G. Group structure and order, and examples over five elements

Let $q > 1$ be a prime power and E a (projective) elliptic curve over the finite field $\mathbb{F}_q$. Then

$$|q + 1 - |E(\mathbb{F}_q)|| \leq 2\sqrt{q}. \tag{G.1}$$

This is known as *Hasse's Theorem*. As a convention, the integer $q + 1 - |E(\mathbb{F}_q)|$ is often denoted by t. Now, $|E(\mathbb{F}_q)|$ is the order of the group $E(\mathbb{F}_q)$ that is constructed upon the set of K-rational points of E. When the number of points is the main focus, then the notation $\#E(\mathbb{F}_q)$ is often used. Hence

$$|E(\mathbb{F}_q)| = \#E(\mathbb{F}_q) = q + 1 - t \text{ and } |t| \leq 2\sqrt{q}. \tag{G.2}$$

Note that if E is an affine Weierstraß curve, then $t = q - r$, where r is the number of affine $\mathbb{F}_q$-rational points.

Let now K be any field, and E an elliptic curve over K. Let L be a subfield of $\bar{K}$ such that $L \supseteq K$. Each K-rational point of E is also L-rational. It follows that $E(K)$ is a subgroup of $E(L)$. In particular, $E(K) \leq E(\bar{K})$.

For each integer $m \geq 1$ put

$$E[m] = \{\alpha \in E; [m]\alpha = \mathcal{O}\}.$$

The symbol $\mathcal{O}$ is used to denote the neutral element of $E(K)$ and $E(\bar{K})$. That is a generic notation that makes especially sense when the form of E is not specified. (In Weierstraß curves the neutral element is denoted by ∞, while in Edwards curves $(0, 1)$ has been chosen. Some authors use $\mathcal{O}$ also in these situations, while some use 0—which may be confusing.)

Note that $E[m]$ is a subgroup of $E(\bar{K})$. This follows from $[m](\alpha \oplus \beta) = [m]\alpha \oplus [m]\beta$ and $[m](\ominus\alpha) = \ominus([m]\alpha)$.

Theorem G.1. *Let K be a field of characteristic p.*

- *If p does not divide $m \geq 2$, then $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$.*
- *If $m \geq 2$ is a power of $p > 0$, then either $E[m] \cong \mathbb{Z}_m$, or $E[m] = \mathcal{O}$.*

By basic properties of abelian groups,

$$E[m_1 m_2] \cong E[m_1] \times E[m_2] \text{ whenever } \gcd(m_1, m_2) = 1.$$

Hence $E[m]$ is known for any $m \geq 1$. Indeed, if $m = np^r$, $p \nmid n$, then $E[m] = E[n] \times E[p^r]$, and Theorem G.1 can be used.

If H is a finite subgroup of $E(\bar{K})$, then there exists $m \geq 1$ such that $H \leq E[m]$. (The choice of $m = |H|$ is always possible.) Hence each finite subgroup of $E(\bar{K})$ embeds into $\mathbb{Z}_m \times \mathbb{Z}_m$ for some $m \geq 1$.

Every subgroup of $\mathbb{Z}_m \times \mathbb{Z}_m$ is isomorphic to some $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, where $m_1 \mid m_2$ and $m_2 \mid m$. We have:

Corollary G.2. *Let E be an elliptic curve over a field K, and let H be a finite subgroup of $E(K)$. Then there exist integers $m_2 \geq m_1 \geq 1$ such that $m_1 \mid m_2$ and $H \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$.*

If E is an elliptic curve over $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ is finite. Hence Corollary G.2 applies to $E(\mathbb{F}_q)$. However, a somewhat stronger result is true:

Theorem G.3. *Let E be an elliptic curve over $\mathbb{F}_q$. Then there exist integers $m_2 \geq m_1 \geq 1$ such that $m_1 \mid m_2$, $m_1 \mid q - 1$, and $E(\mathbb{F}_q) \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$.*

There is a relationship between Theorem G.1 and the fact that complex elliptic curves take the shape of a torus. A rigorous description is not easy. Intuitively, think of the torus as being obtained from a rectangle by identifying the opposite sides. Suppose that the rectangle is a square of size m, and equip it with equidistant

lines parallel to the axes so that a lattice of m^2 squares is formed. Think of the lattice points as of elements of $\mathbb{Z}_m \times \mathbb{Z}_m$.

