
Designs, Codes and Cryptography, 36, 245–261, 2005

Hyperelliptic Curves With Compact Parameters

EZRA BROWN brown@math.vt.edu
Virginia Tech, Blacksburg, VA 24061-0123, USA

BRUCE T. MYERS
Wheaton College, Wheaton, IL 60187, USA

JEROME A. SOLINAS
National Security Agency, Ft. Meade, MD 20755-6511, USA

Communicated by: A. Menezes

Received June 24, 2003; Revised December 30, 2003; Accepted February 4, 2004

Abstract. We present a family of hyperelliptic curves whose Jacobians are suitable for cryptographic use, and whose parameters can be specified in a highly efficient way. This is done via complex multiplication and identity-based parameters. We also present some novel computational shortcuts for these families.

Keywords: hyperelliptic curves, certificates, public-key cryptography, complex multiplication

AMS Classification: 14G50, 11G20, 14K22, 14H45

1. Introduction

In our earlier paper [1] we introduced the notion of elliptic curves with compact parameters. These are fixed-coefficient elliptic curves having complex multiplication over the rationals, but implemented as curves defined over a finite field $\mathbb{F}_p$, where each user can specify his own prime p. Finding an appropriate prime p is a simple search process, beginning with a random start value. We suggested that this random start value be determined by the hash output of an ID string chosen by the user. A small integer – the offset – determines how far past the random start value the user searched before finding p. To enable communication, the user need only transmit the domain ID and (optionally) the offset to another user. This represents a savings of bandwidth when compared to transmission of the typical set of elliptic curve parameters (see [1] for a fuller discussion).

Compact elliptic curves are easy to use because they come equipped with convenient base points, independent of the prime p. Furthermore, the complex-multiplication feature, which enables the order of the curve to be quickly computed, also enables the use of an ingenious speedup to scalar multiplication, as presented in [3].

In recent years, hyperelliptic curves (particularly of genus 2) have emerged as a viable alternative to elliptic curves. (See, e.g. [7].) Since genus 2 curves achieve the same security level using smaller base fields, they can sometimes be preferable to

elliptic curves when used on embedded processors where memory and speed are constrained.

The mathematics of compact elliptic curves generalizes to the genus-2 case. The present paper explores this generalization. Our family of compact Jacobians is based on the hyperelliptic curve $H: y^2 = x^5 + 8$, together with the base point $(1, 3)$ embedded in the Jacobian of H. As a curve defined over the rationals, $H/\mathbb{Q}$ has genus 2 and admits complex multiplication by the 5th roots of unity. For p a prime of the form $p \equiv 1 \pmod{10}$ we consider the curve $H/\mathbb{F}_p$, that is, the reduction of H to $\mathbb{F}_p$. Since 5 divides the order of $\mathbb{F}_p^\times$, complex multiplication descends to $H/\mathbb{F}_p$. This means we can quickly compute the order $\#H(\mathbb{F}_p)$ of the set of $\mathbb{F}_p$-rational points of $H/\mathbb{F}_p$ and the order $\#\mathcal{J}_H(\mathbb{F}_p)$ of the group of $\mathbb{F}_p$-rational points in the Jacobian of H, using the technique of Jacobi sums. The user of this cryptosystem will presumably want to work in a Jacobian group of prime order, so several primes p will have to be tried until the associated Jacobian group order $\#\mathcal{J}_H(\mathbb{F}_p)$ is prime. In this case, the base point $(1, 3)$ is a generator of the group $\mathcal{J}_H(\mathbb{F}_p)$.

The 'compact' aspects of compact elliptic curve cryptosystems – low-bandwidth transmission of domain ID and offset, plus quick extraction of system parameters – carry over to compact Jacobians. In addition, the speedup of Gallant et al. [3] generalizes to scalar multiplication in the Jacobian of H.

2. A Cyclotomic Number Ring

We introduce notation which will remain fixed throughout the paper. Let

$$K = \mathbb{Q}(\nu),$$

where $\nu = e^{2\pi i/5}$ is a primitive 5th root of unity. Thus, ν satisfies the cyclotomic polynomial $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = 0$. We will reserve the symbol ζ for the particular 10th root of unity

$$\zeta = -\nu^3 = e^{2\pi i/10}.$$

Let $\mathcal{O}$ be the ring of integers of K. By well-known results on cyclotomic fields (see [12], for example), we have

$$\mathcal{O} = \mathbb{Z}[\nu] = \mathbb{Z} \oplus \mathbb{Z}\nu \oplus \mathbb{Z}\nu^2 \oplus \mathbb{Z}\nu^3.$$

$\mathcal{O}$ is a principal ideal domain, and so $\mathcal{O}$ has unique factorization of elements.

We denote by F the maximal real subfield of K, namely

$$F = \mathbb{Q}(\nu + \nu^{-1}) = \mathbb{Q}(\zeta + \zeta^{-1}).$$

Let U denote the units group of $\mathcal{O}$. There are no real embeddings and two conjugate pairs of complex embeddings of K, so by the Dirichlet Unit Theorem, the $\mathbb{Z}$-rank of U is 1. More precisely, we have

$$U \cong \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z},$$

where ζ generates the torsion part and the fundamental real unit $\zeta+\zeta^{-1}=(\sqrt{5}+1)/2$ generates the infinite cyclic part of U. (For details, see [4], p. 561–562.)

Let the Galois group of $K/\mathbb{Q}$ be $\{\sigma, \sigma^2, \sigma^3, \sigma^4=1\}$, where σ is the automorphism $\nu \mapsto \nu^3$ (and hence also $\zeta \mapsto \zeta^3$). Thus, σ^2 is complex conjugation. We will write the general element of $\mathcal{O}$ as

$$\alpha = a + b\nu + c\nu^2 + d\nu^3, \quad a, b, c, d \in \mathbb{Z}.$$

Then the four Galois conjugates of α are

$$\begin{aligned}
\alpha &= a + b\nu + c\nu^2 + d\nu^3 \\
\sigma(\alpha) &= a + b\nu^3 + c\nu + d\nu^4 \\
\sigma^2(\alpha) = \bar{\alpha} &= a + b\nu^4 + c\nu^3 + d\nu^2 \\
\sigma^3(\alpha) = \sigma(\bar{\alpha}) &= a + b\nu^2 + c\nu^4 + d\nu
\end{aligned}$$

We need some information on the splitting of rational primes p in the ring $\mathcal{O}$; we follow the standard procedure outlined in [10], Chapter 3. The discriminant of the integral basis $[1, \nu, \nu^2, \nu^3]$ of $\mathcal{O}$ equals 125, so the only rational prime which ramifies is 5. We have

$$(5) = (1-\nu)^4 \quad \text{as ideals in } \mathcal{O}.$$

Primes congruent to $\pm 3 \pmod{10}$ are inert ($p\mathcal{O}$ is a prime ideal). Primes congruent to $-1 \pmod{10}$ split into the product of two prime ideals of inertial degree 2. Primes congruent to $+1 \pmod{10}$ split into the product of four prime ideals of inertial degree 1.

