Mordell-Weil lattices in characteristic 2
II: The Leech lattice as a Mordell-Weil lattice

Noam D. Elkies

Introduction. In the first paper [3] of this series we constructed a family of lattices in dimensions 2^{n+1} for positive integers n. In this paper we show that a modification of the construction also recovers the Leech lattice Λ_{24} in dimension 24. This yields a new description of Λ_{24}: it consists in effect of $\mathbf{0}$ together with the solutions of the equation $y^2+y=x^3+t^{13}$ in rational functions $x(t), y(t)$ defined over $\bar{\mathbf{F}}_2$, the algebraic closure of the two-element field. Call this set L as long as we have not yet identified it with Λ_{24}. The addition law on an elliptic curve makes L a commutative group, on which we define an integer-valued function $\hat{h}$ by the simple formula (2) below.

It is known that Λ_{24} is the only even unimodular lattice of rank 24 with no vectors of norm 2. We show using the methods of [3] that L is a free abelian group of rank 24, that $\hat{h}$ is a positive-definite quadratic form on that group, that the pairing $\langle P,Q\rangle = (\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q))/4$ on L associated to the quadratic form $\hat{h}/2$ has determinant 1, and that $\hat{h}/2$ does not attain the value 2 on L. This is enough to identify L with Λ_{24} once we prove that $\hat{h}(P)/2$, already shown integral in [3], is even for all $P \in L$. We do this by proving a more general "lemma on linear descents", which will also be useful in a subsequent paper analyzing the Mordell-Weil lattices of rank 2^{n+1} for $n \leq 4$. We conclude with a description of the (x, y) corresponding to the 196560 minimal vectors of Λ_{24}.

As in [3] we can also interpret $L \cong \Lambda_{24}$ as the Mordell-Weil lattice over $\bar{\mathbf{F}}_2$ of a constant curve E_0 over the function field $\bar{\mathbf{F}}_2(C)$, where C is a certain hyperelliptic curve (see (4) below) and E_0 is a supersingular elliptic curve. Of the isometry group Co_0 of Λ_{24} our construction exhibits only a very small subgroup of size $3744 = 24 \cdot 13 \cdot 12$, generated by the 24 automorphisms of E_0, the maps $t \mapsto \beta t$ for each 13-th root of unity β, and the field automorphisms of $\bar{\mathbf{F}}_2$ over $\mathbf{F}_2$. Gross showed [4] that if one uses instead of C the Fermat quintic curve then one again obtains Λ_{24} as a Mordell-Weil lattice, this time with many more isometries (though still few compared with the size of $Co_0 \ldots$) due to the large automorphism group $\mathrm{PGU}_3(\mathbf{F}_4)$ of the Fermat quintic in characteristic 2; indeed it is thanks to those automorphisms that Gross can prove that $\hat{h}(P) \equiv 0 \bmod 4$ for all P in his Mordell-Weil lattice, and thus identify that lattice with Λ_{24}. In a later paper we shall obtain the same isometries from our construction of Λ_{24} by relating it with the Barnes-Wall lattices.

Acknowledgements. As detailed in [3], I am grateful to Conway, Sloane, Tsfasman and Gross for inspiration; to Gross, Serre and Shioda for technical conversations and correspondence; and to the Harvard Society of Fellows, the

National Science Foundation, and the Packard Foundation for funding. I also acknowledge the assistance of MACSYMA with symbolic computations.

A Mordell-Weil lattice. Let k be the finite field of $2^{12} = 4096$ elements, and $K = k(t)$. Fix $a_6 \in k$ of trace $\sum_{m=0}^{11} a_6^{2^m} = 1$, and let E/K be the potentially constant supersingular curve

$$y^2 + y = x^3 + t^{13} + a_6, \tag{1}$$

and L its Mordell-Weil lattice; recall from [3] that this is the group $E(K)$ whose nonzero elements are solutions of (1) in rational functions $x(t), y(t) \in K$, a group endowed with the positive-definite form

$$\hat{h} : L = E(K) \to \mathbf{Z}, \quad \mathbf{0} \mapsto 0, \ (x, y) \mapsto \deg(x). \tag{2}$$

Our main goal is:

Theorem. *The curve E/K has trivial Tate-Šafarevič group. Its Mordell-Weil lattice L has rank 24, discriminant 2^{24}, minimal norm 8 and normalized center density $\delta(L) = 1$; it is homothetic with the Leech lattice Λ_{24}.*

In this section we use the techniques of [3] to prove the claims concerning the rank, Tate-Šafarevič group, and discriminant of L, and show that the minimal norm and normalized center density are at least 8 and 1 respectively.

