Arithmetic geometry as a toolbox for computer algebra

Part I - 05/03/2026

Pierre-Jean Spaenlehauer

Inria Nancy

JNCF 2026

Computer algebra and arithmetic geometry

Arithmetic geometry: $\approx$ rational points of algebraic varieties.

Computer algebra: provider of **tools** for arithmetic geometry.

$\rightsquigarrow$ point counting, isogeny computations (Bostan/Salvy/Morain/Schost'06), etc.

Computer Algebra

Arithmetic Geometry

This talk: **using arithmetic geometry** for computer algebra.

Deterministic root-finding in $\mathbb{F}_q[X]$ with elliptic curves.

FFT polynomial multiplication with elliptic curves.

Probabilistic factorization in $\mathbb{F}_q[X]$ using Drinfeld modules.

Rational cyclotomy in computer algebra

Using rational roots of unity in a field k

Cantor-Zassenhaus'81 (probabilistic root-finding in $\mathbb{F}_q[X]$): uses the fact that $\mathbb{F}_q$ (q odd) always has a **$(q-1)/2$-th primitive root of unity.**

Deterministic root-finding algorithms over $\mathbb{F}_q$ (Mignotte-Schnorr'88, von zur Gathen'87) rely on powersmooth decompositions of $\mathbb{F}_q^\times$.

FFT: needs a large **group of roots of unity with smooth order** in $\mathbb{F}_q^\times$.

Root of unity of order N in $\mathbb{F}_q \Leftrightarrow N$ divides $q-1$.

Special primes q (or prime powers): $q-1$ is divisible by a large number **free of large prime factors** $\rightsquigarrow$ rarely satisfied.

Goal: Replace **cyclotomic condition** by other arithmetico-geometric conditions.

N-th root of unity in $\mathbb{F}_q \rightsquigarrow$ rational N-torsion point on an **elliptic curve**.

There is only one cyclotomic group $/\mathbb{F}_q$; there are **many elliptic curves** $/\mathbb{F}_q$.

Slogan: Elliptic curves make every prime (power) special.

A motivating example

$p = 92233720368547784 87$
$\rightsquigarrow$ first prime number $> 2^{63}$ such that $(p-1)/2$ is also **prime**.

Elliptic curve with equation
$E : Y^2 = X^3 + 10345053799823400 77 \cdot X + 45493703649291324 5$
$\rightsquigarrow$ 9223372033588249600 **rational points**.

$9223372033588249600 = 2^{10} \cdot 5^2 \cdot 7 \cdot 139 \cdot 181 \cdot 251 \cdot 1787 \cdot 4561.$
$+$ group structure on $E(\mathbb{F}_q)$.

Contents

Today: Elliptic curves and deterministic root-finding.

Tomorrow: More polynomial factorization, Fast Fourier Transform, Drinfeld modules.

Cyclotomy, elliptic curves, Drinfeld modules

Cyclotomy: algebraic action of $\mathbb{Z}$ on $\overline{\mathbb{F}_q}^\times$.

$\rightsquigarrow [n] \cdot x = x^n$.

Elliptic curves: algebraic action of $\mathbb{Z}$ on $\overline{\mathbb{F}_q}$, parametrized by $a, b \in \overline{\mathbb{F}_q}$.

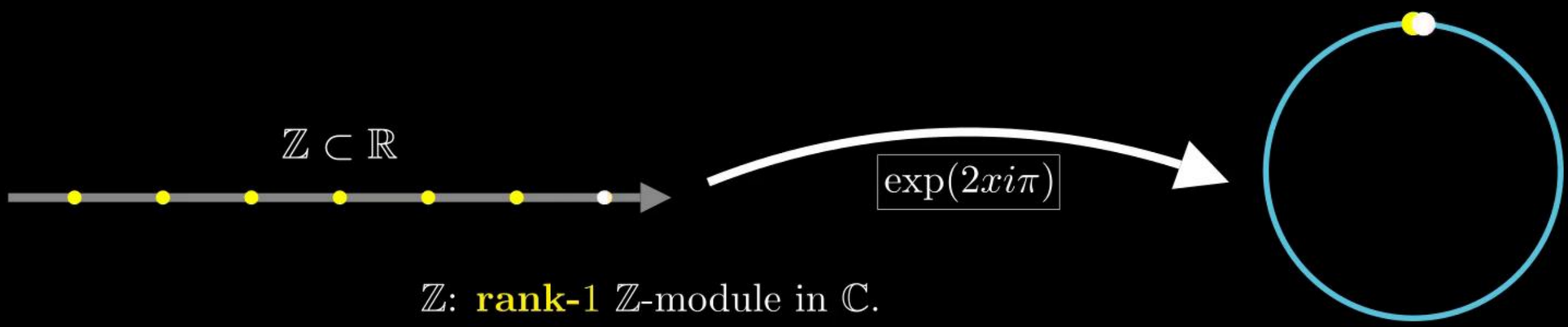
$\rightsquigarrow$ (n odd)

$$[n] \cdot x = \frac{\psi_{a,b,n}(x)^2 - \psi_{a,b,n-1}(x)\psi_{a,b,n+1}(x)}{\psi_{a,b,n}(x)^2}.$$

Drinfeld modules: algebraic action of $\mathbb{F}_q[X]$ on $\overline{\mathbb{F}_q}$, parametrized by $\Delta, g, \gamma \in \overline{\mathbb{F}_q}$.

$\rightsquigarrow \phi_X(x) = \Delta x^{q^2} + g x^q + \gamma x$.

Complex cyclotomy



$\mathbb{Z}$: **rank-1** $\mathbb{Z}$-module in $\mathbb{C}$.

all rank-1 $\mathbb{Z}$-modules in $\mathbb{C}$ are **homothetic**.

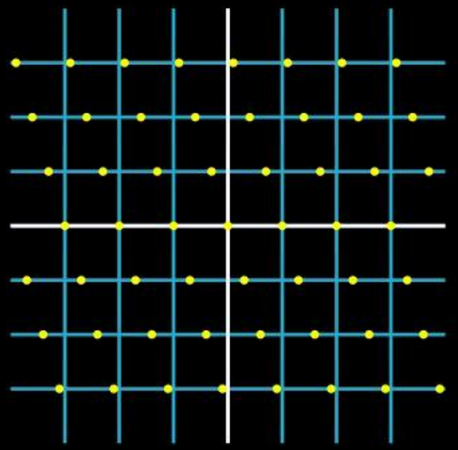
$\mathbb{Z}/n\mathbb{Z}$: n-torsion in $\mathbb{R}/\mathbb{Z}$ $\rightsquigarrow$ sent to solutions of $X^n - 1$.

exp is **transcendental** but solutions of $X^n - 1$ are **algebraic**.

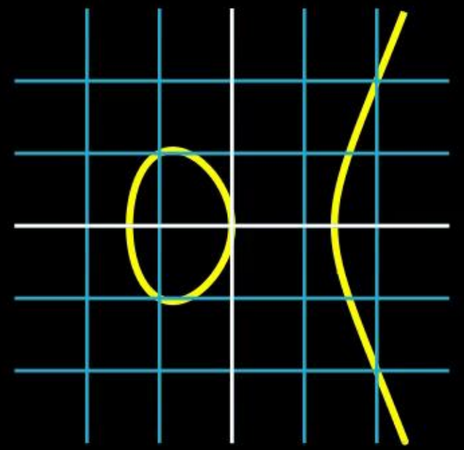
Complex elliptic curves

Complex cyclotomy: rank-1 $\mathbb{Z}$-modules in $\mathbb{C}$ (up to homothety).

Complex elliptic curves: rank-2 $\mathbb{Z}$-modules in $\mathbb{C}$ (up to homothety).



$$\wp(x) = \frac{1}{z^2} + \sum_{\lambda \in \Gamma \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$



$\sin(x)$, $2i\pi\mathbb{Z}$-periodic: compositional inverse to $\int_0^x \frac{dy}{\sqrt{1-y^2}}$.

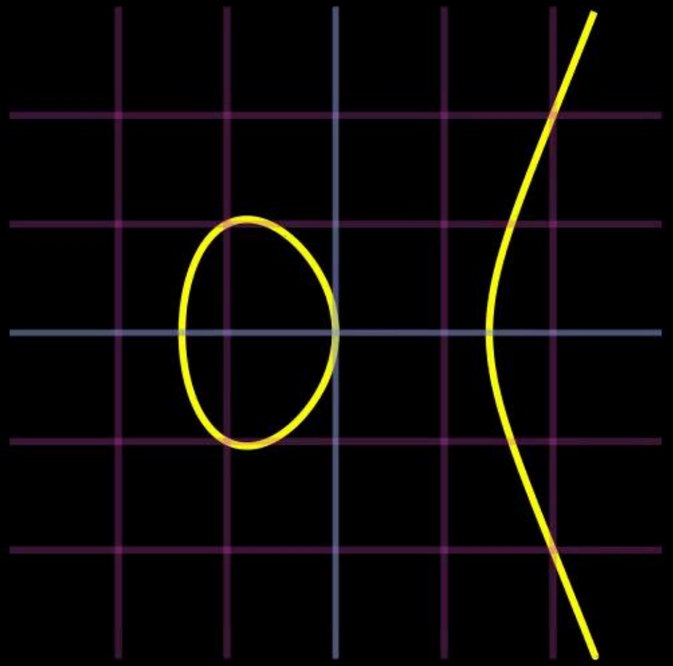
$\wp(x)$, Γ periodic: compositional inverse to $\int_s^\infty \frac{ds}{\sqrt{4s^3 - g_2 s - g_3}}$.

Group law on elliptic curves

Elliptic curve: smooth projective curve of genus 1.

Assume $\mathrm{char}(k) \neq 2, 3$.

Short Weierstrass equation: $Y^2 = X^3 + aX + b$, with $4a^3 + 27b^2 \neq 0$.



$$s = (y_P - y_Q)/(x_P - x_Q).$$

$$x_R = s^2 - x_P - x_Q.$$

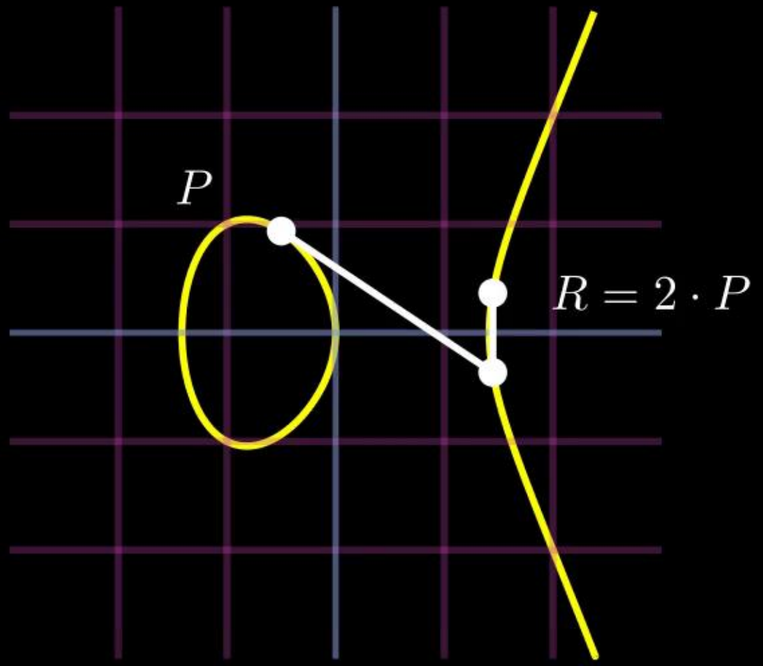
$$y_R = -y_P + s(x_P - x_R).$$

Group law on elliptic curves

Elliptic curve: smooth projective curve of genus 1.

Assume $\mathrm{char}(k) \neq 2, 3$.

Short Weierstrass equation: $Y^2 = X^3 + aX + b$, with $4a^3 + 27b^2 \neq 0$.