We are interested in describing those primes $p > 5$ which can be written as $p = \pi\bar{\pi}$ for some $\pi \in \mathcal{O}$. Clearly no prime congruent to $\pm 3 \pmod{10}$ can be written thus. Neither is this possible for $p \equiv -1 \pmod{10}$, for we have the decomposition $p\mathcal{O} = \mathcal{P}_1 \cdot \mathcal{P}_2$ for prime ideals $\mathcal{P}_1$ and $\mathcal{P}_2$. Since σ fixes $p\mathcal{O}$, the action of σ on the set $\{\mathcal{P}_1, \mathcal{P}_2\}$ is an involution of order at most 2. Hence $\overline{\mathcal{P}}_1 = \sigma^2(\mathcal{P}_1) = \mathcal{P}_1$. This means that every product $\pi\bar{\pi}$ for $\pi \in \mathcal{P}_1$ lies in the ideal $\mathcal{P}_1^2 \neq \mathcal{P}_1 \cdot \mathcal{P}_2$ and thus cannot equal p. Hence no prime $p \equiv -1 \pmod{10}$ can be written in this way.

We are left with the congruence class $p \equiv 1 \pmod{10}$. We can always decompose such a prime as $p = \pi\bar{\pi}$. To see this, we observe that the factorization of $p\mathcal{O}$ into principal prime ideals as

$$p\mathcal{O} = \mathcal{P} \cdot \sigma(\mathcal{P}) \cdot \sigma^2(\mathcal{P}) \cdot \sigma^3(\mathcal{P})$$

implies that there exist elements of norm p in $\mathcal{O}$. If $\mathcal{P} = \alpha\mathcal{O}$, we define

$$\pi = \alpha \cdot \sigma(\alpha),$$

and it follows that

$$\pi\bar{\pi} = \alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha \cdot \sigma(\alpha)) = \mathbf{Norm}_{K/\mathbb{Q}}(\alpha) = p.$$

LEMMA 1. *$\pi+\bar{\pi}$ is prime to p.*

Proof. Suppose not. Then $\pi+\bar{\pi}$ is contained in at least one of the prime ideals into which p splits, say $\pi+\bar{\pi}\in\alpha\mathcal{O}$. Then we have

$$\begin{aligned}\alpha\sigma(\alpha)+\sigma^2(\alpha\sigma(\alpha))\in\alpha\mathcal{O}, &\quad \text{giving}\\ \sigma^2(\alpha)\sigma^3(\alpha)\in\alpha\mathcal{O}, &\quad \text{which implies}\\ \sigma^2(\mathcal{P})\cdot\sigma^3(\mathcal{P})\subset\mathcal{P};&\end{aligned}$$

this is impossible because the ideals $\sigma^i(\mathcal{P})$ are prime and distinct. ■

LEMMA 2. *Let $p\equiv 1 \pmod{10}$. Then there are 40 distinct values of π which arise as $\pi=\alpha\cdot\sigma(\alpha)$, as α ranges over all (infinitely many) elements of $\mathcal{O}$ of norm p.*

Proof. Select an element $\alpha\in\mathcal{O}$ of norm p. This entails a choice of one of the four ideals into which (p) splits in $\mathcal{O}$, followed by selection of a generator of that ideal. Set $\upsilon=\nu+\nu^{-1}$, so that υ^{-1} is the fundamental real unit. Then the complete set of associates of α in $\mathcal{O}$ is given by $\{\zeta^k\upsilon^\ell\alpha\}$, $0\le k\le 9$, $\ell\in\mathbb{Z}$. We replace α by $\zeta^k\upsilon^\ell\alpha$ and compute

$$\begin{aligned}\zeta^k\upsilon^\ell\alpha\cdot\sigma(\zeta^k\upsilon^\ell\alpha)&=(\zeta^k(\nu+\nu^{-1})^\ell\zeta^{3k}(\nu^3+\nu^{-3})^\ell)\alpha\cdot\sigma(\alpha)\\ &=\zeta^{4k}(\nu+\nu^2+\nu^3+\nu^4)^\ell\alpha\cdot\sigma(\alpha)\\ &=(\nu^{2k}(-1)^\ell)\alpha\cdot\sigma(\alpha)\\ &=(\zeta^j)\alpha\cdot\sigma(\alpha)\quad \text{for some } j \text{ in } \{0,\dots,9\}.\end{aligned}$$

Thus, for the class of associates of a fixed α there are only 10 possibilities for $\pi=\alpha\cdot\sigma(\alpha)$. The other 30 values are $\sigma(\pi),\sigma^2(\pi),\sigma^3(\pi)$. ■

Let $\beta\in\mathcal{O}$ be relatively prime to 5. Then there is a unique 5th root of unity ν^k such that $\nu^k\beta$ is congruent (mod $(1-\nu)^2$) to a rational integer (see [5], p. 206). We call $\nu^k\beta$ the *primary twist* of β. If the primary twist of β is β itself (i.e., $\nu^k=1$) then we call β *primary*. In general, a primary β might be congruent to any nonzero value modulo 5. But for primary integers of the form $\pi=\alpha\cdot\sigma(\alpha)$ we can say more.

LEMMA 3. *Let $p\equiv 1 \pmod{10}$ and suppose that $p=\pi\bar{\pi}$ with π primary. Then $\pi\equiv\pm 1 \pmod{(1-\nu)^2}$.*

Proof. Let a primary π be chosen as described, so there is a rational integer n with $\pi\equiv n \pmod{(1-\nu)^2}$. Then $\bar{\pi}\equiv n \pmod{(1-\nu)^2}$ as well, whence $p=\pi\bar{\pi}\equiv n^2 \pmod{(1-\nu)^2}$. Expressed another way,

$$p-n^2\in(1-\nu)^2\mathcal{O},$$

so that

$$(p-n^2)^2\in(1-\nu)^4\mathcal{O}=5\mathcal{O}.$$

This implies that 5 divides $p-n^2$, which in turn implies that $n^2 \equiv 1 \pmod 5$ and hence $n^2 \equiv 1 \pmod{(1-\nu)^2}$. ■

We will call a factorization $p=\pi\bar{\pi}$ a *primary splitting* of p if $\pi \equiv -1 \pmod{(1-\nu)^2}$. Note that in any primary splitting $p=\pi\bar{\pi}$, all four conjugates of π are congruent to $-1 \pmod{(1-\nu)^2}$.

