Mordell–Weil Lattices in Characteristic 2, III: A Mordell–Weil Lattice of Rank 128

Noam D. Elkies

CONTENTS

We analyze the 128-dimensional Mordell–Weil lattice of a certain elliptic curve over the rational function field $k(t)$, where k is a finite field of 2^{12} elements. By proving that the elliptic curve has trivial Tate–Šafarevič group and nonzero rational points of height 22, we show that the lattice's density achieves the lower bound derived in our earlier work. This density is by a considerable factor the largest known for a sphere packing in dimension 128. We also determine the kissing number of the lattice, which is by a considerable factor the largest known *for a lattice* in this dimension.

1. INTRODUCTION

In [Elkies 1994], the first paper of this series — from now on referred to as Part I — we constructed a family of lattices in dimensions 2^{n+1} for positive integers n. From the theory of elliptic curves over function fields we obtained upper bounds on the discriminants and lower bounds on the minimal norms of these lattices, showing that their associated lattice packings of spheres equal the previous records for $n \leqslant 4$ and exceed them for $5 \leqslant n \leqslant 9$. We then showed, for $n = 5$ (the first case of a new record), that our lower bound on the density of the lattice packing in $\mathbb{R}^{64}$ is sharp, and reported on the computation of the kissing number of the lattice, which was at the time the largest kissing number known in $\mathbb{R}^{64}$. Both of these records have since been superseded by G. Nebe [1998], and the kissing number was pushed still higher by a nonlattice packing [Edel et al. 1998]. Thus $n = 6$ is now the first case in which the construction of Part I yields a previously unknown lattice of record density.

In this paper we analyze this 128-dimensional lattice MW_{128}. We determine its density, again showing that the lower bound from Part I is sharp by proving that the elliptic curve (see (2–1) below) has

1058-6458/2001 $0.50 per page
Experimental Mathematics 10:3, page 467

trivial Tate–Šafarevič group and nonzero rational points of height 22, as small as possible by Proposition 2 of Part I. We then report on a computation that determined all the rational points of that minimal height, thus obtaining the kissing number of MW_{128}. Like the packing density, the kissing number of MW_{128} is by a considerable factor the largest known kissing number *of a lattice* in this dimension, though once more [Edel et al. 1998] gives a much larger nonlattice kissing configuration.

MW_{128} is the Mordell–Weil lattice of an elliptic curve (2–1) over the rational function field $k(t)$, for k a finite field of 2^{12} elements. To compute the minimal vectors of MW_{128} we listed all solutions in k of a system of simultaneous nonlinear equations in several variables (the coefficients of x as a polynomial in t). We reduced the search space by using the automorphisms of MW_{128} described in Part I and solving for some of the variables. This left about $2 \cdot 10^{12}$ possibilities on which to check the remaining, now much more complicated, equations. An exhaustive search over this space would still take months on a single fast computer. Fortunately the first of these equations can be written as a quadratic in one of the variables; this reduced the search space by three orders of magnitude, to the point that the computer time was comparable to the time it took to program the search. The relatively simple form of that equation, though welcome, was unexpected and is still unexplained. This is one of several open questions we raise in the concluding section of the present paper.

2. STATEMENT OF RESULTS

To simplify notation we henceforth denote the lattice MW_{128} by M. We refer to the earlier papers in this series [Elkies 1994; 1997] as Parts I and II.

Let k be a finite field of $2^{12} = 4096$ elements, let K be the rational function field $k(t)$, and let E/K be the potentially constant elliptic curve

$$y^2 + y = x^3 + t^{65} + a_6, \tag{2–1}$$

where a_6 is any of the 2^{11} elements of k whose absolute trace $\sum_{m=0}^{11} a_6^{2^m}$ equals 1. (As noted in Parts I and II, all these choices of a_6 yield isomorphic curves; if we worked over $\bar{k} = \overline{\mathbb{F}}_2$ instead of k, we could drop a_6 and simplify the equation of E to $y^2 + y = x^3 + t^{65}$.) Let M be the Mordell–Weil group of E, consisting of $\mathbf{0}$ together with solutions $(x, y) \in K \times K$ of (2–1). The map

$$\phi : E \to E,\ (x, y) \mapsto (x^2, y^2 + t^{65} + a_6)$$

is an inseparable 2-isogeny whose square is multiplication by -2. By Theorem 2 of Part I, the image of ϕ on $E(K)$ is the kernel of the map

$$\epsilon : E(K) \to K/K^2, \qquad \mathbf{0} \mapsto 0,\ (x, y) \mapsto x \bmod K^2$$

in which K and K^2 have the structure of additive groups.

