Elliptic curves, number theory and cryptography

Week 11, Lecture 11: Pairings and pairing-friendly curves

Aurore Guillevic

Aarhus University

Spring semester, 2022

These slides at

`https://members.loria.fr/AGuillevic/files/Enseignements/AU/lectures/lecture11A.pdf`

Outline

Materials

Washington's book: Chapter 11 Section 3
Galbraith's book: Chapter 26
https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf
Advances in Elliptic Curve Cryptography, Chapter IX by Galbraith
(pdf on Brightspace)

Outline

What is a pairing?

$(\mathbf{G}_1, +), (\mathbf{G}_2, +), (\mathbf{G}_T, \cdot)$ three cyclic groups of large prime order ℓ
Pairing: map $e : \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$

1. bilinear: $e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$, $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$
2. non-degenerate: $e(G_1, G_2) \neq 1$ for $\langle G_1 \rangle = \mathbf{G}_1$, $\langle G_2 \rangle = \mathbf{G}_2$
3. efficiently computable.

Most often used in practice:

$$e([a]P, [b]Q) = e([b]P, [a]Q) = e(P, Q)^{ab} \ .$$

$\rightsquigarrow$ Many applications in asymmetric cryptography.

Pairings in cryptography: 1993 and 2001

1993

Menezes–Okamoto–Vanstone attack on supersingular curves

2001

- Joux' tri-partite key exchange
- Boneh Frankin Identity based encryption
- Boneh Lynn Shacham short signature

Example of application: identity-based encryption

- 1984: idea of identity-based encryption formalized by Shamir
- 1999: first practical identity-based cryptosystem of Sakai-Ohgishi-Kasahara
- 2000: constructive pairings, Joux's tri-partite key-exchange
- 2001: IBE of Boneh-Franklin

Example of application: identity-based encryption

- 1984: idea of identity-based encryption formalized by Shamir
- 1999: first practical identity-based cryptosystem of Sakai-Ohgishi-Kasahara
- 2000: constructive pairings, Joux's tri-partite key-exchange
- 2001: IBE of Boneh-Franklin

Rely on one of

- Discrete Log Problem (DLP): given $g, y \in \mathbf{G}$, compute x s.t. $g^x = y$
- Diffie-Hellman Problem (DHP): given $g, x, y \in \mathbf{G}$, compute $z \in \mathbf{G}$ s.t. $z = g^{ab}$ where a, b satisfy $x = g^a$, $y = g^b$
- bilinear DLP : Given $\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_T, g_1, g_2, g_T$ and $y \in G_T$, compute $P \in \mathbf{G}_1$ s.t. $e(P, g_2) = y$, or $Q \in \mathbf{G}_2$ s.t. $e(g_1, Q) = y$ if $g_T^x = y$ then $e(g_1^x, g_2) = e(g_1, g_2^x) = g_T^x = y$
- bilinear DHP: 3-dimensional DHP
- pairing inversion problem

Pairing setting: elliptic curves

$$E/\mathbb{F}_p: \; y^2 = x^3 + ax + b, \;\; a, b \in \mathbb{F}_p, \;\; p \geq 5$$

- proposed in 1985 by Koblitz, Miller
- $E(\mathbb{F}_p)$ has an efficient group law (chord an tangent rule) $\rightarrow$ $\mathbf{G}_1$
- $\#E(\mathbb{F}_p) = p + 1 - t$, trace t: $|t| \leq 2\sqrt{p}$
- efficient group order computation (*point counting*)
- large subgroup of prime order ℓ s.t. $\ell \mid p + 1 - t$ and ℓ coprime to p
- $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ (for crypto)
- only generic attacks against DLP on well-chosen genus 1 and genus 2 curves
- optimal parameter sizes

Tate Pairing and modified Tate pairing

$\ell \mid p^n - 1$, $E[\ell] \subset E(\mathbb{F}_{p^n})$
Tate Pairing: $e: \ E(\mathbb{F}_{p^n})[\ell] \times E(\mathbb{F}_{p^n})/\ell E(\mathbb{F}_{p^n}) \to \mathbb{F}_{p^n}^*/(\mathbb{F}_{p^n}^*)^\ell$ (equivalence classes)
For cryptography,