Let E_0 be the supersingular curve

$$y^2 + y = x^3 + a_6 \tag{3}$$

over K, and C the hyperelliptic curve

$$u^2 + u = t^{13} \tag{4}$$

of genus 6. As in [3] we identify L with the group of k-rational maps: $C \to E_0$ sending the point at infinity to $\mathbf{0}$, and thus with $\mathrm{Hom}_k(\mathrm{Jac}(C), E_0)$. Clearly C is dominated by the curve $u^2 + u = t^{65}$, so $\mathrm{Jac}(C)$ is contained in the Jacobian of that curve. Since that Jacobian is isogenous with a power of E_0 (this is the case $n = 6$ of [3, Prop.1]), the same is true of $\mathrm{Jac}(C)$. Since $\mathrm{Jac}(C)$ is isogenous with E_0^6, the rank of $\mathrm{Hom}_k(\mathrm{Jac}(C), E_0)$ is the same as that of $\mathrm{Hom}_k(E_0^6, E_0) = (\mathrm{End}_k(E))^6$, that is, $6 \cdot 4 = 24$.

Still proceeding as in [3], we find that E/K has good reduction at all finite primes, and additive bad reduction of Kodaira type[1] IV* at $t = \infty$ with discriminant t^{-36}; that its L-function is $L(E/k, s) = (|k|^{-s} - |k|^{-1})^{24}$, so the analytic rank of E/K equals its arithmetic rank 24; and thus that by Milne's theorem [5] the conjecture of Birch and Swinnerton-Dyer (formulated in this geometric setting by Artin and Tate [7]) holds for E/K, producing the formula

$$\Delta(L)\,|Ш(E/K)| = |k|^{2(\frac{36}{12}-1)} = 2^{24}. \tag{5}$$

[1]The Kodaira type IV* did not arise in [3] because there the exponent $2^n + 1$ was always congruent to either 3 or 5 mod 6, whereas here we have $13 \equiv 1 \bmod 6$.

Since L is an even integral lattice, its discriminant $\Delta = \Delta(L)$ is an integer. Of course $|Ш(E/K)|$ is an integer as well, so it follows from (5) that both these integers are powers of 2. In particular, to demonstrate the triviality of $Ш(E/K)$ it suffices as in [3] to prove that the rank of the Selmer group for the 2-isogeny

$$\phi : E \to E, \quad (x, y) \mapsto (x^2, y^2 + t^{13} + a_6) \tag{6}$$

(with $\phi^2 = -2$) is at most half the rank of L, that is, at most 12. But as in [3, Thm.2] we can use the "descent map"

$$\epsilon : E(K)/\phi E(K) \hookrightarrow K/K^2, \quad \mathbf{0} \mapsto 0, \ (x, y) \mapsto x \bmod K^2 \tag{7}$$

to identify this Selmer group with a group of odd polynomials of t, the degree of each of whose nonzero elements is $< 13/3$ and congruent to 13 mod 4. Thus the Selmer group is contained in $\{at | a \in k\} \cong (\mathbf{Z}/2)^{12}$, whence $Ш(E/K)$ is indeed trivial and $\Delta = 2^{24}$.

If $P = (x, y)$ is a nonzero point in $E(K)$ then x must have a pole of even order $\geq 13/3$, i.e. at least 6, at $t = \infty$ for (1) to hold there. Thus $\hat{h}(P) \geq 6$ with equality if and only if $x(t)$ is a polynomial of degree 6. But a computation reveals that this is not possible. Indeed assume that $x = \sum_{j=0}^{6} x_j t^j$ with $x_j \in k$; since $\epsilon(P)$ is a linear polynomial we have $x_5 = x_3 = 0$. Let

$$\eta = y^2 + y = x^3 + t^{13} + a_6 = \sum_{j \leq 18} \eta_j t^j. \tag{8}$$

Then (cf. the Lemma in [3, Prop.3]) we must have

$$\eta_{13} = \eta_9^2 + \eta_{18} = \eta_7^2 + \eta_{14} = \eta_5^2 + \eta_{10} = 0. \tag{9}$$

