and $R^+ = (\mathbb{F}_p)^n$ $(n = \dim_{\mathbb{F}_p} R)$.

Define $F : R \to R$, $x \mapsto x^p$. This is an $\mathbb{F}_p$-linear ring endomorphism of R.

Note that F (represented by a matrix) is computable in poly'l time.

Also, it is a fact that $R \supset \sqrt{0} \supset (\sqrt{0})^2 \supset \cdots \supset \sqrt{0}^N = 0$

Note that $\exists\, m \leq n$ s.t. $(\sqrt{0})^m = (\sqrt{0})^{m+1} = \sqrt{0}^{m+2} = \cdots = 0$ so $N \leq n$.

So, to compute the nilradical, pick an integer $t \in \mathbb{Z}$ s.t. $p^t \geq n$.

Then $F^t(x) = x^{p^t}$ so $(\ker F^t) = \sqrt{0}$

So in this case $\sqrt{0}$ is computable in polynomial time.

Also, $\underset{\text{subring of } R}{(F^t R)} \oplus \underset{\sqrt{0}}{(\ker F^t)} \xrightarrow{\sim} R$ (so $0 \to \sqrt{0} \to R \to R/\sqrt{0} \to 0$ splits) as ring homomorphisms

Pf: Note! $\ker F^t = \ker F^{2t}$ and $F^t R = F^{2t} R$.

So $F^t r = F^{2t} s \Rightarrow r = F^t s + \left(\text{elt of } \ker F^t\right)$ so the map is surjective, and is isomorphism because they have the same cardinality. ∎

Consider $R/\sqrt{0}$. See that $R/\sqrt{0} \cong F^t R \cong \prod_{i=1}^{s} \mathbb{F}_{p^{n_i}}$, with $F-1$ acting on each.

ker of $F-1$ on each $\mathbb{F}_{p^{n_i}}$ is $\mathbb{F}_p$.
ker of $F-1$ on $R/\sqrt{0}$ is $\mathbb{F}_p^s$
ker of $F-1$ on $\sqrt{0}$ is 0

$\Rightarrow$

- $s = \#\operatorname{Spec} R = \dim_{\mathbb{F}_p} \ker(F-1)$ (computable in poly'l time.)
- we can test if R is a field: R field $\Leftrightarrow [\operatorname{rank}_{\mathbb{F}_p}(F) = n \ \& \ \operatorname{rank}_{\mathbb{F}_p}(F-1) = n-1]$
- There is a poly'l time algorithm that given a finite field K and an element $f \in K[X]$, $f \notin K$, tests whether f is irreducible in $K[X]$.

(just test whether $K[X]/(f)$ is a field).

Example:

Let $R = k[X]/(f)$, where k is a finite field of char$(k) = p$, $f \in k[X] \setminus k$.

Proposition: There is a poly'l-time algorithm that given $p, R, \alpha \in R$ determines the minimal polynomial of α over $\mathbb{F}_p$, i.e. the unique monic polynomial in $\mathbb{F}_p[X]$ that generates $\ker[\mathbb{F}_p[X] \to R; X \mapsto \alpha]$

Pf/ Use linear algebra to determine the least $d \in \mathbb{Z}_{>0}$ with $\alpha^d \in \mathbb{F}_p \cdot 1 + \mathbb{F}_p \cdot \alpha + \cdots + \mathbb{F}_p \alpha^{d-1}$. Then $\alpha^d = \sum_{i<d} c_i \alpha^i$, $f = X^d - \sum_{i<d} c_i X^i$ //

In the previous example, the minimal polynomial of the image of X in $R/\sqrt{0_R}$ is $\prod_{\substack{g \mid f \\ g \text{ monic irred. in } k[X]}} g$ (if $k = \mathbb{F}_p$).

We can also extend previous proposition to change $\mathbb{F}_p$ for any subfield $k \subset R$ (not necessarily $\mathbb{F}_p$).

Hence: $\exists$ poly'l-time algorithm that given k and f determines the largest squarefree divisor of f in $k[X]$.

Now, we'll restrict to the case where R is reduced (i.e. $\sqrt{0_R} = 0$).

Then $R \cong \prod_{m \in \operatorname{Spec} R} (R/m) = \prod_{i=1}^{s} \mathbb{F}_{p^{n_i}}$

There is no known deterministic polynomial-time for exhibiting this isomorphism (although there is a probabilistic poly'l-time which is very good).

We call R homogeneous if $R = \prod_{i=1}^{s} \mathbb{F}_{p^k}$, k fixed.

$\mathrm{Ker}(F-1) = R_0 = \prod_{i=1}^{s} \mathbb{F}_p$ is a homogeneous ring.

Proposition: There is a poly'l-time algorithm that writes a given finite reduced $\mathbb{F}_p$-algebra as a product of homogeneous ones.

Pf: Suppose α is a zero divisor in R. Then the natural map

$$R \longrightarrow \left(R/R\alpha\right) \times \left(R/\mathrm{Ann}\,\alpha\right) \quad \text{where } \mathrm{Ann}\,\alpha = \{\beta \in R : \alpha\beta = 0\}.$$

is an isomorphisms. So backdoors are fine!