- $\mathbf{G}_1 = E(\mathbb{F}_p)[\ell] = \{P \in E(\mathbb{F}_p), [\ell]P = \mathcal{O}\}$
- embedding degree $n > 1$ w.r.t. ℓ: smallest[1] integer n s.t. $\ell \mid p^n - 1$
  $\Leftrightarrow E[\ell] \subset E(\mathbb{F}_{p^n})$
- $\mathbf{G}_2 \subset E(\mathbb{F}_{p^n})[\ell]$
- $\mathbf{G}_1 \cap \mathbf{G}_2 = \mathcal{O}$ by construction for practical applications
- $\mathbf{G}_T = \boldsymbol{\mu}_\ell = \{u \in \mathbb{F}_{p^n}^*, \ u^\ell = 1\} \subset \mathbb{F}_{p^n}^*$

When n is small i.e. $1 \leqslant n \leqslant\sim 50$, the curve is *pairing-friendly*.
This is very rare: For a given curve, $\log n \sim \log \ell$ (Balasubramanian–Koblitz).

[1] $n = 1$ is possible too in rare circumstances

Divisors

Let E be an elliptic curve defined over a field K.

Definitions

A **divisor** is a *finite* formal sum of points $P_i \in E(K)$, $D = \sum_{i=1}^{n} a_i(P_i)$, $a_i \neq 0 \in \mathbb{Z}^\times$
Degree: $\deg(D) = \sum_{i=1}^{n} a_i \in \mathbb{Z}$: sum of the weights a_i, can be 0
Sum: $\text{sum}(D) = a_1P_1 + \ldots + a_nP_n$ the sum on E of the weigted points a_iP_i.
Support: $\text{supp}(D) = \{P_i\}_{1 \leq i \leq n}$ the set of points of D of weight $a_i \neq 0$.

Evaluating a function at a divisor

Let $D = \sum_{i=1}^{n} a_i(P_i) - (\sum_{j=1}^{m} a_j(P_j))$ where $a_i, a_j > 0$.

$$f(D) = \frac{\prod_{i=1}^{n}(f(P_i))^{a_i}}{\prod_{j=1}^{m}(f(P_j))^{a_j}}$$

Tate pairing

Let E be an elliptic curve over a finite field $\mathbb{F}_q$, let $\ell \mid \#E(\mathbb{F}_q)$, $\gcd(\ell, q) = 1$

pre-$\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_T$

With $\ell E(\mathbb{F}_q) = \{[\ell]Q \colon Q \in E(\mathbb{F}_q)\}$

- $E(\mathbb{F}_q)[\ell] = \{P \in E(\mathbb{F}_q) \colon [\ell]P = \mathcal{O}\}$ has order ℓ
- $E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) = \{P + \ell E(\mathbb{F}_q) \colon P \in E(\mathbb{F}_q)\}$ has order ℓ
- $\mathbb{F}_q^*/(\mathbb{F}_q^*)^\ell$ has order ℓ

The multiplication-by-ℓ map $[\ell]$ on $E(\mathbb{F}_q)$ has image $\ell E(\mathbb{F}_q)$ and kernel $E(\mathbb{F}_q)[\ell]$.
$E(\mathbb{F}_q)/\ell E(\mathbb{F}_q)$ is a notation for an *equivalence relation* $P, Q \in G/H \iff P - Q \in H$
$P, Q \in E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) \iff P - Q \in \ell E(\mathbb{F}_q)$
$E(\mathbb{F}_q)/\ell E(\mathbb{F}_q)$ is the quotient of $E(\mathbb{F}_q)$ by the image of $[\ell]$, and has order ℓ.