Theorem. (i) *M has rank 128 and trivial torsion.*

(ii) *The canonical height $\hat{h}$ on M is given by $\hat{h}(\mathbf{0}) = 0$ and $\hat{h}(x, y) = \deg x$, the degree of x as a rational function of t. This height gives M the structure of an even integral lattice in Euclidean space of dimension 128.*

(iii) *The Selmer group for ϕ is the subspace S of K/K^2 represented by the polynomials of the form*

$$\left(x_{21}t^{21}+x_{21}^4t^{19}+x_{21}^{16}t^{11}\right) + \left(x_{17}t^{17}+x_{17}^4t^3\right) + x_{13}t^{13} + x_9t^9 + x_5t^5 + x_1t \tag{2–2}$$

with

$$x_j \in k, \quad x_{13}^{16} = x_{13}; \tag{2–3}$$

S is an elementary abelian 2-group of rank

$$12 + 12 + 4 + 12 + 12 + 12 = 64.$$

(iv) *The Tate–Šafarevič group of E/K is trivial. The discriminant of M is 2^{120}.*

(v) *The minimal norm of M is 22, attained by (x, y) if and only if x, y are polynomials in t of degrees 22 and 33 respectively. There are*

$$218044170240 = 2^{17}\ 3\ 5\ 13\ 19\ 449 \tag{2–4}$$

vectors of this minimal norm in M.

(vi) *The normalized center density of M is*

$$11^{64}/2^{124} = 2^{97.4036+}. \tag{2–5}$$

3. PROOF OF PARTS (i)–(iv): RANK, DISCRIMINANT, AND Tate–Šafarevič GROUP

Each of (i), (ii), and the implication (iii)$\Longrightarrow$(iv) is contained in the special case $(n, q) = (6, 64)$ of the results in Part I. We briefly go over these in the next two paragraphs.

Define curves C, E_0 over k by

$$C : u^2 + u = t^{65}, \qquad E_0 : Y^2 + Y = X^3 + a_6.$$

Then E_0 is a supersingular elliptic curve, and C is a hyperelliptic curve of genus 32 whose Jacobian $\operatorname{Jac}(C)$ is isogenous with E_0^{32} (Part I, Proposition 1). The K-rational points of E correspond bijectively with maps from C to E_0 that take the point at infinity of C to the origin of E_0: such a map is either constant or of the form $(t,u) \mapsto (x(t), y(t)+u)$ with (x,y) a nonzero point of E. This correspondence respects the group laws on E and E_0, and yields an identification of M with $\operatorname{Hom}(\operatorname{Jac}(C), E_0)$, a group of the same rank as $\operatorname{Hom}(E_0^{32}, E_0) = \operatorname{End}(E_0)^{32}$. Thus M has rank $4 \cdot 32 = 128$, as claimed in (i). The formula for $\hat{h}$ and the fact that $\hat{h}(P) \in 2\mathbb{Z}$ for all $P \in M$ are the case $(n,q) = (6, 64)$ of Part I, Proposition 2.

The discriminant of the Mordell–Weil lattice of an elliptic curve over a global field is related to the order of the curve's Tate–Šafarevič group by the conjecture of Birch and Swinnerton-Dyer. In our case of a curve over a function field, this conjecture was formulated by Artin and Tate [Tate 1968] and proved under certain hypotheses by Milne [1975].[1] In Theorem 1 of Part I we observed that these hypotheses were satisfied by each of our curves E, and computed the resulting relationship between the order of the Tate–Šafarevič group $Ш(E)$ and the discriminant Δ of its Mordell–Weil lattice. Their product is always a power of 2, so $Ш(E)$ is a 2-group, and is trivial if and only if $Ш_\phi$ is trivial; that is, if and only if $E(K)/\phi(E(K))$ is all of the Selmer group for ϕ. Now $E(K)/\phi(E(K))$ is an elementary abelian 2-group whose rank is half the rank of $E(K)$, because $\phi^2 = -2$. In our present case of $q = 64$, we already know that the half-rank is $128/2 = 64$, so once we prove (iii) the triviality of $Ш(E)$ will follow. The formula of Theorem 1 of Part I gives

$$|Ш(E)|\,\Delta = 2^{120},$$

for $q = 64$, so the discriminant claim of (iv) will follow as well.