Algorithm: Apply linear algebra over R_0, to either find a zero divisor, or find a basis of R as a module over R_0.

If this basis has d elements, then $R \cong R_0^d$ as an R_0-module. Tensor this with the i-th $\mathbb{F}_p$ over R_0, so $\mathbb{F}_{p^{n_i}} \cong \mathbb{F}_p^d$ as an $\mathbb{F}_p$-module.

Corollary: We can compute $n_1, \dots, n_s$ in polynomial time.

Corollary (distinct degree factorization): There is a polynomial time algorithm that, given k, f and ~~an~~ integer $d \geq 0$, computes

$$\prod_{\substack{g \mid f \\ \text{irr. monic} \\ \text{of degree } d \\ \text{in } k[X]}} g$$

From now on, we can assume all n_i are equal to 1, because of the previous proposition. If we have

$R_0 \cong \prod \mathbb{F}_p$, then take $(0, 1, 1, \dots, 1)$ and send it to R_0.

Call it e. Then R/eR is $\mathbb{F}_{p^{n_1}}$. Doing it for all i, we're done!

Proposition: There is an algorithm that writes any given reduced finite commutative $\mathbb{F}_p$-algebra as a product of fields and that runs in time $\leq (p+n)^c$. There is a probabilistic algorithm doing the same with expected polynomial run-time.

Proof: Find a zero divisor. Reduce to the case $R = R_0$ (then, we can do for all).

$\forall \alpha \in R$: $\alpha^p = \alpha$, so $0 = \alpha^p - \alpha = \prod_{i \in \mathbb{F}_p} (\alpha - i)$

If $\mathbb{F}_p = R$, we are done. If not, take $\alpha \in R \setminus \mathbb{F}_p$.

~~So~~ using $0 = \prod_{i \in \mathbb{F}_p} (\underbrace{\alpha - i}_{\neq 0})$ will find a zero divisor in $\leq (p+n)^c$ steps.

After ~~that~~, it splits in two factors, and apply induction.

Assume $p > 2$. If $p = 2$, it is fine the other algorithm.

For the probabilistic algorithm, use $0 = \alpha^p - \alpha = \alpha\left(\alpha^{\frac{p-1}{2}} - 1\right)\left(\alpha^{\frac{p-1}{2}} + 1\right)$

Take α at random. If we are lucky, neither $\alpha^{\frac{p-1}{2}} - 1$, $\alpha^{\frac{p-1}{2}} + 1$

$\alpha^{\frac{p-1}{2}} - 1 = 0$ for $\left(\frac{p-1}{2}\right)^s$ different α's. (and the other also).

So $\text{Prob}[\text{bad luck}] = \dfrac{1 + 2\left(\frac{p-1}{2}\right)^s}{p^s} \leq \dfrac{1}{2^{s-1}} \leq \dfrac{1}{2}$ if $s \geq 2$

- Factoring f in $K[X]$ into irreducible factors:
- Can be done in time $\leq (\text{char}\, K + \log \# K + \deg f)^c$ deterministically
  $\leq (\log \# K + \deg f)^c$ probabilistically.

- The general case can be reduced to the special case $K = \mathbb{F}_p$, and f a product of distinct linear factors in $\mathbb{F}_p[X]$.

- The problem of finding a polynomial time algorithm ~~for~~ is <u>open</u>, even assuming GRH.

• Primitive elements.

Take $\mathbb{F}_q \subset \mathbb{F}_{q^m}$. We call $\alpha \in \mathbb{F}_{q^m}$ a <u>primitive element</u> if $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$.

$\{\text{non-primitive elements}\} = \bigcup_{\substack{d \mid m \\ d < m}} \mathbb{F}_{q^d}$

$\mathbb{F}_{q^d} = \{\beta \in \mathbb{F}_{q^m} : \overset{\text{Frobenius}}{F_K^d}\,\beta = \beta\}$ (solutions of $\beta^{q^d} - \beta = 0$).

So the number of non-primitive elements is $\leq \sum_{\substack{d \geq 1 \\ d \leq m/2}} q^d \leq \frac{q^{(m/2)+1} - 1}{q - 1} < 2q^{m/2} = o(q^m)$.

(there are lots of primitive elements).

Therefore, $\#\{\text{primitive elements}\} = q^m(1 - o(1))$ for $q^m \to \infty$.

$\underbrace{\#\{f \in \mathbb{F}_q[X] : \deg f = m,\ f \text{ irred monic}\}}_{a_m(q)} \geq \frac{1}{m}\left(q^m - o(q^m)\right)$ $q^m \to \infty$.

(Exercise: $a_m(q) = \frac{1}{m} \sum_{d \mid m} \mu\left(\frac{m}{d}\right) q^d$ (μ Möbius Formula).)

Consequence: There is a probabilistic algorithm with expected polynomial runtime that, given p and n produces $\mathbb{F}_{p^n}$.

(Algorithm: pick $f \in \mathbb{F}_p[X]$ monic of degree n at random, and ~~test~~ test it for irreducibility; repeat until success).