Tate Pairing

$\ell \mid p^n - 1$, $E[\ell] \subset E(\mathbb{F}_{p^n})$
$P \in E(\mathbb{F}_{p^n})[\ell]$, $Q \in E(\mathbb{F}_{p^n})/\ell E(\mathbb{F}_{p^n})$

Definition: Tate pairing

Let D_Q be a divisor such that $\mathrm{sum}(D_Q) = Q$, $\deg(D_Q) = 0$, and $P, \mathcal{O} \notin \mathrm{supp}(D_Q)$.
Let f_P be a function whose divisor is $\mathrm{Div}(f_P) = [\ell]P - [\ell]\mathcal{O}$.
One has $\mathrm{supp}(f_P) \cap \mathrm{supp}(D_Q) = \emptyset$.

$$e_{\mathrm{Tate}}(P, Q) = f_P(D_Q) \in \mathbb{F}_{p^n}^*/(\mathbb{F}_{p^n}^*)^\ell$$

Example: choose some point $R \neq \mathcal{O}, P$ s.t. $R + Q \neq \mathcal{O}, P$ and set
$D_Q = (Q + R) - (R)$, then

$$e_{\mathrm{Tate}}(P, Q) = \frac{f_P(Q + R)}{f_P(R)} \ .$$

Tate pairing

From its definition to its efficient implementation

- John Tate, 1958
- Stephen Lichtenbaum, 1969
- Victor Miller, 1986, Miller algorithm for f_P
- Frey–Rück, 1994: the MOV attack with the Tate pairing instead of the Weil pairing
- Harasawa, Shikata, Suzuki, Imai, 1999, 161467 s (112 days)
  163-bit supersingular curve, $\mathbf{G}_T \subset \mathbb{F}_{p^2}$ of 326 bits.
- Antoine Joux, 2000: how to compute Miller algorithm more efficiently
  1 s on a supersingular 528-bit curve, $\mathbf{G}_T \subset \mathbb{F}_{p^2}$ of 1055 bits)

Modified Tate pairing

Avoid equivalence classes:
need one representative of the equivalence class instead.
Ensure the pairing is non-degenerate: $\mathbf{G}_1 \cap \mathbf{G}_2 = \mathcal{O}$

$$E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}\ell\mathbb{Z} = \mathbf{G}_1 \times \mathbf{G}_2$$

Let $P \in \mathbf{G}_1 = E(\mathbb{F}_p)[\ell], Q \in \mathbf{G}_2 \subset E(\mathbb{F}_{p^n})[\ell]$.
Let $f_{\ell,P}$ the function s. t. $\mathrm{Div}(f_{\ell,P}) = \ell(P) - \ell(\mathcal{O})$.
Modified Tate pairing (in cryptography):

$$\begin{array}{rccccc} & E(\mathbb{F}_p)[\ell] & & E(\mathbb{F}_{p^n})[\ell] & & \\ & \wr\| & & \cup & & \\ e_{\mathsf{Tate}}: & \mathbf{G}_1 & \times & \mathbf{G}_2 & \to & \boldsymbol{\mu}_\ell \subset \mathbb{F}_{p^n}^* \\ & (P, & & Q) & \mapsto & (f_{\ell,P}(Q))^{\frac{p^n-1}{\ell}} \end{array}$$

Modified Tate pairing

Final exponentiation to avoid equivalence classes in $\mathbb{F}_{p^n}^*$

$x \mapsto x^{(p^n-1)/\ell}$ clears the cofactors in $(\mathbb{F}_{p^n}^*)^\ell$.