3. Characters and Jacobi Sums

We review some standard notions first. For details on the material in this section, see [9], Chapter 5. A *character* of a finite group G is a homomorphism of G into the multiplicative group of the roots of unity. The characters of G form a group under composition, called the *character group* of G. By a character on $\mathbb{F}_q$ we mean a character χ of the multiplicative group $\mathbb{F}_q^\times$, extended to all of $\mathbb{F}_q$ by $\chi(0)=0$. Thus, we do not count as a character of $\mathbb{F}_q$ the function $\varepsilon: \mathbb{F}_q \longrightarrow \{1\}$. The multiplicative group $\mathbb{F}_q^\times$ is cyclic; once a generator is chosen, any character of $\mathbb{F}_q^\times$ is completely determined by the value it assigns to that generator.

Let p be a prime of the form $p \equiv 1 \pmod{10}$ and let $p=\pi\bar{\pi}$ be a primary splitting of p, arising from $\pi=\alpha\sigma(\alpha)$ for an α of norm p. Then $\pi \equiv -1 \pmod{(1-\nu)^2}$. The ideal $\pi\mathcal{O}$ factors into primes as

$$\pi\mathcal{O} = \mathscr{P}\cdot\sigma(\mathscr{P}),$$

where we assume that $\alpha \in \mathscr{P}$. Let g be a fixed generator of $\mathbb{F}_p^\times$ and define a character χ_{P} of $\mathbb{F}_p$ of order 5 by

$$\chi_{\mathrm{P}}(g) = \nu^k,$$

where ν^k is the unique 5th root of unity for which

$$g^{(p-1)/5} \equiv \nu^k \pmod{\mathscr{P}}.$$

Now let h be a generator of $\mathbb{F}_{p^2}^\times$ and define the *lifted character* χ'_{P} on $\mathbb{F}_{p^2}$ by

$$\chi'_{\mathrm{P}}(h) = \chi_{\mathrm{P}}(\mathbf{Norm}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(h)).$$

We should not view the lifted character χ'_{P} as an extension of χ_{P}, since χ'_{P} and χ_{P} do not take the same values on $\mathbb{F}_p$—note that $\chi'_{\mathrm{P}}(g) = \chi_{\mathrm{P}}(g\cdot g^p) = \chi_{\mathrm{P}}(g^2)$.

For any n there is a unique non-trivial character ρ of $\mathbb{F}_{p^n}$ of order 2. For $n=1$ this is the familiar Legendre symbol modulo p; for $n=2$ it is the lift of the Legendre symbol. Since $\rho'(g) = \rho(g\cdot g^p) = \rho(g)^2$, the lifted character ρ' is identically equal to $+1$ on $\mathbb{F}_p^\times$.

We now define the *Jacobi sum* $J(\mathbb{F}_q; \chi_1, \chi_2)$ of two characters on $\mathbb{F}_q$ by

$$J(\mathbb{F}_q; \chi_1, \chi_2) = \sum_{\substack{u,v\in\mathbb{F}_q \\ u+v=1}} \chi_1(u)\chi_2(v) = \sum_{j=1}^{q-2} \chi_1(h^j)\chi_2(1-h^j),$$

where h is a generator of $\mathbb{F}_q^\times$.

LEMMA 4. *Let* $p \equiv 1 \pmod{10}$ *and* $q = p^n$. *Let* χ_1, χ_2 *be characters of* $\mathbb{F}_q$ *of order* 5. *Then*

$$J(\mathbb{F}_q; \chi_1, \chi_2) \equiv -1 \pmod{(1-\nu)^2}.$$

Proof. Let h be a generator of $\mathbb{F}_q^\times$. Replacing χ_i by $1-\chi_i$ in the sum, we compute the difference

$$\begin{aligned}
&\sum_{j=1}^{q-2} \chi_1(h^j)\chi_2(1-h^j) - \sum_{j=1}^{q-2}(1-\chi_1(h^j))(1-\chi_2(1-h^j)) \\
&\quad = -\sum_{j=1}^{q-2} 1 + \sum_{j=1}^{q-2} \chi_1(h^j) + \sum_{j=1}^{q-2} \chi_2(1-h^j) \\
&\quad = -(q-2) + (-1) + (-1) = -q.
\end{aligned}$$

Hence we may write

$$\begin{aligned}
J(\mathbb{F}_q; \chi_1, \chi_2) &= -q + \sum_{j=1}^{q-2}(1-\chi_1(h^j))(1-\chi_2(1-h^j)) \\
&= -q + \sum_{j=1}^{q-2}(1-\nu^{k_j})(1-\nu^{\ell_j}) \\
&\equiv -q \pmod{(1-\nu)^2} \\
&\equiv -1 \pmod{(1-\nu)^2}.
\end{aligned}$$

The exponents k_j, ℓ_j are unspecified integers, but since $1-\nu^{k_j}$ is always divisible by $1-\nu$ (even when $k_j = 0$), each term in the sum is divisible by $(1-\nu)^2$. The last line follows because $(1-\nu)^2$ divides 5, which divides $p-1$, whence $q \equiv 1 \pmod{(1-\nu)^2}$. ∎

LEMMA 5. *With* $p, \pi, \mathfrak{P}, \chi_{\mathfrak{P}}$, *and* $\chi'_{\mathfrak{P}}$ *defined as above, we have*

$$\begin{aligned}
J(\mathbb{F}_p; \chi_{\mathfrak{P}}, \chi_{\mathfrak{P}}) &= \pi \\
J(\mathbb{F}_p; \chi_{\mathfrak{P}}^2, \chi_{\mathfrak{P}}^2) &= \sigma(\pi) \\
J(\mathbb{F}_p; \chi_{\mathfrak{P}}^3, \chi_{\mathfrak{P}}^3) &= \sigma^3(\pi) = \sigma(\bar{\pi}) \\
J(\mathbb{F}_p; \chi_{\mathfrak{P}}^4, \chi_{\mathfrak{P}}^4) &= \sigma^2(\pi) = \bar{\pi},
\end{aligned} \tag{1}$$

and

$$\begin{aligned}
J(\mathbb{F}_{p^2}; \chi'_{\mathfrak{P}}, \chi'_{\mathfrak{P}}) &= -\pi^2 \\
J(\mathbb{F}_{p^2}; \chi'^2_{\mathfrak{P}}, \chi'^2_{\mathfrak{P}}) &= \sigma(-\pi^2) \\
J(\mathbb{F}_{p^2}; \chi'^3_{\mathfrak{P}}, \chi'^3_{\mathfrak{P}}) &= \sigma^3(-\pi^2) = \sigma(-\bar{\pi}^2) \\
J(\mathbb{F}_{p^2}; \chi'^4_{\mathfrak{P}}, \chi'^4_{\mathfrak{P}}) &= \sigma^2(-\pi^2) = -\bar{\pi}^2.
\end{aligned} \tag{2}$$