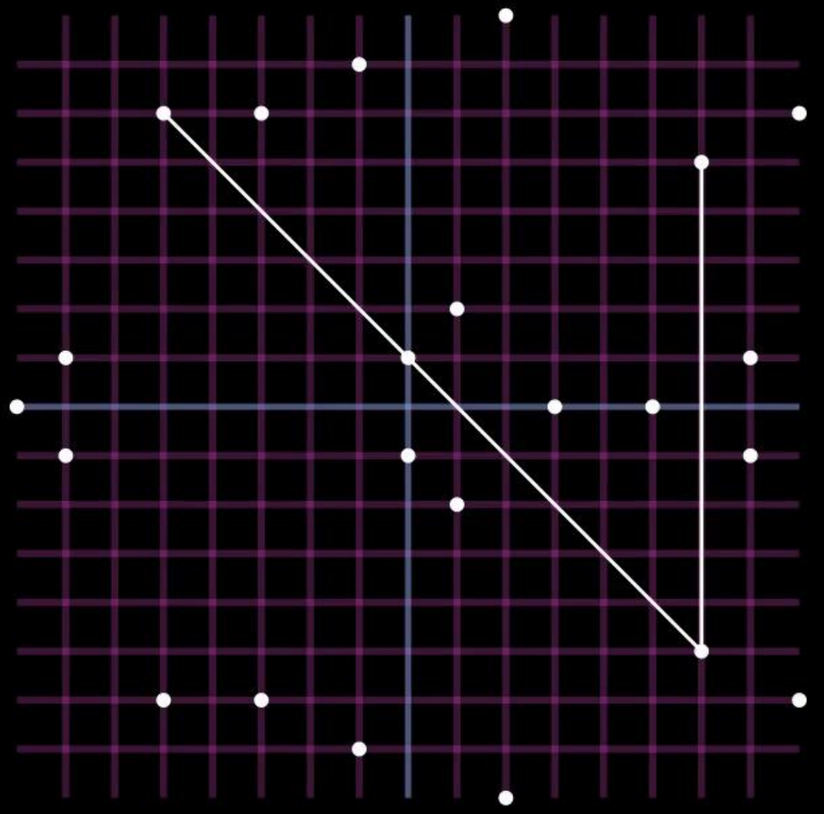
$$s = (3x_P^2 + a)/(2y_P).$$

$$x_R = s^2 - 2x_P.$$

$$y_R = -y_P + s(x_P - x_R).$$

Elliptic curves over finite fields

$Y^2 \equiv X^3 + 2X + 1 \bmod 17$



Hasse'33: $q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}$.

Deuring'41: for any $t \in [-2\sqrt{q}, 2\sqrt{q}]$ coprime with q, there is a curve E s.t. $|E(\mathbb{F}_q)| = q + 1 - t$.

Cassels'66: $E(\mathbb{F}_q) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ with $m_1 \mid m_2$.

$x([n]P)$ function of $x(P)$.

Division polynomials

Kernels of the multiplication maps $P \mapsto [n] \cdot P$ on $E(\overline{\mathbb{F}_q})$.

$\rightsquigarrow$ **Division polynomials!**

$\psi_n(X, Y) \in \mathbb{F}_q[X, Y]/(Y^2 - X^3 - aX - b)$ generator of the ideal of functions vanishing at $\ker(P \mapsto [n] \cdot P)$.

$\psi_n(x, y) = 0 \Leftrightarrow [n] \cdot (x, y) = \infty$.

Recurrence relations!

$$\psi_{2n+1}(X, Y) = \psi_{n+2}(X, Y)\psi_n(X, Y)^3 - \psi_{n-1}(X, Y)\psi_{n+1}(X, Y)^3 \text{ for } n \geq 2.$$

$$\psi_{2n}(X, Y) = \frac{\psi_n(X, Y)}{2Y}\left(\psi_{n+2}(X, Y)\psi_{n-1}(X, Y)^2 - \psi_{n-2}(X, Y)\psi_{n+1}(X, Y)^2\right) \text{ for } n \geq 3.$$

$\rightsquigarrow$ Computing $\psi_n(X, Y) \bmod f(X)$ in $\widetilde{O}(\log n \deg(f))$ ops in $\mathbb{F}_q$.

$\rightsquigarrow$ Analog of computing $X^n - 1 \bmod f(X)$ in $\widetilde{O}(\log n \deg(f))$ ops in $\mathbb{F}_q$.

Summing up - Elliptic curves over finite fields

Elliptic curves over $\mathbb{F}_q$

Defined by **equations** of the form $Y^2 = X^3 + aX + b$, with $a, b \in \mathbb{F}_q$.

Abelian group structure $E(\mathbb{F}_q)$ on the **rational** solutions of $Y^2 = X^3 + aX + b$ (+ point at infinity).

Arise from a **rank-2 analog** of complex cyclotomy.

There are **many elliptic curves**: for any $t < 2\sqrt{q}$ coprime with q, there exist an elliptic curve with $|E(\mathbb{F}_q)| = q + 1 \pm t$ (Deuring'41).

$E(\mathbb{F}_q) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ with $m_1 \mid m_2$ (Cassels'66).

Goal: replace a cyclotomic **smoothness** condition on $q - 1$ by a **smoothness** condition on $|E(\mathbb{F}_q)|$ for a good elliptic curve E.

Deterministic root-finding in $\mathbb{F}_q[X]$ with elliptic curves

Deterministic root-finding with elliptic curves

Root-finding: upon input of the coefficients of $f(X) \in \mathbb{F}_q[X]$, compute the set of $x \in \mathbb{F}_q$ s.t. $f(x) = 0$.

No general **deterministic polynomial-time** algorithm.

Why do we care about deterministic algorithms?

Camion'83: Theoretical deterministic polynomial-time algorithm with precomputations on q.

Focus (S.'2026): A practical deterministic algorithm with precomputations, conjecturally polynomial-time.

Complexity: Requires a (precomputed) **elliptic curve** $E/\mathbb{F}_q$.

$\widetilde{O}(\Xi(E)^2 \log q(\deg(f)^\omega + \deg(f) \log q))$ ops in $\mathbb{F}_q$.

$\Xi(E)$: **largest prime factor** in $(q+1-U)$ and $(q+1+U)$, where $U = q+1-|E(\mathbb{F}_q)|$.

Polynomial factoring and root-finding

Berlekamp'70: polynomial factoring reduces to root-finding

Step 1: Make $f(X)$ **squarefree**
$\rightsquigarrow f(X) \to f(X)/\operatorname{GCD}(f(X), f'(X))$.

Step 2: **Distinct-degree factorization**
$\rightsquigarrow$ Compute $\operatorname{GCD}(f(X), X^{q^i} - X))$ for successive i.

Step 3: **Root-finding**
$\rightsquigarrow$ Factor $f(X)$ assuming that it divides $X^{q^i} - X$.

Root finding over finite fields

Classical topic in **computer algebra**. Ideas already in **Legendre**'s works.

Very fast **probabilistic** methods.

No general **deterministic** poly-time algorithm.

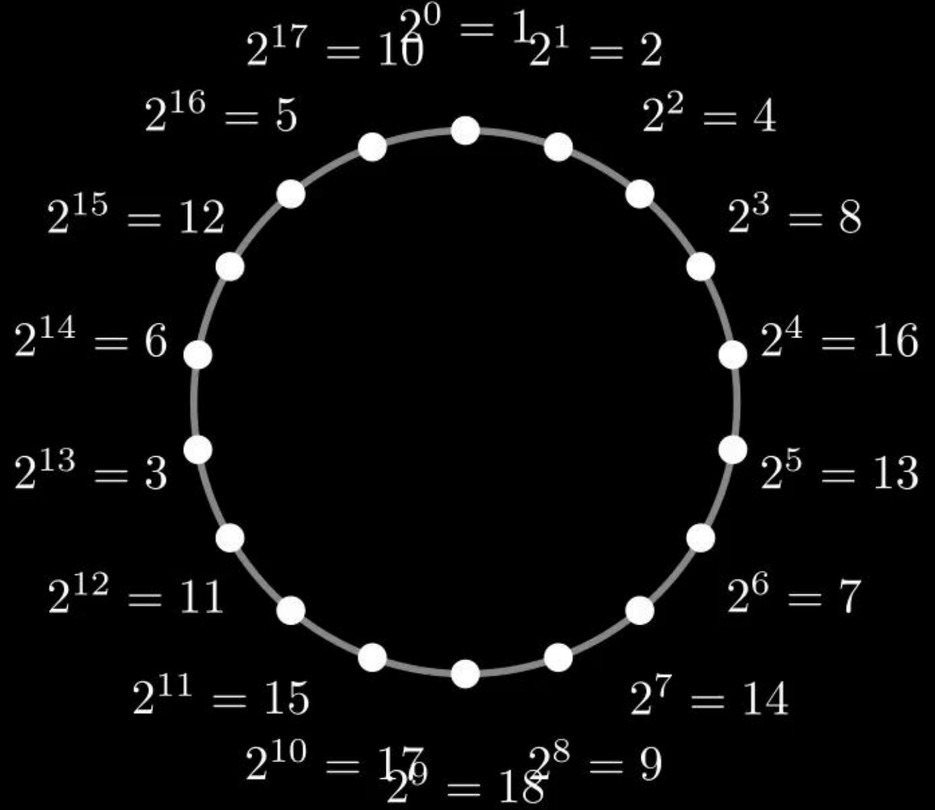
Polynomial factoring and root-finding (II)

$\prod_{\alpha \in \mathbb{F}_q} (X - \alpha) = X^q - X = X(X^{(q-1)/2} - 1)(X^{(q-1)/2} + 1)$.

$X^{(q-1)/2} \pm 1 \bmod f(X)$ can be computed efficiently by **binary exponentiation**.

This works because $\mathbb{F}_q^\times$ contains a **subgroup of index 2**.

Additivity vs. multiplicativity $\rightsquigarrow$ **randomize** $f(X) \mapsto f(X + r)$.



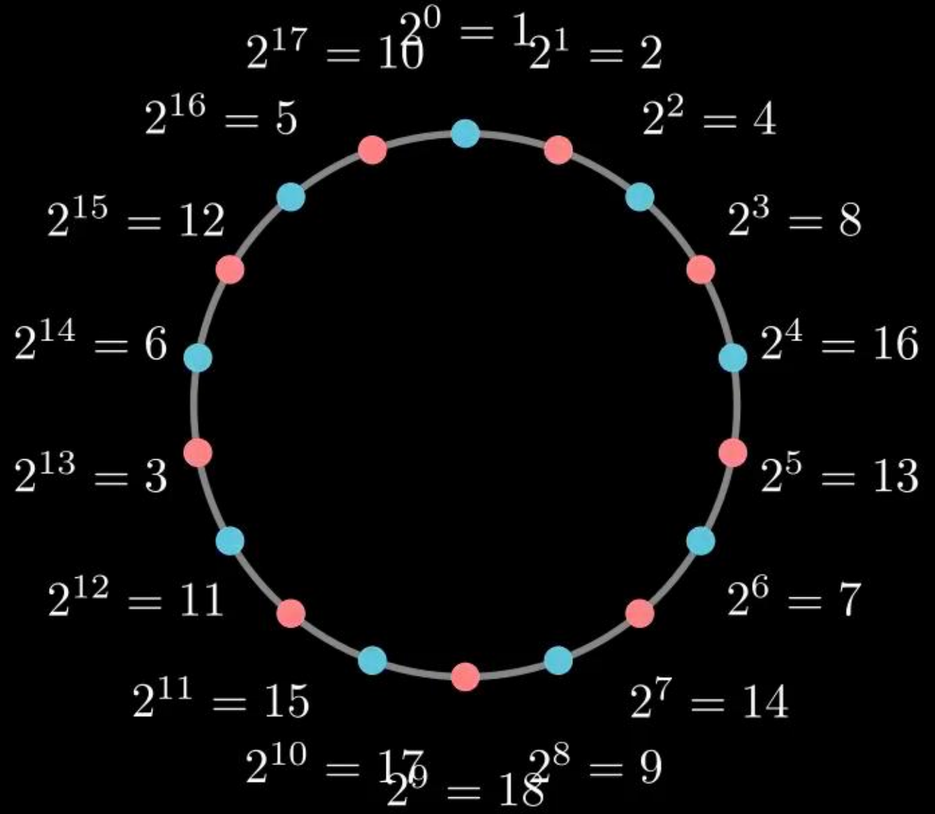
Polynomial factoring and root-finding (II)

$\prod_{\alpha \in \mathbb{F}_q} (X - \alpha) = X^q - X = X(X^{(q-1)/2} - 1)(X^{(q-1)/2} + 1)$.