Writing the η_j in terms of the x_j (this is easy because

$$x^3 = x \cdot x^2 = \left(\sum_{j=0}^{6} x_j t^j \right) \left(\sum_{j=0}^{6} x_j^2 t^{2j} \right) \tag{10}$$

in characteristic 2) we thus obtain $x_1 x_6^2 = 1$, $(x_1 x_4^2)^2 = x_6^3$, and

$$x_6(x_2 x_6 + x_4^2) = x_1^2 x_2^4 + x_2(x_2 x_6 + x_4^2) = 0. \tag{11}$$

But the first two equations imply that x_1, x_4, x_6 are nonzero; then the vanishing of $x_6(x_2 x_6 + x_4^2)$ means that $x_2 x_6 = x_4^2$ and $x_2 \neq 0$, but then

$$x_1^2 x_2^4 + x_2(x_2 x_6 + x_4^2) = x_1^2 x_2^4 \tag{12}$$

cannot vanish, and we reach a contradiction. Thus L has minimal norm at least 8, the smallest even integer > 6, and normalized center density

$$\delta(L) = \Delta^{-1/2} (N_{\min}/4)^{24/2} \geq 2^{-12} (8/4)^{12} = 1. \tag{13}$$

A lemma on linear descents. It is believed (see e.g. [2, p.13]) that the maximal normalized packing density for a 24-dimensional lattice is 1, and Λ_{24} is, up to scaling, the unique lattice attaining this maximum. Thus the estimate (13) strongly suggests that our Mordell-Weil lattice is homothetic with Λ_{24}. Since Λ_{24} is a lattice of discriminant 1 all of whose points have even norm, this would mean that every point $P \in L$ has $\hat{h}(P)$ divisible by 4. Conversely, to identify L with $2^{1/2}\Lambda_{24}$ it is enough to prove that $4|\hat{h}(P)$ for all $P \in L$, because it is known that Λ_{24} is the unique unimodular lattice in dimension 24 with no vectors of norm 2 [1, 6, 8].

Let $P \in L$, then, be a nonzero point, with coordinates (x, y). We have already seen by local methods that $\hat{h}(P) = \deg(x)$ is even. Those methods do not suffice to determine $\hat{h}(P) \bmod 4$, but since $\epsilon(P)$ is known to be a linear polynomial we can apply the following global result:

Lemma. *Let k be a field of characteristic 2 and let K be the rational function field $K = k(t)$. Fix a polynomial $A_6(t)$ of odd degree d, and let E/K be the elliptic curve with Weierstrass model*

$$y^2 + y = x^3 + A_6. \tag{14}$$

Let $P \in E(K)$ be a nonzero point with coordinates (x, y), and assume that $x(t)$ is of the form $\xi(t^2) + at$ for some rational function ξ and nonzero $a \in k$ (equivalently, that $dx/dt = a$). Then x has a pole of order $(d-1)/2$ at $t = \infty$, and all its other poles have degree 2. Furthermore, let

$$x = \sum_{j=-\infty}^{(d-1)/2} x_j t^j, \tag{15}$$

be the Laurent expansion of x about $t = \infty$, with $x_1 = a$ and $x_j = 0$ for odd $j \neq 1$. Then

$$x_{-2} = a^{-2} \text{ or } 0, \tag{16}$$

and

$$\frac{1}{2}\left(\deg(x) - \frac{d-1}{2}\right) \equiv a^2 x_{-2} \bmod 2. \tag{17}$$

Thus d and x_{-2} determine $\hat{h}(P) \bmod 4$.

(Note that necessarily $d \equiv 1 \bmod 4$ or $d = 3$, else $x = \xi(t^2) + at$ cannot have a pole of order $(d-1)/2$ at infinity.)

Proof: Without loss of generality we may assume that k is algebraically closed. That x has a pole at infinity of degree $(d-1)/2$ we deduce as usual by differentiating (14) to obtain

$$\frac{dy}{dt} = ax^2 + \frac{dA_6}{dt} \tag{18}$$

and comparing valuations at $t = \infty$. Now let $t_0 \in k$ be a finite pole of x and y, of order $2z, 3z$ respectively. Then $ax^2 + dA_6/dt$ has a pole of order $4z$ at $t = t_0$, while dy/dt has a pole of order at most $3z+1$. Thus $z=1$ and t_0 is a double pole of x. Moreover, if the leading terms of x, y at this pole are $\alpha^2(t-t_0)^{-2}$ and $\alpha^3(t-t_0)^{-3}$ then by equating leading terms in (18) we find $\alpha^3 = a\alpha^4$, whence $\alpha = a^{-1}$ (since by assumption $\alpha \neq 0$).