Proof. Let g be a generator of $\mathbb{F}_p^\times$ and define $k \in \{1, 2, 3, 4\}$ to be the unique exponent for which $g^{(p-1)/5} \equiv \nu^k \pmod{\mathscr{P}}$. Applying σ to this congruence yields $g^{(p-1)/5} \equiv \nu^{3k} \pmod{\sigma(\mathscr{P})}$, so that $g^{2(p-1)/5} \equiv \nu^{6k} \equiv \nu^k \pmod{\sigma(\mathscr{P})}$. Writing J for $J(\mathbb{F}_p; \chi_\mathfrak{P}, \chi_\mathfrak{P})$, we have the congruences

$$J \equiv \sum_{u=0}^{p-1} u^{(p-1)/5}(1-u)^{(p-1)/5} \pmod{\mathscr{P}}, \tag{3}$$

$$J \equiv \sum_{u=0}^{p-1} u^{2(p-1)/5}(1-u)^{2(p-1)/5} \pmod{\sigma(\mathscr{P})}. \tag{4}$$

But in fact

$$\sum_{u=0}^{p-1} u^{(p-1)/5}(1-u)^{(p-1)/5} \equiv \sum_{u=0}^{p-1} u^{2(p-1)/5}(1-u)^{2(p-1)/5} \equiv 0 \pmod{p},$$

which follows from the fact that $1^r + 2^r + \cdots + (p-1)^r \equiv 0 \pmod{p}$ as long as $(p-1) \nmid r$. Thus,

$$J \in \mathscr{P} \cdot \sigma(\mathscr{P}) = \pi\mathscr{O}.$$

We have $|J| = |\pi| = \sqrt{p}$ (see, e.g., [5], p. 94), which implies that $|\sigma(J)| = |\sigma(\pi)| = \sqrt{p}$. Thus, J/π is an algebraic integer all of whose conjugates have absolute value 1 and hence is a root of unity. But π and $\pm\nu^k\pi$ cannot both be primary unless $k = 0$. The possibility $\pi \equiv -J \pmod{(1-\nu)^2}$ cannot occur because it implies $2 \in (1-\nu)^2\mathscr{O}$, whereas only 5 ramifies in $\mathscr{O}$. Hence $J(\mathbb{F}_p; \chi_\mathfrak{P}, \chi_\mathfrak{P}) = \pi$.

The other equations in (1) follow from the first by considering the action of σ and by noting that $\chi_\mathfrak{P}^4 = \overline{\chi_\mathfrak{P}}$.

Finally, the equations (2) follow from (1) by the Davenport–Hasse relation ([9], p. 210). ∎

4. Counting Points on Hyperelliptic Curves

Let $p \equiv 1 \pmod{10}$ be a prime and let $q = p^n$ for some integer n. Let D be an arbitrary integer and consider the hyperelliptic curve $H_D : y^2 = x^5 + D$ as a curve defined over $\mathbb{F}_p$. We write $N_q(\cdot)$ to denote the number of $\mathbb{F}_q$-solutions (i.e., affine solutions only) of an integer polynomial equation. Let χ be any character of $\mathbb{F}_q^\times$ of order 5, and let ρ denote the unique character of $\mathbb{F}_q^\times$ of order 2. Let $\pi\bar{\pi}$ be a primary splitting of the prime p. Including 1 for the unique (desingularized) point at infinity, the number of points on H is

$$\begin{aligned} \#H_D(\mathbb{F}_q) &= 1 + N_q(y^2 = x^5 + D) \\ &= 1 + \sum_{u+v=D} N_q(y^2 = u) N_q(x^5 = -v) \end{aligned}$$

$$
\begin{aligned}
&= 1 + \sum_{u+v=D} (1+\rho(u))(1+\chi(-v)+\chi^2(-v)+\chi^3(-v)+\chi^4(-v)) \\
&= q+1+\sum_{u+v=D} \rho(u)\chi(v) + \sum_{u+v=D} \rho(u)\chi^2(v) \\
&\quad + \sum_{u+v=D} \rho(u)\chi^3(v) + \sum_{u+v=D} \rho(u)\chi^4(v).
\end{aligned}
$$

We change the variables of summation to $u = Du'$ and $v = Dv'$, factor out the D's, and rename u', v' back to u, v. This gives

$$
\begin{aligned}
\#H_D(\mathbb{F}_q) &= q+1+\rho\chi(D)\sum_{u+v=1}\rho(u)\chi(v) + \rho\chi^2(D)\sum_{u+v=1}\rho(u)\chi^2(v) \\
&\quad + \rho\chi^3(D)\sum_{u+v=1}\rho(u)\chi^3(v) + \rho\chi^4(D)\sum_{u+v=1}\rho(u)\chi^4(v) \\
&= q+1+\rho\chi(D)J(\rho,\chi) + \rho\chi^2(D)J(\rho,\chi^2) + \rho\chi^3(D)J(\rho,\chi^3) \\
&\quad + \rho\chi^4(D)J(\rho,\chi^4).
\end{aligned}
$$

Using the lemma in [5], p. 305, we can rewrite this as

$$
\begin{aligned}
\#H_D(\mathbb{F}_q) &= q+1+\rho\chi(4D)J(\chi,\chi) + \rho\chi^2(4D)J(\chi^2,\chi^2) + \rho\chi^3(4D)J(\chi^3,\chi^3) \\
&\quad + \rho\chi^4(4D)J(\chi^4,\chi^4).
\end{aligned}
$$

We now specialize to the curve $H := H_8 : y^2 = x^5 + 8$. We have $4D = 2^5$, so $\chi(4D) = 1$ and $\rho(4D) = \rho(2)$. We thus obtain

$$
\begin{aligned}
\#H(\mathbb{F}_q) &= q+1+\rho(2)J(\chi,\chi) + \rho(2)J(\chi^2,\chi^2) + \rho(2)J(\chi^3,\chi^3) \\
&\quad + \rho(2)J(\chi^4,\chi^4).
\end{aligned}
$$

Applying the results of Lemma 3 we have

$$\#H(\mathbb{F}_p) = p+1+\rho(2)\mathbf{Trace}_{K/\mathbb{Q}}(\pi),$$

and using $\mathbb{F}_{p^2}$-lifted characters $\chi = \chi'_{\mathrm{P}}$ and $\rho = \rho'$ we have

$$\#H(\mathbb{F}_{p^2}) = p^2+1-\mathbf{Trace}_{K/\mathbb{Q}}(\pi^2).$$

Since the curve H has genus 2, there exist algebraic integers $\alpha, \beta, \gamma, \delta$ (called the *Weil numbers* of H) with $\alpha\beta = \gamma\delta = p$ and

$$\#H(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha^n + \beta^n + \gamma^n + \delta^n)$$

for every $n \geq 1$. Our Jacobi sum computations (1) and (2) show that the Weil numbers of H are

$$-\rho(2)\pi, \quad -\rho(2)\sigma(\pi), \quad -\rho(2)\sigma^2(\pi), \quad -\rho(2)\sigma^3(\pi).$$

With the Weil numbers in hand, we may now conclude (see [11], pp. 158–166) that the order r of the Jacobian $\mathscr{J}_H(\mathbb{F}_p)$ of H is given by

$$r = \mathbf{Norm}_{K/\mathbb{Q}}(1+\rho(2)\pi).$$

5. Choosing the System Parameters

We now sketch a method by which a suitable prime $p \equiv 1 \pmod{10}$ may be chosen so that the order r of the Jacobian $\mathcal{J}_H(\mathbb{F}_p)$ is prime.