Consider the ℓ-powering $x \mapsto x^\ell$ as an endomorphism of $\mathbb{F}_{p^n}^*$

- $(\cdot)^\ell$ has image $(\mathbb{F}_{p^n}^*)^\ell$ and kernel $\mu_\ell = \{x \in \mathbb{F}_{p^n}^* : x^\ell = 1\}$
- $x_1 \equiv x_2 \in \mathbb{F}_{p^n}^*/(\mathbb{F}_{p^n}^*)^\ell \iff x_1 \cdot x_2^{-1} \in (\mathbb{F}_{p^n}^*)^\ell \iff (x_1/x_2)^{(p^n-1)/\ell} = 1$

Replace Divisor D_Q by point Q in the evaluation

Replace $f_{\ell,P}(Q+R)/f_{\ell,P}(R)$ by $(f_{\ell,P}(Q))^{\frac{p^n-1}{\ell}}$
Lemma 26.3.11 in Galbraith's book

Miller algorithm

Principal divisor

A divisor D is **principal** $\iff$ $\deg(D) = 0$ and $\text{sum}(D) = \mathcal{O}$.
In that case there exists a function f_D whose divisor is D.

Miller function

The Tate pairing requires a function f_P of divisor $\ell(P) - \ell(\mathcal{O})$.
$D = \ell(P) - \ell(\mathcal{O})$ is principal $\implies$ f_P exists.
Define the Miller function $f_{i,P}$ to have divisor

$$D_{i,P} = \text{Div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O})$$

- $\deg(D_{i,P}) = 0$
- $\text{sum}(D_{i,P}) = 0$
- $D_{i,P}$ is principal
- $D_{\ell,P} = \ell(P) - \ell(\mathcal{O}) = \text{Div}(f_P)$

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{\ell})$)

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \ : \ E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{\ell})$)
- discrete logarithm computation in $\mathbb{F}_{p^n}^*$: **easier, subexponential** $\rightarrow$ take a large enough field

Outline

First ordinary pairing-friendly curves: MNT

Miyaji, Nakabayashi, Takano, $\#E(\mathbb{F}_p) = p(u) + 1 - t(u)$, $r(u) \mid \#E(\mathbb{F}_p)$

k	param	MNT
3	$t(u)$	$-1 \pm 6u$
	$r(u)$	$12u^2 \mp 6u + 1$
	$p(u)$	$12u^2 - 1$
	Dy^2	$12u^2 \pm 12u - 5$
4	$t(u)$	$-u,\ u + 1$
	$r(u)$	$u^2 + 2u + 2,\ u^2 + 1$
	$p(u)$	$u^2 + u + 1$
	Dy^2	$3u^2 + 4u + 4$
6	$t(u)$	$1 \pm 2u$
	$r(u)$	$4u^2 \mp 2u + 1$
	$p(u)$	$4u^2 + 1$
	Dy^2	$12u^2 - 4u + 3$

CODA: $k = 6$, 753 bits, ≈ 137 bits of security, $D = -241873351932854907$, seed $u =$

`0xaa3a58eb20d1fec36e5e772ee6d3ff28c296465f137300399db8a5521e18d33581a262716214583d3b89820dd0c000`

Very popular pairing-friendly curves: Barreto-Naehrig (BN)

$$E_{BN}: \ y^2 = x^3 + b, \ p \equiv 1 \bmod 3, \ D = -3 \text{ (ordinary)}$$

$$\begin{aligned} p &= 36x^4 + 36x^3 + 24x^2 + 6x + 1 \\ t &= 6x^2 + 1 \\ \ell &= p + 1 - t = 36x^4 + 36x^3 + 18x^2 + 6x + 1 \\ t^2 - 4p &= -3(6x^2 + 4x + 1)^2 \ \rightarrow \text{ no CM method needed} \end{aligned}$$

Comes from the Aurifeuillean factorization of Φ_{12} :
$\Phi_{12}(6x^2) = \ell(x)\ell(-x)$

Security level	$\log_2 \ell$	finite field	n	$\log_2 p$	$\deg P, \ p = P(u)$	ρ
102	256	3072	12	256	4	1
123	384	4608	12	384	4	1
132	448	5376	12	448	4	1