Then put $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(f)$. //

Given a finite field extension $\mathbb{F}_q \subset \mathbb{F}_{q^m}$, we can produce a primitive element in polynomial time (i.e. if someone has a poly-time algorithm for constructing field extensions, we can derive an algorithm for finding irreducible polynomials).

The test for primitivity is: α is primitive $\Leftrightarrow$ deg (min pol of α over $\mathbb{F}_q$) $= m$ $\Leftrightarrow$

$\Leftrightarrow \min\{d > 0 : F_q^d \alpha = \alpha\} = m$ (So we have two tests for primitivity, which give probabilistic trivial ~~tests~~ algorithms).

Proposition: $\sum_{\substack{d|m \\ d<m}} \mathbb{F}_{q^d} \neq \mathbb{F}_{q^m}$

$\uparrow$ subgroup generated by nonprimitive elements (= sub $\mathbb{F}_q$-vectorspace).

(from this position, any vectorspace basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ contains a primitive element).

<u>Proof</u> View $\mathbb{F}_{q^m}$ as a <u>module</u> over $\mathbb{F}_q[T]$ by:

$$\mathbb{F}_q[T] \ni \left(\sum a_i T^i\right) \circ \underset{\mathbb{F}_{q^m}}{\beta} := \sum a_i F_k^i(\beta) = \sum a_i \beta^{q^i}$$

We will now build an element that kills all ~~sub~~ subgroups, but not $\mathbb{F}_{q^m}$:

Φ_m = m-th cyclotomic poly'l (in $\mathbb{Z}[T]$, in $\mathbb{F}_q[T]$) monic of degree $\varphi(m)$.

$T^m - 1 = \Phi_m \cdot \Psi_m$, $\deg \Psi_m = m - \varphi(m)$.

(<u>Fact</u>: $T^d - 1 \mid \Psi_m$ for every $d \mid m$, $d \neq m$.)

$\underbrace{T^d - 1}_{= F_k^d - 1}$ acts as 0 on $\mathbb{F}_{q^d}$, so Ψ_m annihilates $\mathbb{F}_{q^d}$ for all $\substack{d<m \\ d|m}$.

So Ψ_m annihilates all $\sum_{\substack{d|m \\ d<m}} \mathbb{F}_{q^d}$.

The $\#\{\text{elements killed by } \Psi_m\} \leq q^{\deg \Psi_m} = q^{m-\varphi(m)} < q^m$ //.

So in fact any vectorspace basis will contain at least $\varphi(m)$ of them.

Exercise: $\mathbb{F}_{q^m} \Big/ \sum_{\substack{d<m \\ d|m}} \mathbb{F}_{q^d}$ has $\dim_{\mathbb{F}_q} = \varphi(m)$.

Given $\mathbb{F}_q$ and an irreducible polynomial in $\mathbb{F}_q[X]$ of degree m, as well as a divisor d of m, one can produce in polynomial time an irreducible polynomial of degree d.

Given two irreducible polynomials, of degree m_1 and m_2, one can construct one of degree $\operatorname{lcm}(m_1, m_2)$.

• Normal basis theorem:

Note that the primitive element we have constructed satisfies that

$\alpha, T\alpha, \dots, T^{m-1}\alpha$ are pairwise distinct.

The NB. Theorem says that $\exists \alpha$ s.t. $\alpha, T\alpha, \dots, T^{m-1}\alpha$ are linearly independent/$\mathbb{F}_q$.

If $\alpha \in \mathbb{F}_{q^m} \supset \mathbb{F}_q$, $\quad \mathbb{F}_q[T] \longrightarrow \mathbb{F}_{q^m}$, $\; g \longmapsto g(\alpha)$ in fact, $\mathbb{F}_q[T]/(T^m-1) \xrightarrow{*} \mathbb{F}_{q^m}$, $\; [g] \longrightarrow g(\alpha)$.

Can state NB Th as: $\exists \alpha$ s.t. ~~$\alpha, T\alpha, \dots, T^{m-1}\alpha$ is an~~

$*$ is an isomorphism of $\mathbb{F}_q[T]$-modules.

Note that $\ker(*)$ is generated by a unique monic polynomial, called Order(α).

Proof of existence of the normal basis: ($\equiv$ proof of $\mathbb{F}_q^*$ is cyclic!).

Obs that $\mathrm{Order}(\alpha) \mid T^m-1$.

$$\sum_{\substack{d \mid T^m-1 \\ \in \mathbb{F}_q[T] \text{ monic}}} \underbrace{\#\{\alpha : \mathrm{Order}(\alpha) = d\}}_{\varkappa(d)} = q^m.$$

$$\sum_{d \mid T^m-1} \#\left(\mathbb{F}_q[T]/(d)\right)^* = \# \mathbb{F}_q[T]/(T^m-1) = q^m$$

NBT: claims that $\varkappa(T^m-1) > 0$. In fact, we'll prove $\varkappa(d) = \varphi(d)$!

Suffices to show that:

$\varkappa(d) > 0$ then $\varkappa(d) = \# \left(\mathbb{F}_q[T]/(d)\right)^*$ (then looking again at the two summands, we're done)

Suppose $\mathrm{Order}(\alpha) = d$.

