ELLIPTIC CURVES OF MAXIMAL RANK

JULIÁN AGUIRRE, ÁLVARO LOZANO-ROBLEDO, AND JUAN CARLOS PERAL

Abstract. The article introduces a notion of maximal Selmer rank and maximal Mordell-Weil rank for an elliptic curve with non-trivial 2-torsion. It is shown that there exist infinite elliptic curves over $\mathbb{Q}$ with maximal Selmer rank, and examples of curves with moderately high Mordell-Weil rank are produced.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve defined over the rationals with Weierstrass equation:

$$E : y^2 = x^3 + Ax^2 + Bx$$

with $A, B \in \mathbb{Z}$ and discriminant $\Delta_E = 16B^2(A^2 - 4B) \neq 0$. Using the method known as *descent via 2-isogeny* one can provide a 'trivial' upper bound for the rank of $E(\mathbb{Q})$, the Mordell-Weil group of E:

Proposition 1.1. *Let $\nu(N)$ be the number of positive prime divisors of a non-zero integer N. Then:*

$$\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq \nu(A^2 - 4B) + \nu(B) - 1. \tag{1}$$

More generally, let $E/\mathbb{Q}$ be any elliptic curve with a non-trivial point of 2-torsion and let a (resp. m) be number of primes of additive (resp. multiplicative) bad reduction of $E/\mathbb{Q}$. Then:

$$\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq m + 2a - 1. \tag{2}$$

Remark 1.2. *If the Weierstrass equation $y^2 = x^3 + Ax^2 + Bx$ is a minimal model for $E/\mathbb{Q}$ (or all the prime divisors of Δ_E are primes of bad reduction) then $m + 2a - 2 \leq \nu(A^2 - 4B) + \nu(B) \leq m + 2a$, because $p = 2$ is always a prime of additive reduction and $p > 2$ is of additive reduction if and only if p divides both B and $A^2 - 4B$.*

It turns out that there exist elliptic curves $E/\mathbb{Q}$ where the bound given by Eq. (1) holds with equality, which prompt the following definition:

Definition 1.3. *We say that an elliptic curve $E : y^2 = x^3 + Ax^2 + Bx$ is of maximal Mordell-Weil rank (with respect to the number of bad primes) if* $\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = \nu(A^2 - 4B) + \nu(B) - 1$.

1991 *Mathematics Subject Classification.* Primary: 14H52, Secondary: 11Y50.

Key words and phrases. elliptic curves, maximal Mordell-Weil rank, selmer rank.

Example 1.4. (1) *Let $E : y^2 = x^3 + 2308x^2 + 665858x$. The primes* 2 *and* 577 *are the only prime divisors of (both) B and $A^2 - 4B$. Moreover,* $\operatorname{rank}_{\mathbb{Z}}(E/\mathbb{Q}) = 3$ *and E is of maximal Mordell-Weil rank.*

(2) [Kretschmer 1986] *has found examples of elliptic curves of maximal rank r, for all r within $1 \le r \le 9$, of the form $y^2 = x^3 + Ax^2 + Bx$ where $A^2 - 4B > 0$ is prime and B has exactly r divisors. For example, he lists $y^2 = x^3 + 76171105x^2 + 163762302832128x$, of maximal rank equal to* 9.

(3) *The elliptic curve $E : y^2 = x^3 + Bx$ with $B = -73 \cdot 673 \cdot 2129 \cdot 2393 \cdot 4129$ satisfies* $\operatorname{rank}_{\mathbb{Z}}(E/\mathbb{Q}) = 10$*, thus it is of maximal Mordell-Weil rank. The family of curves $E_B : y^2 = x^3 + Bx$ is a nice and abundant source of examples (see Section 6).*

(4) *The elliptic curve defined by*

$$E : y^2 = x^3 + 4510328029x^2 + 622726581362777216x$$

is of maximal Mordell-Weil rank equal to 12 *and the largest maximal rank known to us. Here:*

$$\begin{aligned} B &= 2^7 \cdot 13^2 \cdot 29 \cdot 41 \cdot 71 \cdot 73 \cdot 107 \cdot 149 \cdot 293, \ \nu(B) = 9; \\ A^2 - 4B &= 857 \cdot 1193 \cdot 180241 \cdot 96875897, \ \nu(A^2 - 4B) = 4. \end{aligned}$$

Section 2 concentrates on a similar notion of maximality with respect to certain Selmer groups associated to E, which is a necessary condition for a curve to be of maximal Mordell-Weil rank. Section 3 provides criteria to decide whether a homogeneous space is locally solvable over $\mathbb{Q}_p$. In Section 4 it is shown that there exist infinitely many non-isomorphic elliptic curves of maximal Selmer rank of any given rank. Searching among explicit families of curves of maximal Selmer rank we find examples of maximal Mordell-Weil rank, for every rank up to 12 (see Section 6). Section 5 is devoted to describe infinite families of curves where the Selmer rank is arbitrarily large, although not necessarily maximal. In Section 6 we also show that, if we assume some standard conjectures, then there exist infinitely many elliptic curves of maximal Mordell-Weil rank 1 and 2. Finally, in the last section we give some empirical data about the mean rank in families of maximal Selmer rank.

The constructions presented in this note rely solely on the theory of 2-descents and quadratic reciprocity. In [Lemmermeyer, Mollin 2003], a similar approach is used to show that the 2-part of the Tate-Shafarevich (Sha) group of an elliptic curve can be arbitrarily large, a result which had been previously shown ([Kramer 1983]) using the Cassels pairing. Both authors show explicit curves where both the 2-Selmer group and Sha are arbitrarily large. The aim of this article is to construct curves where the 2-Selmer group is large but the 2-primary component of Sha may remain small or even trivial, as occurs in examples of maximal Mordell-Weil rank.

2. Maximal Selmer Rank

In this section we briefly review the method of descent via 2-isogeny (see [Silverman 1986], Ch. X, for detailed proofs). Let $E/\mathbb{Q}$ be as before and let $E'/\mathbb{Q}$ be defined by the equation:

$$E' : y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x.$$

The curves E and E' are 2-isogeneous, i.e., there exists an isogeny $\phi : E \to E'$ and a dual isogeny $\hat{\phi} : E' \to E$ such that $\hat{\phi} \circ \phi = [2]$. The pair of isogenies yields an exact sequence:

$$(3) \qquad 0 \to \frac{E'(\mathbb{Q})[\hat{\phi}]}{\phi(E(\mathbb{Q})[2])} \to \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \to \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \to 0$$

where $E'(\mathbb{Q})[\hat{\phi}]$ is the kernel of $\hat{\phi}$ and $E(\mathbb{Q})[2]$ is the rational 2-torsion of $E/\mathbb{Q}$. As usual, one also defines a ϕ-Selmer group, here denoted by $S^{(\phi)}(E/\mathbb{Q})$, which fits into an exact sequence together with the ϕ-torsion of $Ш(E/\mathbb{Q})$, the Shafarevich-Tate group of E:

$$(4) \qquad 0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to S^{(\phi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi] \to 0.$$

The order of $S^{(\phi)}(E/\mathbb{Q})$ (resp. $S^{(\hat{\phi})}(E'/\mathbb{Q})$) is a power of two, 2^s say (resp. $2^{s'}$). Hence, by equations (3) and (4) we obtain:

$$(5) \qquad \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq s + s' - 2.$$

We will refer to the number $Sb(E) = s + s' - 2$ as the *Selmer bound* for $E/\mathbb{Q}$.

Moreover, a simple and efficient description of the Selmer groups $S^{(\phi)}$ and $S^{(\hat{\phi})}$ is provided by the theory. Let T be a set of places of $\mathbb{Q}$ consisting of ∞ and all primes of bad reduction for $E/\mathbb{Q}$ (a prime of bad reduction divides $2B(A^2 - 4B)$ in this case). We define:

$$\mathbb{Q}(T, 2) := \{d \in \mathbb{Q}^*/\mathbb{Q}^{*2} : \operatorname{ord}_p(d) \equiv 0 \mod 2 \text{ for all } p \notin T\}$$

and let C_d and C'_d be the homogeneous spaces given by equations:

$$\begin{aligned} C_d &: dZ^2 = d^2U^4 - 2dAU^2V^2 + (A^2 - 4B)V^4, \\ C'_d &: dZ^2 = d^2U^4 + dAU^2V^2 + BV^4. \end{aligned}$$

Then one has the following:

$$S^{(\phi)}(E/\mathbb{Q}) \cong \{d \in \mathbb{Q}(T, 2) : C_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \in T\}$$

$$S^{(\hat{\phi})}(E'/\mathbb{Q}) \cong \{d \in \mathbb{Q}(T, 2) : C'_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \in T\}$$

where $\mathbb{Q}_\infty = \mathbb{R}$ (see [Silverman 1986], X.4.9 for more details).