$X^{(q-1)/2} \pm 1 \bmod f(X)$ can be computed efficiently by **binary exponentiation**.

This works because $\mathbb{F}_q^\times$ contains a **subgroup of index 2**.

Additivity vs. multiplicativity $\rightsquigarrow$ **randomize** $f(X) \mapsto f(X + r)$.



Example: $\mathbb{F}_{19}$

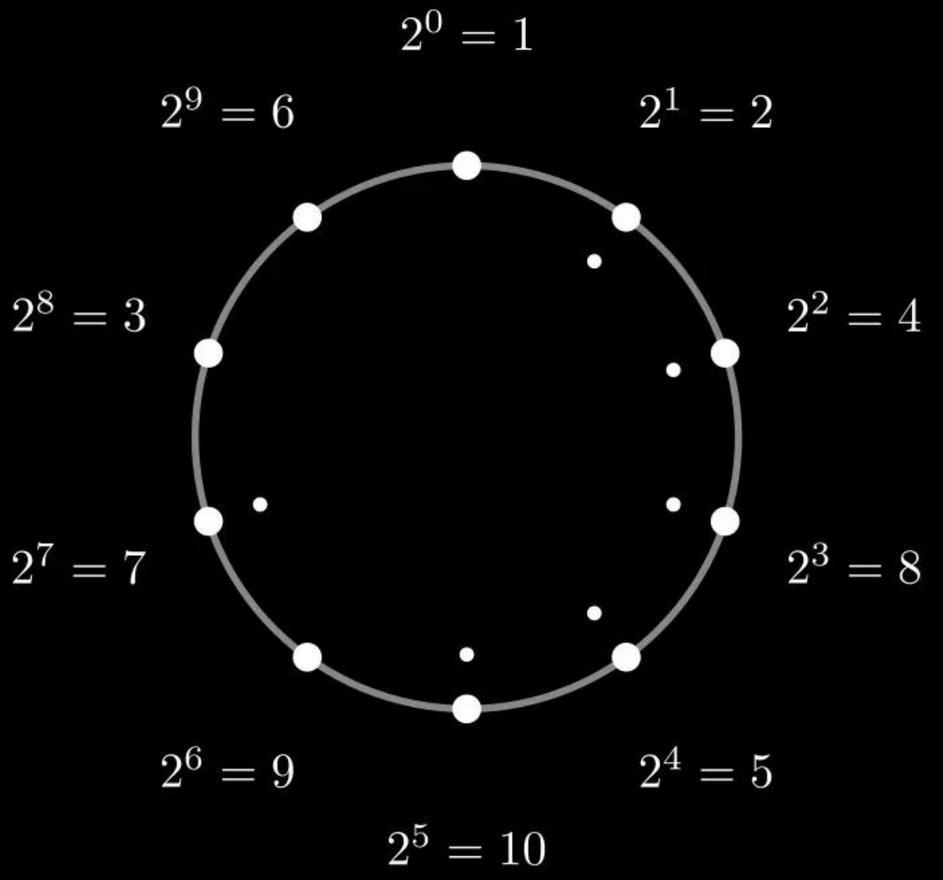
$$X^9 - 1 = (X-1)(X-4)(X-16)(X-7)(X-9)(X-17)(X-11)(X-6)(X-5)$$

$$X^9 + 1 = (X-2)(X-8)(X-13)(X-14)(X-18)(X-15)(X-3)(X-12)(X-10)$$

$\mathrm{GCD}(X^3 + X^2 + 14X + 17, X^9 - 1) = X - 13$

Mignotte-Schnorr'88: derandomizing root-finding

Example: $f(X) = X^6 + 8X^5 + 2X^4 + X^3 + 6X^2 + 4X + 4 \in \mathbb{F}_{11}[X]$

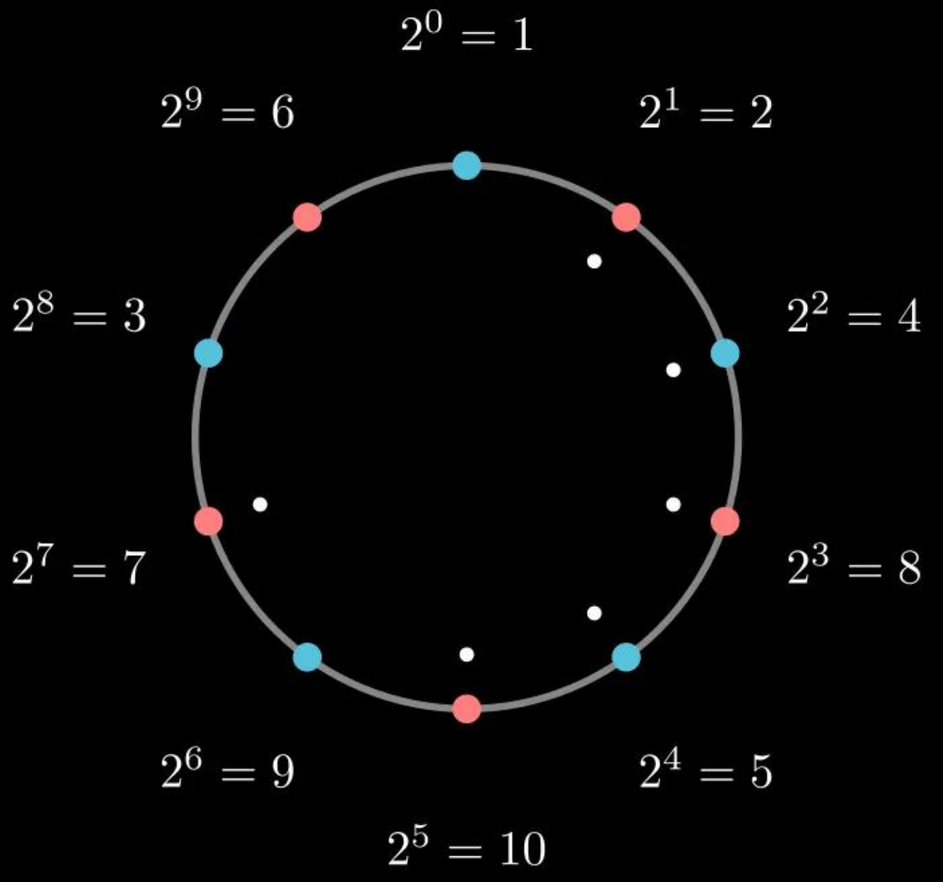


Mignotte-Schnorr'88: derandomizing root-finding

Example: $f(X) = X^6 + 8X^5 + 2X^4 + X^3 + 6X^2 + 4X + 4 \in \mathbb{F}_{11}[X]$

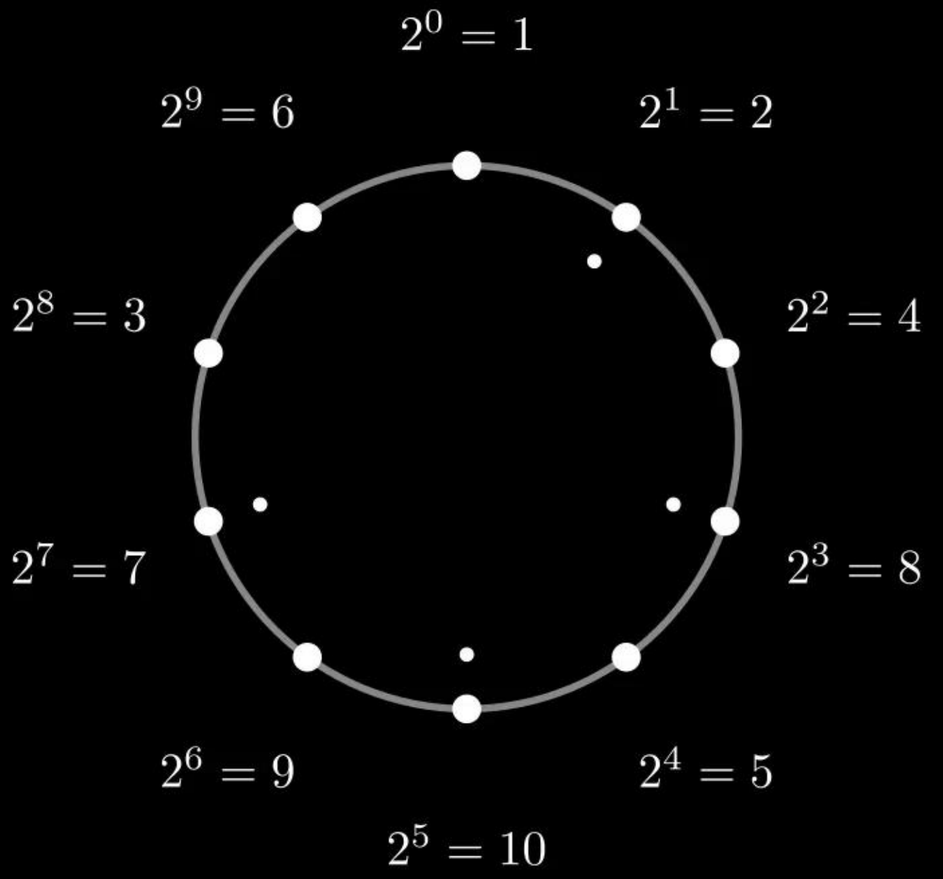
GCD with $X^5 - 1$.

$\rightsquigarrow f(X) = (X^2 + 2X + 9)(X^4 + 6X^3 + 3X^2 + 7X + 9)$.



Mignotte-Schnorr'88: derandomizing root-finding

Example: $f(X) = X^6 + 8X^5 + 2X^4 + X^3 + 6X^2 + 4X + 4 \in \mathbb{F}_{11}[X]$



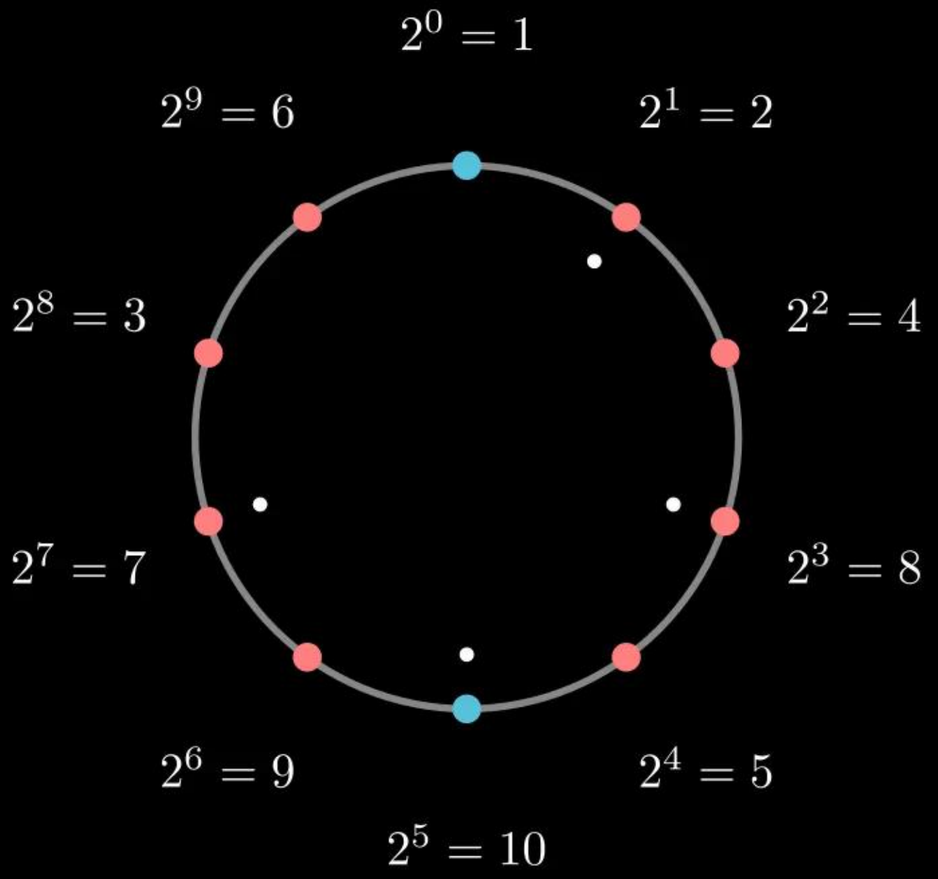
GCD with $X^5 - 1$.