Then $\underbrace{\mathbb{F}_q[T] \circ \alpha}_{q^{\deg d} \text{ elements}} \simeq \mathbb{F}_q[T]/(d)$, all of them annihilated by d

So each element in $\mathbb{F}_{q^m}$ annihilated by d belongs to $\mathbb{F}_q[T] \circ \alpha$.

If β is annihilated by d, then $\beta = g \circ \alpha$ has Order $= d$ iff $(g, d) = 1$.

This allows us to count, and done. //

Let $k \subset \ell$ be finite fields, $\# k = q$, $[\ell : k] = m$.

Make ℓ into a $k[T]$-module by $T \cdot x := x^q$ $(x \in \ell)$

(i.e. $(\sum a_i T^i) \cdot x := \sum a_i x^{q^i}$), and $\mathrm{Ord}\, x$ = the unique monic pol'l of least degree in $k[T]$ annihilating x.

And remember $\mathrm{Ord}\, x \mid T^m - 1$, and $\mathrm{Ord}\, x \mid T - 1 \Leftrightarrow x \in k$.

Rember that the Normal Basis theorem said that $\ell \cong k[T]/(T^m - 1)$ as a $k[T]$-module.

(equivalently, $\exists \alpha \in \ell$: $\mathrm{Ord}\, \alpha = T^m - 1$).

As a subproduct of the proof we obtained that the number of such α equals $\Phi(T^m - 1) = \# \left(k[T]/(T^m - 1) \right)^*$

Exercise: prove that $\ell^* \cong \mathbb{Z}/(q^m - 1)\mathbb{Z}$ as a $\mathbb{Z}$-module. Also, note that for $\alpha, \beta \in \ell^\times$, one has $\mathrm{ord}\, \beta \mid \mathrm{ord}\, \alpha \Leftrightarrow \beta \in \alpha^{\mathbb{Z}} \Leftrightarrow \exists \gamma \in \ell^* : \beta = \gamma^{\frac{q^m - 1}{\mathrm{ord}\, \alpha}}$.

Also, for $\alpha, \beta \in \ell$, one has:

$$\mathrm{Ord}\, \beta \mid \mathrm{Ord}\, \alpha \Leftrightarrow \beta \in k[T] \cdot \alpha \Leftrightarrow \exists \gamma \in \ell : \beta = \left(\frac{T^m - 1}{\mathrm{Ord}\, \alpha} \right) (\gamma).$$

Examples:

a) $m = 2 = \mathrm{char}\, k$. $\mathrm{Ord}\, \alpha \mid \overbrace{(T-1)^2}^{= T^2 - 1}$.
$$\begin{cases} \mathrm{Ord}\, \alpha = 1 \Leftrightarrow \alpha = 0 \\ \mathrm{Ord}\, \alpha = T - 1 \Leftrightarrow \alpha \in k^\times \\ \mathrm{Ord}\, \alpha = (T - 1)^2 \Leftrightarrow \alpha \in \ell \setminus k \end{cases}$$

b) $m = 2 \neq \mathrm{char}\, k$

$T^2 - 1 = (T + 1)(T - 1)$. If $\ell = k(\sqrt{b})$, $b \in k^* \setminus k^{*2}$.

$T \cdot \sqrt{b} = -\sqrt{b}$. So $\mathrm{Ord}\, \alpha = T + 1 \Leftrightarrow \alpha \in k^\times \sqrt{b}$

So the elements which have $\mathrm{Ord}\, \alpha = T^2 - 1$ are those of the form $x + y\sqrt{b}$ with $x, y \neq 0$.

c) $\mathrm{char}\, k \nmid m$, $T^m - 1 = \prod_{i=0}^{m-1} (T - \zeta^i)$. $\zeta \in k^*$. Then,

$$k[T]/(T^m - 1) \underset{k[T]\text{-module}}{\cong} \prod_i \underbrace{\left(k[T]/(T - \zeta^i) \right)}_{\cong \text{ a 1-dim } k\text{-vect. space on which } T \text{ acts as } T \cdot x = \zeta^i x} \quad \text{(by CRM.)}$$

So $\ell = \underbrace{\bigoplus_{i=0}^{m-1} \kappa \cdot \alpha_i}_{= \{\alpha \in \ell : T\alpha = \zeta^i \alpha\}}$ $\alpha_i \neq 0$, $\alpha_i^q = \zeta^i \alpha_i$

We can choose $\alpha_0 = 1$, $\alpha_i := \alpha_1^i$ $(i > 1)$. So we want $\alpha_1 \in \ell^\times : \alpha_1^q = \zeta \alpha_1$

If $\mathrm{Ord}\, \alpha = T^m - 1$, then we can use $\alpha_1 := \frac{T^m - 1}{T - \zeta} \cdot \alpha$. (provided it is nonzero!).

Also, $\ell = \kappa(\alpha_1)$.

Theorem: There is a poly'l time algorithm that, given finite fields $\kappa \subset \ell$, produces $\alpha \in \ell$ with $\mathrm{Ord}\, \alpha = T^{[\ell:\kappa]} - 1$.