Lemma 2.1. *Let E, E' be elliptic curves as above. The orders of the associated Selmer groups satisfy:*

$$s \leq \nu(A^2 - 4B) + 1, \quad s' \leq \nu(B) + 1.$$

Furthermore:

$$Sb(E) = s + s' - 2 \leq \nu(A^2 - 4B) + \nu(B) - 1.$$

Proof. Let $d \in \mathbb{Q}(T,2)$ such that d is square-free and does not divide $A^2 - 4B$. Hence, there is a prime $p|d$ with $\gcd(A^2-4B,p)=1$. Suppose for a contradiction that $d \in S^{(\phi)}$, so that $C_d(\mathbb{Q}_p) \neq \emptyset$. Notice that if $(u',v',z') \in C_d(\mathbb{Q}_p)$ then there exist $u,v,z \in \mathbb{Z}_p$ such that (at least) two of them are in $\mathbb{Z}_p^\times$ and $(u,v,z) \in C_d(\mathbb{Q}_p)$. Since $p|d$ and $p \nmid (A^2-4B)$ then $p|v$. Hence p must divide z^2, which contradicts the fact that at least two of u,v,z are units.

Thus, we must have $d|A^2-4B$ and so:

$$S^{(\phi)}(E/\mathbb{Q}) \cong \{d \in \mathbb{Q}(T_1,2) : C_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \in T\}$$

where T_1 consists of ∞ and all bad primes dividing A^2-4B. We conclude that $s \leq \nu(A^2-4B)+1$. Similarly one shows that

$$S^{(\hat{\phi})}(E'/\mathbb{Q}) \cong \{d \in \mathbb{Q}(T_2,2) : C'_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \in T\}$$

where T_2 consists of ∞ and all bad primes dividing B, which in turn shows that $s' \leq \nu(B)+1$.

In order to prove the last inequality in the lemma, notice that:

$$\begin{aligned} C_d : dZ^2 &= d^2U^4 - 2dAU^2V^2 + (A^2-4B)V^4 \\ &= (dU^2 - AV^2)^2 - 4BV^4, \\ C'_d : dZ^2 &= d^2U^4 + dAU^2V^2 + BV^4 \\ &= (dU^2 + AV^2)^2 - \left(\frac{A^2-4B}{4}\right)V^4. \end{aligned}$$

We claim that either $C_d(\mathbb{R}) = \emptyset$ or $C'_d(\mathbb{R}) = \emptyset$ for all $d \in \mathbb{Q}(T,2)$ with $d<0$. Indeed, let $d<0$ be fixed. As the equations for C_d, C'_d above show, if $B<0$ then $C_d(\mathbb{R}) = \emptyset$ and if $A^2-4B<0$ then $C'_d(\mathbb{R}) = \emptyset$. Hence, if both $C_d(\mathbb{R})$ and $C'_d(\mathbb{R})$ were non-empty then $B>0$ and $A^2-4B>0$ must hold. However, if $A^2-4B>0$ and $A \geq 0$ then $C_d(\mathbb{R})$ is empty and if $B>0$ and $A \leq 0$ then $C'_d(\mathbb{R})$ is empty, as claimed. In particular, either $S^{(\phi)}$ is a subset of $\mathbb{Q}(T_1 \setminus \{\infty\},2)$ or $S^{(\hat{\phi})}$ is a subset of $\mathbb{Q}(T_2 \setminus \{\infty\},2)$. Consequently, either $s \leq \nu(A^2-4B)$ or $s' \leq \nu(B)$ and the inequality follows. □

Proof of Proposition 1.1. Proposition 1.1 is a direct consequence of the previous lemma and equation (5). □

Definition 2.2. *We say that an elliptic curve $E : y^2 = x^3 + Ax^2 + Bx$ is of maximal Selmer rank (or maximal 2-Selmer rank) with respect to the number of bad primes if*

$$Sb(E) = s + s' - 2 = \nu(A^2-4B) + \nu(B) - 1.$$

Example 2.3. *Let $A = 68 = 2^2 \cdot 17$ and $B = 578 = 2 \cdot 17^2$. Then $2B(A^2 - 4B) = 314432 = 2^6 17^3$. Moreover, the elliptic curve $E : y^2 = x^3 + 68x^2 + 578x$ satisfies $Sb(E) = 3$, thus E is of maximal Selmer rank. However,* $\operatorname{rank}_{\mathbb{Z}}(E/\mathbb{Q}) = 1$ *so E is not of maximal Mordell-Weil rank.*

For examples of curves with maximal Mordell-Weil rank equal to 3*, let* $A = 4p$ *and* $B = 2p^2$ *where* $p = 577, 4273,$ *or* 4657*.*

We finish this section with a remark. Let $E/\mathbb{Q}$ be an arbitrary elliptic curve given in Weierstrass form by $y^2 = x^3 + Ax + B$ with A, B integers with trivial 2-torsion. It can be shown that $\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq 2b + 2h_2$ where b is the number of primes of bad reduction of $E/\mathbb{Q}$ and h_2 is the 2-part of the ideal class group of $\mathbb{Q}(E[2])$ (see [Silverman 1986], p. 235). How sharp is this more general bound? Are there any examples where the equality holds?

3. Local Solvability of Homogeneous Spaces

In this section we provide criteria for the local solvability of the spaces C_d and C'_d. These spaces are of the general form:

$$C \quad : \quad Z^2 = d_1U^4 + FU^2V^2 + d_2V^4.$$

where D, F, d_1, d_2 are integers such that $D = d_1 \cdot d_2$. The space C_d corresponds to the choice $(D, F) = (A^2 - 4B, -2A)$ and C'_d corresponds to $(D, F) = (B, A)$.

The solvability of more general spaces of the form $y^2 = ax^4 + bx^3 + cx^2 + dx + e$ has been studied by [Birch, Swinnerton-Dyer 1963]. Also, [Cremona 1997] provides an efficient computational algorithm to determine the solvability of such spaces. In particular, the space C is solvable over $\mathbb{Q}_p$ for all primes which do not divide $2^4D(F^2 - 4D)^2$, the discriminant of the polynomial in the variables U and V. Below, ν_p is the usual p-adic valuation and $\left(\frac{\cdot}{p}\right)$ stands for the Legendre symbol.

Lemma 3.1. *Let* $p > 3$ *be a prime and let* C *be the homogeneous space given above.*

(1) *If* $p|F^2 - 4D$ *but* $p \nmid D$ *then* C *is solvable in* $\mathbb{Q}_p$ *if and only if one of the following conditions is satisfied*
   (a) d_1 *or* d_2 *is a quadratic residue modulo* p*;*
   (b) $\nu_p(F^2 - 4D)$ *is even and* $\left(\frac{-2F}{p}\right) = -1$*, or equivalently:*

$$\left(\frac{F}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 5, 7 \mod 8, \\ -1 & \text{if } p \equiv 1, 3 \mod 8. \end{cases}$$

(2) *If* $p|D$ *but* $p \nmid F$ *then* C *is solvable in* $\mathbb{Q}_p$ *if and only if one of the following is satisfied*
   (a) $p \nmid \gcd(d_1, d_2)$*;*
   (b) $p \mid \gcd(d_1, d_2)$ *and either* $\left(\frac{F}{p}\right) = 1$ *or* $\nu_p(d_1)$ *or* $\nu_p(d_2)$ *is even.*

The previous lemma appears in [Kretschmer 1986] (cf. Lemmas 1, 2 and 3) and is proved in [Kretschmer 1983]. The proof is an straightforward exercise with p-adic numbers. Part (2) is shown using the fact that $y^2 = d_1x^4 + Fx^2 + d_2$ is equivalent to $(2d_1x^2 + F)^2 = F^2 - 4D + 4d_1y^2$. In fact, the latter equality also shows:

Lemma 3.2 ($p=\infty$)**.** *Let $D=d_1\cdot d_2$ and let C be the homogeneous space given by $Z^2=d_1U^4+FU^2V^2+d_2V^4$.*

1. *If d_1 is a positive divisor of D then the space C is solvable over $\mathbb{R}$. In particular, if $D<0$ then $C(\mathbb{R})\neq\emptyset$.*
2. *If d_1 is a negative divisor of D and $D>0$ then C is solvable over $\mathbb{R}$ if and only if $F>0$ and $F^2-4D>0$.*

The next two lemmas provide similar solvability criteria for the primes $p=2$ and $p=3$.

Lemma 3.3 ($p=2$)**.** *Suppose one of the following conditions is satisfied:*

- (A_2) *:* $F\equiv 1 \mod 8$ *and* $\nu_2(D)\geq 7$*;*
- (B_2) *:* $F\equiv 5 \mod 8$ *and* $\nu_2(D)$ *is odd and* ≥ 5*;*
- (C_2) *: All prime divisors of D are congruent to 1 or 7 modulo 8 and ($D\equiv 7 \mod 8$ or $F\equiv 3 \mod 8$);*

Then the homogeneous spaces C are solvable in $\mathbb{Q}_2$, for all square-free divisors d_1 of D. Moreover, if $D>0$ and one of the following conditions is satisfied:

- (D_2) *: D is odd, $D\equiv q \mod 8$ and all prime divisors of D are either congruent to 1 or q modulo 8;*
- (E_2) *: F is odd and all prime divisors of D are 1 modulo 4;*
- (F_2) *: $F\equiv 7 \mod 8$ and $D=2^eD'$ with $e\geq 4$ and all primes dividing D' are congruent to 1 modulo 4.*

then the space C is solvable in $\mathbb{Q}_2$ for all positive square-free $d_1|D$.