$\rightsquigarrow f(X) = (X^2 + 2X + 9)(X^4 + 6X^3 + 3X^2 + 7X + 9)$.

$\rightsquigarrow$ Factoring $X^4 + 6X^3 + 3X^2 + 7X + 9$.

Mignotte-Schnorr'88: derandomizing root-finding

Example: $f(X) = X^6 + 8X^5 + 2X^4 + X^3 + 6X^2 + 4X + 4 \in \mathbb{F}_{11}[X]$



GCD with $X^5 - 1$.

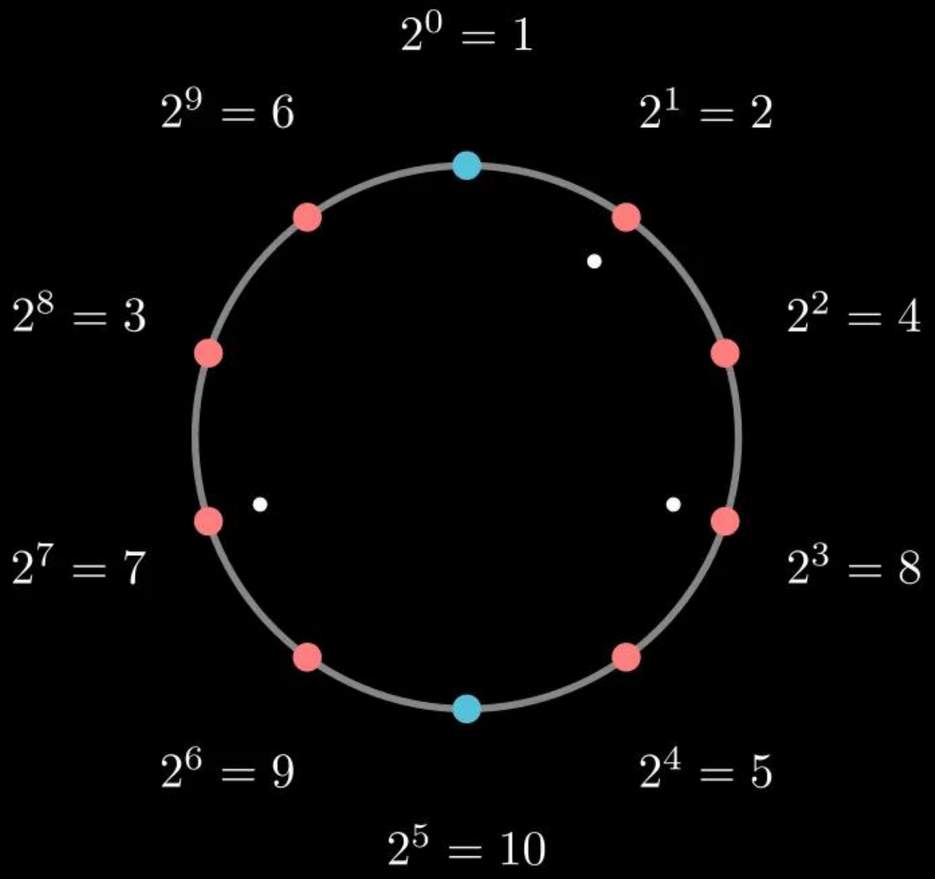
$\rightsquigarrow f(X) = (X^2 + 2X + 9)(X^4 + 6X^3 + 3X^2 + 7X + 9)$.

$\rightsquigarrow$ Factoring $X^4 + 6X^3 + 3X^2 + 7X + 9$.

GCD with $X^2 - 1 \rightsquigarrow (X - 10)(X^3 + 5X^2 + 9X + 9)$.

Mignotte-Schnorr'88: derandomizing root-finding

Example: $f(X) = X^6 + 8X^5 + 2X^4 + X^3 + 6X^2 + 4X + 4 \in \mathbb{F}_{11}[X]$



GCD with $X^5 - 1$.

$\rightsquigarrow f(X) = (X^2 + 2X + 9)(X^4 + 6X^3 + 3X^2 + 7X + 9)$.

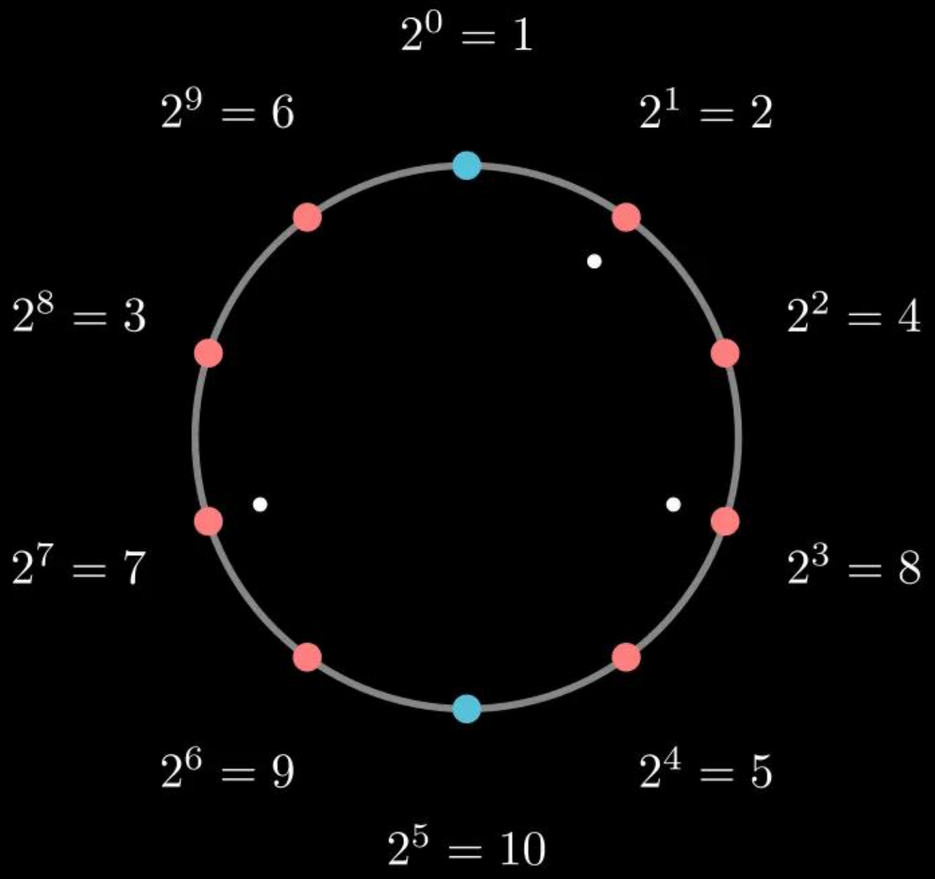
$\rightsquigarrow$ Factoring $X^4 + 6X^3 + 3X^2 + 7X + 9$.

GCD with $X^2 - 1 \rightsquigarrow (X - 10)(X^3 + 5X^2 + 9X + 9)$.

$\rightsquigarrow$ Factoring $X^3 + 5X^2 + 9X + 9$.

Mignotte-Schnorr'88: derandomizing root-finding

Example: $f(X) = X^6 + 8X^5 + 2X^4 + X^3 + 6X^2 + 4X + 4 \in \mathbb{F}_{11}[X]$



GCD with $X^5 - 1$.

$\rightsquigarrow f(X) = (X^2 + 2X + 9)(X^4 + 6X^3 + 3X^2 + 7X + 9)$.

$\rightsquigarrow$ Factoring $X^4 + 6X^3 + 3X^2 + 7X + 9$.

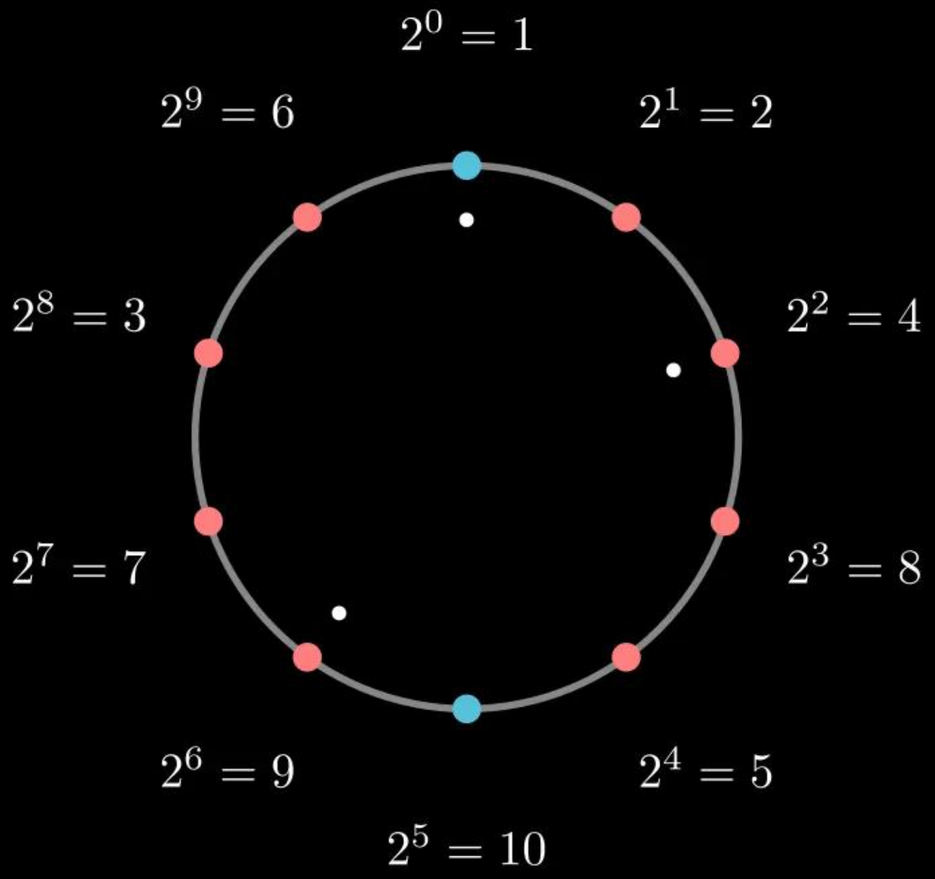
GCD with $X^2 - 1 \rightsquigarrow (X - 10)(X^3 + 5X^2 + 9X + 9)$.

$\rightsquigarrow$ Factoring $X^3 + 5X^2 + 9X + 9$.

Rotate! $X \mapsto 2X$.

Mignotte-Schnorr'88: derandomizing root-finding

Example: $f(X) = X^6 + 8X^5 + 2X^4 + X^3 + 6X^2 + 4X + 4 \in \mathbb{F}_{11}[X]$



GCD with $X^5 - 1$.

$\rightsquigarrow f(X) = (X^2 + 2X + 9)(X^4 + 6X^3 + 3X^2 + 7X + 9)$.

$\rightsquigarrow$ Factoring $X^4 + 6X^3 + 3X^2 + 7X + 9$.