Among primes $p \equiv 1 \pmod{10}$, those primes which are congruent to $\pm 1 \pmod 8$ will be rejected out of hand, as the associated Jacobian orders are automatically composite. Such primes have Legendre symbol $\rho(2) = +1$, which gives $\#\mathcal{J}_H(\mathbb{F}_p) = \mathbf{Norm}_{K/\mathbb{Q}}(1+\pi)$. Since π and its conjugates are primary, each factor in the norm of $1+\pi$ is divisible by $(1-\nu)^2$ and the overall product consequently divisible by $(1-\nu)^8$; thus, the integer $\mathbf{Norm}_{K/\mathbb{Q}}(1+\pi)$ is divisible by 25.[1] For this reason, we shall require $p \equiv \pm 3 \pmod 8$ and hence $\rho(2) = -1$.

We will set up our search for parameters p and r with the condition $\pi \equiv -1 \pmod{(1-\nu)^2}$ built into the starting values. We begin by setting

$$\alpha := a + b\nu + c\nu^2 + d\nu^3, \quad a, b, c, d \in \mathbb{Z}$$

and impose the condition $\alpha \cdot \sigma(\alpha) \equiv -1 \pmod{(1-\nu)^2}$. Expanding $\alpha \cdot \sigma(\alpha)$ in powers of $(1-\nu)$, we obtain

$$\alpha \cdot \sigma(\alpha) \equiv F - G(1-\nu) \pmod{(1-\nu)^2},$$

where

$$F = a^2 + 2ab + 2ac - 3ad - 4b^2 + 2bc + 2bd + c^2 - 3cd + d^2$$
$$G = 4ab + 3ac - 3ad - 6b^2 + 2bc + bd + 3c^2 - 5cd + 2d^2.$$

The condition $\alpha \cdot \sigma(\alpha) \equiv -1 \pmod{(1-\nu)^2}$ becomes

$$F + 1 \equiv G \equiv 0 \pmod 5.$$

These two congruences can be replaced by simpler ones. A reduced Gröbner Basis calculation—using the computational algebra package MAGMA–for the ideal generated by $F+1$ and G over the field $\mathbb{F}_5$ yields the following equivalent generators for this ideal:

$$a^2 - 2ac + ad + c^2 - cd - d^2 + 1 \equiv 0 \pmod 5 \tag{5}$$
$$b + 2c - 2d \equiv 0 \pmod 5. \tag{6}$$

The relation (5) does not contain b and (6) does not contain a. Also, relation (5) factors, giving

$$(a - c - 2d - 2)(a - c - 2d + 2) \equiv 0 \pmod 5. \tag{7}$$

If the first factor in (7) evaluates to 0 for (a, b, c, d), then the second factor evaluates to 0 for $(-a, -b, -c, -d)$, and both 4-tuples generate the same value of $\alpha \cdot \sigma(\alpha)$. Without loss of generality, then, we require

$$a \equiv c + 2d + 2 \pmod 5 \tag{8}$$

and are assured that every value of $\alpha \cdot \sigma(\alpha)$ appears for some choice of a, b, c, d.

The free parameters are c and d, and the dependent parameters a and b are only determined up to an additive multiple of 5. However, we will treat the congruences in (6) and (8) as equalities, adding no multiples of 5. Such an arbitrary choice probably means that certain primes p cannot be obtained with our construction, but a definite statement along these lines seems difficult to formulate. In practice, there seem to be plenty of primes p arising from our choice of (a, b, c, d), and among them, we seem to obtain $\rho(2) = -1$ about half the time.

Algorithm 1. (*System Parameters*)

Input: the hash value c of the user's ID
Output: p, r, d

1. Set $d \leftarrow 0$
2. Set $a \leftarrow c + 2d + 2$
3. Set $b \leftarrow -2c + 2d$
4. Set $\alpha \leftarrow a + b\nu + c\nu^2 + d\nu^3$
5. Set $\pi \leftarrow \alpha \cdot \sigma(\alpha)$
6. Set $p = \pi\bar{\pi}$
7. If $p \equiv \pm 1 \pmod 8$, set $d \leftarrow d + 1$ and go to step 2
8. If p is composite, set $d \leftarrow d + 1$ and go to step 2
9. $r \leftarrow \mathbf{Norm}_{K/\mathbb{Q}}(1 - \pi)$
10. If r is composite, set $d \leftarrow d + 1$ and go to step 2
11. Output p, r, d

We conclude this section with explicit formulas for some of the system parameters in terms of the free variables c and d.

We have

$$\alpha = a + b\nu + c\nu^2 + d\nu^3$$

where

$$a = c + 2d + 2$$
$$b = -2c + 2d,$$

$$\pi = A + B\nu + C\nu^2 + D\nu^3,$$

where

$$\begin{aligned} A &= 4 + 4c - 5c^2 + 6d + 10cd \\ B &= -2c - 5c^2 + 2d + 5cd \\ C &= 2c - 5c^2 - 2d + 10cd - 5d^2 \\ D &= -4c - 5c^2 + 4d + 5cd, \end{aligned} \tag{9}$$

$$p = 25c^4 - 75c^3d + 100c^2d^2 + 50c^2d + 40c^2 - 50cd^3 + 40cd + 40c + 25d^4 + 50d^3 + 60d^2 + 40d + 16, \tag{10}$$

$$\begin{aligned} r = {} & 625c^8 - 3750c^7d + 10625c^6d^2 + 2500c^6d + 2125c^6 \\ & - 17500c^5d^3 - 7500c^5d^2 - 4875c^5d + 1500c^5 + 18750c^4d^4 \\ & + 12500c^4d^3 + 9375c^4d^2 + 1250c^4d + 2225c^4 - 13750c^3d^5 \\ & - 12500c^3d^4 - 6875c^3d^3 + 4500c^3d^2 + 4325c^3d + 2550c^3 \\ & + 7500c^2d^6 + 12500c^2d^5 + 15625c^2d^4 + 13000c^2d^3 \\ & + 10400c^2d^2 + 5250c^2d + 1665c^2 - 2500cd^7 - 5000cd^6 \\ & - 4250cd^5 + 1500cd^4 + 5675cd^3 + 5250cd^2 + 2340cd \\ & + 540c + 625d^8 + 2500d^7 + 5375d^6 + 7250d^5 + 6725d^4 \\ & + 4350d^3 + 1935d^2 + 540d + 81. \end{aligned} \tag{11}$$

One can also compute $\#H(\mathbb{F}_p) = p + 1 - \mathbf{Trace}_{K/\mathbb{Q}}(\pi)$; however, the cryptographic application does not require that we know the number of points on the hyperelliptic curve itself. The compact cryptosystem is the Jacobian, where the group operation resides, so it is r that is needed.