Lemma 3.4 ($p=3$)**.** *Suppose one of the following conditions is satisfied:*

- (A_3) *:* $D\equiv 2 \mod 3$ *or* $F\equiv 0 \mod 3$*;*
- (B_3) *:* $D\equiv 0 \mod 3^3$ *and* $F\equiv 1 \mod 3$*;*

Then the homogeneous spaces C are solvable in $\mathbb{Q}_3$, for all square-free divisors d_1 of D. Moreover, if $D>0$ and

- (C_3) *: All prime divisors of D are congruent to 1 modulo 3.*

then the space C is solvable in $\mathbb{Q}_3$, for all positive square-free $d_1|D$.

The proofs of the previous lemmas are again trivial exercises with 2-adic and 3-adic numbers. The lemmas above prove the following theorem:

Theorem 3.5. *Let $E: y^2=x^3+Ax^2+Bx$ be an elliptic curve and put $(D,F)=(B,A)$ and $(D',F')=(A^2-4B,-2A)$. Suppose that $\gcd(A,B)=1$ and:*

1. *($p=\infty$) $B<0$ or ($A>0$, $B>0$ and $A^2-4B>0$);*
2. *($p=2$) The pair (D,F) satisfies one of the conditions (A_2), (B_2) or (C_2), and the pair (D',F') satisfies one of the conditions (A_2) through (F_2);*
3. *($p=3$) The pair (D,F) satisfies one of the conditions (A_3) or (B_3), and the pair (D',F') satisfies one of (A_3), (B_3) or (C_3);*

(4) *If $p \geq 5$ and $p|A^2-4B$ then p satisfies condition (1.a) or (1.b) of Lemma 3.1 with respect to the pair (D,F), and condition (2.a) or (2.b) with respect to the pair (D',F');*

(5) *If $p \geq 5$ and $p|B$ then p satisfies condition (1.a) or (1.b) of Lemma 3.1 with respect to the pair (D',F'), and condition (2.a) or (2.b) with respect to the pair (D,F).*

Then the elliptic curve E is of maximal Selmer rank.

As an example, we apply the theorem to the curve given in Example 1.4.(3):

Corollary 3.6. *The elliptic curve defined by $E : y^2 = x^3 + Ax^2 + Bx$, with $A = 4510328029$ and $B = 622726581362777216$ is of maximal Selmer rank equal to 12.*

Proof. One has the following factorizations into primes:

$$\begin{aligned} B &= 2^7 \cdot 13^2 \cdot 29 \cdot 41 \cdot 71 \cdot 73 \cdot 107 \cdot 149 \cdot 293,\ \nu(B) = 9; \\ A^2-4B &= 857 \cdot 1193 \cdot 180241 \cdot 96875897,\ \nu(A^2-4B) = 4. \end{aligned}$$

Clearly, $A^2-4B > 0$. Put $(D,F) = (B,A)$ and $(D',F') = (A^2-4B,-2A)$ as in the theorem. Then (D,F) satisfies condition (B_2) since $\nu_2(B) = 7$ and $A \equiv 1 \mod 8$. On the other hand, the pair (D',F') satisfies condition (C_2) because the four primes dividing A^2-4B are all congruent to 1 modulo 8.

Next, $A^2-4B \equiv B \equiv 2 \mod 3$, thus both (D,F) and (D',F') satisfy (A_3). Finally, conditions (4) and (5) in the theorem are verified because all primes p dividing A^2-4B are congruent to 1 modulo 4 and $\left(\frac{q}{p}\right) = 1$, for all $q|B$ (and therefore, by quadratic reciprocity $\left(\frac{p}{q}\right) = 1$ as well). Notice that also $\left(\frac{A}{13}\right) = 1$, and so $p = 13$ satisfies condition (2.b) of Lemma 3.1. Thus, all hypotheses of Theorem 3.5 are verified. □

Corollary 3.7. *Let $E : y^2 = x^3 + Ax^2 + Bx$ be an elliptic curve and put $(D,F) = (B,A)$ and $(D',F') = (A^2-4B,-2A)$. Suppose that $B = 2^e3^fB'$, with $e,f \geq 0$ and B' square-free, $\gcd(A,B) = 1$ and:*

(1) *($p = \infty$) $B < 0$ or ($A > 0$, $B > 0$ and $A^2-4B > 0$);*

(2) *($p = 2$) A is odd and the pair (D,F) satisfies one of the conditions (A_2), (B_2) or (C_2), and the pair (D',F') satisfies one of the conditions (A_2) through (F_2);*

(3) *($p = 3$) The pair (D,F) satisfies one of the conditions (A_3) or (B_3), and the pair (D',F') satisfies one of (A_3), (B_3) or (C_3);*

(4) *A^2-4B is prime.*

Then the elliptic curve E is of maximal Selmer rank.

Proof. It suffices to show that under the conditions in the statement of the corollary the elliptic curve E satisfies conditions (4) and (5) in Theorem 3.5. Let $p = A^2-4B$ be a prime. Notice that A is odd and under either hypothesis (A_2), (B_2) or (C_2) we must have $p \equiv 1 \mod 4$. Let q be any prime dividing B. Then:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{A^2-4B}{q}\right) = \left(\frac{A^2}{q}\right) = 1.$$

□

The previous corollary is essentially due to Krestchmer (in Theorem 3 of [Kretschmer 1986] he states the result above, but only for curves such that (B, A) satisfies conditions (A_2) and (B_3)).

4. The Family $y^2 = x^3 + Bx$

In this section we restrict our attention to the family $y^2 = x^3 + Bx$ (i.e. $A = 0$). We fix a number $N \geq 1$ and assume B factors as:

$$B = (-1)^a p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$$

where $a = 0$ or 1 and $\alpha_i \in \mathbb{Z}^{>0}$. We may assume that B is fourth power free, so that $1 \leq \alpha_i \leq 3$. First, we restate Lemma 2.1 in this special case, recovering a theorem of Tate:

Corollary 4.1 ([Tate 1961])**.**

$$\operatorname{rank}_{\mathbb{Z}}(E/\mathbb{Q}) \leq Sb(E) \leq \begin{cases} 2N-1, & \textit{if } B \textit{ is even;} \\ 2N, & \textit{if } B \textit{ is odd.} \end{cases}$$

Thus, a curve $E : y^2 = x^3 + Bx$, with odd $B \in \mathbb{Z}$ (resp. even integer $B \neq 0$), is of maximal Selmer rank if $Sb(E) = 2N$ (resp. $Sb(E) = 2N - 1$).

Definition 4.2. *We say that a set of distinct primes* $\{p_1, \dots, p_N\}$ *satisfy the* **Legendre condition** *if* $p_i \equiv 1 \mod 8$ *for* $i = 1, \dots, N$ *and* p_i *is a quadratic residue modulo* p_j *for all* $j \neq i$.

We will show in Corollary 4.6 that for each N there exist infinitely many distinct N-tuples satisfying the Legendre condition.

Theorem 4.3 (Odd B)**.** *Let* $B = (-1)^a p_1 p_2 \dots p_N$ *be an odd square-free integer and let* E *be the elliptic curve given by* $y^2 = x^3 + Bx$ *. Then:*

(1) *Assume* $B > 0$. *The curve* E *is of maximal Selmer rank if and only if the primes* p_i *satisfy the Legendre condition (4.2).*
(2) *Assume* $B < 0$. *The curve* E *is of maximal Selmer rank if and only if the* $\{p_i\}$ *satisfy the Legendre condition and* $|B| \equiv 1 \mod 16$. *Moreover, if the Legendre condition is satisfied and* $|B| \equiv 9 \mod 16$ *then* $Sb(E) = 2N - 1$.

Proof. Let N, B and $E/\mathbb{Q}$ be as in the statement of the theorem. In order to prove the result we need to provide necessary and sufficient conditions for the homogeneous spaces

$$C'_d : Z^2 = dU^4 + \frac{B}{d}V^4, \; C_d : Z^2 = dU^4 - \frac{4B}{d}V^4, \; C_{2d} : Z^2 = 2dU^4 - \frac{2B}{d}V^4$$

(here $Z = UW$) to be everywhere locally soluble (ELS) and we recall that it suffices to consider solubility for those primes p dividing $2B$. Moreover, by Lemma 2.1 d is a square-free divisor of B.