BLS12

Barreto, Lynn, Scott method.
Becomes more and more popular, replacing BN curves

$$E_{BLS}: \ y^2 = x^3 + b, \ p \equiv 1 \bmod 3, \ D = -3 \text{ (ordinary)}$$

$$\begin{aligned} p &= (u-1)^2/3(u^4 - u^2 + 1) + u \\ t &= u + 1 \\ r &= (u^4 - u^2 + 1) = \Phi_{12}(u) \\ p + 1 - t &= (u-1)^2/3(u^4 - u^2 + 1) \\ t^2 - 4p &= -3y(u)^2 \ \rightarrow \text{ no CM method needed} \end{aligned}$$

BLS12-381 with seed -0xd201000000010000

The Cocks–Pinch method

Three equations:

$$\begin{aligned} \ell &\mid p+1-t && (1)\\ \ell &\mid \Phi_n(p) && (2)\\ t^2-4p &= -Dy^2 && (3) \end{aligned}$$

From (1), $p \equiv t-1 \bmod \ell$
From (2) and (1), $\ell \mid \Phi_n(t-1) \iff t-1 = \zeta_n \bmod \ell$
where ζ_n is a primitive n-th root of unity modulo ℓ, ζ_n exists $\iff \ell \equiv 1 \bmod n$.

$$\boldsymbol{t = \zeta_n + 1 \bmod \ell}$$

From (3) and (1), with $p = (t^2+Dy^2)/4$,

$$p+1-t = \frac{1}{4}\left(t^2-4t+4+Dy^2\right) = \frac{1}{4}\left((t-2)^2+Dy^2\right)$$

Because $\ell \mid p+1-t$, assuming ℓ odd,

$$(t-2)^2+Dy^2 = 0 \bmod \ell \implies \boldsymbol{y = \frac{t-2}{\sqrt{-D}} \bmod \ell}$$

The Cocks–Pinch method

Algorithm 1: Cocks–Pinch method
Input: A positive integer n and a positive square-free integer D
Output: $E/\mathbb{F}_q$ with an order-ℓ subgroup and embedding degree n

1 Choose a prime ℓ such that n divides $\ell - 1$ and $-D$ is a square modulo ℓ
2 Compute $t = 1 + x^{(\ell-1)/n}$ for x a generator of $(\mathbb{Z}/\ell\mathbb{Z})^\times$, $t - 1 \equiv \zeta_n \bmod \ell$
3 Compute $y = (t-2)/\sqrt{-D} \bmod \ell$
4 Lift t and y in $\mathbb{Z}$
5 Compute $q = (t^2 + Dy^2)/4$ in $\mathbb{Q}$
6 **if** *q is a prime integer* **then**
7 | Use CM method ($D < 10^{20}$) to get the coefficients of $E/\mathbb{F}_q$ with order-ℓ subgroup
8 **else**
9 | Go back to 1
10 **return** *$E/\mathbb{F}_q$ with an order-ℓ subgroup and embedding degree n*

The Cocks–Pinch method

Drawback: $\log|t|, \log|y| \approx \log \ell \implies \log p \approx 2 \log \ell$
rho-value:

$$\rho = \frac{\log p}{\log \ell} \approx 2$$

The optimal would be $\rho = 1$ for a prime-order curve, $\ell = p + 1 - t$.

How to compute primitive n-th roots of unity:

Input: prime ℓ, integer $n > 0$, $\ell \equiv 1 \bmod n$
Output: $\zeta_n \bmod \ell$

1 $z \leftarrow \texttt{random}(\ell)$
2 $z \leftarrow z^{(\ell-1)/n}$
3 **while** $\Phi_n(z) \neq 0 \bmod \ell$ *(or:* $z^d = 1 \bmod \ell$ *for some* $d \mid n$, $1 \leq d < n$*)* **do**
4 $\quad z \leftarrow \texttt{random}(\ell)$
5 $\quad z \leftarrow z^{(\ell-1)/n}$
6 **return** z

The CM method (Complex Multiplication)

Hard problem to compute the curve coefficients (a, b) given a prime p and a trace t.
The other way: given p and (a, b) in $E/\mathbb{F}_p$: : $y^2 = x^3 + ax + b$ and computing the order $\#E(\mathbb{F}_p)$ is done with the SEA algorithm (Schroof–Elkies–Atkin).
The *CM* method computes a j-invariant, given p, t.