It remains to verify that the ϕ-Selmer group is given by (2–2), (2–3). The analysis proceeds as in Part I (for $y^2+y = x^3+t^{33}$) and Part II (for $y^2+y = x^3 + t^{13} + a_6$), but takes more steps to complete. As happened there, it is enough to show that S is contained in the Selmer group, because it has the correct size $2^{128/2}$. The Selmer group consists of 0 together with all elements of K/K^2 that represent the x-coordinate of a solution of (2–1) with x, y in $k((t^{-1}))$, the completion of K at the place $t = \infty$.

By Theorem 2 of Part I, every element of the ϕ-Selmer group has a unique representative ξ that is an odd polynomial in t (that is, a k-linear combination of t^j for odd positive integers j) whose degree d satisfies $3d < 65$ and $d \equiv 65 \bmod 4$. Thus d is one of $1, 5, 9, 13, 17, 21$. We give the proof in the case $d = 21$, which is also relevant to our computation of the minimal vectors. The other cases are similar but easier. Alternatively, once we find a single $P_0 \in M$ with $\hat{h}(P) = 22$, and thus with $\epsilon(P_0)$ represented by a polynomial of degree 21, we know that for any other point P at least one of $\epsilon(P)$ and $\epsilon(P+P_0)$ has $d = 21$; so once we have done $d = 21$ the other cases will follow.

Suppose $x = \sum_{j=-\infty}^{d'} x_j t^j$ is the x-coordinate of a point of E over $k((t^{-1}))$, with $x_{21} \neq 0$. Necessarily $d' = (65-d)/2 = 22$. Let

$$\eta := x^3 + t^{65} + a_6 = \sum_{j=-\infty}^{66} \eta_j t^j.$$

since

$$x^3 = x \cdot x^2 = \Bigl(\sum_{j=-\infty}^{22} x_j t^j\Bigr)\Bigl(\sum_{j=-\infty}^{22} x_j^2 t^{2j}\Bigr),$$

we have $\eta_{65} = x_{21}x_{22}^2 + 1$ and

$$\eta_j = \sum_{j_1+2j_2=j} x_{j_1} x_{j_2}^2$$

for all $j \neq 0, 65$. By the Lemma in Part I, if η is of the form $y^2 + y$ for some $y \in K((t^{-1}))$ then

$$\sum_{m=0}^{\infty} (\eta_{2^m j_0})^{2^{-m}} = 0 \tag{3–1}$$

for each odd $j_0 > 0$ (note that this sum is finite, and the fractional exponents make sense in k). Taking $j_0 = 65, 63, 61, \ldots$ in (3–1), and using MACSYMA to simplify the resulting equations, we find the results shown at the top of the next page.

[1] As noted in Part II, Milne had to also assume odd characteristic, but this assumption was later eliminated by work of Illusie [1979], so we may use Milne's results also in our characteristic-2 setting.