Let $p = p_i \neq 2$, for some $i = 1, \ldots, N$. By Hensel's lemma, it is clear that $C_d(\mathbb{Q}_p)$, $C'_d(\mathbb{Q}_p)$ and $C_{2d}(\mathbb{Q}_p)$ will be both non-empty for all d if and only if

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{p_j}{p}\right) = 1, \text{ for all } j \neq i. \tag{6}$$

The first two conditions are equivalent to $p = p_i \equiv 1 \mod 8$. So equation (6) is a restatement of the Legendre condition.

Now, we let $p = 2$ and assume that the primes p_i for $i = 1, \ldots, N$ satisfy $p_i \equiv 1 \mod 8$. Thus, $|B| = \prod p_i \equiv 1 \mod 8$. Under these conditions, for any square-free divisor d of B, both $|d|$ and $|B/d|$ are squares in $\mathbb{Q}_2$ and so $C_d(\mathbb{Q}_2)$ and $C'_d(\mathbb{Q}_2)$ are non-empty (whenever $C_d(\mathbb{R})$ and $C'_d(\mathbb{R})$ are non-empty). Finally, working modulo 16 (and 32 when necessary) shows that if $B > 0$ and $|B| \equiv 1 \mod 8$ then $C_{2d}(\mathbb{Q}_2)$ is non-empty, and if $B < 0$ then $C_{2d}(\mathbb{Q}_2)$ is non-empty if and only if $|B| \equiv 1 \mod 16$. Indeed if $|B| \equiv 1 \mod 16$ then $|d| \equiv |B/d| \equiv 1$ or $9 \mod 16$ and $C_{2d}(\mathbb{Q}_2) \neq \emptyset$ while if $|B| \equiv 9 \mod 16$ then $(|d|, |B/d|) \equiv (1, 9)$ or $(9, 1) \mod 16$ and $C_{2d}(\mathbb{Q}_2)$ is empty in both cases.

In particular, if the primes p_i satisfy eq. (6), $B < 0$ and $|B| \equiv 9 \mod 16$ then $C'_d(\mathbb{Q}_2)$, $C_d(\mathbb{Q}_2)$ are non-empty while $C_{2d}(\mathbb{Q}_2)$ is necessarily empty. Hence $Sb(E) = s + s' - 2 = 2N - 1$. □

Remark 4.4. *Let p be a positive odd prime and let $E_p/\mathbb{Q}$ be defined by $y^2 = x^3 - p^2x$. A similar argument to the one above shows that $\operatorname{rank}_{\mathbb{Z}}(E_p(\mathbb{Q})) \leq 1$. In this case, one can show that $E_p(\mathbb{Q})$ has 'maximal' rank equal to 1 infinitely often. In fact the rank is maximal for all $p \equiv 5 \mod 8$ (*[Koblitz 1984]*, Ch. II, §6, Proposition 12). The curves E_p are related to the congruent number problem (*[Koblitz 1984]*, Ch. I).*

Similar standard p-adic arguments show the following result.

Theorem 4.5 (Even B)**.** *Let $B = (-1)^a 2p_2p_3 \ldots p_N$ (here $p_1 = 2$) be an even square-free integer and let E be the elliptic curve given by $y^2 = x^3 + Bx$. Then:*

1. *Assume $B < 0$. The curve E is of maximal Selmer rank ($Sb(E) = 2N - 1$) if and only if the primes $\{p_i\}_{i=2}^N$ satisfy the Legendre condition.*
2. *Assume $B > 0$. If the Legendre condition is satisfied for $\{p_i\}_{i=2}^N$ then the curve E satisfies $Sb(E) = 2N - 2$.*

Corollary 4.6. *Let $n > 1$ be a integer. There exist infinitely many elliptic curves of the form $E : y^2 = x^3 + Bx$ which are of maximal Selmer rank and Selmer bound $Sb(E) = n$. In particular, there exist elliptic curves with arbitrarily high Selmer bound.*

Proof. Let $n > 1$ be fixed. By theorems 4.3 and 4.5, if $\{p_1, \ldots, p_N\}$ is a set of distinct odd primes satisfying $p_i < p_{i+1}$ and the Legendre symbol conditions

$$\left(\frac{-1}{p_i}\right) = \left(\frac{2}{p_i}\right) = \left(\frac{p_j}{p_i}\right) = 1, \text{ for all } i \text{ and } j \neq i, \tag{7}$$

then the elliptic curves $E_B : y^2 = x^3 + (\prod p_i)x$ and $E_{-2B} : y^2 = x^3 - 2(\prod p_i)x$ are of maximal Selmer rank, satisfying respectively $Sb(E_B) = 2N$ and $Sb(E_{-2B}) = 2N + 1$. Therefore, it suffices to show that for every $N > 1$ we can choose infinitely many different N-tuples of primes $(p_1, \ldots, p_N)$ which satisfy eq. (7). The latter is a simple consequence of Dirichlet's theorem on primes in arithmetic progressions. Indeed, given an N-tuple of primes $(p_1, \ldots, p_N)$ which satisfy eq. (7) there exist distinct primes $p_{N+1,k} \equiv 1 \mod 8\prod_{i=1}^{N} p_i$, one for each $k \geq 1$. Thus, by quadratic reciprocity, each of the $N + 1$-tuples $(p_1, \ldots, p_N, p_{N+1,k})$ satisfies eq. (7), and they are all distinct. □

Remark 4.7. *The proof of Corollary 4.6 provides explicit N-tuples of primes with the required properties. However, the method described is (by far) not the most computationally efficient. Suppose that $(p_1, \ldots, p_N)$ have already been chosen to satisfy the Legendre condition, or equivalently eq. (7), and let $M = \prod p_i$. Let $Q \subsetneq (\mathbb{Z}/M\mathbb{Z})^\times$ be the set of all equivalence classes of numbers q such that q is a quadratic residue modulo p_i for all $i = 1, \ldots, N$. Thus, $1 \in Q$ but there are many other elements. Hence, we may choose $p_{N+1} \equiv 1 \mod 8$ such that $p_{N+1} \equiv q \mod M$ for some $q \in Q$.*

Remark 4.8. *We owe the following remark to Farshid Hajir: let $S = \{p_1, \ldots, p_N\}$ be a set of distinct odd primes which satisfy the Legendre condition, let $B = \prod p_i$ and let $K = \mathbb{Q}(\sqrt{B})$. It is a classical theorem due to* [Rédei 1934] *that the quartic extensions of K which are unramified outside ∞ correspond with every factorization $B = d_1 d_2$ with positive $d_1, d_2 \in \mathbb{N}$. Moreover, each quartic extension is of the form $K(\sqrt{\alpha})$ where $\alpha = x + y\sqrt{B}$ and x, y, z are solutions of $x^2 - d_1 y^2 = d_2 z^2$.*

5. Large Selmer Bound

In practice, one is interested in finding elliptic curves $E/\mathbb{Q}$ with high Mordell-Weil rank. It is conjectured that curves with arbitrarily high rank do exist, but only curves with rank less or equal than 28 have been shown. Over all elliptic curves with fixed torsion group $\mathbb{Z}/2\mathbb{Z}$ (these have a model of the form $E : y^2 = x^3 + Ax^2 + Bx$) the highest rank found is 17 (by N. Elkies, see [Dujella Web]). By Corollary 4.1, the elliptic curve $E : y^2 = x^3 + Bx$ satisfies

$$\operatorname{rank}_{\mathbb{Z}}(E/\mathbb{Q}) \leq Sb(E) \leq \begin{cases} 2N - 1, & \text{if B is even;} \\ 2N, & \text{if B is odd,} \end{cases}$$

where $N = \nu(B)$, as before, is the number of positive prime divisors of B. In particular, a necessary condition for the Mordell-Weil rank to be high is that $Sb(E)$, the Selmer bound, should be high as well. Unfortunately, $Sb(E)$ being high is far from being a sufficient condition for high algebraic rank.

Section 2 provides the explicit description of infinite families of curves with maximal Selmer bound $Sb(E) = n$ for every $n \geq 2$. However, the coefficients which appear in those curves are usually of elevated height, which make the methods to compute the Mordell-Weil group lengthy and tedious. With this in mind, we provide descriptions of explicit families with 'large' Selmer bound which, in general, have smaller coefficients. The following theorem is a modification of Theorem 3.5:

Theorem 5.1. *Let $E : y^2 = x^3 + Ax^2 + Bx$ be an elliptic curve and put $(D, F) = (B, A)$ and $(D', F') = (A^2-4B, -2A)$. Suppose that $\gcd(A, B) = 1$ and:*

1. *($p = \infty$) $B < 0$ or ($A > 0$, $B > 0$ and $A^2 - 4B > 0$);*
2. *($p = 2$) The pairs (D, F) and (D', F') satisfy one of the conditions (A_2) through (F_2);*
3. *($p = 3$) The pairs (D, F) and (D', F') satisfy one of (A_3), (B_3) or (C_3);*
4. *If $p \geq 5$ and $p|A^2 - 4B$ then p satisfies condition $(1.a)$ or $(1.b)$ of Lemma 3.1 with respect to the pair (D, F), and condition $(2.a)$ or $(2.b)$ with respect to the pair (D', F');*
5. *If $p \geq 5$ and $p|B$ then p satisfies condition $(1.a)$ or $(1.b)$ of Lemma 3.1 with respect to the pair (D', F'), and condition $(2.a)$ or $(2.b)$ with respect to the pair (D, F).*

Then the elliptic curve E has Selmer bound $Sb(E) = \nu(A^2-4B) + \nu(B) - 2$, that is, the Selmer bound is one unit less than the trivial bound of Prop. 1.1.