Let us now turn to Hasse's theorem and its consequences. Suppose that $N = |E(\mathbb{F}_q)|$ is divisible by a prime $\ell > 4\sqrt{q}$. Then there exists a unique $c \geq 1$ such that $N = c\ell$ and this c can be easily established. This is because Hasse's Theorem stipulates that

$$q + 1 - 2\sqrt{q} \leq c\ell \leq q + 1 + 2\sqrt{q},$$

and there can be at most one multiple of ℓ in an interval of length $\leq 4\sqrt{q}$.

The existence of a big prime ℓ that divides $N = |E(\mathbb{F}_q)|$ is essential for elliptic curve cryptography. It is called a *factor* and $c = N/\ell$ is known as *cofactor*. There exist methods how to find E with a large factor and a small cofactor. They are based on what is known as *complex multiplication*. The first step is to choose (d, D), where d is square free, $D = d$ if $d \equiv 3 \bmod 4$ and $D = 4d$ otherwise, and to look for x and y such that $x^2 + dy^2 = \ell$. This method has much to do with algebraic number theory, and uses the fact that $-D$ is a discriminant of a primitive positive definite quadratic form. A recommendation is to choose d such that the class number of $\mathbb{Q}(\sqrt{-D})$ is small, but not too small.

Cryptosystems in public use are constructed in such a way that E is a fixed ingredient of the system (or possibly, there may be several options for the choice of E). The choice of E is a substantial part of devising the cryptosystem, and takes into account both the speed of computation and the resilience to possible attacks.

Another application of elliptic curves are factorization algorithms. An important fact that works in their favour is a uniform distribution of $\#E(\mathbb{F}_q)$ in the *Hasse interval*

$$[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}].$$

If q is a prime, then not only for each N from the Hasse interval there exists a Weierstraß curve with N projective points, but the number of such curves seems to be, by experience, relatively independent of the choice of N.

In the remaining part of this section examples over $\mathbb{Z}_5$ are considered. We shall make an explicit list of all Weierstraß curves, up to $\mathbb{Z}_5$-equivalence, and associate them with Montgomery and twisted Edwards curves. We shall also list points incident to these curves, and describe their group structure.

G.1. **Weierstraß curves over $\mathbb{Z}_5$ and quadratic twists.** For the sake of brevity denote by $W_{a,b}$ a smooth Weierstraß curve over $\mathbb{Z}_5$ given by $y^2 = x^3 + ax + b$. Then condition for smoothness is $4a^3 + 27b^2 \neq 0$, i.e. either $a = b = 0$, or $2b^2a \not\equiv 1 \bmod 5$. The latter is the same as $b^2a \not\equiv 3 \bmod 5$. If $b^2 = 1$, then $a \neq 3$. If $b^2 = 4$, then $a \neq 2$. Hence we are considering (a, b) that **do not** belong to

$$\{(0,0),\ (2,2),\ (2,3),\ (3,1),\ (3,4)\}.$$

Further on it is always assumed that (a, b) are not from such a set.

Let us now address the question when (a, b) and $(\tilde{a}, \tilde{b})$ yield K-equivalent curves. By (M.1) this happens if and only if $\tilde{a} = a$ and $\tilde{b}b$ is a nonzero square. Hence we may restrict our attention only to the case of $b \in \{0, 1, 2\}$.

Suppose for example that $(a, b) = (1, 1)$. By direct computation, the set of affine points is equal to

$$\{(0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}.$$

This will be recorded as $\{(0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}$. Note that if $\beta^2 = \alpha^3 + a\alpha + b$, then $(-\beta)^2 = \alpha^3 + a\alpha + b$ as well.