$$
\begin{aligned}
j_0 = 65: &\quad x_{22} = x_{21}^{-1/2} \\
j_0 = 63: &\quad x_{19}x_{22}^2 + x_{21}^3 = 0 \qquad\qquad \Longrightarrow\ x_{19} = x_{21}^4 \\
j_0 = 61: &\quad x_{17}x_{22}^2 + x_{19}x_{21}^2 + x_{21}x_{20}^2 = 0 \quad \Longrightarrow\ x_{20} = \bigl(x_{21}^{-1}(x_{21}^{-1}x_{17} + x_{21}^7)\bigr)^{1/2} = x_{21}^{5/2} + x_{21}^{-1}x_{17}^{1/2} \\
j_0 = 59: &\quad x_{15} = x_{21}\bigl(x_{17}x_{21}^2 + (x_{21}^9 + x_{21}^2x_{17}) + x_{21}^9\bigr) = 0 \\
j_0 = 57: &\quad x_{18} = a_{21}^{11/2} + a_{21}^2a_{17}^{1/2} + a_{21}^{-3/2}a_{17} + a_{21}^{-1}a_{13}^{1/2} \\
j_0 = 55: &\quad x_{11} = x_{21}\bigl(x_{13}x_{21}^2 + x_{17}x_{21}^8 + x_{21}^4x_{18}^2 + x_{21}x_{17}^2\bigr) = x_{21}^{16} \\
j_0 = 53: &\quad x_{16} = a_{21}^{17/2} + a_{21}^5a_{17}^{1/2} + a_{21}^{-2}a_{17}^{3/2} + a_{21}^2a_{13}^{1/2} + a_{21}^{-1}a_9^{1/2} \\
j_0 = 51: &\quad x_7 = x_{21}\sum_{j=15}^{21} x_j^2x_{51-2j} = \cdots = 0 \\
j_0 = 49: &\quad x_{14} = x_{21}^{-1/2}\sum_{j=15}^{22} x_jx_{49-2j}^{1/2} = x_{21}^{23/2} + x_{21}^8x_{17}^{1/2} + x_{21}^{9/2}x_{17} + x_{21}^{-5/2}x_{17}^2 + x_{21}^{-2}x_{13}^{1/2}x_{17} + x_{21}^5x_{13}^{1/2} \\
&\qquad\qquad + x_{21}^{-3/2}x_{13} + x_{21}^2x_9^{1/2} + x_{21}^{-1}x_5^{1/2} \\
j_0 = 47: &\quad x_3 = x_{21}\sum_{j=13}^{21} x_j^2x_{47-2j} = \cdots = x_{17}^4
\end{aligned}
$$

In particular, for each odd j the coefficient x_j depends on the ξ coefficients $x_1, x_5, x_9, x_{13}, x_{17}, x_{21}$ according to (2–2). To finish the proof of (iii) we must also show that x_{13} is in the 16-element subfield of k. Continuing our computation we find that the conditions (3–1) with $j_0 = 45, 41, 37$ yield (increasingly complicated) formulas for x_{12}, x_{10}, x_8 in terms of the ξ coefficients, while the conditions with $j_0 = 43, 39, 35$ are satisfied automatically. When $j_0 = 33$, the first case in which the sum in (3–1) has more than one term, we obtain a much longer expression for x_6. When this and our previous formulas are substituted into the $j_0 = 31$ condition $\eta_{31}^2 = \eta_{62}$, all but two of the terms cancel, leaving only $x_{13}^{16} + x_{13} = 0$, and we are done.

This massive cancellation and the simple equations for $x_3, x_7, x_{11}, x_{15}, x_{19}$ are in striking contrast to the increasingly complicated formulas for x_j with j even. But the coefficients of odd order are constrained by the requirement that they constitute a group. Moreover, the Selmer group inherits the symmetries of M coming from the automorphisms of C noted in Equation 10 of Part I. Namely, if $x(t) \bmod K^2$ is in the Selmer group, then so is $x(at+b) \bmod K^2$ for all $a, b \in k$ such that $a^{65} = 1$. This severely constrains the possibilities for the Selmer group; for instance, x_{15} must vanish, and x_{19} must be proportional to x_{21}^4, else we could use linear combinations of $x(at)$ with $a^{65} = 1$ to obtain a solution in $k((t^{-1}))$ of (2–1) with x a square plus a polynomial of degree 19 or 15, contradicting Theorem 2 of Part I. (Similar arguments arise in Dummigan's investigation [Dummigan 1995] of the Tate–Šafarevič groups of certain constant elliptic curves related to those of Part I.) The even-order coefficients need not constitute a group, but are still constrained by the invariance under the $65 \cdot 2^{12}$ transformations $t \mapsto at + b$; this provides a sanity check on our formulas for those coefficients.

4. PARTS (v)–(vi): MINIMAL NORM, DENSITY, AND KISSING NUMBER

By Theorem 1 of Part I, any nonzero $(x, y) \in M$ has height at least 22, with equality if and only if x, y are polynomials in t of degrees 22 and 33. Thus we can prove that M has minimal norm 22, and normalized norm density given by (2–5), by finding a single such pair (x, y). To verify that the kissing number is given by (2–4) we must enumerate all (x, y) of that form.