Proof. By Lemmas 3.1 through 3.4, under the hypotheses of the theorem, the homogeneous spaces C_d and C'_d are solvable for all positive divisors d (of A^2-4B and B, respectively) over $\mathbb{Q}_p$, for all p, and also over $\mathbb{R}$. However, C_d may not be everywhere locally solvable for negative d. Hence the result. □

Example 5.2. *The elliptic curve given by $E : y^2 = x^3 - 9749057x^2 + 21653921827156x$ has trivial bound 9 but the previous theorem shows that the actual Selmer bound is $Sb(E) = 8$. Moreover, Magma verifies that E has algebraic rank equal to 8. By the way, the torsion of E is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. See Section 6 for examples of curves of maximal rank and different torsion subgroups.*

Before we state the following theorem, we fix some notation. Let $S = \{p_1, \ldots, p_N\}$ be a set of N distinct *odd* prime numbers. We define non-negative integers:

$$\begin{aligned} N_3(S) = N_3 &:= \#\{p \in S : p \equiv 3 \mod 4\}, \\ N_5(S) = N_5 &:= \#\{p \in S : p \equiv 5 \mod 8\}. \end{aligned}$$

We split the Legendre conditions in Def. 4.2 into two statements.

Definition 5.3. *We say that a set $S = \{p_1, \dots, p_N\}$ of distinct odd primes satisfies* (L1) *if $N_3 = N_5 = 0$. The set S satisfies* (L2) *if p is a quadratic residue modulo q for all distinct p, q in S.*

Theorem 5.4. *Let $S = \{p_1, \dots, p_N\}$ be a collection of N distinct odd primes. Then:*

(1) *If $N_3(S) \in \{0, 1\}$ and* (L2) *then the elliptic curves $E_\pm : y^2 = x^3 \pm (\prod p_i)x$ satisfy $Sb(E_\pm) \geq 2N - 3$.*
(2) *If $N_3(S) = 0$, $N_5 \in \{0, 1\}$ and* (L2) *then the elliptic curves $E_{\pm,2} : y^2 = x^3 \pm 2(\prod p_i)x$ satisfy $Sb(E_{\pm,2}) \geq 2N - 2$.*

Notice also that using the method described in Corollary 4.6 it can be shown that, for every $N \geq 2$, every family described in Theorem 5.4 is infinite. Moreover, explicit examples are easily found for each case. The proof of the theorem is a case by case p-adic exercise, very similar to the proof of Theorem 4.3.

6. Examples of Maximal Rank

We start by showing that, if we assume two well-known conjectures (one of conjectures 1 or 2, and conjecture 3 below), then there exist infinitely many non-isomorphic elliptic curves with maximal Mordell-Weil rank equal to 1 and infinitely many of maximal rank 2.

Conjecture 1 (Parity conjecture)**.** *The rank of an elliptic curve $E/\mathbb{Q}$ is even if and only if the root number of $E/\mathbb{Q}$ is $+1$, otherwise (if the root number is -1) the rank is odd.*

Conjecture 2 (Finiteness of 'Sha')**.** *The Shafarevich-Tate group of $E/\mathbb{Q}$, $Ш(E/\mathbb{Q})$, is a finite group.*

Conjecture 3 (Primes represented by polynomials)**.** *If a, b, c are relatively prime, a is positive, $a + b$ and c are not both even, and $b^2 - 4ac$ is not a perfect square, then there are infinitely many primes of the form $an^2 + bn + c$.*

The parity conjecture is a consequence of the also well-known Birch and Swinnerton-Dyer conjecture (see [Silverman 1986], p. 362). The finiteness of Ш has been established for elliptic curves $E/\mathbb{Q}$ with complex multiplication such that $L(E/\mathbb{Q}, 1) \neq 0$ (see [Rubin 1987], [Rubin 1989]). Conjecture 3 can be found, for example, in [Hardy, Wright 1979], p. 19.

Theorem 6.1. *Let n be a natural number such that $p = (8n + 5)^2 - 128 = 64n^2 + 80n - 103$ is prime. Let $E/\mathbb{Q}$ be defined by $y^2 = x^3 + (8n+5)x^2 + 32x$. Then, if the parity conjecture holds for $E/\mathbb{Q}$ or if $Ш(E/\mathbb{Q})$ is finite then the Mordell-Weil rank of E is exactly equal to 1.*

Proof. Let $A = 8n + 5$ and let $B = 32$. By Corollary 3.7, the elliptic curve $y^2 = x^3 + Ax^2 + Bx$ is of maximal Selmer rank equal to $Sb(E) = 1$. On the other hand, a quick calculation gives that the root number of this curve is -1 (the only primes which need to be consider are 2, p and ∞; see

[Rohrlich 1982]). Hence, if the parity conjecture holds then the rank must be exactly 1.

Alternatively, if the Tate-Shafarevich group of $E/\mathbb{Q}$ is finite then Cassels has shown that its order must be a perfect square and the order of the 2-primary component $Ш(E/\mathbb{Q})[2]$ is also a perfect square, say 2^{2t} (see [Cassels 1962], in fact one only needs to assume that the 2-primary component is finite for our purposes). On the other hand, the fact that $Sb(E) = s + s' - 2 = 1$ implies that the $\mathbb{Z}/2\mathbb{Z}$-rank of $S^{(2)}(E/\mathbb{Q})$ is $s + s' - 1 = 2$. Finally, the fact that there is only a non-trivial point of two torsion in $E(\mathbb{Q})$, $\operatorname{rank}_{\mathbb{Z}}(E/\mathbb{Q}) \leq 1$ and the exact sequence:

$$0 \to E(\mathbb{Q})/2(E(\mathbb{Q})) \to S^{(2)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0$$

imply that the rank of E must be exactly 1 and $Ш(E/\mathbb{Q})[2]$ is trivial. □

Example 6.2. *The first ten values of A which verify the hypothesis of the theorem are* 13, 21, 61, 77, 93, 125, 141, 149, 181 *and* 189. *In fact, the set $K = \{1 \leq k \leq 2^{23} : (8k+5)^2 - 128$ is prime$\}$ has* 915266 *elements (the number* $2^{23} = 8388608$*).*

We present another construction which yields elliptic curves of maximal rank 1 and which only relies on a variant of Conjecture 3:

Theorem 6.3. *Let p be a prime such that $p \equiv 17 \bmod 24$ and let n be an odd integer such that $q = (p+1+n^2)^2 - 4p = n^4 + 2(p+1)n^2 + (p-1)^2$ is prime. Then the elliptic curve $E : y^2 = x^3 + (p+1+n^2)x^2 + px$ is of maximal rank* 1.

Proof. Let $p \equiv 17 \mod 24$ be a prime (the existence of infinitely many of these primes is of course provided by Dirichlet's theorem) and let n and q be as in the statement of the theorem. Put $A = p + 1 + n^2$ and $B = p$. We claim that the curve $E : y^2 = x^3 + Ax^2 + Bx$ satisfies the hypotheses of Corollary 3.7. Indeed, $A > 0$, $B > 0$ and $A^2 - 4B = q > 0$. Moreover, A is odd (p must be odd and n is odd by assumption), (B, A) satisfies condition (C_2) (because $B = p \equiv 1 \mod 8$) and (A_3) because $B = p \equiv 2 \mod 3$. The pair $(A^2 - 4B, -2A)$ satisfies (D_2) because $A^2 - 4B = q \equiv 5 \mod 8$, and (A_3) because either $-2A \equiv 0 \mod 3$ or $A^2 - 4B \equiv 2 \mod 3$. Hence, by Corollary 3.7, E is of maximal Selmer rank 1.

