Schertz, Construction of elliptic curves over finite fields with prime cardinality

$$K = \mathbb{Q}(\sqrt{d}), \quad d = d_K < 0, \qquad d \equiv 5 \bmod 8 \qquad (\text{ and } 3 \nmid d \text{ for simplicity})$$
$$\mathfrak{O} = [\alpha, 1] = \qquad \text{maximal order in } K, \quad \alpha = \frac{3+\sqrt{d}}{2},$$

Weierstraß-model belonging to the lattice $\mathfrak{O}$:

$$\boxed{E: \quad y^2 = x^3 + a_4 x + a_6,} \qquad a_4 = -\tfrac{1}{4\cdot 12}\sqrt[3]{j(\alpha)}, \quad a_6 = -\tfrac{1}{4\cdot 6^3}\sqrt{j(\alpha) - 12^3}.$$

with the modular invariant $j(\alpha)$ of $\mathfrak{O}$ defined over Ω, the Hilbert class field over K with uniformizing functions

$$\xi \mapsto (x(\xi) : y(\xi) : 1) \;=\; \left(\frac{\wp(\xi|\mathfrak{O})}{\sqrt[6]{\Delta(\mathfrak{O})}} : \frac{\wp'(\xi|\mathfrak{O})}{2\sqrt[4]{\Delta(\mathfrak{O})}} : 1\right). \qquad \left(\Delta(\mathfrak{O}) = (2\pi)^{12}\eta(\alpha)^{24}\right)$$

AIM: Reduction of E modulo a suitable prime ideal with a nice cardinality:

Choose a prime number p, $p = \pi\overline{\pi}$ in K, $p \nmid 6d$.

Construction of an elliptic curve over $\mathbb{F}_p$ from the $(\pi-1)$-torsion points of $E(\mathbb{Q}^c)$:

$$\begin{array}{lll} M & = \Omega(E[\pi-1]) & \mathfrak{P} \\ | & & \\ \Omega & & \mathfrak{P}_0 \qquad deg(\mathfrak{P}_0) = 1 \\ | & & \\ K & & (\pi) \end{array}$$

AIM: normalization of

$$\pi = u\alpha + v, \qquad u, v \in \mathbb{Z},$$

such that

(1) $$\boxed{deg(\mathfrak{P}) = 1} \text{ for all } \mathfrak{P} \text{ over } (\pi).$$

Then by the Riemann hypothesis $E(\mathfrak{O}_M/\mathfrak{P}) = E(\mathbb{F}_p)$ is an elliptic curve over $\mathbb{F}_p$ having the cardinality

$$|E(\mathbb{F}_p)| = |E[\pi-1]| = norm(\pi-1) = p + 1 - tr(\pi).$$

(1) $\iff$ $x(\xi)^{\sigma(\pi)} = x(\xi), \quad y(\xi)^{\sigma(\pi)} = y(\xi) \quad$ for all $\xi \in \frac{1}{\pi-1}\mathfrak{O} \setminus \mathfrak{O}$

By reciprocity law of complex multiplication we obtain

$$x(\xi)^{\sigma(\pi)} = x(\xi), \quad y(\xi)^{\sigma(\pi)} = \epsilon\, y(\xi), \quad \epsilon = \left\{ \begin{array}{ll} \zeta_4^{(-uvn+1)p-uv-v}, & \text{if} \quad 2 \nmid v, \\ \zeta_4^{sp+p-u+1}, & \text{if} \quad 2|v, \end{array} \right\} = \pm 1.$$

with $n = norm(\alpha),\ s = tr(\alpha)$. So by replacing π by $-\pi$ we can achieve $\epsilon = 1$ thereby obtaining (1).

AIM: Finding $\overline{a}_4, \quad \overline{a}_6$

step 1: compute $\quad m(X) = \prod_{i=1}^{h} (X - j(\alpha_i)) \in \mathbb{Z}[X]$

step 2: factor $\quad m(X) \equiv (X - \overline{j}_1) \cdot \ldots \cdot (X - \overline{j}_h) \bmod p$

Hierein $\overline{j}_1, ..., \overline{j}_h$ are residues mod all prime ideals $\mathfrak{P}_i$ of M over (π).