To find these (x, y), set $x_j = 0$ for all $j < 0$, write η_j $(0 \leqslant j \leqslant 66)$ as polynomials in $x_0, \ldots, x_{22}$, and solve (3–1) for each odd $j_0 \leqslant 65$ together with the equation

$$\eta_0 = x_0^3 = y(0)^2 + y(0) + a_6 \tag{4–1}$$

for the constant coefficient $y(0)$ of y. We have already used the equations for $j_0 \geqslant 35$ to solve for all x_j except x_0, x_2, x_4 in terms of the ξ coefficients; the $j_0 = 29$ and $j_0 = 25$ equations give us x_4 and x_2 as well, and $j_0 = 21$ determines $x_0^4 + x_0$. (We already saw in Equation 21 of Part I that, due to automorphisms of E_0 of order 4, if $(x, y) \in M$ and $c^4 = c$ then $x + c$ is also the x-coordinate of a rational point of E; thus even once we know all x_j for $j > 0$ we can at most determine $x_0^4 + x_0$, not x_0.) Meanwhile, the $j_0 = 23$ equation simplifies to $x_{21}^{4095} = 1$, which only confirms that $x_{21} \in k^*$. The remaining ten equations, for $j_0 = 19$ through $j_0 = 1$, yield complicated polynomial equations in the six ξ coefficients.

Finding a single solution turns out to be easy: set $x_{21} = 1$ and $x_{17} = x_{13} = x_9 = x_5 = 0$, when the equations for $j_0 \geqslant 25$ give

$$\begin{aligned} x = t^{22} &+ t^{21} + t^{20} + t^{19} + t^{18} + t^{16} + t^{14} + x_1 t^{12} + t^{11} \\ &+ (x_1{+}1)t^{10} + x_1 t^8 + x_1 t^6 + (x_1{+}1)t^4 \\ &+ x_1^2 t^2 + x_1^2 t + x_0, \end{aligned} \tag{4–2}$$

and the $j_0 = 19, 21$ equations yield the conditions

$$x_1^2 + x_1 + 1 = 0, \quad x_0^4 + x_0 = x_1 \tag{4–3}$$

on the unknown coefficients x_0, x_1. We calculate that the equations (3–1) for the remaining j_0 are then satisfied automatically. This leaves only (4–1), which as expected has solutions $y(0) \in k$. (In all 8 solutions of (4–3), x_1 and x_0 are of degrees $2, 4$ respectively over $\mathbb{F}_2$; thus x_0^3 is a fifth root of unity, so its trace as an element of k equals 1, whence $x_0^3 + a_6$ is of the form $y(0)^2 + y(0)$ with $y(0) \in k$.) This proves that M has minimal norm 22 and normalized center density $11^{64}/2^{124}$.

Enumerating all the minimal vectors is a more demanding task. There are $2^{64} - 2^{52}$ possibilities for the ξ coefficients, far too many for an exhaustive search. But our equations have many automorphisms, coming from the symmetries of M described in Part I, after the proof of Proposition 2. We saw already the $65 \cdot 2^{12}$ maps

$$x(t) \mapsto x(at + b) \quad (a, b \in k,\ a^{65} = 1).$$

We may augment these by $x \mapsto \alpha x$ for α^3 (again inherited from $\mathrm{Aut}(E_0)$) and by the twelve field automorphisms of k (Part I, Equation 22). This lowers the total to $(63 \cdot 2^{40})/(3 \cdot 12) \approx 2 \cdot 10^{12}$. The 8-element quaternion group acting on E_0 also acts on the minimal vectors, but only by permuting the 8 choices of x_0 and $y(0)$ associated to each valid sextuple of ξ coefficients. Thus these automorphisms do not further cut down our search space, though the condition that x_0 and $y(0)$ must be in k will somewhat reduce the average work per candidate.

We might now organize the search as follows. Initialize various tables for arithmetic in k, such as multiplication and multiplicative inverse, squaring, and exponentiation. (For addition we use the bitwise exclusive-or operator that is already built into the programming language C.) Using the automorphisms $t \mapsto at$, we may assume that x_{21} is in the quadratic subfield $\mathbb{F}_{64}$ of k. Thanks to $x \mapsto \alpha x$, we may further limit attention to one representative of each of the 21 cosets of the cube roots of unity in $\mathbb{F}_{64}^*$. Each of these 21 choices of x_{21} then represents $3(2^6 + 1) = 195$ choices of x_{21} in k^*. Then, since $t \mapsto t + b$ fixes x_{21} and translates x_{17} by

$$\begin{aligned} b^4 x_{21} + b^2 x_{19} &= b^4 x_{21} + b^2 x_{21}^4 \\ &= x_{21}^7 \big((b^2 x_{21}^{-3})^2 + b^2 x_{21}^{-3} \big), \end{aligned}$$