Proof (by exhibiting the algorithm): Let $m = [\ell : \kappa]$.

- Step 0: Choose $\alpha \in \ell$
- Step 1: Use linear algebra to compute $\mathrm{Ord}\, \alpha$

  [compute $1 \cdot \alpha = \alpha$

  $T \cdot \alpha = \alpha^q$

  until: $T^i \cdot \alpha = \alpha^{q^i} \in \mathrm{Span} \langle \alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{i-1}} \rangle$]

  $\rightarrow$ If $\mathrm{Ord}\, \alpha = T^m - 1$ $\boxed{\text{stop}}$

- Step 2: Compute $d := \frac{T^m - 1}{\mathrm{Ord}\, \alpha}$, and find $\gamma \in \ell$ with $\boxed{d \cdot \gamma = \alpha}$ (possible for the exercise).

  linear algebra to solve this system

- Step 3: If $\gamma \notin \kappa[T] \cdot \alpha$, skip to Step 4.

  Otherwise, pick $\delta \in \ell$, $\delta \notin \kappa[T] \cdot \alpha$, and solve $\{d \cdot \delta = f \cdot \alpha\}$ for f (linear eq.)

  [Then, $d \cdot \delta = f\alpha = d \cdot f \cdot \gamma$, so $d(\underbrace{\delta - f\gamma}_{\notin \kappa[T] \cdot \alpha}) = 0$].

  Replace γ by $\gamma + (\delta - f\gamma)$ $[\notin \kappa[T] \cdot \alpha]$.

- Step 4: Replace α by γ and return to step 1.

  [$\alpha \in \kappa[T] \cdot \gamma$, so $\kappa[T] \cdot \alpha \subsetneq \kappa[T] \cdot \gamma$ so the algorithm ends after at most m steps].

Remember *partial result #2*: $\exists$ algorithm that given p and $n \in \mathbb{Z}_{>0}$, produces an explicit model for $\mathbb{F}_{p^n}$ in time $\leq (p+n)^c$ for some universal c.

It follows from:

Proposition. There $\exists$ $c \in \mathbb{R}_{>0}$ and an algorithm that, given a finite field and a *prime number r*, produces an r^{th} degree field extension of K in time $\leq \left(\text{char } K + (\log \# K) + r\right)^c$

Proof (by exhibiting algorithm):

Case 1: $r = p$ ($=\text{char } K$).

Find $\alpha \in K$ such that $\text{Tr}_{K/\mathbb{F}_p} \alpha \neq 0$.

[E.g. take α s.t. α generates a normal basis of $K/\mathbb{F}_p$. Or try basis elements of K over $\mathbb{F}_p$].

Now $K[X]/(X^p - X - \alpha)$ is a field extension of K, of degree p $(=r)$.

[If $\beta \in \overline{K}$ is a zero of $X^p - X - \alpha$, then $\beta+1, \beta+2, \ldots, \beta+(p-1)$ are the others, so all irreducible factors of $X^p - X - \alpha$ have the same degree $/K$, i.e. either p or 1. But if it was 1, $\beta \in K$, and $\beta^p - \beta = \alpha \Rightarrow$ $\text{Tr}\,\alpha = \text{Tr}\,\beta^p - \text{Tr}\,\beta = \text{Tr}\,\beta - \text{Tr}\,\beta = 0 \Rightarrow$!!].

Case 2: $r \neq p = \text{char } K$.

Factor the poly'l $\frac{X^r - 1}{X - 1}$ into irreducible factors over K (not poly'l time!)

Let g be an irreducible factor, and put $K' = K[X]/(g) = K(\zeta_r)$ where $\zeta_r = (X \bmod g)$, $\text{ord } \zeta_r = r$.

We write $\# K' - 1 = r^N \cdot u$, $u \in \mathbb{Z}$, $r \nmid \mathbb{Z}$. ($N \geq 1$!).

for $i := 1 .. N$, find an element $\zeta_{r^i} \in K'^*$, of order $(\zeta_{r^i}) = r^i$, by factoring $X^r - \zeta_{r^{i-1}}$ into irreducibles $/K$.

Now $K[X]/(X^r - \zeta_{r^N})$ is a field ext'n of K' of degree r

Now, find (in poly'l time) find a subfield of the required degree. //

Theorem: There is a poly'l time algorithm that, given two finite fields of the same cardinality, produces an isomorphism between them.

Theorem: There is a poly'l time algorithm that, given a finite field k, an irreducible polynomial $f \in k[X]$, and $m \in \mathbb{Z}_{>0}$ such that each prime dividing m divides $\deg f$, produces an irreducible polynomial in $k[X]$ of degree m.

It suffices to prove the existence of these two poly'l time algorithm:

(A) algorithm that, given finite fields $k \subset l$, $k \subset l'$ with $[l:k] = [l':k] = r$ prime, produces a field isomorphism $l \xrightarrow{\sim} l'$ that is the identity on k.

(B) algorithm that, given finite fields $k \subset l$ with $[l:k] = r$ (prime), produces a field extension $l \subset l'$ with $[l':l] = r$.