Furthermore, the elliptic curve $E/\mathbb{Q}$ has a rational point $P = (-p, pn)$. We only need to check that P is not a torsion point. If P was torsion then by the Nagell-Lutz theorem all the multiples of P would have integer coordinates. A simple calculation shows that the x coordinate of $2P$ and $4P$ are

$$x(2P) = \frac{(p-1)^2}{4n^2}, \qquad x(4P) = \frac{(-1 + 4p + 16n^4p - 6p^2 + 4p^3 - p^4)^2}{16n^2(-1+p)^2(1 + 2n^2 - 2p + 2n^2p + p^2)^2}$$

Since $p \equiv 17$ mod 24 and n is odd (otherwise q would not be prime) the fraction in lowest terms defining $x(4P)$ is of the form $\frac{\text{odd}}{\text{even}}$ so is not an integer. Therefore P is not torsion, the Mordell-Weil rank equals 1 and $E/\mathbb{Q}$ is of maximal algebraic rank. $\square$

Example 6.4. *Fix $p = 17$. The first ten values of n which satisfy the hypotheses of the theorem are $n = 1, 3, 7, 9, 19, 33, 49, 51, 59$ and 61. Let $K_p = \{1 \leq k \leq 2^{23} : (p + 1 + k^2)^2 - 4p$ is prime$\}$. We have calculated $|K_{17}| = 326450$ and $|K_{41}| = 190243$.*

By Theorem 4.3, if p is a prime then the curve $y^2 = x^3 - px$ is of maximal Selmer rank 2 if and only if $p \equiv 1 \mod 16$. In the following theorem we slightly modify a result of [Silverman 1986], Prop. 6.2, p. 311, in order to provide examples of curves where the algebraic rank is maximal and equal to 2.

Theorem 6.5. *Let n be a natural number such that $p = 16n^2 + 1$ is prime and let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 - px$. If either Ш$(E/\mathbb{Q})$ is finite or the parity conjecture holds for E then the curve $E/\mathbb{Q}$ is of maximal Mordell-Weil rank equal to 2.*

Proof. Let $p = 16n^2 + 1$ be prime and let $E : y^2 = x^3 - (16n^2 + 1)x$. By Theorem 4.3, $Sb(E) = 2$ and E is of maximal Selmer rank. Also, the point $P = (16n^2 + 1, 4n(16n^2 + 1))$ belongs to $E(\mathbb{Q})$ and we claim that P is not a torsion point. Indeed, by the Nagell-Lutz theorem, P is not a 2-torsion point (because $y(P) \neq 0$) and if P is a torsion of order > 2 then $y(P)^2 = 2^8 n^2 (16n^2 + 1)^2$ must divide $-4(16n^2 + 1)^3$, which clearly cannot happen. Thus, $E_{\text{Tors}} \cong \mathbb{Z}/2\mathbb{Z}$, P is a point of infinite order and $\mathit{rank}_{\mathbb{Z}}(E/\mathbb{Q}) \geq 1$. Another quick calculation gives that the root number of this curve is $+1$.

Thus, if the parity conjecture holds for E then the Mordell-Weil rank must be equal to 2. Alternatively, if the Tate-Shafarevich group of $E/\mathbb{Q}$ is finite then a similar argument to the one given in the proof of Theorem 6.1 shows that the rank of E must be exactly 2. $\square$

Example 6.6. *The first 10 primes of the form $16n^2 + 1$ are 17, 257, 401, 577, 1297, 1601, 3137, 7057, 13457 and 14401. The set $K = \{1 \leq k \leq 2^{23} : 16k^2 + 1$ is prime$\}$ consists of 708166 numbers.*

It would be quite interesting to prove the existence of infinitely many curves of maximal rank unconditionally, or even the existence of infinitely many curves of maximal rank ≥ 3 relying on conjectures, if necessary. Next, we provide examples of moderately high maximal Mordell-Weil and different torsion subgroups. In order to find these examples, the authors have used previous known families of curves with moderate rank and fixed torsion, as described by [Kulesz, Sthalke 2001], [Lecacheux 2003] and [Campbell, Goins], among others cited below.

6.1. Examples with $\mathbb{Z}/2\mathbb{Z}$ torsion subgroup.

As pointed out in the previous section, elliptic curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z}$ and rank ≤ 17 have already been found. However, these curves are not of maximal Mordell-Weil

Table 1. Known examples with $\mathbb{Z}/2\mathbb{Z}$ torsion.

Author (year)	M-W(E)	$Sb(E)$	$Tb(E)$
Elkies (2005)	17	17	29
Dujella (2002)	15	15	26
Fermigier (1996)	14	14	27
Kulesz - Stahlke (2001)	14	14	25
Dujella (2001)	14	14	19
Watkins (2002)	14	14	36

Table 2. Examples of maximal Mordell-Weil rank and $\mathbb{Z}/2\mathbb{Z}$ torsion

Rank	B
1	-2
2	-17
3	$-82 = (-1) \cdot 2 \cdot 41$
4	$-10081 = (-1) \cdot 17 \cdot 593$
5	$-108322 = (-1) \cdot 2 \cdot 41 \cdot 1321$
6	$-11813521 = (-1) \cdot 17 \cdot 281 \cdot 2473$
7	$-1577047042 = (-1) \cdot 2 \cdot 41 \cdot 2593 \cdot 7417$
8	$-141262310897 = (-1) \cdot 41 \cdot 769 \cdot 2081 \cdot 2153$
9	$-727465200962 = (-1) \cdot 2 \cdot 41 \cdot 1601 \cdot 2137 \cdot 2593$
10	$-1033477836241777 = (-1) \cdot 73 \cdot 673 \cdot 2129 \cdot 2393 \cdot 4129$

rank. Table 1 contains a list of some current records (as of 5/4/2006), together with the actual rank, M-W(E), the Selmer bound, $Sb(E) = s + s' - 2$ and the 'trivial' bound, $Tb(E) = \nu(A^2 - 4B) + \nu(B) - 1$. For a Weierstrass model of the curves, see [Dujella Web]. In order to calculate the trivial bound we rewrote each curve in the form $y^2 = x^3 + Ax^2 + Bx$.

The set of elliptic curves which are of maximal Selmer rank contains the set of elliptic curves which are of maximal Mordell-Weil rank. Looking through the curves described by Theorems 4.3 and 4.5, the authors of the present article have been able to find curves of maximal rank up to 10 among the curves of the form $E : y^2 = x^3 + Bx$. Table 2 provides examples of square-free numbers B such that the elliptic curve E is of the indicated maximal Mordell-Weil rank. The search was performed with Mathematica running on desktop computers and with programs written by the authors (details of the algorithms can be found in [Aguirre, Castañeda, Peral 2003]); the ranks were verified using Magma and Cremona's mwrank.

We have also found the following elliptic curves:

$$\begin{aligned} E_{11} &: y^2 = x^3 + 1630368370x^2 + 134972837533033073x \\ E_{12} &: y^2 = x^3 + 4510328029x^2 + 622726581362777216x. \end{aligned}$$

The curves E_{11} and E_{12} are of maximal rank 11 and 12, respectively. These examples were found searching through a 6-parameter family of elliptic curves, which we briefly describe next.

Let a_i, with $i = 1, \ldots, 6$, be arbitrary integers and let $P(x)$ be the polynomial $P(x) = \prod_{i=1}^{6}(x^2 - a_i^2)$. Let s_i be the (symmetric) polynomials in the variables a_i^2 such that:

$$P(x) = x^{12} - s_1x^{10} + s_2x^8 - s_3x^6 + s_4x^4 - s_5x^2 + s_6.$$

If we define another polynomial $Q(x)$ by

$$Q(x) = x^6 - \frac{s_1}{2}x^4 + \frac{4s_2 - s_1^2}{8}x^2 - \frac{s_1^3 - 4s_1s_2 + 8s_3}{16}$$

then there exist polynomials t_1, t_2, t_3 in the s_i such that if $C(x) = t_1x^4 + t_2x^2 + t_3$ then $Q(x)^2 - P(x) = C(x)$. Let $E/\mathbb{Q}$ be the curve defined by:

$$E : y^2 = C(x).$$

Notice that $P(a_i) = 0$ for all $i = 1, \ldots, 6$, thus $C(a_i) = Q(a_i)^2$ is a square. Hence the points $(a_i, Q(a_i))$, $i = 1, \ldots, 6$, are rational points on E. Finally, $y^2 = C(x)$ is birationally equivalent to the curve in Weierstrass form

$$y^2 = x^3 + Ax^2 + Bx \quad \text{with } A = -\frac{t_2}{2}, \quad B = \frac{t_2^2 - 4t_1t_3}{16}.$$

Therefore, the above construction yields a 6-parameter family of elliptic curves with a point of two torsion, namely $(0, 0)$. It can be shown that the generic rank of the family is 6. The elliptic curves E_{11} and E_{12} appeared as specializations of this family, for particular values of the a_i.

6.2. **Examples with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion subgroup.** The elliptic curve with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion subgroup and largest rank known has been given by Elkies, the rank is 14 but the trivial bound predicts 30 for that particular curve, thus it is not of maximal rank. Similarly, none of the previously known examples (Elkies (rank 11, 2005), Dujella-Kulesz (rank 11, 2006); see [Dujella Web]) are of maximal rank.