For the remainder of the paper we assume p has been chosen to satisfy both $p \equiv 1 \pmod{10}$ and $p \equiv \pm 3 \pmod{8}$.

6. Complex Multiplication on $H/\bar{\mathbb{F}}_p$

The curve $H/\bar{\mathbb{Q}}: y^2 = x^5 + 8$ admits complex multiplication by the 5th roots of unity, namely by the map $(x, y) \longmapsto (\nu x, y)$ and its powers. For a prime $p \equiv 1 \pmod{10}$, this structure descends to the curve $H/\bar{\mathbb{F}}_p$. Namely, let $\nu \in \mathbb{F}_p$ be a primitive 5th root of unity and define the map ψ and its powers by

$$\begin{aligned} \psi &: H/\bar{\mathbb{F}}_p \longrightarrow H/\bar{\mathbb{F}}_p \\ \psi^n(x, y) &= (\nu^n x, y), \quad n \geq 0 \end{aligned}$$

The maps ψ^n extend pointwise to endomorphisms of the Jacobian $\mathscr{J}_H(\bar{\mathbb{F}}_p)$ and satisfy the characteristic equation

$$\psi^4 + \psi^3 + \psi^2 + \psi + 1 = 0.$$

The *Frobenius endomorphism* ϕ, defined by

$$\begin{aligned} \phi &: H(\bar{\mathbb{F}}_p) \longrightarrow H(\bar{\mathbb{F}}_p) \\ \phi(x, y) &= (x^p, y^p), \end{aligned}$$

also extends pointwise to an endomorphism of $\mathscr{J}_H(\bar{\mathbb{F}}_p)$ and satisfies a characteristic equation involving the Weil numbers $\pi, \sigma(\pi), \sigma^2(\pi), \sigma^3(\pi)$ of H, namely

$$\prod_{i=0}^{3} (\phi - \sigma^i(\pi)) = \phi^4 - \mathbf{Trace}_{K/\mathbb{Q}}(\pi)\phi^3 + \cdots + p^2 = 0.$$

The Jacobian $\mathscr{J}_H(\bar{\mathbb{F}}_p)$ is ordinary for the prime p. This can be deduced from the fact that $\pi + p/\pi$ is prime to p (see [13] for background), which we showed in Lemma 1. Consequently, the endomorphism ring $\mathbf{End}(\mathscr{J}_H(\bar{\mathbb{F}}_p))$ is commutative and has rank 4 as a $\mathbb{Z}$-module. The Frobenius ϕ thus has four representations in the powers of ψ:

$$\phi = A_k + B_k\psi^k + C_k\psi^{2k} + D_k\psi^{3k}, \quad k = 1, 2, 3, 4. \tag{12}$$

Because the same quartic is satisfied by the Weil numbers of $H/\bar{\mathbb{F}}_p$ as by the four representations of the Frobenius and the same quartic is satisfied by ν and its powers as by ψ and its powers, the representations (12) correspond to the Weil numbers of $H/\bar{\mathbb{F}}_p$ in some order. Thus, for some value of k we have

$$A_k = A, \quad B_k = B, \quad C_k = C, \quad D_k = C,$$

corresponding to the particular Weil number $\pi = A + B\nu + C\nu^2 + D\nu^3$. We now develop a criterion for determining this value of k.

Since H has genus 2, the $\bar{\mathbb{F}}_p$-vector space of holomorphic differentials on the hyperelliptic curve $H/\bar{\mathbb{F}}_p$ is 2-dimensional, spanned by dx/y and $x\,dx/y$. Endomorphisms of $\mathscr{J}_H(\bar{\mathbb{F}}_p)$ induce linear pullback maps on differentials. In particular, the endomorphism $[N]$ (multiplication by the integer N in the Jacobian) induces scalar multiplication by N and ϕ induces scalar multiplication by 0 on each basis differential. We now compute the pullback map corresponding to ψ.

$$\psi^*\left(\frac{dx}{y}\right) = \frac{d(\nu x)}{y} = \nu \cdot \frac{dx}{y}, \tag{13}$$

and

$$\psi^*\left(\frac{x\,dx}{y}\right) = \frac{(\nu x)\,d(\nu x)}{y} = \nu^2 \cdot \frac{x\,dx}{y}. \tag{14}$$

Applying (13) to (12) yields

$$\begin{aligned} \phi^*\left(\frac{dx}{y}\right) &= ([A_k] + [B_k]\psi + [C_k]\psi^2 + [D_k]\psi^3)^*\left(\frac{dx}{y}\right), \\ 0 \cdot \frac{dx}{y} &= A_k\frac{dx}{y} + B_k\nu\frac{dx}{y} + C_k\nu^2\frac{dx}{y} + D_k\nu^3\frac{dx}{y}, \\ 0 &\equiv A_k + B_k\nu + C_k\nu^2 + D_k\nu^3 \pmod{p}. \end{aligned} \tag{15}$$

Similarly, applying (14) to (12) yields

$$\begin{aligned} \phi^*\left(\frac{x\,dx}{y}\right) &= ([A_k] + [B_k]\psi + [C_k]\psi^2 + [D_k]\psi^3)^*\left(\frac{x\,dx}{y}\right), \\ 0 \cdot \frac{x\,dx}{y} &= A_k\frac{x\,dx}{y} + B_k\nu^2\frac{x\,dx}{y} + C_k\nu^4\frac{x\,dx}{y} + D_k\nu^6\frac{x\,dx}{y}, \\ 0 &\equiv A_k + B_k\nu^2 + C_k\nu^4 + D_k\nu^6 \pmod{p}. \end{aligned} \tag{16}$$

Table 1. The Weil numbers of $H/\bar{\mathbb{F}}_p$.