Case 1: $r = \operatorname{char} k = p$

A) write $l \underset{k}{\cong} k[X]/(f)$, find a zero of f in l' by factoring f in $l'[X]$, and map $l \to l'$, $(X \bmod f) \mapsto \alpha$

B) Use the algorithm used in "partial result #2" which also runs in poly'l time, as $p = r$.

Case 2: $r = 2 \neq \operatorname{char} k$

B) Write $l = k(\alpha)$, $\alpha^2 = a \in k^* \setminus k^{*2}$ (need $a^{\frac{q-1}{2}} = -1$ where $q = \#k$).

We are looking for $\beta \in l$ with $\beta^{(q^2-1)/2} = -1$ (if β has that property, then $l' = l[X]/(X^2-\beta)$)

$$\alpha^{(q^2-1)/2} = \left(\left(\alpha^2\right)^{\frac{q-1}{2}}\right)^{\frac{q+1}{2}} = (-1)^{\frac{q+1}{2}}$$ so $\beta = \alpha$ works if $q \equiv 1 \bmod 4$

Suppose $q \equiv 3 \bmod 4$. Then $\alpha^{2 \cdot \underbrace{\frac{q-1}{2}}_{\text{odd}}} = -1$ so $4 \,\|\, \operatorname{order}(\alpha)$.

If $2^N \| q^2-1$, we want β s.t. ~~ord β~~ $2^N \| \operatorname{ord}(\beta)$. Take $\beta = \underbrace{\sqrt{\cdots\sqrt{\sqrt{\alpha}}}}_{N-2 \text{ square roots}}$.

~~Lemma: There is a poly'l time algorithm for taking square roots in finite fields l that have a subfield~~

Lemma: There is a polynomial time algorithm for taking $\sqrt[2]{\ }$ in finite fields ℓ that have a subfield k with $\# k \equiv 3 \mod 4$.

Pf of lemma: $\alpha \in \ell$. If $\alpha = \delta^2$ is solvable, then (if $q = \# k$), $\alpha^{\frac{q-1}{2}} = \delta^{q-1}$ is also solvable, so $\delta \alpha^{\frac{q-1}{2}} = \delta^q$ has a nonzero solution.

Algorithm:

- Find a nonzero solution δ in ℓ in $\delta^q = \delta \alpha^{\frac{q-1}{2}}$ (done by linear algebra over k).
- $\delta^{q-1} = \alpha^{\frac{q-1}{2}} \Rightarrow (\delta^2 \alpha^{-1})^{\frac{q-1}{2} = 2m+1} = 1$, so $(\delta^2 \alpha^{-1})^{2m} \delta^2 = \alpha \Rightarrow$ $\Rightarrow (\delta^2 \alpha^{-1})^m \delta$ is a square root of α.

A) Write $\begin{cases} \ell = k(\alpha) & \text{where } \alpha^2 = a \in k,\ a^{\frac{q-1}{2}} = -1 \quad (q = \# k) \\ \ell' = k(\beta) & \text{where } \beta^2 = b \in k,\ b^{\frac{q-1}{2}} = -1 \end{cases}$

Finding a k-iso $\ell \to \ell'$ means $\alpha \mapsto c\beta$, $c \in k^*$, $c^2 = \frac{a}{b}$. So we have to find a square root of a/b in k.

- Discrete Logarithm

Proposition (Shanks–Tonelli) There is an algorithm that, given a finite ring R, elements $\alpha, \beta \in R^*$, and $n \in \mathbb{Z}$, $0 < n \leq \# R$, decides whether $[\# \langle \beta \rangle = n \ \& \ \alpha \in \langle \beta \rangle]$ and if yes computes $x \in \mathbb{Z}$ with $\alpha = \beta^x$, and does so in time $\leq \left(\log(\# R) + \begin{pmatrix}\text{largest prime}\\ \text{factor of } n\end{pmatrix}\right)^C$

Pf Algorithm

- Factor n by trial division.
- Take a prime factor r of n. Compute $\gamma = \beta^{n/r}, \gamma^2, \dots, \gamma^r$ and $\alpha^{n/r}$
- If $\gamma = 1$ or $\gamma^r \neq 1$ or $\alpha^{n/r} \notin \{\gamma, \gamma^2, \dots, \gamma^r\}$, then NO. Otherwise,
- Let y s.t. $\alpha^{n/r} = \gamma^y$ (so $x \equiv y \pmod r$). Then apply the algorithm to $\begin{cases} \alpha\beta^{-y} \\ \beta^r \\ n/r \end{cases}$

The previous discrete logarithm problem allows us to go on with the proofs:

<u>Algorithm for Ⓐ, $r=2\neq \mathrm{char}\, K$</u>

Find $\alpha\in \ell$, $\ell=K(\alpha)$, $\alpha^2\in K^*$

Write $\# K^* = 2^t\cdot u$, $t, u\in \mathbb{Z}_{>0}$, u odd.

Replace α by α^u. [Now $\mathrm{order}(\alpha)=2^{t+1}$].