For fixed i let $\overline{A}_4, \overline{A}_6$ be solutions in $\mathbb{F}_p$ of $\overline{A}_4^3 = -\left(\frac{1}{4\cdot 12}\right)^3 \overline{j}_i, \quad \overline{A_6}^2 = \left(\frac{1}{4\cdot 6^3}\right)^2 (\overline{j}_i - 12^3)$

Then the reduced curve mod $\mathfrak{P}_i$ is one of the following

$$E_{\rho,\nu} : y^2 = x^3 + \rho\overline{A}_2 x + (-1)^\nu \overline{A}_6, \qquad \rho^3 = 1, \nu = 0, 1$$

For $\underline{p \equiv 1 \bmod 4}$ all these curves are isomorphic and have the cardinality

$$|E_{\rho,\nu}(\mathbb{F}_p)| = p + 1 - tr(\pi).$$

For $\underline{p \equiv 3 \bmod 4}$ we only have

$$|E_{\rho,\nu}(\mathbb{F}_p)| = |E_{\rho',\nu}| \quad \text{for all } \rho, \rho',$$

and

$$\{|E_{\rho,0}(\mathbb{F}_p)|, |E_{\rho,1}(\mathbb{F}_p)|\} = \{p + 1 - tr(\pi),\ p + 1 + tr(\pi)\}$$

and we have to decide the cardinality of $\underline{\text{one}}$ curve by counting points.

Example: $d = -2555$, class number $=12$

$p = 131248351609 = \pi\overline{\pi}$, $\pi = -11145\alpha - 211112$, $\epsilon(\pi) = 1$

equation for $j(\mathfrak{O})$:
$m(X) =$
$X^{12} + 92287362237154168700999050806204357857610098291713635485724483584000\, X^{11}$
$-89851012864826355015716506949944697418703763454997214899764384840222488902423723609423872000\, X^{10}$
$+87478982207921712797007670980733964800197531257211079770749705906493415379196119729805474726744514221540638720000000\, X^{9}$
$+ 54322697178077064858246841761468296129646322472622348724331797399278862246909836539357414059009613587593911818414559592448000000\, X^{8}$
$+ 38175257376243289402415940422528689271032175376997006129044209067072947823225650466899907613503336773514360021389955115995145175040000000\, X^{7}$
$- 33314867270876789438839274214721289511837265066512888699186816206902582469735426828500835995108964178960488228970839555704922445963067392000000000\, X^{6}$
$+ 81938282987207301740905440123123291888100647933649689908693369495936834654379304056329812866014742915865258335293990643439414649986128680058880000000000000\, X^{5}$
$- 36674947257297422276734520578332006959112378982823162604842902217855570149122835435685163793897229046312061466028133637326058351884318809016762368000000000000000\, X^{4}$
$+ 14357087640371043150160203938241984186535248176428749836840258501306588289005767987949956097504081331820042895766598823663074127388602566799288958976000000000000000000\, X^{3}$
$- 50144896540683302591477508580714255774643123539055651823851601418404839765662885092092714984119250426106792101742328810974977933621063375632668957868032000000000000000000\, X^{2}$
$+ 80626844261542580436978911659411578980645813370825181898027886101682866954347404962975668596137998979275916462035385647498001004251682589485467669889024000000000000000000\, X$
$-12361712498447472613758544043383329658667734086100920483853028268004402061979840936498324661696256906338519756906123772976249059473530419426118471249821696000000000000000000000$

factorization mod p=131248351609:

$\overline{j}_1 = 41742721008, \overline{j}_2 = 2114130094, \overline{j}_3 = 125455538846, \overline{j}_4 = 130335548897,$
$\overline{j}_5 = 122669249072, \overline{j}_6 = 68825531373, \overline{j}_7 = 82419947698, \overline{j}_8 = 30416066768,$
$\overline{j}_9 = 100557227810, \overline{j}_{10} = 81229135406, \overline{j}_{11} = 6524603739, \overline{j}_{12} = 95044570395$

Elliptic curves obtained from $\overline{j}_1 = 41742721008$:

$$E(\mathbb{F}_{131248351609}): \qquad y^2 = x^3 + a_4 x + a_6,$$

$$a_4 = 115595064444, 109069982605, 37831656169$$
$$a_6 = \pm 33300320683$$

All 6 elliptic curves have cardinality

$$\#E(\mathbb{F}_{131248351609}) = p + 1 - tr(\pi) = 131248807279 \qquad (PRIME)$$

Using Weber's functions instead of j:

$$f(\omega) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)},$$

relation with j:

$$j(\alpha) = -\frac{\left(\left(\frac{\sqrt{2}}{f(\sqrt{d})}\right)^{24} + 16\right)^3}{\left(\frac{\sqrt{2}}{f(\sqrt{d})}\right)^{24}}$$

equation for $f(\sqrt{d}), \quad d = -2555$:

$X^{36} - 740\,X^{35} - 5576\,X^{34} + 38864\,X^{33} + 217388\,X^{32} - 1641560\,X^{31} + 2427368\,X^{30} + 5721552\,X^{29} - 26437184\,X^{28} + 34413984\,X^{27} + 18585616\,X^{26} - 141474752\,X^{25} + 241459440\,X^{24} - 160215168\,X^{23} - 166796160\,X^{22} + 583142528\,X^{21} - 783022976\,X^{20} + 512563456\,X^{19} + 237373184\,X^{18} - 1107810304\,X^{17} + 1465448960\,X^{16} - 895317504\,X^{15} - 233253376\,X^{14} + 1030334464\,X^{13} - 1072218368\,X^{12} + 632040448\,X^{11} - 71012352\,X^{10} - 339048448\,X^9 + 389827584\,X^8 - 192313344\,X^7 + 41510912\,X^6 - 16437248\,X^5 + 20930560\,X^4 - 11321344\,X^3 + 2527232\,X^2 - 180224\,X + 4096$

Remark: $degree = 3h$

Using a double η-quotient instead of j:

$$g(\omega) = \frac{\eta\left(\frac{\omega}{5}\right)\eta\left(\frac{\omega}{7}\right)}{\eta\left(\frac{\omega}{35}\right)\eta\left(\omega\right)}$$

relation to j: $\Phi(g, j) = 0$,

$$\begin{aligned}
\Phi(g,j) \;=\; & X^{48} + (-j + 708)X^{47} + (35j + 171402)X^{46} \\
& +(-525j + 15185504)X^{45} + (4340j + 248865015)X^{44} \\
& +(-20825j + 1763984952)X^{43} + (52507j + 6992359702)X^{42} \\
& +(-22260j + 19325688804)X^{41} + (-243035j + 42055238451)X^{40} \\
& +(596085j + 70108209360)X^{39} + (-272090j + 108345969504)X^{38} \\
& +(-671132j + 121198179480)X^{37} + (969290j + 155029457048)X^{36} \\
& +(-1612065j + 97918126080)X^{35} + (2493785j + 141722714700)X^{34} \\
& +(647290j - 1509796288)X^{33} + (-3217739j + 108236157813)X^{32} \\
& +(3033590j - 93954247716)X^{31} + (-5781615j + 91135898154)X^{30} \\
& +(1744085j - 108382009680)X^{29} + (1645840j + 66862445601)X^{28} \\
& +(-2260650j - 66642524048)X^{27} + (6807810j + 38019611082)X^{26} \\
& +(-2737140j - 28638526644)X^{25} + (2182740j + 17438539150)X^{24} \\
& +(-125335j - 8820058716)X^{23} + (-1729889j + 5404139562)X^{22} \\
& +(1024275j - 1967888032)X^{21} + (-1121960j + 1183191681)X^{20} \\
& +(395675j - 370697040)X^{19} + (-54915j + 103145994)X^{18} \\
& +(15582j - 42145404)X^{17} + (34755j - 15703947)X^{16} \\
& +(-6475j - 3186512)X^{15} + (1120j - 4585140)X^{14} \\
& +(-176j + 1313040)X^{13} + (j^2 - 1486j - 38632)X^{12} \\
& +(-7j + 399000)X^{11} + (-19j + 211104)X^{10} + (-9j + 6771)X^{8} \\
& +(8j - 6084)X^{7} + (7j - 5258)X^{6} + (j - 792)X^{5} - 105X^{4} + 16X^{3} \\
& +42X^{2} + 12X + 1
\end{aligned}$$

Remark: $deg_j(\Phi) = 2$.

Equation for $g(\alpha)$:

$$X^6 + 86X^5 - 574X^4 + 1972X^3 + 574X^2 + 86X - 1.$$

Remark: $deg = \frac{h}{2}$

Enge's implementation

$d = -1170195$, $h = 208$
$p = 156927543384665904058634809165896123325184743505585089096 9$

Time for finding an elliptic curve over $\mathbb{F}_p$ with prime cardinality

$$\#E(\mathbb{F}_p) = 156927543384665904058634809173818939576611149117441813067 9$$

function	time
using j	∞
using Weber's function	46.12 s
using double η-quotients	0.78 s $\approx \frac{46.12}{59} s$

$$\boxed{\frac{Weber}{double \quad eta} \approx 59}$$

$d = -88787595$, $h = 1896$
$p = 156927543384665904058634809118359225816626320353986911889 1$

Time for finding an elliptic curve over $\mathbb{F}_p$ with prime cardinality

$$\#E(\mathbb{F}_p) = 156927543384665904058634809126282042068052725965843635858 9$$

function	time
using j	∞
using Weber's function	4220.76s
using double η-quotients	16.29 s $\approx \frac{4220.76}{259} s$

$$\boxed{\frac{Weber}{double \quad eta} \approx 259}$$