Here we present examples of elliptic curves of maximal rank up to 7 and fixed torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. [Kihara 2004a] describes a family of elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and generic rank equal to six (in fact, this family attains the highest rank known for an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and defined over the function field $\mathbb{Q}(t)$). We will use an intermediate result in its construction. Kihara considers the quartic

$$x^4 + y^4 + z^4 = a(x^2y^2 + y^2z^2 + z^2x^2).$$

The change of variables

$$X = \frac{(2y^2 - ax^2 - az^2)^2}{(xz)^2}; \quad Y = \frac{(a^2 - 4)(z^4 - x^4)(2y^2 - ax^2 - az^2)}{(xz)^3},$$

transforms the quartic to the elliptic curve in Weierstrass form

$$Y^2 = X(X - 4a + 8)(X - 4a^2 - 4a + 8).$$

TABLE 3. Examples of maximal rank and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion

Rank	A	B
2	0	-1156
3	-962	148417
4	-13058	9450241
5	-21802898	108062188059601
6	-17838722	70235412808321
7	-35516402	310039977013297
8	-580951202	30945774466708897

Moreover, it can be shown that the value of a given by

$$a = \frac{u^4 + v^4 + w^4}{u^2v^2 + u^2w^2 + v^2w^2}$$

produces three rational points on the curve, for any $u, v, w \in \mathbb{Q}$ such that the denominator is non-zero. After reducing the coefficients we obtain the family

$$\begin{aligned} y^2 = \quad & x^3 - (u^4 + v^4 + w^4)x^2 \\ & +(u^4 + v^4 + w^4 - u^2v^2 - u^2w^2 - v^2w^2)(u^2v^2 + u^2w^2 + v^2w^2)x \end{aligned}$$

which has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and generic rank equal to 3. Using values $1 \leq u, v, w \leq 100$ we have found examples of elliptic curves of maximal rank $2, 3, 4, 5, 6$ and 7. Writing the curve as $y^2 = x^3 + Ax^2 + Bx$ the examples are given in Table 3.

6.3. **Examples with $\mathbb{Z}/4\mathbb{Z}$ torsion subgroup.** The highest known rank for an elliptic curve with torsion group $\mathbb{Z}/4\mathbb{Z}$ is 11, an example due to Elkies:

$$y^2 = x^3 + 7590966489764049 05x^2 + 1735444137630231611532757178574 4384x.$$

However, the trivial bound equals 16, thus it is not of maximal rank.

In [Kihara 2004a] and [Kihara 2004b] it has been shown the existence of an elliptic curve over $\mathbb{Q}(t)$ of rank 5 with a rational point of order 4. Since we use variants of Kihara's construction in order to obtain our examples of maximal curves with torsion $\mathbb{Z}/4\mathbb{Z}$, we present a brief description of his method.

The curve $Y^2 = X^3 + 2(a^2 + b^2)X^2 + (a^2 - b)^2X$ has a torsion point of order 4, namely $P = (a^2 - b, 2a(a^2 - b))$. The rational transformation

$$X = \frac{(a^2 - b)y^2}{x^2}; \quad Y = \frac{(a^2 - b)y(b + a(x^2 + y^2))}{x^3}$$

shows that the curve is birationally equivalent to the quartic given by

$$b + (x^2 - y^2)^2 + 2a(x^2 + y^2) = 0.$$

Table 4. Examples of maximal rank and $\mathbb{Z}/4\mathbb{Z}$ torsion

Rank	A	B
1	66	1
2	321	256
3	7105	1327104
4	21331	22325625
5	2205649	269336088576
8	2099985032881	306447571101199933440000

Now Kihara imposes that (r, s) and (r, u) are points in the quartic, which is equivalent to solve a linear system in a, b. The appropriate values of a and b are

$$a = \frac{2r^2 - s^2 - u^2}{2}; \quad b = s^2u^2 + s^2r^2 + u^2r^2 - 3r^4.$$

Now he imposes new solutions given by (s, p), (u, q) and (p, m), which is equivalent to solving a system of three quadratic equations. In [Kihara 2004a], he gives a parametric solution of two of the equations and in [Kihara 2004b] he is able to find parametric solutions for the full system, leading to the construction of the surface $E/\mathbb{Q}(t)$ of rank 5. When the surface is written in the form $E : Y^2 = X^3 + A(t)X^2 + B(t)X$, the coefficients $A(t)$ and $B(t)$ are polynomials in t with degree 52 and 104 respectively, so even small values of t result in huge values of A and B, and this is a great difficulty for the computations.

For our search, we have used other similar parametrizations for the solution of the system of quadratic equations, producing several elliptic surfaces. Then sieving along those families we have found the examples of maximal rank that appear in Table 4. The ranks were verified using Magma.

6.4. **Examples with $\mathbb{Z}/6\mathbb{Z}$ torsion subgroup.** For curves with a torsion point of order 6 we use the model given in [Hadano 1977]:

$$y^2 - 2(a + b)xy + 2aby + x^3 = 0.$$

In Weierstrass form this is

$$E_{a,b} : y^2 = x^3 + (a^2 + 2ab - 2b^2)x^2 + (b^3(b - 2a))x$$

Notice that since $E_{a,b}$ has a point of order 6, then there exists a 2-isogenous curve $E'_{a,b}$ and a 3-isogenous curve $E''_{a,b}$. The 3-isogenous curve is given by

$$E''_{a,b} : y^2 = x^3 + (a^2 - 10ab - 2b^2)x^2 + ((2a - b)^3b)x.$$

Searching among elliptic curves of the form $E_{a,b}$ we have found examples of maximal rank $0, 1, 2, 3$ and 4. In Table 5 we list the coefficients A, B that yield such curves. The corresponding 3-isogenous curves $E''_{a,b}$ are also maximal of the same rank and also have torsion subgroup $\mathbb{Z}/6\mathbb{Z}$.

Table 5. Examples of maximal rank and $\mathbb{Z}/6\mathbb{Z}$ torsion

Rank	A	B
0	1	-1
1	13	11
2	541	60507
3	3061	15875
4	300133	-276401197

6.5. **Other torsion subgroups.** The remaining possibilities for torsion subgroups with non-trivial 2 torsion are $\mathbb{Z}/N\mathbb{Z}$, with $N = 8, 10$ or 12, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2M\mathbb{Z}$, with $M = 2, 3$ or 4. Finding examples of maximal rank with any of these torsion subgroups seems challenging because of the size of the coefficients of the known families with such torsion. In fact, the highest known ranks (not necessarily maximal) are quite low for the same reason.

7. Statistics

7.1. **The average rank in families of fixed Selmer rank.** Let S_N be a finite set of elliptic curves $E/\mathbb{Q}$ such that $Sb(E) = N$ and let $R_N = \{\mathrm{rank}_{\mathbb{Z}}(E/\mathbb{Q}) : E \in S_N\}$. What is the mean value of the set R_N? In this section we provide some data related to this interesting question.

For each $N = 2, 3, 4, 5, 6$ we construct a sample set S_N as follows. Let m be a natural number and let $d > 2$ be real. Then S_N is a set of all elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$, where the coefficients A and B satisfy the following properties:

- Let M be the set formed by the first m odd natural numbers b which are square-free, have exactly $N-1$ (odd) prime divisors, and $2^7 b \equiv 2 \mod 3$;
- For each $b \in M$, put $B = 2^7 b$ and we let A be any positive integer such that $A \equiv 1 \mod 4$, $A^2 - 4B > 0$ is prime and $2\sqrt{B} < A < d\sqrt{B}$.

The numbers m and d are now chosen so that the set S_N is of a reasonable size in terms of computer power and computing time. For our calculations, we used the following values (N, m, d, t), where t indicates the computation time in minutes: $(2, 1544, 8, 217)$, $(3, 1151, 8, 360)$, $(4, 588, 8, 511)$, $(5, 289, 8, 1057)$ and $(6, 118, 8, 2139)$. The computations were carried on a Power Mac G5 with two 2.3 GHz processors, 1.5 Gb RAM memory, under the Mac OSX 10.4.6 operating system and running Mathematica 5.1. with programs written by the authors. Once the set S_N is determined, we produced lower bounds for the algebraic rank by finding rational solutions in the homogeneous spaces

$$C'_d : Z^2 = dU^4 + AU^2V^2 + \frac{B}{d}V^4$$

TABLE 6. Lower estimates for the ranks in the families S_N

		Number of curves with rank at least						
N	$\lvert S_N \rvert$	0	1	2	3	4	5	6
2	501911	420955	63582	17374				
3	300957	184478	99402	5203	11874			
4	207233	118749	32303	54174	40	1967		
5	200117	75395	98629	3091	22800		202	
6	202263	94527	31450	71006	109	5159		12

TABLE 7. The data in Table 6, taking into account the parity conjecture

		Number of curves with rank at least								
N	$\lvert S_N \rvert$	0	1	2	3	4	5	6	%	$A(N)$
2	501911	420955		80956					16.13	0.32
3	300957		283880		17077				5.67	1.11
4	207233	118749		86477		2007			0.97	0.87
5	200117		174024		25891		202		0.10	1.26
6	202263	94527		102456		5268		12	0.006	1.12

for all square-free divisors d of B. In order to determine whether $C'_d(\mathbb{Q})$ is non-empty, we tried the 439 pairs (U,V) with $1 \leq U,V \leq 21$ with $\gcd(U,V) = 1$, and the pairs $(1,k)$, $(k,1)$ with $1 \leq k \leq 101$. Some remarks are in order:

(1) Notice that a curve E with coefficients A and B as above is of maximal Selmer rank N, by Corollary 3.7, so there is no need to calculate the Selmer bound.