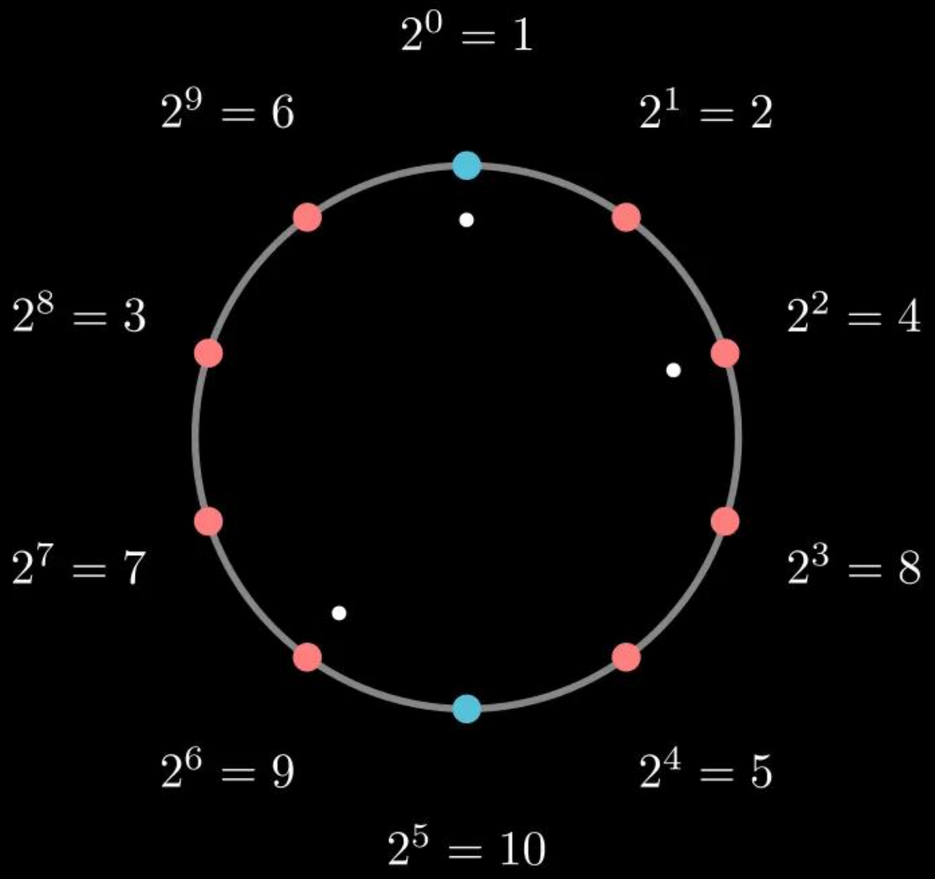
GCD with $X^2 - 1 \rightsquigarrow (X - 10)(X^3 + 5X^2 + 9X + 9)$.

$\rightsquigarrow$ Factoring $X^3 + 5X^2 + 9X + 9$.

Rotate! $X \mapsto 2X$.

Mignotte-Schnorr'88: derandomizing root-finding

Example: $f(X) = X^6 + 8X^5 + 2X^4 + X^3 + 6X^2 + 4X + 4 \in \mathbb{F}_{11}[X]$



GCD with $X^5 - 1$.

$\rightsquigarrow f(X) = (X^2 + 2X + 9)(X^4 + 6X^3 + 3X^2 + 7X + 9)$.

$\rightsquigarrow$ Factoring $X^4 + 6X^3 + 3X^2 + 7X + 9$.

GCD with $X^2 - 1 \rightsquigarrow (X - 10)(X^3 + 5X^2 + 9X + 9)$.

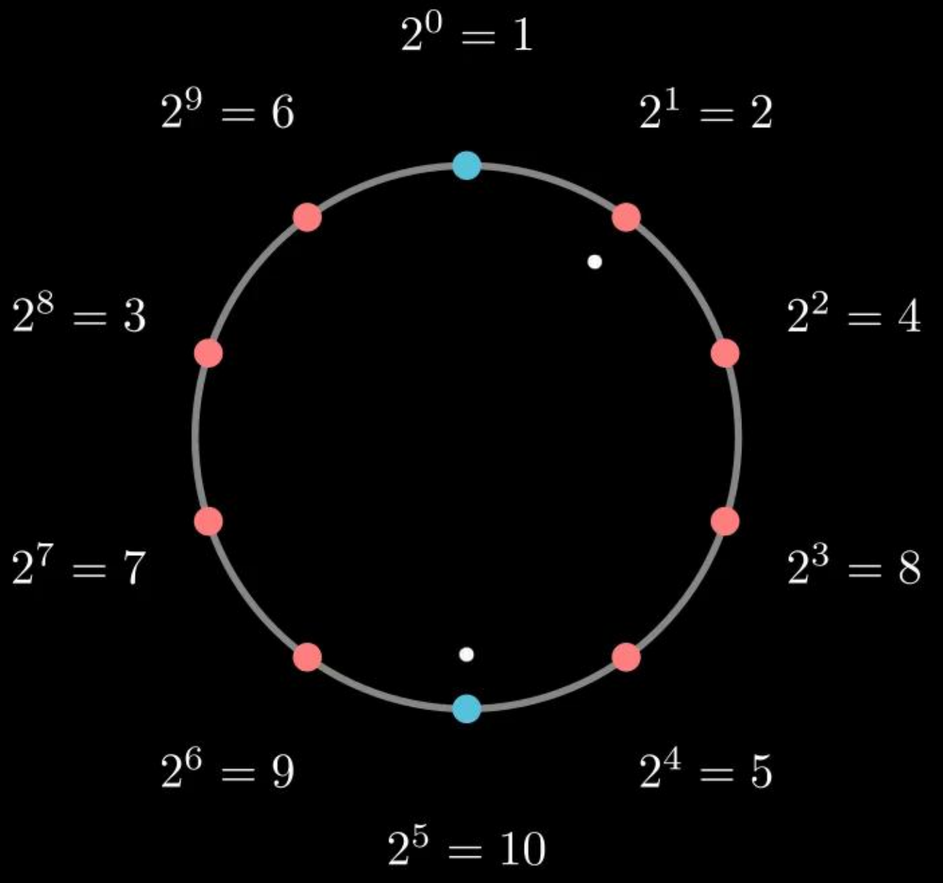
$\rightsquigarrow$ Factoring $X^3 + 5X^2 + 9X + 9$.

Rotate! $X \mapsto 2X$.

$\mathrm{GCD}((2X)^3 + 5(2X)^2 + 9(2X) + 9, X^2 - 1) = X - 1$.

Mignotte-Schnorr'88: derandomizing root-finding

Example: $f(X) = X^6 + 8X^5 + 2X^4 + X^3 + 6X^2 + 4X + 4 \in \mathbb{F}_{11}[X]$



GCD with $X^5 - 1$.

$\rightsquigarrow f(X) = (X^2 + 2X + 9)(X^4 + 6X^3 + 3X^2 + 7X + 9)$.

$\rightsquigarrow$ Factoring $X^4 + 6X^3 + 3X^2 + 7X + 9$.

GCD with $X^2 - 1 \rightsquigarrow (X - 10)(X^3 + 5X^2 + 9X + 9)$.

$\rightsquigarrow$ Factoring $X^3 + 5X^2 + 9X + 9$.

Rotate! $X \mapsto 2X$.

$\mathrm{GCD}((2X)^3 + 5(2X)^2 + 9(2X) + 9, X^2 - 1) = X - 1$.

$\rightsquigarrow X^3 + 5X^2 + 9X + 9 = (X - 2)(X^2 + 7X + 1)$.

Rotate again!

$X^2 + 7X + 1 = (X - 7)(X - 8)$.

Mignotte-Schnorr's algorithm

Deterministic algorithm using cyclotomy. Mignotte/Schnorr'88, von zur Gathen'87.

Relies on $q-1 = \ell_1^{n_1} \cdots \ell_r^{n_r}$ having **no large prime factor**.

Assume $n_1 = \cdots = n_r = 1$ (for now).

Fact 1: $\mathbb{F}_q^\times$ is cyclic.

Fact 2: $\mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z} \simeq \mathbb{Z}/\ell_1\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell_r\mathbb{Z}$; let φ be an isomorphism.

Fact 3: any $x \in \varphi^{-1}(0, i_2, \ldots, i_r)$ satisfies $x^{(q-1)/\ell_1} = 1$.

$\rightsquigarrow \varphi(x) \equiv i \bmod \ell_1 \leftrightarrow$ roots of $(X/\alpha^i)^{(q-1)/\ell_1} - 1 = \bullet(X^{(q-1)/\ell_1} - \alpha^{-i(q-1)/\ell_1})$, where α is primitive.

Fact 4: GCDs with $X^{(q-1)/\ell_1} - \alpha^{-i(q-1)/\ell_1}$ efficiently computed via binary exponentiation.

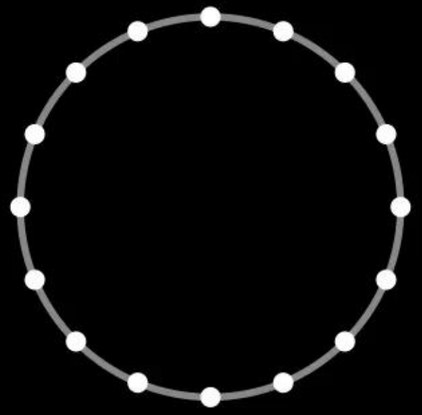
Complexity: $\widetilde{O}(\deg(f)(S_1(q-1)\log q + (\log q)^2))$.

$S_1(q-1)$: largest prime factor of $q-1$.

Dealing with powers

Use **FFT-like recursivity**.

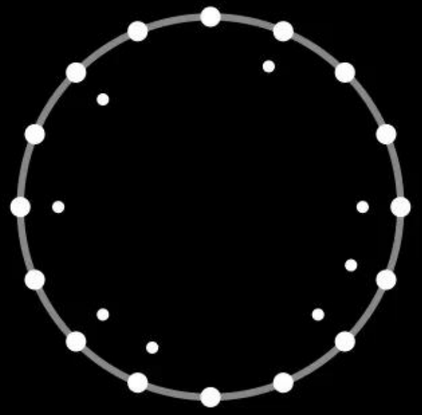
Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.



Dealing with powers

Use **FFT-like recursivity**.

Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

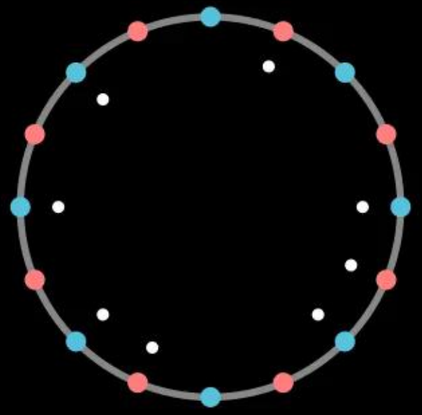


Dealing with powers

Use **FFT-like recursivity**.

Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

$f(X) = f_0(X)f_1(X)$, $f_0(X) = \mathrm{GCD}(X^{(p-1)/2} - 1, f(X))$.

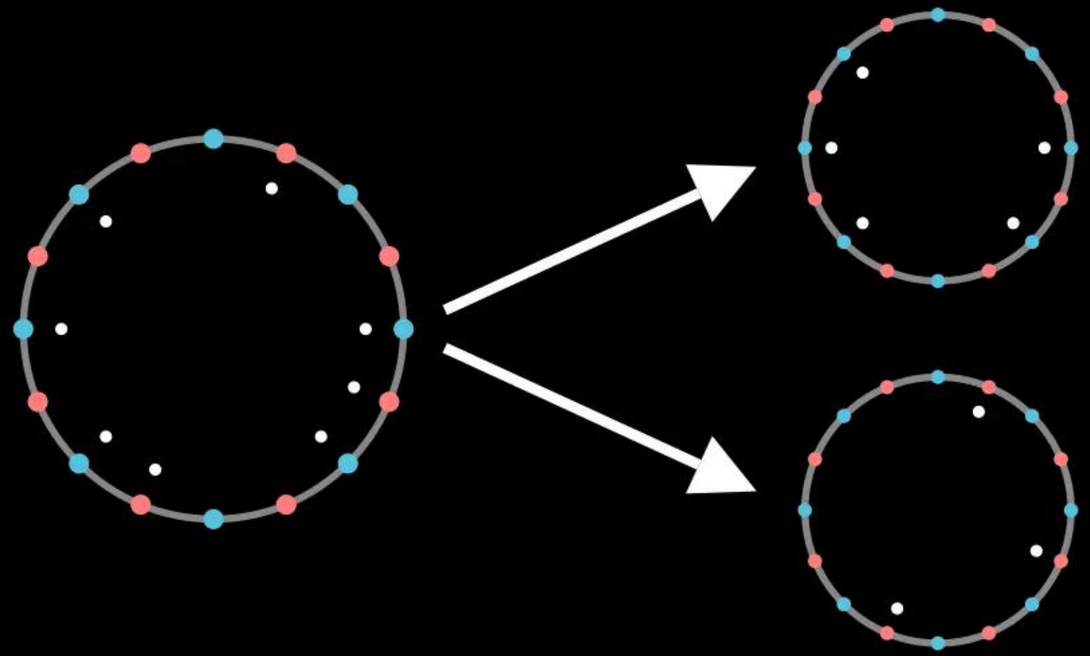


Dealing with powers

Use **FFT-like recursivity**.

Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

$f(X) = f_0(X)f_1(X)$, $f_0(X) = \mathrm{GCD}(X^{(p-1)/2} - 1, f(X))$.

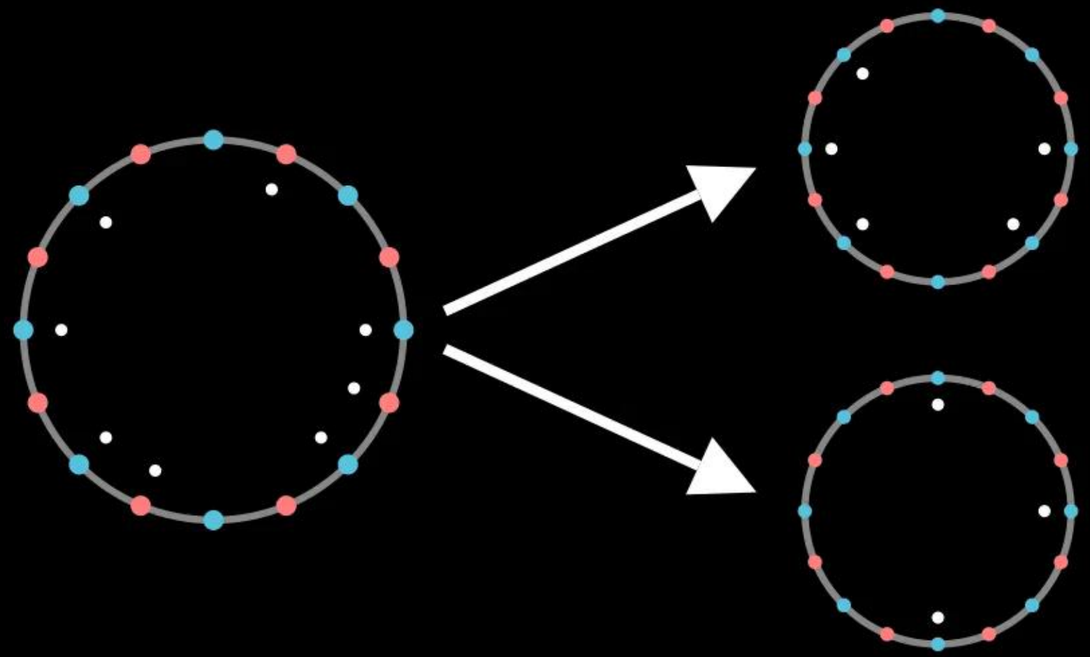


Dealing with powers

Use **FFT-like recursivity**.

Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

$f(X) = f_0(X)f_1(X)$, $f_0(X) = \mathrm{GCD}(X^{(p-1)/2} - 1, f(X))$.

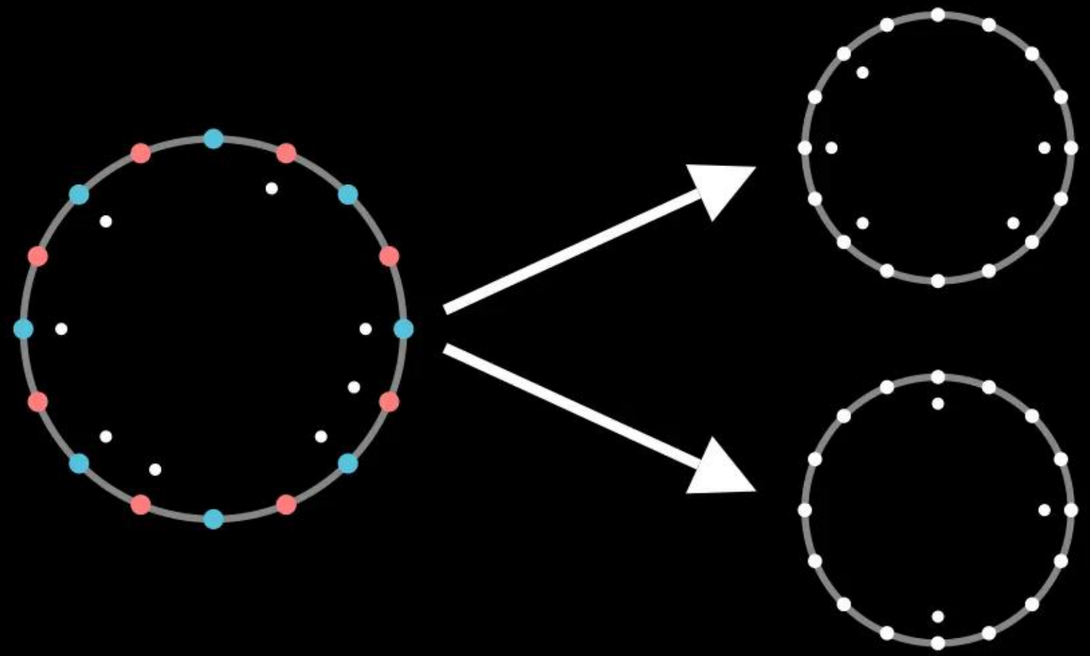


Dealing with powers

Use **FFT-like recursivity**.

Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

$f(X) = f_0(X)f_1(X)$, $f_0(X) = \mathrm{GCD}(X^{(p-1)/2} - 1, f(X))$.



Dealing with powers

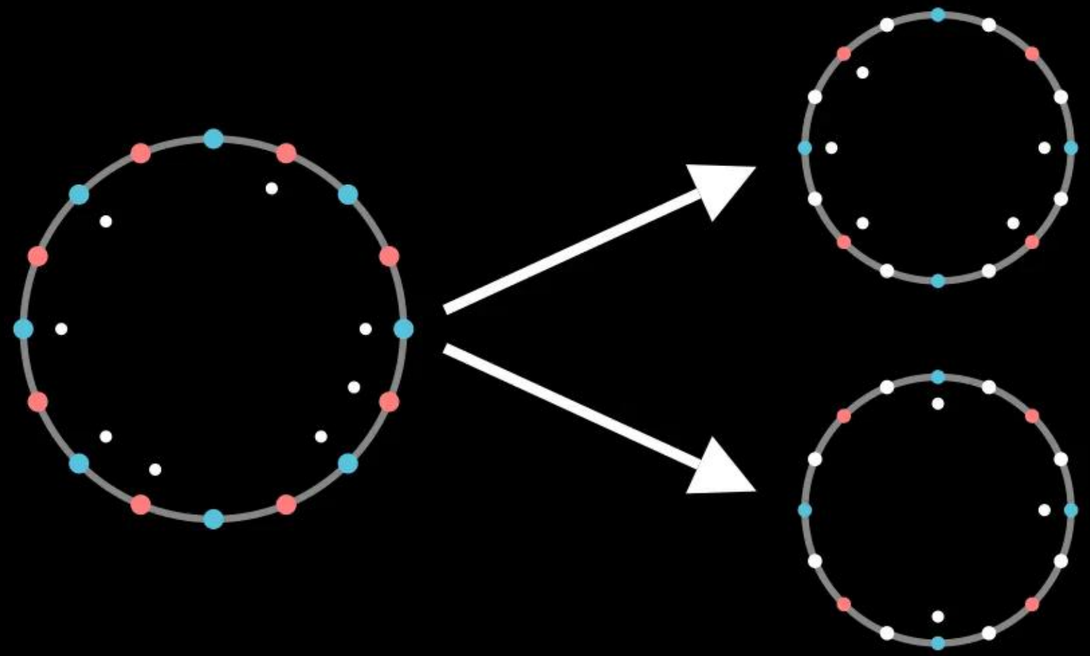
Use **FFT-like recursivity**.

Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

$f(X) = f_0(X)f_1(X)$, $f_0(X) = \mathrm{GCD}(X^{(p-1)/2} - 1, f(X))$.

Then **recurse**: $f_0(X) = f_{00}(X)f_{01}(X)$, $f_{00}(X) = \mathrm{GCD}(f_0(X), X^{(p-1)/4} - 1)$.

$f_1(\beta X) = f_{10}(X)f_{11}(X)$, $f_{10}(X) = \mathrm{GCD}(f_1(\beta X), X^{(p-1)/4} - 1)$.



Dealing with powers

Use **FFT-like recursivity**.

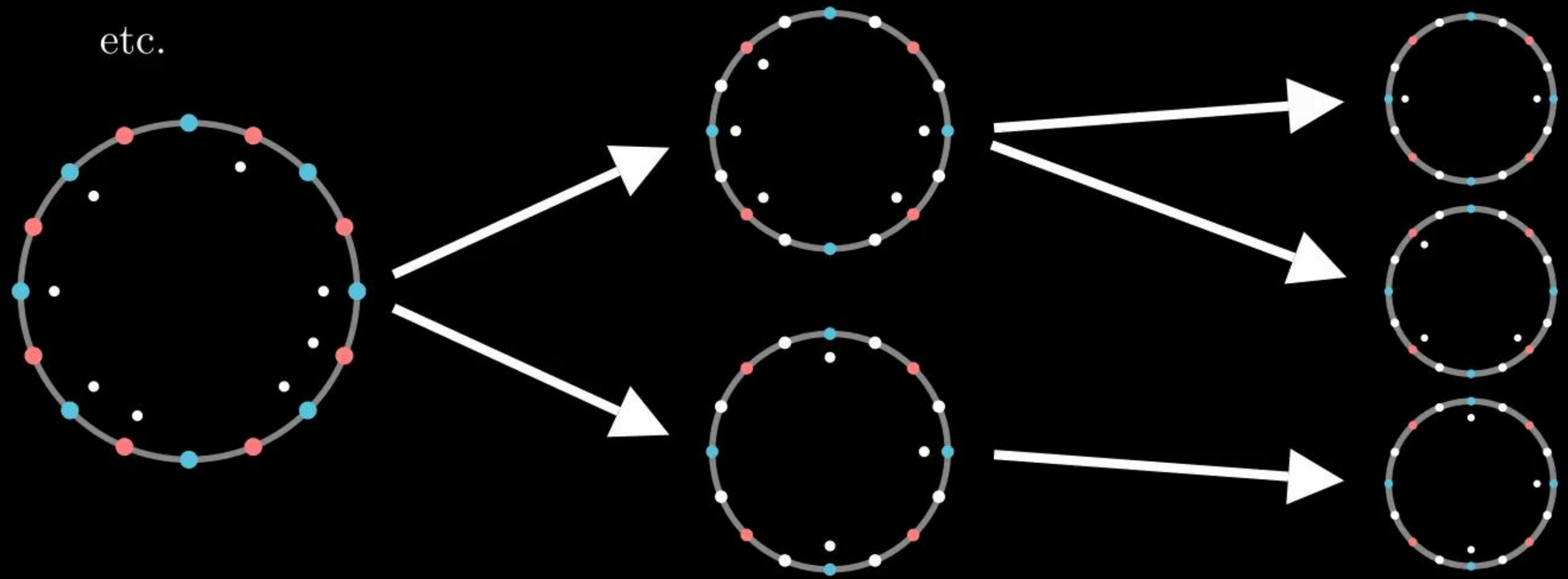
Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

$f(X) = f_0(X)f_1(X)$, $f_0(X) = \mathrm{GCD}(X^{(p-1)/2} - 1, f(X))$.

Then **recurse**: $f_0(X) = f_{00}(X)f_{01}(X)$, $f_{00}(X) = \mathrm{GCD}(f_0(X), X^{(p-1)/4} - 1)$.