The following table enumerates the affine points of all smooth curves $W_{a,b}$, $b \in \{0,1,2\}$. It also gives the order $N = N_{a,b}$ of the group $W_{a,b}(\mathbb{Z}_5)$ and the parameter $t = 6 - N$. By Hasse's Theorem, $|t| \leq [2\sqrt{5}] = 4$.

a	b	Affine points of $W_{a,b}$	N	t
0	1	$(0,\pm1),(2,\pm2),(4,0)$	6	0
0	2	$(2,0),(3,\pm2),(4,\pm1)$	6	0
1	0	$(0,0),(2,0),(3,0)$	4	+2
1	1	$(0,\pm1),(2,\pm1),(3,\pm1),(4,\pm2)$	9	−3
1	2	$(1,\pm2),(4,0)$	4	+2
2	0	$(0,0)$	2	+4
2	1	$(0,\pm1),(1,\pm2),(3,\pm2)$	7	−1
3	0	$(0,0),(1,\pm2),(2,\pm2),(3,\pm1),(4,\pm1)$	10	−4
3	2	$(1,\pm1),(2,\pm1)$	5	+1
4	0	$(0,0),(1,0),(2,\pm1),(3,\pm2),(4,0)$	8	−2
4	1	$(0,\pm1),(1,\pm1),(3,0),(4,\pm1)$	8	−2
4	2	$(3,\pm1)$	3	+3

Observations:

(1) The Hasse interval is equal to $[2,10]$. For each integer in the interval there exists at least one (a,b) with $N = N_{a,b}$.
(2) If $N_{a,b} \in \{2,3,5,6,7,10\}$, then $W_{a,b}(\mathbb{Z}_5)$ is cyclic since every abelian group of such an order is cyclic.
(3) Since $3 \nmid 4$, the group $W_{1,1}(\mathbb{Z}_5)$ is cyclic as well, by Theorem G.3.
(4) As will be explained, groups $W_{4,0}(\mathbb{Z}_5)$ and $W_{4,1}(\mathbb{Z}_5)$ are not isomorphic. The former group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$, while the latter group to $\mathbb{Z}_8$. Similarly, $W_{1,0}(\mathbb{Z}_5) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $W_{1,2}(\mathbb{Z}_5) \cong \mathbb{Z}_4$.
(5) Pairs (a,b) for which $a \neq 0$ and $b \neq 0$ may be grouped by two into $\{(1,1),(4,2)\}$, $\{(2,1),(3,2)\}$, $\{(1,2),(4,1)\}$. The two pairs in each of these sets share the value of ab^2, and that is equal to 1, 2 and 4, respectively. If $\{(a,b),(\tilde{a},\tilde{b})\}$ is one of these sets, then $N_{a,b} + N_{\tilde{a},\tilde{b}} = 12 = 2(q+1)$. In other words, $t_{a,b} = -t_{\tilde{a},\tilde{b}}$.

The explanation of the last phenomenon needs the notion of *j-invariant*. If C is a smooth Weierstraß curve given by $y^2 = x^3 + ax + b$ and $\mathrm{char}(K) \neq 2,3$, then the j-invariant $j(C)$ is defined as $1728\tilde{\jmath}(C)$, where $\tilde{\jmath}(C) = 4a^3/(4a^3 + 27b^2)$.

Note that $\tilde{\jmath}(C) = 0 \Leftrightarrow a = 0$, and $\tilde{\jmath}(C) = 1 \Leftrightarrow b = 0$. Thus $\tilde{\jmath}(C) \in \{0,1\}$ if and only if $ab = 0$.

If $\tilde{\jmath}(C) \notin \{0,1\}$ and $\tilde{C}$ is given by $y^2 = x^3 + \tilde{a}x + \tilde{b}$, then $\tilde{\jmath}(C) = \tilde{\jmath}(\tilde{C})$ if and only if $b^2/a^3 = \tilde{b}^2/\tilde{a}^3$.

If this is true, and the equations $y^2 = x^3 + ax + b$ and $y^2 = x^3 + \tilde{a}x + \tilde{b}$ are **not** K-equivalent, then $\tilde{C}$ is said to be a (quadratic) *twist* of C.

Let K be equal to $\mathbb{R}$ or to $\mathbb{F}_q$, where q is not divisible by 2 or 3. If $\tilde{\jmath}(C) \neq 0, 1$, then there exists $\tilde{C}$ that is a quadratic twist of C. If $\tilde{\tilde{C}}$ is another quadratic twist of C, then $\tilde{C}$ and $\tilde{\tilde{C}}$ are defined by K-equivalent Weierstraß equations.