We can now prove (16,17) by decomposing x into partial fractions. Let $S \subset k$ be the set of finite poles of x; this is a finite set whose cardinality $|S|$ equals the left-hand side of (17). Then

$$x = \sum_{j \geq 0} x_j t^j + a^{-2} \sum_{t_0 \in S} \frac{1}{(t-t_0)^2}. \tag{19}$$

Thus for each $j > 0$ the t^{-2j} coefficient in (15) is given by

$$x_{-2j} = a^{-2} \sum_{t_0 \in S} t_0^{2j-2}. \tag{20}$$

In particular $x_{-2} = a^{-2}|S|$, which proves both (16) and (17). $\square$

In our case $A_6 = t^{13} + a_6$ so $d = 13$. If $P \in \phi L$ then $\hat{h}(P)$ must be doubly even because L is an even lattice and $\phi : L \to L$ is a norm-doubling map. Otherwise P satisfies the hypotheses of our Lemma. Expand x in the Laurent series (15) and define η_j again by (8). Then the conditions (9) yield the same equations on x_1, x_2, x_4, x_6, except that η_{10} now has an additional term $x_{-2}x_6^2$. Solving the first three equations

$$x_1 x_6^2 = 1, \quad (x_1 x_4^2)^2 = x_6^3, \quad x_6(x_2 x_6 + x_4^2) = 0 \tag{21}$$

for x_2, x_4, x_6 in terms of $x_1 = a$ yields

$$(x_2, x_4, x_6) = (a^{-5/4}, a^{-7/8}, a^{-1/2}). \tag{22}$$

The last equation $\eta_5^2 = \eta_{10}$ then becomes

$$0 = x_1^2 x_2^4 + x_2(x_2 x_6 + x_4^2) + x_{-2} x_6^2 = a^{-3} + 0 + a^{-1} x_{-2}. \tag{23}$$

Thus $x_{-2} = a^{-2}$, and we conclude by (17) that $\deg(x) \equiv 0 \bmod 4$. This completes the proof of our Theorem.

Minimal vectors. The Leech lattice Λ_{24} has 196560 vectors of minimal norm 4. Thus L has as many points of minimal height 8, each with x-coordinate

$$x = a^{-1/2}t^6 + a^{-7/8}t^4 + a^{-5/4}t^2 + at + x_0 + \frac{a^{-2}}{(t-t_0)^2} \tag{24}$$

for some $a \in k^*$ and $x_0, t_0 \in k$. Consider two such points P, Q with the same value of a. Then $P \pm Q \in \phi L$, so either $P = \pm Q$ or $\hat{h}(P \pm Q) \geq 16$. By the parallelogram law

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\big(\hat{h}(P) + \hat{h}(Q)\big) = 2(8+8) = 32; \tag{25}$$

thus if $P \neq \pm Q$ then $\hat{h}(P+Q) = \hat{h}(P-Q) = 16$ and P, Q are orthogonal in L. Now a set of pairwise orthogonal nonzero vectors in L (or even in $L \otimes \mathbf{R} \cong \mathbf{R}^{24}$) can have at most 24 elements; thus each of the $2^{12}-1 = 4095$ possible a accounts for at most 48 minimal points. But $48 \cdot 4095 = 196560$, the kissing number of L! Thus each a must be represented by 24 pairs of minimal vectors, forming an orthogonal frame.[2]

To find for each $a \in k^*$ the 24 values of (x_0, t_0) that make (24) the x-coordinate of a minimal point we solve the two equations

$$\eta_3^4 + \eta_6^2 + \eta_{12} = \eta_1^{16} + \eta_2^8 + \eta_4^4 + \eta_8^2 + \eta_{16} = 0. \tag{26}$$

Note that if (x_0, t_0) works then so does $(x_0 + \mu, t_0)$ for each cube root of unity μ, so (26) must give rise to equations in t_0 and

$$X_0 := x_0^4 + x_0. \tag{27}$$

The equation $\eta_3^4 + \eta_6^2 + \eta_{12} = 0$ yields (after multiplying by a)

$$X_0 = a^{13} + a^{13/4} + a^{-13/8} + a^{-5} t_0^8; \tag{28}$$

substituting this into the second equation and taking fourth roots we find that t_0 is one of the solutions of the sextic

$$t_0^6 + a^{-3/8} t_0^4 + a^{-3/4} t_0^2 + a^{3/2} t_0 = a^{33} + a^{69/8} + a^{15/2} + a^{81/32} + a^{-9/8}. \tag{29}$$

(These solutions are necessarily distinct because the derivative of (29) with respect to t_0 is the nonzero constant $a^{3/2}$.) From each of these 6 solutions we obtain 4 possible x_0 by solving (28) and (27) for a total of 24 (x_0, t_0) pairs; thus each of these must make (24) the x-coordinate of a point of $E(K)$ of minimal height 8.