$f_1(\beta X) = f_{10}(X)f_{11}(X)$, $f_{10}(X) = \mathrm{GCD}(f_1(\beta X), X^{(p-1)/4} - 1)$.

etc.



Dealing with powers

Use **FFT-like recursivity**.

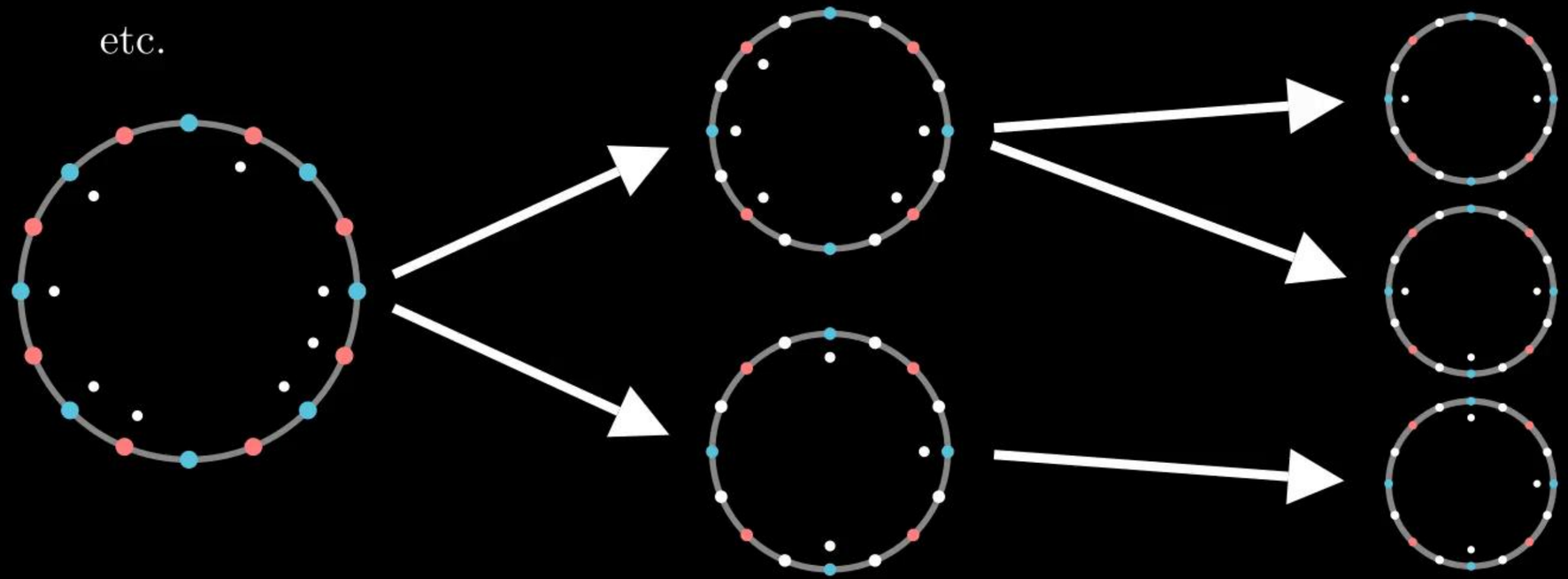
Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

$f(X) = f_0(X)f_1(X)$, $f_0(X) = \mathrm{GCD}(X^{(p-1)/2} - 1, f(X))$.

Then **recurse**: $f_0(X) = f_{00}(X)f_{01}(X)$, $f_{00}(X) = \mathrm{GCD}(f_0(X), X^{(p-1)/4} - 1)$.

$f_1(\beta X) = f_{10}(X)f_{11}(X)$, $f_{10}(X) = \mathrm{GCD}(f_1(\beta X), X^{(p-1)/4} - 1)$.

etc.



Dealing with powers

Use **FFT-like recursivity**.

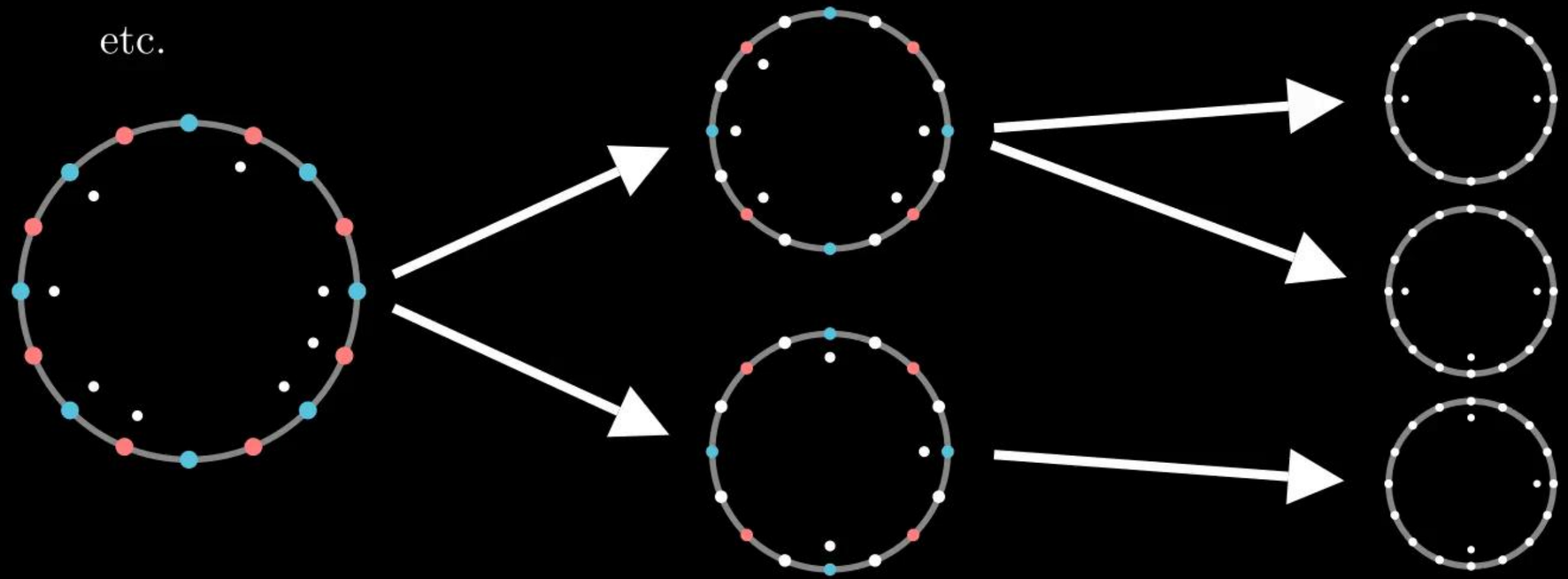
Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

$f(X) = f_0(X)f_1(X)$, $f_0(X) = \mathrm{GCD}(X^{(p-1)/2} - 1, f(X))$.

Then **recurse**: $f_0(X) = f_{00}(X)f_{01}(X)$, $f_{00}(X) = \mathrm{GCD}(f_0(X), X^{(p-1)/4} - 1)$.

$f_1(\beta X) = f_{10}(X)f_{11}(X)$, $f_{10}(X) = \mathrm{GCD}(f_1(\beta X), X^{(p-1)/4} - 1)$.

etc.



Dealing with powers

Use **FFT-like recursivity**.

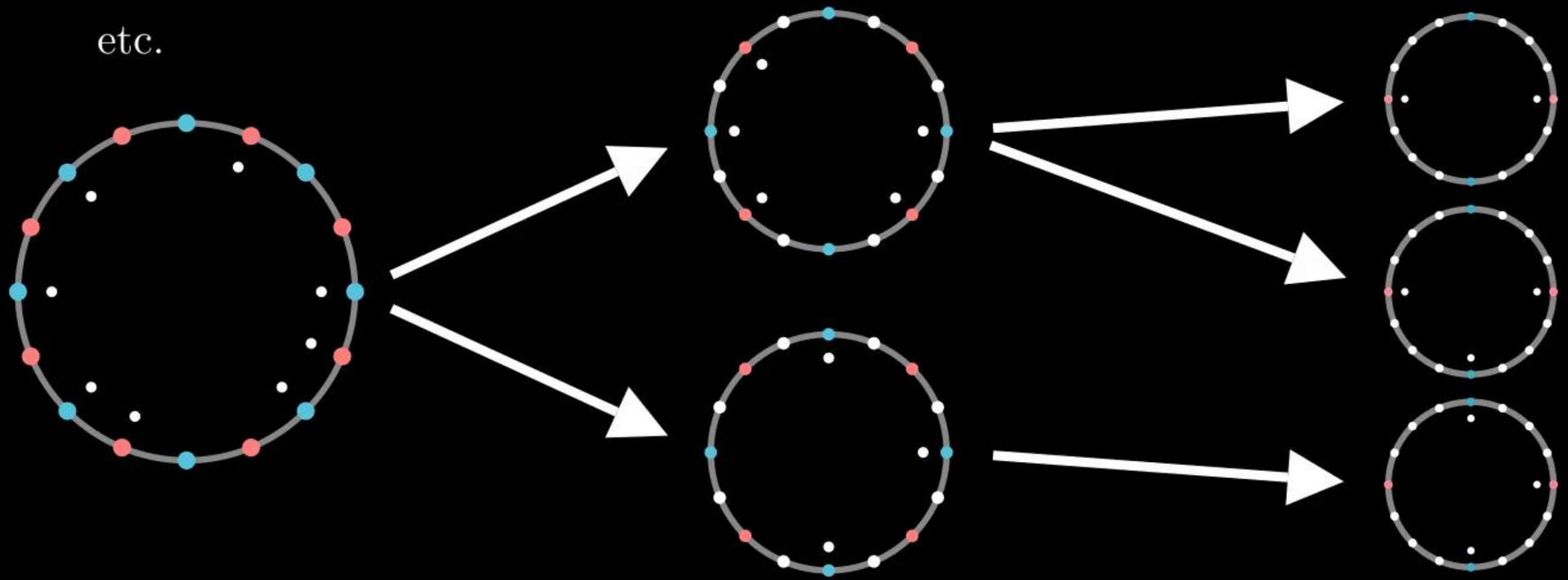
Example: $p = 17$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/2^4\mathbb{Z}$, β primitive element.

$f(X) = f_0(X)f_1(X)$, $f_0(X) = \mathrm{GCD}(X^{(p-1)/2} - 1, f(X))$.

Then **recurse**: $f_0(X) = f_{00}(X)f_{01}(X)$, $f_{00}(X) = \mathrm{GCD}(f_0(X), X^{(p-1)/4} - 1)$.

$f_1(\beta X) = f_{10}(X)f_{11}(X)$, $f_{10}(X) = \mathrm{GCD}(f_1(\beta X), X^{(p-1)/4} - 1)$.

etc.



A "dual" approach to Mignotte-Schnorr

Mapping roots to **subgroups** by low-degree maps.

Example: $\mathbb{F}_{17}^{\times} \simeq \mathbb{Z}/16\mathbb{Z} \rhd \mathbb{Z}/8\mathbb{Z} \rhd \mathbb{Z}/4\mathbb{Z} \rhd \mathbb{Z}/2\mathbb{Z}$.

Use the map $x \mapsto x^2$ on the roots $\rightsquigarrow$ **Graeffe transform**.

$f_{i+1}(X) = \mathrm{Res}_T(f_i(T), X - T^2)$.

$\rightsquigarrow$ Grenet/van der Hoeven/Lecerf'15, Monagan/van der Hoeven'21.

Complexity: $(\sqrt{S_1(q-1)}\deg(f)(\log q)^2)^{1+\varepsilon}$.

Elliptic curve analogs: Ronyai'92 (multiplication maps), Davenport/Petit/Pring'17 (isogenies).

Main difficulty: **going back** to the original roots.

$\rightsquigarrow$ **Tangent Graeffe transform**.

$\rightsquigarrow$ **Galois techniques** for elliptic curves.

Using elliptic curves in Mignotte-Schnorr algorithm

Goal: A deterministic root-finding algorithm that do not require smoothness assumptions on $q-1$.

Principle: replace $\mathbb{F}_q^\times$ by the **group of rational points** of an elliptic curve.