If $K = \mathbb{F}_q$, $2 \nmid q$ and $3 \nmid q$, $\tilde{\jmath}(C) \neq 0, 1$ and $\tilde{C}$ is a quadratic twist of C, then

$$|C(\mathbb{F}_q)| + |\tilde{C}(\mathbb{F}_q)| = 2(q+1). \tag{G.3}$$

This confirms the observations above since if $K = \mathbb{Z}_5$ and $ab \neq 0$, then $b^2/a^3 = b^2 a$.

Suppose that $\tilde{\jmath}(C) = \tilde{\jmath}(\tilde{C}) \notin \{0,1\}$. To decide whether $\tilde{C}$ is a quadratic twist of C is easy. If $\tilde{b}b$ is a nonsquare, then $\tilde{C}$ is a quadratic twist. If $\tilde{b}b$ is a square, then $\tilde{C}$ and C are defined by K-equivalent Weierstraß equations.

To prove the latter from (M.1) is not difficult. Since $b^2/a^3 = \tilde{b}^2/\tilde{a}^3$ is assumed, we have $\alpha^3 = \beta^2$, where $\alpha = \tilde{a}/a$ and $\beta = \tilde{b}/b$. Put $\gamma = \beta/\alpha$. Then $\gamma^3 = (a^3\tilde{b}^3)/(\tilde{a}^3b^3) = \tilde{b}/b$ and $\gamma^2 = (a^2\tilde{b}^2)/(\tilde{a}^2b^2) = \tilde{a}/a$. If $\tilde{b}/b = \gamma^3$ is a square, then γ is also a square. If $\gamma = \lambda^2$, then $\tilde{b} = \lambda^6 b$ and $\tilde{a} = \lambda^4 a$, as required by (M.1).

The relationship between quadratic twists C and $\tilde{C}$ turns into a birational equivalence when the curves are considered over $\mathbb{F}_{q^2}$. Indeed, $\tilde{b}/b$ is always a square in $\mathbb{F}_{q^2}$. Therefore $\mathbb{F}_{q^2}(C) \cong \mathbb{F}_{q^2}(\tilde{C})$ and $C(\mathbb{F}_{q^2}) \cong \tilde{C}(\mathbb{F}_{q^2})$.

If $\tilde{\jmath}(C) \in \{0, 1\}$, then extensions of $\mathbb{F}_q$ offer even more symmetries. This is one of reasons why such curves are usually not considered to be safe for cryptographic purposes.

Let us give a proof of (G.3):

Proof. As explained above, it may be assumed that C is given by $y^2 = x^3 + ax + b$ and $\tilde{C}$ is given by $y^2 = x^3 + \gamma^2 ax + \gamma^3 b$, where $\gamma \in \mathbb{F}_q$ is a nonsquare.

For each $\alpha \in \mathbb{F}_q$ denote by $s(\alpha)$ the number of $\beta \in \mathbb{F}_q$ such that $(\alpha, \beta) \in C$, and by $\tilde{s}(\alpha)$ the number of $\beta \in \mathbb{F}_q$ such that $(\gamma\alpha, \beta) \in \tilde{C}$. Note that

$$|C(\mathbb{F}_q)| = 1 + \sum s(\alpha) \text{ and } |\tilde{C}(\mathbb{F}_q)| = 1 + \sum \tilde{s}(\alpha).$$

To finish it thus suffices to verify that $s(\alpha) + \tilde{s}(\alpha) = 2$ for each $\alpha \in \mathbb{F}_q$. Substituting $x = \gamma\alpha$ into $x^3 + \gamma^2 ax + \gamma^3 b$ yields $\gamma^3(\alpha^3 + b\alpha + c)$. This means that α is a root of $x^3 + ax + b$ if and only if $\gamma\alpha$ is a root of $x^3 + \gamma^2 ax + \gamma^3 b$. In such a case $(\alpha, 0) \in C$, $(\gamma\alpha, 0) \in \tilde{C}$ and $s(\alpha) = \tilde{s}(\alpha) = 1$. If α is not a root, then exactly one of $\alpha^3 + b\alpha + c$ and $\gamma^3(\alpha^3 + b\alpha + c)$ is a (nonzero) square in $\mathbb{F}_q$. This results into $s(\alpha) + \tilde{s}(\alpha) = 2 + 0 = 0 + 2 = 2$. □

G.2. **Tangents and cyclic subgroups.** Let C be a Weierstraß curve over K, and let P be an affine point of $C(K)$. Denote by t_P the (affine) tangent of C at P. To compute $[2]P$ is practically equivalent to finding an intersection of t_P with C. If t_P is parallel to the axis y, then $[2]P = \infty$. If this is not the case and t_P intersects C at no affine point, then $[3]P = \infty$ and $[2]P = \ominus P$. The other only remaining possibility is that t_P intersects C in $Q \neq P$. In such a case t intersects C in no other point, $[2]P = \ominus Q$, and $Q = [-2]P$.