Likewise, write $\ell'=K(\alpha')$, with $\mathrm{order}(\alpha')=2^{t+1}$

Apply Discrete-Logarithm to $R=K$, α^2, α'^2 in the roles of α, β and $n:=2^t$. We get $x\in\mathbb{Z}$, with $\alpha^2=(\alpha'^2)^x$

Now $\ell=K(\alpha)\longrightarrow K(\alpha')=\ell'$ is an isomorphism of fields $/K$.

$\alpha\longmapsto (\alpha')^x$

As we cannot take r^{th} roots, we'll have to change the strategy.

"For a finite field K and a prime number $r\neq \mathrm{char}\, K$, giving a field extension $K\subset \ell$ of degree r is equivalent to giving a generator of the Teichmüller group $T=T_{K,r}\subset K[\zeta_r]^*$"

(Where $K[\zeta_r] = K[X]\Big/\left(\frac{X^r-1}{X-1}\right)$ and ζ is the class of X).

$K[\zeta_r]$, as a K-algebra, is $K[\zeta_r]\underset{K}{\cong}\overbrace{K'\times\cdots\times K'}^{\frac{r-1}{d}}$ where

$K'\supset K$ field, $[K':K]=d$ (= order of q (mod r) in $\mathbb{F}_r^*$)

($T_{K,2}=\langle\alpha^2\rangle=(2\text{-Sylow of } K^*)=(K^*)_2$).

$T_{K,r}\subset \left(K[\zeta]^*\right)_r \cong (\text{cyclic group of order } r^t\,\|\, q^d-1)^{\oplus\frac{r-1}{d}}$

To define $T_{K,r}$, we need to know more about $(K[\zeta]^*)_r$

r-Sylow group.

$k[\zeta_r] = k[C] / \sum_{\sigma \in C} \sigma$. So $\underbrace{\mathrm{Aut}\, C}_{\cong \mathbb{F}_r^*}$ acts upon $k[\zeta_r]$

cyclic group of order r

So for each $a \in \mathbb{F}_r^*$, there is a k-algebra automorphism σ_a of $k[\zeta_r]$ with $\sigma_a \zeta = \zeta^a$.

$$\Delta = \{\sigma_a : a \in \mathbb{F}_r^*\} \subset \mathrm{Aut}_k\, k[\zeta]$$

$$\begin{tikzcd}
1 \arrow[r] & \begin{pmatrix} \text{group of} \\ \text{order } r^{t-1} \end{pmatrix} \arrow[r] & (\mathbb{Z}/r^t\mathbb{Z})^* \arrow[r] & \mathbb{F}_r^* \arrow[r] \arrow[l, bend right] & 1 \\
 & & a^{r^{(t-1)}} \bmod r^t & \Delta \arrow[u, "\cong"'] \arrow[ul, bend left] & \\
 & & & \sigma_a \arrow[ul, mapsto] &
\end{tikzcd}$$

split exact sequence.

Then $T_{k,r} = T = \{\varepsilon \in (k[\zeta]^*)_r : \forall \sigma_a \in \Delta,\ \sigma_a(\varepsilon) = \varepsilon^{\omega(a)}\}$

__Obs__: $\zeta \in T_{k,r}$. as $\mathrm{ord}(\zeta) = r$, $r \mid \# T_{k,r}$.

__Fact__: T is cyclic of order r^t, and $\zeta \in T$

__Exercise__: If $T_i := \{\varepsilon \in k[\zeta]^*_r : \forall a \in \mathbb{F}_r^*;\ \sigma_a(\varepsilon) = \varepsilon^{\omega^i(a)}\}$ $(T = T_1)$, then for each $i \pmod{r-1}$ one has:

$T_i \neq \{1\} \iff T_i$ is cyclic of order $r^t \iff \omega^i(\sigma_q) = (q \bmod r^t) \iff i \equiv 1 \bmod d$

Also, $k[\zeta]^*_r \underset{\mathbb{Z}[\Delta]}{\cong} \bigoplus_{\substack{i \equiv 1 \bmod d \\ i \bmod r-1}} T_i$

Suppose $T = \langle \alpha \rangle$. Write $k[\zeta][\sqrt[r]{\alpha}] = k[\zeta][Y] / (Y^r - \alpha)$.

Extend the Δ-action on $k[\zeta]$ on a Δ-action on $k[\zeta][\sqrt[r]{\alpha}]$ by.

$$\sigma_a(\underbrace{\sqrt[r]{\alpha}}_{\text{order } r^{t+1}}) = (\sqrt[r]{\alpha})^{\omega(a)} \text{ (defined with } t+1 \text{ instead of } t) = (\sqrt[r]{\alpha})^{a^{r^t}}$$

Now put $\ell := (k[\zeta][\sqrt[r]{\alpha}])^{\Delta}$ ← the Δ-invariants.

Theorem: ~~this~~ ℓ is a field extension of k of degree r.

• Polynomial-time algorithm that, given k, l, r constructs $\alpha \in k[\zeta]$ such that $\langle\alpha\rangle = T = T_{k,r}$, and an isomorphism $l \xrightarrow{\sim} k[\zeta][\sqrt[r]{\alpha}]^\Delta$ of k-algebras.

<u>Algo</u>

• Compute $\beta \in l$ giving a normal basis over k.