	1	v	v^2	v^3
π	A	B	C	D
$\sigma(\pi)$	$A-D$	$C-D$	$-D$	$B-D$
$\sigma^2(\pi)$	$A-B$	$-B$	$D-B$	$C-B$
$\sigma^3(\pi)$	$A-C$	$D-C$	$B-C$	$-C$

Table 2. Choosing the correct k.

if (16), (15) are satisfied by rows	then set k equal to
1, 2	3
2, 3	4
3, 4	2
4, 1	1

The congruences (15) and (16) are the mod p analogue of the fact that exactly two of the characteristic roots of Frobenius are p-adic non-units, while the other two are units.

Beginning with $\pi = A + Bv + Cv^2 + Dv^3$, we repeatedly apply the action $\sigma : v \longmapsto v^3$ and reduce by $v^4 = -v^3 - v^2 - v - 1$ to compute the coefficients of the other Weil numbers of $H/\bar{\mathbb{F}}_p$. The results are shown in Table 1.

Note that the congruences (15) and (16) must correspond to adjacent rows (modulo circular rotation) in Table 1. This is because non-adjacent rows represent complex conjugate pairs of Weil numbers, which cannot both be non-units, since their product equals p. Furthermore, since successive rows in the the table are constructed by $v \longmapsto v^3$, we see that (16) will precede (15).

Thus, having picked a primitive 5th root v at random, we construct the four linear combinations of $\{1, v, v^2, v^3\}$ with coefficients from Table 1 and we proceed as in Table 2.

Redefining $\psi(x, y) = (v^k x, y)$ for the correct k then yields

$$\pi = A + Bv + Cv^2 + Dv^3 \tag{17}$$

$$\phi = A + B\psi + C\psi^2 + D\psi^3 \tag{18}$$

Finally, we use this infrastructure to determine the integer N giving the equivalence

$$\psi \cong [N] \quad \text{on } \mathscr{J}_H(\mathbb{F}_p).$$

Beginning with

$$\phi = A + B\psi + C\psi^2 + D\psi^3,$$

we compute

$$\phi^2 = A' + B'\psi + C'\psi^2 + D'\psi^3$$
$$\phi^3 = A'' + B''\psi + C''\psi^2 + D''\psi^3,$$

where

$$A' = A^2 - 2BD + 2CD - C^2$$
$$B' = 2AB - 2BD - C^2 + D^2$$
$$C' = 2AC + B^2 - 2BD - C^2$$
$$D' = 2AD + 2BC - 2BD - C^2$$

and

$$A'' = A^3 - 6ABD - 3AC^2 + 6ACD - 3B^2C + 3B^2D + 3BC^2 - D^3$$
$$B'' = 3A^2B - 6ABD - 3AC^2 + 3AD^2 - 3B^2C + 6BCD + C^3 - D^3$$
$$C'' = 3A^2C + 3AB^2 - 6ABD - 3AC^2 - 3B^2C + 3BD^2 + 3C^2D - D^3$$
$$D'' = 3A^2D + 6ABC - 6ABD - 3AC^2 + B^3 - 3B^2C + 3CD^2 - D^3.$$

We then have the matrix equation in $\mathbf{End}(\mathscr{J}_H(\bar{\mathbb{F}}_p))$

$$\begin{bmatrix} 1 \\ \phi \\ \phi^2 \\ \phi^3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ A & B & C & D \\ A' & B' & C' & D' \\ A'' & B'' & C'' & D'' \end{bmatrix} \begin{bmatrix} 1 \\ \psi \\ \psi^2 \\ \psi^3 \end{bmatrix} \tag{19}$$

and the analogous matrix equation in $\mathcal{O}$

$$\begin{bmatrix} 1 \\ \pi \\ \pi^2 \\ \pi^3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ A & B & C & D \\ A' & B' & C' & D' \\ A'' & B'' & C'' & D'' \end{bmatrix} \begin{bmatrix} 1 \\ \nu \\ \nu^2 \\ \nu^3 \end{bmatrix}. \tag{20}$$

Applying the Galois action to the column vectors in (20) we have

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ \pi & \sigma(\pi) & \sigma^2(\pi) & \sigma^3(\pi) \\ \pi^2 & \sigma(\pi^2) & \sigma^2(\pi^2) & \sigma^3(\pi^2) \\ \pi^3 & \sigma(\pi^3) & \sigma^2(\pi^3) & \sigma^3(\pi^3) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ A & B & C & D \\ A' & B' & C' & D' \\ A'' & B'' & C'' & D'' \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ \nu & \nu^3 & \nu^4 & \nu^2 \\ \nu^2 & \nu & \nu^3 & \nu^4 \\ \nu^3 & \nu^4 & \nu^2 & \nu \end{bmatrix} \tag{21}$$

The outer matrices in (21) are of Vandermonde form. Taking determinants and using (9) and (10) we find that

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ A & B & C & D \\ A' & B' & C' & D' \\ A'' & B'' & C'' & D'' \end{bmatrix} = 125p(c-d)^6(5c^2 + 5cd + 10c - 5d^2 - 10d - 4). \tag{22}$$

Since $c \gg d$, $p \sim c^4$, and $r \sim c^8$, we deduce that the determinant is nonzero and cannot be divisible by the prime r. Then we can invert (19) and obtain

$$\begin{bmatrix} 1 \\ \psi \\ \psi^2 \\ \psi^3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ t_A & t_B & t_C & t_D \\ * & * & * & * \\ * & * & * & * \end{bmatrix} \begin{bmatrix} 1 \\ \phi \\ \phi^2 \\ \phi^3 \end{bmatrix}, \tag{23}$$

where the denominators of t_A, t_B, t_C, t_D are prime to r. This gives

$$\begin{aligned} \psi &= t_A + t_B\phi + t_C\phi^2 + t_D\phi^3 \\ &= (t_A + t_B + t_C + t_D) - t_B(1-\phi) - t_C(1-\phi^2) - t_D(1-\phi^3), \end{aligned}$$

hence

$$\psi \sim [t_A + t_B + t_C + t_D] \quad \text{on } \mathscr{J}_H(\mathbb{F}_p), \tag{24}$$

because any endomorphism which factors through $1-\phi$ vanishes on $\mathscr{J}_H(\mathbb{F}_p)$. Note that $t_A + t_B + t_C + t_D$ may be interpreted as an integer (mod r), because the denominators of the t's are prime to r.

7. The Shamir–Gallant Speedup

We next apply this apparatus to enable the use of the Gallant–Shamir speed-ups for scalar multiplication, as was done in [1] for elliptic curves. We develop a procedure which, given an integer N with $1 \le N \le r$, produces integers e, f, g, h of size around $\sqrt[4]{\#\mathscr{J}_H(\mathbb{F}_p)}$ such that $[N]P = [e] + [f]\psi + [g]\psi^2 + [h]\psi^3(P)$.