Suppose we compute intersections of tangents with the curve for all K-rational points. Since the opposite element is easy to find, this gives us the value of $[2]P$ for every $P \in C(K)$. Hence we know $[2^k]P$ for each $k \geq 0$. If the set $\{[2^k]P;\ k \geq 1\}$ contains P, then P is of odd order, otherwise it is of even order. If P is of odd order, and $|C(K)| = 2^r\ell$, where ℓ is a prime $\equiv 3, 5 \bmod 8$, then the cyclic group generated by P coincides with the set $\{[2^k]P;\ k \geq 0\}$ since 2 is a primitive element of $\mathbb{Z}_\ell^*$.

Let us illustrate this by computing $[2]P$ for elements of of the curve C given by $y^2 = x^3 + 3x$. The tangent at $P = (\alpha, \beta)$ is given by the equation $\beta y + (\alpha^2 + 1)x + \mu = 0$, where $\mu = -\beta^2 - (\alpha^2 + 1)\alpha$. This is because $\partial(y^2 - x^3 + 2x)/\partial y = 2y$ and $\partial(y^2 - x^3 + 2x)/\partial x = 2(x^2 + 1)$.

If $\lambda y + \nu x + \mu$ gives t_P, then $-\lambda y + \nu x + \mu$ gives $t_{\ominus P}$. This is because $\ominus P = (\alpha, -\beta)$. It is thus needed to compute t_P only in four cases, as shown in the ensuing table. Recall that $P = (\alpha, \beta)$ is an involution if and only if $\beta = 0$. Thus $[2](0, 0) = \infty$, and $I = (0, 0)$ is the only involution of $C(K)$.

P	$\ominus P$	t_P and $t_{\ominus P}$	$[-2]P$	$[2]P$
$(1, 2)$	$(1, 3)$	$\pm y + x + 2$	$(4, 4)$	$(4, 1)$
$(2, 2)$	$(2, 3)$	$\pm y - 2$	$(1, 2)$	$(1, 3)$
$(3, 1)$	$(3, 4)$	$\pm y - 1$	$(4, 1)$	$(4, 4)$
$(4, 1)$	$(4, 4)$	$\pm y + 2x + 1$	$(1, 2)$	$(1, 3)$

Elements $[2]P$ form a subgroup of $W_{3,0}(\mathbb{Z}_5)$. The subgroup consists of ∞, $(1,2)$, $(1,3)$, $(4,1)$ and $(4,4)$. Set $Q = (1,2)$. Then $[2]Q = (4,1)$, $[4]Q = (1,3)$ and $[3]Q = (4,4)$.

Set now $P = (2,3)$. Then $Q = [2]P$, and we thus know each value of $[2m]P$, $m \in \mathbb{Z}$. To get $[2m+1]P$ let us consider an argument of general nature that can be used whenever I is the only involution of $C(K)$ and multiples of Q form a subgroup of $C(K)$ that is of index two and of odd order. If an affine point X is not a multiple of $Q = [2]P$, and $[2]X = [2m]Q$, then $[2](X \ominus [m]Q) = \infty$. This implies $X \ominus [m]Q = I$, and so $X = [m]Q \oplus I = [2m]P \oplus I$. Since multiples of Q form a subgroup of odd order, $2[X]$ can always be expressed as an even multiple of Q.

In our case $I = [5]P$. If, say, $X = (3,1)$, then $[2]X = (4,4) = [3]Q = [8]Q$, and so $(3,1) = [5+8]P = [3]P$. We have

$$P = (2,3),\ [2]P = (1,2),\ [3]P = (3,1),\ [4]P = (4,1),\ [5]P = (0,0),$$
$$[6]P = (4,4),\ [7]P = (3,4),\ [8]P = (1,3) \text{ and } [9]P = (2,2).$$

This describes the addition on $W_{3,0}$ completely, as $[n]P \oplus [m]P = [n+m]P$ for all $n, m \in \mathbb{Z}$.