1. Compute the discriminant $-D$ as the square-free part in $t^2 - 4p = -Dy^2$
2. If $D \equiv 1, 2 \bmod 4$, $D \leftarrow 4D$
3. Compute a Hilbert Class Polynomial $H_{-D}(X)$ mod p with Sutherland's software `classpoly` at `https://math.mit.edu/~drew/`
4. Compute a root j_0 of $H_{-D}(X)$ mod p
5. Set $E\colon y^2 = x^3 + \frac{3j_0}{1728-j_0}x + \frac{2j_0}{1728-j_0}$

The CM method

For specific (small) values of $-D$, the j-invariants are known:

- $-D = -3$, $j = 0$
- $-D = -4$, $j = 1728$
- $-D = -8$, $j = 8000$
- $-D = -7$, $j = -3375$
- $-D = -11$, $j = -32768$
- $-D = -19$, $j = -884736$
- $-D = -43$, $j = -884736000$
- $-D = -67$, $j = -147197952000$
- $-D = -163$, $j = -262537412640768000$

The Brezing–Weng method: The Cocks–Pinch method with polynomials

Start with $r(x)$ an irreducible polynomial s.t. the number field $K = \mathbb{Q}[x]/(r(x))$ contains ζ_n and $\sqrt{-D}$

Algorithm 2: Idea of Barreto–Lynn–Scott and Brezing–Weng methods
Input: A positive integer n and a positive square-free integer D
Output: Polynomials $p(x), r(x), t(x)$ s.t. $t^2(x) - 4p(x) = -Dy^2(x)$,
$r(x) \mid p(x) + 1 - t(x)$, $r(x) \mid \Phi_n(p(x))$

1 Choose an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ with positive leading coefficient such that $\sqrt{-D}$ and $\zeta_n \in K = \mathbb{Q}[x]/(r(x))$
2 Choose $t(x) \in \mathbb{Q}[x]$ a polynomial representing $\zeta_n + 1$ in K
3 Set $y(x) \in \mathbb{Q}[x]$ a polynomial mapping to $(\zeta_n - 1)/\sqrt{-D}$ in K
4 Compute $p(x) = (t^2(x) + Dy^2(x))/4$ in $\mathbb{Q}[x]$
5 If $p(x)$ does not represent primes go back to 1 or 2
6 **return** $p(x), r(x), t(x)$

The BLS family

If $3 \mid n$, then $\sqrt{-3} \in K = \mathbb{Q}[x]/(\Phi_n(x))$

- $n = 3$: $\zeta_3 = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$, $\Phi_3 = x^2 + x + 1$
  For $n \equiv 3 \bmod 6$, $\zeta_3 = x^{n/3} \bmod \Phi_n(x)$
  $\sqrt{-3} = 2x^{n/3} + 1$ and $1/\sqrt{-3} = \sqrt{-3}/3 = (2x^{n/3} + 1)/3$
- $n = 6$: $\zeta_6 = \frac{11+\sqrt{-3}}{2} \in \mathbb{C}$, $\Phi_6 = x^2 - x + 1$
  For $n \equiv 0 \bmod 6$, $\zeta_6 = x^{n/6} \bmod \Phi_n(x)$
  $\sqrt{-3} = 2x^{n/6} - 1$ and $1/\sqrt{-3} = \sqrt{-3}/3 = (2x^{n/6} - 1)/3$

Given n multiple of 3,

1. $r(x) \leftarrow \Phi_n(x)$
2. $t(x) \leftarrow x + 1$
3. $y(x) \leftarrow (x - 1)/\sqrt{-3}$
   - $y(x) = (x - 1)(2x^{n/3} + 1)/3$ if $n \equiv 3 \bmod 6$
   - $y(x) = (x - 1)(2x^{n/6} - 1)/3$ if $n \equiv 0 \bmod 6$
4. $p(x) = (t^2(x) + 3y^2(x))/4$