we may assume that x_{17} is either 0 or $x_{21}^7 a_6$, each possibility representing 2^{11} choices of $x_{17} \in k$ and still invariant under one translation $t \leftrightarrow t + x_{21}^{3/2}$. This translation does not affect x_{13}, but (for most choices of x_{21} and x_{13}) does move x_9. Using this translation as well as the 12 field automorphisms reduces the $21 \cdot 2 \cdot 2^4 \cdot 2^{12} = 21 \cdot 2^{17}$ possibilities for $(x_{12}, x_{17}, x_{13}, x_9)$ to slightly over $21 \cdot 2^{17}/24$ or about 10^5 choices. For each of these, we use the equations at the top of page 470, or the recursion (3–1), to compute $x_{22}, x_{20}, x_{19}, x_{18}, x_{16}, x_{11}, x_3$. Then loop over 2^{24} choices of $x_5, x_1 \in k$. For each one, solve the equations (3–1) with $j_0 = 45, 41, 37, 33, 29, 25, 21$ to obtain $x_{12}, x_{10}, x_8, x_6, x_4, x_2$, and $x_0^4 + x_0$. Look up a precomputed table to choose x_0 and solve (4–1) for $y(0)$, if solutions exist in k (if not, proceed to the next (x_5, x_1) pair). If one of the eight possible $(x_0, y(0))$ is defined over k, then all are, but we need only try one because they constitute an orbit under the 8-element quaternion group. Using the chosen x_0, check whether the conditions (3–1) for odd $j_0 \leqslant 19$ are all satisfied. The kissing number is the sum of the orbit sizes of the resulting minimal points of E.

Unfortunately the size $2 \cdot 10^{12}$ of the search space is too large for this computation to conclude in reasonable time. Fortunately the $j_0 = 19$ equation, expanded as a polynomial in the ξ coefficients, is a quadratic equation in x_1^{16}, namely

$$Ax_1^{32} + A^2 x_1^{16} = B, \tag{4–4}$$

where

$$\begin{aligned} A &= x_{21}^{288} x_{13} + x_{21}^{192} x_9^{16} + x_{21}^{96} x_5^{16} + x_{21}^{496}, \\ B &= (x_{21}^{272} + x_{13} x_{21}^{64}) x_9^{64} + x_{21}^{576} x_9^{48} \\ &\quad + (x_{21}^{480} x_5^{16} + x_{21}^{880} + x_{13} x_{21}^{672} + x_{21}^{100} + x_{13}^4 x_{21}^{48}) x_9^{32} \\ &\quad + (x_{21}^{384} x_5^{32} + x_{21}^{1184} + x_{13}^2 x_{21}^{768}) x_9^{16} + x_{21}^{288} x_5^{48} \\ &\quad + (x_{21}^{688} + x_{13} x_{21}^{480}) x_5^{32} + (x_{13}^2 x_{21}^{672} + x_{13}^4 x_{21}^{256}) x_5^{16} \\ &\quad + (x_{21}^{608} + x_{13}^2 x_{21}^{192}) x_5^4 + x_{13}^3 x_{21}^{864} + x_{21}^{708} + x_{13}^5 x_{21}^{448} \\ &\quad + x_{13}^2 x_{21}^{292} + x_{13}^2 x_{21}^{97}. \end{aligned}$$

Ugly as this may look, it is much better than looping over x_1 — especially since most of the computation of B can be done independently of x_5. Except in the rare case that $A = B = 0$, we are thus left with either 2 or 0 choices of x_1 for each $x_{21}, x_{17}, x_{13}, x_9, x_5$. It is then feasible to test every possible $(x_{21}, x_{17}, x_{13}, x_9, x_5, x_1)$ as outlined in the preceding paragraph.