Let us now turn to $W_{1,1}$.

P	$\ominus P$	t_P and $t_{\ominus P}$	$[-2]P$	$[2]P$
$(0,1)$	$(0,4)$	$\pm y + 2x - 1$	$(4,3)$	$(4,2)$
$(2,1)$	$(2,4)$	$\pm y + x + 2$	$(2,1)$	$(2,4)$
$(3,1)$	$(3,4)$	$\pm y + x + 1$	$(0,4)$	$(0,1)$
$(4,2)$	$(4,3)$	$\pm y - x + 2$	$(3,1)$	$(3,4)$

Put $P = (0,1)$. Then $[2]P = (4,2)$, $[4]P = (3,4)$, $[8]P = (0,4)$, $[7]P = (4,3)$ and $[5]P = (3,1)$. The value of $[3]P = (0,1) \oplus (4,2)$ has to be computed by means of (A.6) and (A.7).

We have $\lambda = 4/1 = -1$, $1 - 4 = 2$ and $[3]P = (2,1)$. Therefore $[6]P = (2,4)$. This completes the description of $W_{1,1}(\mathbb{Z}_5)$.

If C is a smooth Weierstraß curve given by $y^2 = f(x)$, then the involutions are all elements $(\alpha, 0) \in C$, and $(\alpha, 0) \in C$ if and only if $f(\alpha) = 0$. Both $W_{1,0}(\mathbb{Z}_5)$ and $W_{1,4}(\mathbb{Z}_5)$ contain three involutions. Hence they are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$, respectively. Groups $W_{1,2}(\mathbb{Z}_5)$ and $W_{4,1}(\mathbb{Z}_5)$ contain one involution each. They are cyclic.

When the order of a group is small enough to represent each of its element in computer memory, then computing with the group is easy since it suffices to choose one or two generators, and to express each of the group elements by means of these generators. For large orders this is not a viable way.

G.3. **Montgomery curves over $\mathbb{Z}_5$ and the parameter B.** By Proposition M.5, a Weierstraß equation C given by $y^2 = x^3 + ax + b$ is K-equivalent to a Montgomery curve if and only if there exists $\zeta \in K$ such that (1) $\zeta^3 + a\zeta + b = 0$, i.e. $(\zeta, 0) \in C(K)$, and (2) $f'(\zeta)$ is a nonzero square in K.

Suppose that $K = \mathbb{F}_q$, $\mathrm{char}(K) \neq 2, 3$. If (1) holds, then $|C(K)|$ cannot be a prime > 2 since $|C(K)|$ is even. If both (1) and (2) hold, then $|C(K)|$ is divisible by four—a fact that is not completely obvious, but may be proved with a bit of effort. The ideal situation when the cofactor c is equal to 1 hence cannot occur. This is not the only situation when there is a tradeoff between the efficiency of computation and structural parameters.

Before turning to $\mathbb{Z}_5$ let us make a general observation. If 3 is a nonsquare in K, then (2) cannot hold if $a = 0$. Indeed, in that case $f'(\zeta) = 3\zeta^2$ is a nonsquare or a zero.

As explained above, up to $\mathbb{Z}_5$-equivalence there are 12 smooth Weierstraß curves over $\mathbb{Z}_5$. Eight of them are of even order. These are those for which condition (1) may be fulfilled. To fulfill (2) the curves $W_{a,b}$ with $a = 0$ may be put aside. This leaves us with (A) $(a, b) \in \{(1, 0), (2, 0), (3, 0), (4, 0)\}$ and (B) $(a, b) \in \{(1, 2), (4, 1)\}$. If $b = 0$, then $\zeta = 0$ is always a possibility. In that case $f'(\zeta) = a$ should be a square, and that restricts (A) to $(1, 0)$ and $(4, 0)$. In the former case $\zeta = \pm 2$ needs also be tested. However, $3 \cdot 4 + 1$ is not a square. In the latter case $\zeta = \pm 1$ does not supply a square as well. This means that (A) supplies two possibilities. Another two possibilities come from (B).