In fact we could, and at first did, use these 196560 minimal points to give an alternative, albeit unpleasant, proof that L is isometric with $2^{1/2}\Lambda_{24}$, invoking the fact ([2, Ch.14]) that the minimal vectors of Λ_{24} comprise the unique solution of the kissing number problem in dimension 24. (Note that this also independently confirms that $\Delta(L) = 2^{24}$, assuming only that L has rank 24.) To do this we must show that (24) yields a pair of solutions of (1) in K for each choice of $a \in k^*$ and x_0, t_0 satisfying (27,28,29), which so far we have only done with the foreknowledge that 196560 such solutions exist. It might seem that we would first have to prove that $x_0, t_0 \in k$ and the constant coefficient of $x^3 + t^{13} + a_6$ is of the form $y_0^2 + y_0$ for some $y_0 \in k$ (how to prove this directly?), but in fact it suffices to construct 196560 minimal solutions in $\bar{k}(t)$: since L already has maximal rank 24, $\mathrm{Gal}(\bar{k}/k)$ acts trivially on $L \otimes \mathbf{R}$, and thus also on L, so any solution in $\bar{k}(t)$ is automatically defined over k.

[2] All we really used is that $\phi : L \to L$ is a norm-doubling map; this argument shows that any norm-doubling map of Λ_{24} yields a partition of its minimal vectors into 4095 orthogonal frames.

Since the coefficients η_j of the Laurent expansion of $\eta = x^3 + t^{13} + a_6$ satisfy (9,26), η is locally of the form $y^2 + y = 0$ at $t = \infty$. This leaves only the pole at $t = t_0$, which imposes two further conditions on η, one of which is already satisfied by the choice of leading term $a^{-2}/(t-t_0)^2$ of x. To state the remaining condition, let c_0 be the constant term in the expansion of x in powers of $t - t_0$, which is

$$c_0 = a^{-1/2}t_0^6 + a^{-7/8}t_0^4 + a^{-5/4}t_0^2 + at_0 + x_0, \tag{30}$$

and let c_2 be the $(t-t_0)^2$ coefficient $a^{-1/2}t_0^4 + a^{-5/4}$. Then $\eta = y^2 + y$ locally at $t = t_0$ if and only if $a^{-4}(c_0^4 + c_0) = a^{-8}c_2^2$, that is, if and only if

$$c_0^4 + c_0 = a^{-5}t_0^8 + a^{-13/2} = b^4 + b \tag{31}$$

by (28), where

$$b = x_0 + a^{13/4} + a^{-13/8}. \tag{32}$$

Thus $(c+b)^4 = c + b$. But by (29) we see that $c + b$ is simply

$$a^{65/2} + a^{65/8} + a^{65/32}, \tag{33}$$

so the condition $(c+b)^4 = c + b$ becomes $a^{130} = a^{65/32}$ or

$$a^{64}(a^{4096} - a) = 0, \tag{34}$$

which (since $a \neq 0$) is precisely the condition $a \in k^*$! Thus each such a indeed gives rise to $2 \cdot 4 \cdot 6 = 48$ minimal points in L and we are done.

References

[1] Conway, J.H.: A characterization of Leech's lattice. *Invent. Math.* **7** (1969), 137–142 (≅[2, Ch.12]).

[2] Conway, J.H., Sloane, N.J.A.: *Sphere Packings, Lattices and Groups.* New York: Springer 1993.

[3] Elkies, N.D.: Mordell-Weil lattices in characteristic 2, I: Construction and first properties. Preprint, 1993.

[4] Gross, B.H.: Group representations and lattices. *Jour. Amer. Math. Soc.* **3** #4 (Oct. 1990), 929–960.

[5] Milne, J.: On a conjecture of Artin and Tate. *Annals of Math.* **102** (1975), 517–533.

[6] Niemeier, H.-V.: Definite quadratische Formen der Dimension 24 und Diskriminante 1. *Jour. Number Th.* **5** (1973), 142–178.

[7] Tate, J.: On the conjecture of Birch and Swinnerton-Dyer and a geometric analog. *Sém. Bourbaki* **306** (1965–66).

[8] Venkov, B.B.: Even Unimodular 24-Dimensional Lattices (trans. G.A. Kendall), Chapter 18 of [2].

Dept. of Mathematics
Harvard University
Cambridge, MA 02138 USA

November, 1993