The ring $\mathbb{Z}[\nu]$ is norm-Euclidean (see, for example, [8]). Thus, given $\gamma \in K$, there exists an element $\texttt{Round}(\gamma) \in \mathcal{O}$ such that

$$\textbf{Norm}(\gamma - \texttt{Round}(\gamma)) < 1.$$

This leads to a bound on the norm of $\texttt{Round}(\gamma)$; however, this is not good enough to control the individual coefficients of ν^k in $\texttt{Round}(\gamma)$, owing to the presence of non-torsion units in K. Instead, we will define a function $\texttt{Near}(\gamma)$ which produces an element of $\mathcal{O}$ which does give control over the coefficients of ν^k.

An arbitrary $\gamma \in K$ can be written uniquely as

$$\gamma = (e + \varepsilon_0) + (f + \varepsilon_1)\nu + (g + \varepsilon_2)\nu^2 + (h + \varepsilon_3)\nu^3,$$

where $e, f, g, h \in \mathbb{Z}$ and $-1/2 \le \varepsilon_i < 1/2$. Then we define

$$\texttt{Near}(\gamma) = e + f\nu + g\nu^2 + h\nu^3.$$

Thus, $\texttt{Near}$ rounds each coefficient of ν^k to its nearest integer in the usual sense.

In the notation we have developed so far, let

$$\delta = 1 - \pi = 1 - A - B\nu - C\nu^2 - D\nu^3.$$

Then $\mathbf{Norm}(\delta) = r = \#\mathcal{J}_H(\mathbb{F}_p)$, and the endomorphism corresponding to δ, namely $1 - \phi = 1 - A - B\psi - C\psi^2 - D\psi^3$, annihilates $\mathcal{J}_H(\mathbb{F}_p)$. For an arbitrary integer N with $1 \le N < r$ define

$$N \bmod \delta = N - \delta \cdot \mathtt{Near}(N/\delta). \tag{25}$$

Then we have

$$N/\delta - \mathtt{Near}(N/\delta) = \varepsilon_0 + \varepsilon_1 \nu + \varepsilon_2 \nu^2 + \varepsilon_3 \nu^3$$

for ε_i as above. It follows that

$$\begin{aligned} N \pmod{\delta} &= \delta \cdot (N/\delta - \mathtt{Near}(N/\delta)) \\ &= (\varepsilon_0 + \varepsilon_1 \nu + \varepsilon_2 \nu^2 + \varepsilon_3 \nu^3)(1 - A - B\nu - C\nu^2 - D\nu^3) \\ &= A_0 + B_0 \nu + C_0 \nu^2 + D_0 \nu^3, \end{aligned}$$

where

$$\begin{aligned} A_0 &= \varepsilon_0 - \varepsilon_0 A + \varepsilon_1 D + \varepsilon_2 C - \varepsilon_2 D + \varepsilon_3 B - \varepsilon_3 C \\ B_0 &= \varepsilon_1 - \varepsilon_0 B - \varepsilon_1 A + \varepsilon_1 D + \varepsilon_3 B + \varepsilon_2 C - \varepsilon_3 D \\ C_0 &= \varepsilon_2 - \varepsilon_0 C - \varepsilon_1 B + \varepsilon_1 D - \varepsilon_2 A + \varepsilon_2 C + \varepsilon_3 B \\ D_0 &= \varepsilon_3 - \varepsilon_0 D - \varepsilon_1 C + \varepsilon_1 D - \varepsilon_2 B + \varepsilon_2 C - \varepsilon_3 A + \varepsilon_3 B. \end{aligned}$$

It is clear that

$$|A_0|, |B_0|, |C_0|, |D_0| \le 4 \max\{|A|, |B|, |C|, |D|\}.$$

Each of A, B, C, D has order of magnitude c^2, since $c \gg d$. Since the order of the Jacobian $\mathcal{J}_H(\mathbb{F}_p)$ is approximately c^8, we have found the representation

$$N \bmod \delta = A_0 + B_0 \nu + C_0 \nu^2 + D_0 \nu^3$$

which we sought.

8. Example Parameters

We illustrate by constructing parameters for a hyperelliptic cryptosystem of target size 256 bits. We begin with the ID string

$$\mathrm{ID} = \mathtt{brownmyerssolinas}.$$

First we compute the SHA-1 hash of the ID, obtaining the hexadecimal number

$$\mathtt{df9c28d9d642b7ff02a44a478bac3c3f83195f0f}.$$

This is a 160-bit output; however, we only require 32 bits for the value of c in Algorithm 1. The low-order word of the hash (`83195f0f`) converts to the decimal number $c = 2199478031$. Then a run of just over 1 minute using `MAGMA` on a 233 MHz laptop produces

$$p = 585082181864813635386537995607105571411$$
$$r = 342321159535690857663043680151780537625 \backslash$$
$$7061054431751567281595836370186404031 51$$
$$d = 2786.$$

Here p has 129 bits and r has 258 bits. We easily verify with `MAGMA` that the Jacobian of $y^2 = x^5 + 8$ defined over $\mathbb{F}_p$ has order r.

Note

1. In fact, a result of Iwasawa [6] implies that $\pi \equiv -1 \pmod{(1-\nu)^3}$, so $\mathbf{Norm}_{K/\mathbb{Q}}(1+\pi)$ is actually divisible by 125.

References

1. E. Brown, B. T. Myers and J. A. Solinas, Elliptic curves with compact parameters, Tech. Report, Centre for Applied Cryptographic Research (2000). http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-68.ps
2. J. Buhler and N. Koblitz, An application of lattice basis reduction to Jacobi sums and hyperelliptic cryptosystems, *Bulletin of the Australian Mathematical Society*, Vol. 58 (1998) pp. 147–154.
3. R. Gallant, R. Lambert and S. Vanstone, Faster point multiplication on curves with efficient complex multiplication, *Advances in Cryptology — CRYPTO 2001*, Springer-Verlag (2001) pp. 190–200.
4. H. Hasse, *Number Theory*, Akademie-Verlag (1979).
5. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory,* Springer-Verlag (1982).
6. K. Iwasawa, A note on Jacobi sums, *Istituto Nazionale di Alta Matematica,* Symposia Mathematica, Vol. 15, Academic Press (1975).
7. T. Lange, Formulae for arithmetic on genus 2 hyperelliptic curves, 2003, http://www.ruhr-uni-bochum.de/itsc/tanja/preprints.html.
8. F. Lemmermeyer, The Euclidean algorithm in algebraic number fields, *Exposition in Mathematics*, Vol. 13, No. 5 (1995) pp. 385–416.
9. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley (1983).
10. D. Marcus, *Number Fields*, Springer-Verlag (1977).
11. H. Stichtenoth, *Algebraic Function Fields and Codes,* Springer-Verlag (1993).
12. L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag (1982).
13. W. C. Waterhouse, *Abelian Varieties over Finite Fields*, Ann. scient. Éc. Norm. Sup., 4^{e} série, t.2 (1969).