Now, $(x + \zeta)^3 + a(x + \zeta) + b = x^3 + 3\zeta x^2 + f'(\zeta)x$ holds over any field K, $\mathrm{char}(K) \neq 2, 3$, cf. the proof of Proposition M.5. That makes $y^2 = x^3 + ax + b$ an equation that is K-equivalent to $y^2 = x^3 + 3\zeta x^2 + B^2 x$, where $B^2 = f'(\zeta)$. Setting $A = 3\zeta/B$ gives the other parameter of the Montgomery curve.

The four cases over $\mathbb{Z}_5$ that were identified above yield the following parameters:

a	b	ζ	3ζ	$f'(\zeta)$	B	A
1	0	0	0	1	1	0
4	0	0	0	4	2	0
1	2	4	2	4	2	1
4	1	3	4	1	1	4

Up to $\mathbb{Z}_5$-equivalence there are thus four smooth Montgomery curves over $\mathbb{Z}_5$:

$$M_{1,0}\colon y^2 = x^3 + x, \qquad M_{4,0}\colon 2y^2 = x^3 + x,$$
$$M_{1,2}\colon 2y^2 = x^3 + x^2 + x, \qquad M_{4,1}\colon y^2 = x^3 + 4x^2 + x.$$

Curves $M_{1,0}$ and $W_{1,0}$ are the same. For the other three curves the affine points are listed below, using the rational mapping $C \to M$, $(\alpha_1, \alpha_2) \mapsto ((\alpha_1 - \zeta)/B, \alpha_2/B^2)$.

$$M_{4,0}\colon (0, 0), (1, \pm 1), (2, 0), (3, 0), (4, \pm 2);$$
$$M_{1,2}\colon (0, 0), (1, \pm 2);$$
$$M_{4,1}\colon (0, 0), (1, \pm 1), (2, \pm 1), (3, \pm 1).$$

The change $(A, B) \mapsto (-A, -B)$ gives $\mathbb{Z}_5$-equivalent equations $4y^2 = x^3 + x$, $3y^2 = x^3 + x$, $3y^2 = x^3 + 4x^2 + x$ and $4y^2 = x^3 + x^2 + x$. This still does not cover all possible parameters for Montgomery curves that may occur over $\mathbb{Z}_5$. We shall now explain how the remaining cases are $\mathbb{Z}_5$-equivalent to the already described cases.

Let us take a more general perspective. Let M be a Montgomery curve given by (A, B) over K. If $\tilde{M}$ is given by $(-A, -B)$, then $(\alpha, \beta) \mapsto (-\alpha, \beta)$ is a K-rational mapping $M \leftrightarrow \tilde{M}$.

If $\lambda \in K^*$ and $\tilde{M}$ is given by $(A, \lambda^2 B)$, then $(\alpha, \beta) \mapsto (\alpha, \lambda\beta)$ is a K-rational mapping $\tilde{M} \to M$.

The latter means that if $\vartheta \in K$ is a nonsquare such that each element of K is equal to λ^2 or $\vartheta\lambda^2$ for some $\lambda \in K$, then each Montgomery curve over K is K-equivalent to a Montgomery curve with parameters $(A, 1)$ or (A, ϑ). This means that if $K = \mathbb{F}_q$, then the following is true:

Proposition G.4. *Let $q > 1$ be a prime power not divisible by 2 and 3.*

- *If $q \equiv 3 \bmod 4$, then each Montgomery curve is $\mathbb{F}_q$-equivalent to a curve given by $y^2 = x^3 + Ax^2 + x$, $A \in \mathbb{F}_q$.*
- *If $q \equiv 1 \bmod 4$ and $\vartheta \in \mathbb{F}_q$ is a nonsquare, then each Montgomery curve is $\mathbb{F}_q$-equivalent to a curve given by $y^2 = x^3 + Ax^2 + x$, or by $\vartheta y^2 = x^3 + Ax^2 + x$, $A \in \mathbb{F}_q$.*

Proof. As explained above, each Montgomery curve is $\mathbb{F}_q$-equivalent to $y^2 = x^3 + Ax^2 + x$ or $\vartheta y^2 = x^3 + Ax^2 + x$. If $q \equiv 3 \bmod 4$, then ϑ may be chosen as

-1. If this is true, then the latter curve is $\mathbb{F}_q$-equivalent to the curve given by $y^2 = x^3 - Ax^2 + x$. □

G.4. **Edwards curves over $\mathbb{Z}_5$.** Consider an Edwards curve $y^2 + x^2 = 1 + dx^2y^2$. If d is a nonsquare, then the addition upon the curve may be described by a uniform (i.e. closed) formula.