• "project" β to the "Frob $= \zeta$"-eigenspace of $l[\zeta]$:

$$\beta \mapsto \gamma = \sum_{i \bmod r} \zeta^{-i} \beta^{q^i} \quad \text{where } q = \#k.$$

[Frob $\gamma = \zeta \cdot \gamma$].

[$\gamma \in l[\zeta]^*$] because β gives a normal basis.

they are not projections: doing them twice changes the outcome.

[$l[\zeta] \underset{k[\zeta]\text{-alg}}{\cong} k[\zeta][Y]/(Y^r - \gamma^r)$ and $\gamma^r \in k[\zeta]^*$]

• "project" γ multiplicatively to $l[\zeta]^*_r$: $\delta = \gamma^{\frac{q^d-1}{r^t}}$

[So now order $\delta = r^{t+1}$]

• "project" δ to $T_{l,r}$: $\varepsilon = \prod_{a=1}^{r-1} \sigma_a^{-1}(\delta)^{\left(a^{r^t} = \omega(a) \bmod r^{t+1}\right)}$ [Now $\varepsilon \in T_{l,r}$]

• $\alpha := \varepsilon^r$

<u>Exercise</u>: prove that $\alpha \in k[\zeta]^*$, and that $l \simeq k[\zeta][\sqrt[r]{\alpha}]^\Delta$.

<u>Proof of A</u> ($k \subset l$, $k \subset l'$ with $[l:k] = [l':k] = r$ prime, $r \nmid \operatorname{char} k$, finds $l \underset{k}{\simeq} l'$)

Find α, α' with $T = T_{k,r} = \langle\alpha\rangle = \langle\alpha'\rangle$ and

$l \xrightarrow{\sim} k[\zeta][\sqrt[r]{\alpha}]^\Delta$

$l' \xrightarrow{\sim} k[\zeta][\sqrt[r]{\alpha'}]^\Delta$

Write $\alpha = (\alpha')^x$ using Shanks–Tonelli ($R = k[\zeta]$, $n = r^t$).

(fine because the largest prime factor of n will be r).

Now, have an k-algebra isomorphism $k[\zeta][\sqrt[r]{\alpha}] \xrightarrow{\sim} k[\zeta][\sqrt[r]{\alpha'}]$, $\sqrt[r]{\alpha} \longmapsto (\sqrt[r]{\alpha'})^x$

respecting Δ.

Take the Δ invariants $\Rightarrow l \simeq l'$.

//

Proof of B ($k \subset \ell$ with $[\ell:k]=r$ prime $\neq 2$, $r \nmid \operatorname{char} k$; constructs $\ell \subset \ell' =$ field extension with $[\ell':\ell]=r$)

Write $\ell[\zeta] = k[\zeta][\sqrt[r]{\alpha}]$ with $\langle \alpha \rangle = T_{k,r}$.

Now $\sqrt[r]{\alpha} \in T_{\ell,r}$

Claim: $\langle \sqrt[r]{\alpha} \rangle = T_{\ell,r}$

$$\operatorname{order}(\sqrt[r]{\alpha}) = r \cdot \underset{\substack{\parallel \\ r^t \| q^d - 1}}{\operatorname{order}(\alpha)} = r^{t+1}$$

$$r^t \| q^d - 1 \Rightarrow r^{t+1} \| q^{rd} - 1 = (\#\ell)^d - 1 \quad //$$

Exercise: Suppose $r \neq 2$ or $q = \#k \equiv 1 \bmod 4$ and $\langle \alpha \rangle = T_{r,k}$.
Then for each $v \in \mathbb{Z}$, the ring
$$k[\zeta][\sqrt[r^v]{\alpha}]^{\Delta} \quad \text{is a field extension of } k \text{ of degree } r^v.$$

Theorem (partial result #3): There is an algorithm that, given a prime number p and an integer $n > 0$, constructs a field of cardinality p^n, which if GRH is true, has polynomial runtime.

Exercise: Let k be a number field ($\#k = q$), let r be a prime number $\nmid \operatorname{char} k$, and let Γ be a subgroup of $\Delta = \{\sigma_a : a \in \mathbb{F}_r^*\} \subset \operatorname{Aut}_k k[\zeta_r]$

Then: $k[\zeta_r]^{\Gamma}$ is a field $\Leftrightarrow$ Δ/Γ is generated by $(\sigma_{q \bmod r} \cdot \Gamma)$. $(\sigma_a \zeta_r = \zeta_r^a)$

Also, if these statements are true, then:
$$k[\zeta_r]^{\Gamma} = k\Big[\sum_{\sigma \in \Gamma} \sigma \zeta_r\Big] \quad \text{and} \quad [k[\zeta_r]^{\Gamma} : k] = (\Delta : \Gamma).$$

"pf" (sketch):

$k = \mathbb{F}_p$, $(\Delta : \Gamma) = n$, $r \equiv 1 \bmod n$ $\quad \mathbb{F}_r^* / (\mathbb{F}_r^*)^n \overset{?}{=} \langle \text{image of } p \rangle$

and deal also with other special cases.

(due to Adleman & H.W. Lenstra).