Step 1 (precomputation): Find an elliptic curve $/\mathbb{F}_q$ s.t. $|E(\mathbb{F}_q)|$ is **smooth**.

Step 2: **Lift roots** of f (implicitly) to $E(\mathbb{F}_q)$.

Step 3: Use division polynomials to **separate roots**.

Step 4: **Rotate**!

Lifting to elliptic curves (I)

Assume E is given by a **short Weierstrass equation**.

$E : Y^2 = X^3 + aX + b$, (x, y) is solution only if $x^3 + ax + b$ is a square in $\mathbb{F}_q$.

Quadratic twist: elliptic curve with equation $\alpha Y^2 = X^3 + aX + b$.

either $(x, \pm\sqrt{x^3 + aX + b})$ is solution to $Y^2 = X^3 + aX + b$, or
$(\beta x, \sqrt{(x^3 + aX + b)\beta^{-3}})$ is a solution to $Y^2 = X^3 + a\beta^{-2}X + b\beta^{-3}$.

$\rightsquigarrow$ **separate** the roots of $f(X) = f_0(X) \cdot f_1(X)$ depending on whether $x^3 + ax + b$ is a **square**!

Lifting to elliptic curves (II)

$f_0(X)$: all roots x satisfy that $h(x) = x^3 + ax + b$ is a square.

Lifting to $Y^2 = h(X) \to$ computing an **interpolating polynomial** $v(X)$ such that $v(X)^2 \equiv h(X) \bmod f_0(X)$.

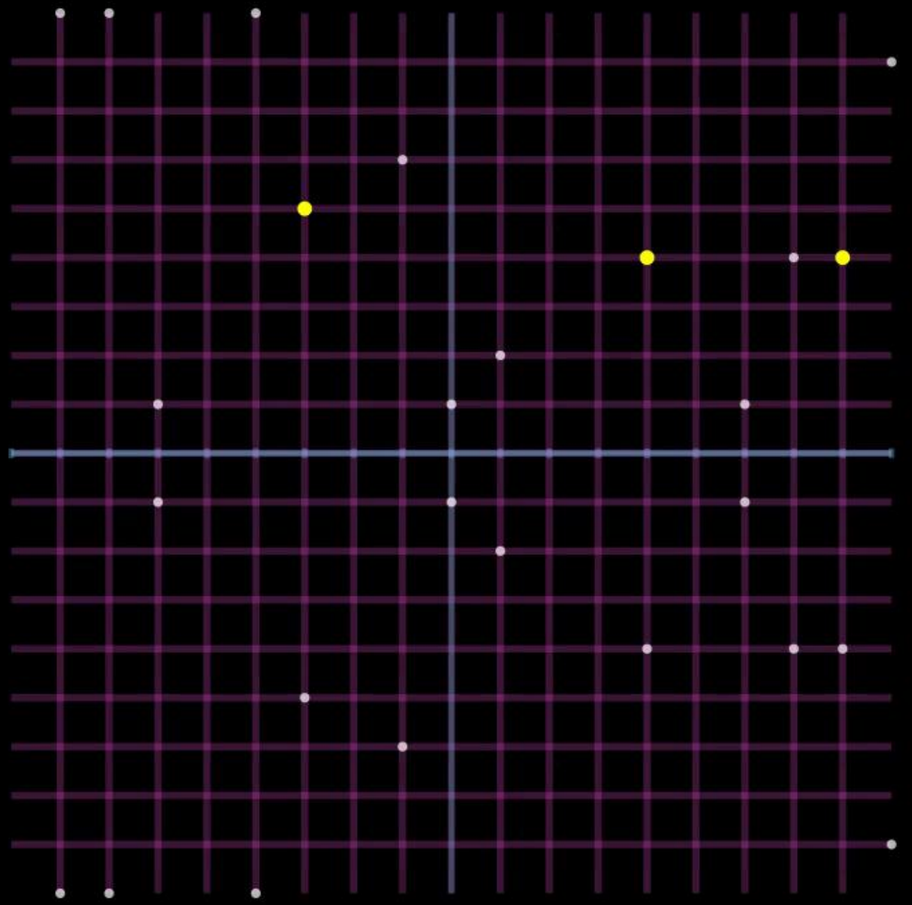
$\rightsquigarrow$ implicit form of **Tonelli-Shanks** algorithm.

Complexity: $\widetilde{O}(\log q \deg(f) + \deg(f)^2)$ ops in $\mathbb{F}_q$.

Lifting to elliptic curves (III)

$f(X) = X^4 + 8X^3 + 14X^2 + 9X + 17$

$E : Y^2 \equiv X^3 + 2X + 1 \bmod 19$



Rational parametrization:

$X^3 + 10X^2 + 15X + 1 = 0$

$Y = 9X^2 + 6X$

Find the liftable points:

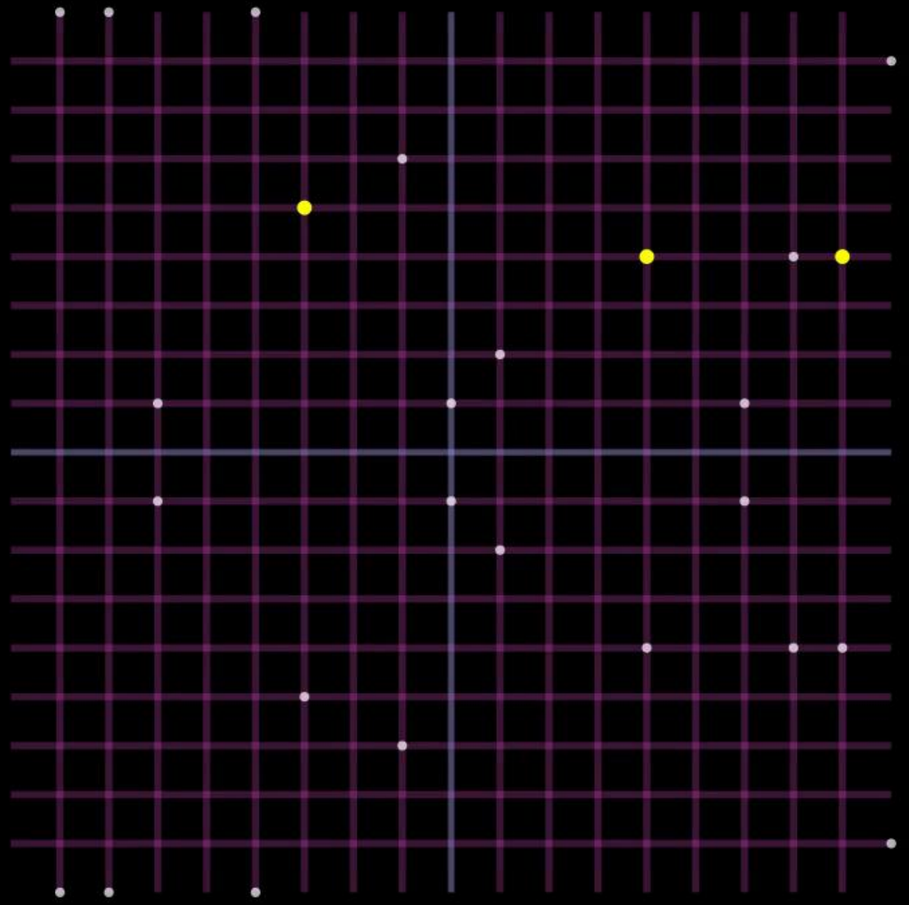
$\mathrm{GCD}(f(X), \mathrm{Res}_T(f(T), X - T(T^3 + 2T + 1)^9)) = X^3 + 10X^2 + 15X + 1$

$v(X) = (X^3 + 2X + 1)^5 \bmod X^3 + 10X^2 + 15X + 1 = 9X^2 + 6X$

Divisors and the decomposition problem

Simple divisor on E: finite sum of distinct rational points encoded by a rational parametrization $f(X) = 0, Y = v(X)$.

Decomposition problem: decompose a **simple divisor** as a sum of degree-1 divisors.



$$f(X) = X^4 + 8X^3 + 14X^2 + 9X + 17$$

$$E : Y^2 \equiv X^3 + 2X + 1 \bmod 19$$

Rational parametrization:

$$X^3 + 10X^2 + 15X + 1 = 0$$

$$Y = 9X^2 + 6X$$

$\rightsquigarrow$ set of elements in
$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ with $m_1 \mid m_2$.

Using division polynomials

GCD with division polynomials: separate $[n]$-torsion points from the rest.

Recurrence relations!

$$\psi_{2n+1}(X,Y) = \psi_{n+2}(X,Y)\psi_n(X,Y)^3 - \psi_{n-1}(X,Y)\psi_{n+1}(X,Y)^3 \text{ for } n \geq 2.$$

$$\psi_{2n}(X,Y) = \frac{\psi_n(X,Y)}{2Y}\left(\psi_{n+2}(X,Y)\psi_{n-1}(X,Y)^2 - \psi_{n-2}(X,Y)\psi_{n+1}(X,Y)^2\right) \text{ for } n \geq 3.$$

$\rightsquigarrow$ Computing $\psi_n(X,Y) \bmod f(X)$ in $\widetilde{O}(\log n \deg(f))$ ops in $\mathbb{F}_q$.

$\rightsquigarrow$ Analog of computing $X^n - 1 \bmod f(X)$ in $\widetilde{O}(\log n \deg(f))$ ops in $\mathbb{F}_q$.

Translating divisors

Goal: Given a **simple divisor** given by a **rational parametrization**, compute a rational parametrization for a **translation** by a fixed point $Q \in E(\mathbb{F}_q)$.

$\rightsquigarrow$ Use the group law on the generic point of the divisor.

$$s(X) = (v(X) - y_Q)/(X - x_Q) \bmod f(X)$$

$$x_R(X) = s(X)^2 - X - x_Q \bmod f(X)$$

$\widetilde{f}(X) =$ charpol of $x_R(X) \bmod f(X)$
$\widetilde{v}(X)$: solution of $\widetilde{v}(x_R(X))^2 = -y_Q + s(X)(x_Q - x_R(X)) \bmod f(X)$

Rational parametrization:

$$X^3 + 10X^2 + 15X + 1 = 0$$

$$Y = 9X^2 + 6X$$

Translated parametrization:

$$\widetilde{f}(X) = 0$$

$$Y = \widetilde{v}(X)$$

An elliptic curve analog of Mignotte-Schnorr's algorithm

Input: $f(X) \in \mathbb{F}_q[X]$ separable and split, an elliptic curve $E/\mathbb{F}_q$, generators for $E(\mathbb{F}_q)$ and $\widetilde{E}(\mathbb{F}_q)$, and a quadratic non-residue $\beta \in \mathbb{F}_q^\times$.

Output: roots of $f(X)$.

Complexity: $\widetilde{O}(\Xi(E)^2 \log q(n^\omega + n \log q))$ ops in $\mathbb{F}_q$ (worst-case).

Pre-preprint available at `https://inria.hal.science/hal-05509822`

A complete example in Magma

$p = 92233720368547784 87$: first prime $> 2^{63}$ such that $(p-1)/2$ is also prime.

$\rightsquigarrow$ Cyclotomic methods cannot be applied without randomization.

Exhaustive search (over $\overline{\mathbb{F}_p}$-isomorphism classes) found:

$E : Y^2 = X^3 + 10345053799823400 77 \cdot X + 45493703649291324 5$

$|E(\mathbb{F}_q)| = 2^{10} \cdot 5^2 \cdot 7 \cdot 139 \cdot 181 \cdot 251 \cdot 1787 \cdot 4561.$

$|\widetilde{E}(\mathbb{F}_q)| = 2^4 \cdot 7 \cdot 11 \cdot 29 \cdot 149 \cdot 173 \cdot 1663 \cdot 2027 \cdot 2971.$

Magma session!

Conclusion of part I

Replacing **cyclotomy** by elliptic curves in **Mignotte-Schnorr** framework.

Complexity depends on the **largest prime factor** of $|E(\mathbb{F}_q)|$ and its quadratic twist.

Practical algorithm, Magma implementation.

Question: Construct efficiently an elliptic curve with smooth order?

Tomorrow: Isogenies, Drinfeld modules, FFT, and more root-finding and factoring!

Thank you!