There exists a simple criterion that decides whether a smooth Weierstraß curve C over K, $\mathrm{char}(K) \neq 2, 3$ is K-equivalent to an Edwards curve with d a nonsquare. This happens if and only if $C(K) \cong \mathbb{Z}_4 \times H$, where $|H|$ is odd.

This criterion is satisfied over $\mathbb{Z}_5$ if and only if $C = W_{1,2}$ or $C = W_{4,1}$. This matches the fact that 2 and 3 are the only nonsquares modulo 5.

By Theorem E.7, an Edwards curve E with parameter d is birationally equivalent to a Montgomery curve M with parameters $A = 2(1+d)/(1-d)$ and $B = 4/(1-d)$, and the birational mapping $M \to E$ sends (α, β) to $(\alpha/\beta, (\alpha-1)/(\alpha+1))$, assuming $\beta \neq 0$ and $\alpha \neq -1$.

Let E be defined over $\mathbb{Z}_5$, and let $d = 2$. Then $A = 4$ and $B = 1$. Thus $M = M_{4,1}$. This is the reason why E will be denoted by $E_{4,1}$. Similarly, if $d = 3$, then E is denoted by $E_{1,2}$ since it is birationally equivalent to $M_{1,2}$. Both $E_{1,2}$ and $E_{4,1}$ contain points $(0, \pm 1)$ and $(\pm 1, 0)$. Using this fact and the birational mapping described above we get:

$$d = 3 \quad E_{1,2} \colon (0, \pm 1), (\pm 1, 0);$$
$$d = 2 \quad E_{4,1} \colon (0, \pm 1), (\pm 1, 0), (\pm 2, 2), (\pm 2, 3);$$

Suppose now that $d = 4$. Then $A = 0$, $B = 2$. The Edwards curve is hence denoted by $E_{4,0}$. For this curve the completed coordinates have to be used if all $\mathbb{Z}_5$-rational points are to be described by coordinates. Since $((2 : 1), (1 : 0))$ fulfils (E.6), the $X \leftrightarrow Y$ symmetry yields the following list of points:

$$d = 4 \quad E_{4,0} \colon ((\pm 1 : 1), (0 : 1)), ((0 : 1), (\pm 1, 1)), ((\pm 2 : 1), (1 : 0)), ((1 : 0), (\pm 2 : 1)).$$

There remains to consider only one class of Montgomery curves over $\mathbb{Z}_5$, and that is the class represented my $M_{1,0} = W_{1,0}$. By Theorem E.7 and Lemma E.6 this curve is birationally equivalent to the twisted Edwards curve with $(a, d) = (2, 3)$. The curve is denoted by $E_{1,0}$. Since we know that $|E_{1,0}(\mathbb{Z}_5)| = 4$, it is easy to verify that it consists of the following points:

$$(a, d) = (2, 3) \quad E_{1,0} \colon ((0 : 1), (\pm 1, 1)), ((1 : 0), (\pm 2 : 1)).$$

Up to now four different twisted Edwards curves have been explicitly described. Of course, that does not exhaust all possible parameters (a, d). However, results of this section allow to find a birational equivalence over $\mathbb{Z}_5$ for each other possible choice. As an example consider the case $(a, d) = (2, 1)$. This is birationally equivalent, by Theorem E.7, to a Montgomery curve with parameters $(A, B) = (1, 4)$, and thus to a Montgomery curve with parameters $(A, B) = (1, 1)$. The equation for this curve is $y^2 = x^3 + x^2 + x$, which is $\mathbb{Z}_5$-equivalent to $y^2 = x^3 - x - 1$, and thus also to $y^2 = x^3 - x + 1$. That is $W_{4,1}$.

While $E_{4,1}$ consists of 8 affine points, the curve given by $2x^2 + y^2 = 1 + x^2y^2$ contains exactly 6 affine points. These are $(\pm 2, \pm 2)$ and $(0, \pm 1)$. The other two points need the completed coordinates. The two points at infinity are $((\pm 1 : 1), (1 : 0))$.