(2) Since $A^2 - 4B$ is prime there is no need to check the homogeneous spaces corresponding to the isogenous curve E'.

(3) The sizes of S_2 and S_3 are significantly larger than the sizes of S_4, S_5 and S_6 because the calculations for $N = 2$ and $N = 3$ run quite faster than in other higher cases, and we were able to study more curves.

Tables 6 indicate the number of curves found in S_N and lower bounds for the rank. The symbol $|S_N|$ stands for the cardinality of the sample set S_N. Table 7 presents the same data but this time we take advantage of the parity conjecture to increase the lower bounds. Table 7 also provides the percentage of curves of maximal Mordell-Weil rank in S_N and, $A(N)$, a lower bound for the average rank in the family.

For the sake of comparison, for $i = 1, 2, 3$, let Q_i be the set of all elliptic curves $E/\mathbb{Q} : y^2 = x^3 + Bx$ where $1 + 10000(i-1) \leq B \leq 10000i$ and B is fourth-power free. Also, let $Q_{i,N}$, $i = 1, 2, 3$ and $N \geq 1$ be the set formed

Table 8. Ranks in the family $y^2 = x^3 - Bx$ with $1 \leq B \leq 30000$.

		Number of curves with rank					
S	$\lvert S \rvert$	0	1	2	3	4	Av. Rank
Q_1	9240	3667	3747	1677	144	5	0.81
$Q_{1,2}$	2890	1266		1624			1.12
$Q_{1,4}$	72	14		53		5	1.75
Q_2	9240	3776	3706	1587	159	12	0.80
$Q_{2,2}$	2991	1460		1531			1.02
$Q_{2,4}$	94	26		56		12	1.70
Q_3	9238	3704	3733	1623	168	10	0.81
$Q_{3,2}$	3019	1469		1550			1.02
$Q_{3,4}$	107	24		73		10	1.74

Table 9. Curves of maximal rank in the family $E^\sharp$

	Curves of maximal rank							
Number of curves	1	2	3	4	5	6	7	%
251904	381	5199	13471	9345	1998	141	3	12.12

by all the curves E in Q_i such that $Sb(E) = N$. We exhibit a chart (Table 8) which describes the ranks found in Q_i and $Q_{i,2}, Q_{i,4}$. Again, the ranks shown are the analytic ranks, computed with Magma.

7.2. **Families with large number of maximal curves.** As we searched for examples of curves with maximal rank, we have found several families which seem to yield an unusual high percentage of maximal curves, and an unusual number of curves of moderately high maximal rank. For example, consider the curves of the form

$$E^\sharp \ : \ y^2 = x^3 + 2(a^2 + b^2)x^2 - 8p(2p + a^2 - b^2)x,$$

with $a, b \in \mathbb{Z}$ and p prime. This family appears by forcing the points $(-p, a)$ and (q, b) to be on $y^2 = x^3 + Ax^2 + pqx$ and then normalizing the coefficients.

Using the method described in the previous section to study the families S_N, we have studied 251904 curves (non-singular and distinct) of the form $E^\sharp$, corresponding to $1 \leq a, b \leq 80$ and the first forty primes p. When the lower bound of the rank coincides with the Selmer rank, the curve is of maximal algebraic rank. Table 9 indicates the number of curves of maximal rank found for each rank between 1 and 7, together with a lower bound for the percentage of maximal curves among those tested (the curves listed were verified to have maximal rank but there may be more curves of maximal rank which our sieve method did not detect).

7.3. **Open questions.** As in many other instances in number theory, and particularly in the theory of elliptic curves, the amount of data available is not sufficient to support conjectures. However, the results presented in this article and the data provided prompt the following natural questions:

- Are there elliptic curves of arbitrarily large maximal rank? This is a question which is even more difficult to decide than whether there are curves of arbitrarily high rank. If the latter holds, the former will most likely be true as well. [Kretschmer 1986] has conjectured that there exist elliptic curves $E/\mathbb{Q}$ of rank n, non-trivial torsion and with bad reduction at most at $n+1$ primes, *for all n*. His conjecture is based on particular case of Corollary 3.7 and some empirical observations. Based on Theorems 4.3 and 4.5 there may exist elliptic curves $E/\mathbb{Q}$ of rank N, non-trivial torsion and with bad additive reduction at $(N+2)/2$ primes if N is even, and $(N+3)/2$ primes if N is odd.
- Fix a (large) natural number T and let $\{S_N\}_{N=1}^{\infty}$ be a collection of sets S_N as above, with fixed cardinality $|S_N| = T$. Let
$$A(N) = \frac{1}{T} \sum_{E \in S_N} \operatorname{rank}_{\mathbb{Z}}(E/\mathbb{Q})$$
be the average rank in S_N for each $N \in \mathbb{N}$. What can we say about the function $A(N)$? What is $\limsup_{N\to\infty} A(N)$? Tables 7 and 8 seems to indicate that $A(2N)$ and $A(2N+1)$ are increasing sequences. If so, are they unbounded? The latter question is of course also intimately related to the existence of curves with arbitrarily high rank.

References

[Aguirre, Castañeda, Peral 2003] J. Aguirre, F. Castañeda, J. C. Peral, *High rank elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z}$*, Math. Comp., Vol. 73, N. 245, p. 323-331 (2003).

[Birch, Swinnerton-Dyer 1963] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic Curves I*, J. reine Angew Math. 212, (1963), 7-25.

[Campbell, Goins] G. Campbell and E. H. Goins, *Heron triangles, Diophantine problems and elliptic curves*, preprint.

[Cassels 1962] J. W. S. Cassels, *Arithmetic on curves of genus 1 (IV). Proof of the Hauptvermutung*, J. Reine Angew. Math. 211 (1962), 95-112.

[Cremona 1997] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, (1997).

[Dujella Web] A. Dujella's website, http://www.math.hr/∼duje/tors/tors.html.

[Hadano 1977] T. Hadano, *Elliptic curves with a torsion point*, Nagoya Math. J. 66, (1977), 99-108.

[Hardy, Wright 1979] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, (1979).

[Kihara 2004a] S. Kihara, *On the rank of elliptic curves with three rational points of order 2. II*, Proc. Japan Acad. 80 A, (2004), 13-14.

[Kihara 2004b] S. Kihara, *On the rank of the elliptic curves with a rational point of order 4*, Proc. Japan Acad. Ser. A Math. Sci. 80 (2004), no. 4, 26–27.

[Kihara 2004c] S. Kihara, *On the rank of the elliptic curves with a rational point of order 4, II*, Proc. Japan Acad. Ser. A Math. Sci. 80 (2004), no. 8, 158–159.

[Koblitz 1984] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984.

[Kramer 1983] K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevitch groups*, Proc. Am. Math. Soc. 89 (1983), pp. 379 − 386.

[Kretschmer 1986] T. Kretschmer, *Construction of elliptic curves with large rank*, Math. Comp., Vol. 46, N. 174, p. 627-635 (1986).

[Kretschmer 1983] T. Kretschmer, *Konstruktion elliptischer Kurven von hohem Rang*, Diploma thesis, Saarbrückern, 1983.

[Kulesz, Sthalke 2001] L. Kulesz and C. Sthalke, *Elliptic Curves of High Rank with Nontrivial Torsion Group over Q*, Experimental Math. 10, no. 3, (2001), 475-480.

[Lecacheux 2003] O. Lecacheux, *Rang de courbes elliptiques avec groupe de torsion non trivial*, J. Theor. Nombres Bordeaux 15, (2003), 231-247.

[Lemmermeyer, Mollin 2003] F. Lemmermeyer, R. Mollin, *On Tate-Shafarevich groups of* $y^2 = x(x^2 - k^2)$, Acta Math. Univ. Comenian. (N.S.) 72 (2003), no. 1, pp. 73 − 80.

[Rédei 1934] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. 171 (1934), 55–60.

[Rohrlich 1982] D. E. Rohrlich, *Root numbers of Hecke L-functions of CM fields*, Amer. J. Math. 104 (1982), no. 3, 517–543.

[Rubin 1987] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), no. 3, 527–559.

[Rubin 1989] K. Rubin, *Tate-Shafarevich groups of elliptic curves with complex multiplication*, Algebraic number theory, 409–419, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 1989.

[Silverman 1986] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[Tate 1961] J. Tate, *Rational points on elliptic curves*, Phillips Lectures, Haverford College, 1961.

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain

E-mail address: julian.aguirre@ehu.es

Department of Mathematics, 584 Malott Hall, Cornell University, Ithaca, NY 14853, USA.

E-mail address: alozano@math.cornell.edu

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain

E-mail address: mtppealj@lg.ehu.es