We ran this computation and found a total of 2940 orbits of minimal points, with stabilizers of orders distributed as follows:

$\lvert\mathrm{Stab}\rvert$	=	1	2	3	4	6	8	12	24
#	=	2766	134	21	11	3	1	3	1

(For instance, (4–2)–(4–3) is in one of the orbits with a 6-element stabilizer, coming from $\mathrm{Gal}(k/\mathbb{F}_4)$. See http://www.math.harvard.edu/~elkies/mv128.txt for a full list of orbit representatives.) Summing $1/\lvert\mathrm{Stab}\rvert$ over the orbits, and multiplying the resulting total of $8531/3$ by the number $2^{12} \cdot 65 \cdot 24 \cdot 12$ of known automorphisms of M, we obtain the kissing number (2–4) of M. □

5. REMARKS AND QUESTIONS

The unique orbit with a 24-element stabilizer is represented by a point P with ξ coefficients

$$(x_{21}, x_{17}, x_{13}, x_9, x_5, x_1) = (1,\ a,\ 1,\ a{+}1,\ a^3{+}a^2{+}a,\ a^2{+}1),$$

where a is a fifth root of unity. This formula shows three stabilizing automorphisms (from $\mathrm{Gal}(k/\mathbb{F}_{16})$), but in fact P is stabilized by two automorphisms for each element of $\mathrm{Gal}(k/\mathbb{F}_2)$: translating t by either a^3 or $a^3 + 1$ has the same effect on its x-coordinate as applying the Galois automorphism $c \mapsto c^2$ of k. This yields a cyclic stabilizer of order 24.

Can the simple form $Ax_1^{32} + A^2 x_1^{16} = B$ of (4–4) be explained conceptually? Can the kissing number (2–4), and more generally the kissing numbers of our Mordell–Weil lattices in dimensions 2^{n+1}, be obtained without such a long computation (which seems out of the question already for the next case $n = 7$)? Must there always be some nonzero vectors in the narrow Mordell–Weil lattice whose norm attains the lower bound $2\lfloor (2^n{+}4)/6 \rfloor$ of Theorem 1 of Part I? Finally, can it be shown that the $48n(q^3{+}q^2)$ known automorphisms of $MW_{2^{n+1}}$ constitute its full automorphism group once $n \geqslant 4$?

A final remark: multiplication of t by a fifth root of unity generates an automorphism of M of order 5; the sublattice fixed by this automorphism is the Mordell–Weil lattice of $y^2 + y = x^3 + t^{13} + a_6$, and is thus homothetic with the Leech lattice by the results of Part II.

ACKNOWLEDGEMENTS

This work was made possible in part by funding from the National Science Foundation and from the Packard Foundation. I thank the Mathematical Sciences Research Institute for its hospitality while I wrote this paper.

REFERENCES

[Dummigan 1995] N. Dummigan, "The determinants of certain Mordell–Weil lattices", *Amer. J. Math.* **117**:6 (1995), 1409–1429.

[Edel et al. 1998] Y. Edel, E. M. Rains, and N. J. A. Sloane, "On kissing numbers in dimensions 32 to 128", *Electron. J. Combin.* **5**:1 (1998), RP22.

[Elkies 1994] N. D. Elkies, "Mordell–Weil lattices in characteristic 2, I: Construction and first properties", *Internat. Math. Res. Notices* no. 8 (1994), 343–361.

[Elkies 1997] N. D. Elkies, "Mordell–Weil lattices in characteristic 2, II: The Leech lattice as a Mordell–Weil lattice", *Invent. Math.* **128**:1 (1997), 1–8.

[Illusie 1979] L. Illusie, "Complexe de de Rham–Witt et cohomologie cristalline", *Ann. Sci. École Norm. Sup.* (4) **12**:4 (1979), 501–661.

[Milne 1975] J. S. Milne, "On a conjecture of Artin and Tate", *Inv. Math.* **102** (1975), 517–533.

[Nebe 1998] G. Nebe, "Some cyclo-quaternionic lattices", *J. Algebra* **199**:2 (1998), 472–498.

[Tate 1968] J. Tate, "On the conjectures of Birch and Swinnerton–Dyer and a geometric analog", pp. 415–440 (exposé 306) in *Séminaire Bourbaki* 1965/66, New York, Benjamin, 1968. Reprinted as pp. 189–214 of *Dix exposés sur la cohomologie des schémas*, edited by A. Grothendieck and N. H. Kuiper, Adv. Stud. Pure Math. **3**, North-Holland, Amsterdam, 1968; also in vol. 9 of the Sém. Bourbaki reprint by Soc. Math. France, Paris, 1995.

Noam D. Elkies, Department of Mathematics, Harvard University, Cambridge, MA 02138, United States (elkies@math.harvard.edu)

Received December 1, 2000; accepted February 22, 2001