ON THE NUMBER OF n-ISOGENIES OF ELLIPTIC CURVES OVER NUMBER FIELDS

MILJEN MIKIĆ AND FILIP NAJMAN

Abstract. We find the number of elliptic curves with a cyclic isogeny of degree n over various number fields by studying the modular curves $X_0(n)$. We show that for $n = 14, 15, 20, 21, 49$ there exists infinitely many quartic fields K such that $\#Y_0(n)(\mathbb{Q}) \neq \#Y_0(n)(K) < \infty$. In the case $n = 27$ we prove that there are infinitely many sextic fields such that $\#Y_0(n)(\mathbb{Q}) \neq \#Y_0(n)(K) < \infty$.

1. Introduction

An isogeny of elliptic curves is a rational morphism from one elliptic curve to another that sends the identity of the first curve to the identity of the second. An isogeny is said to be cyclic if its kernel is cyclic. All the possible degrees of cyclic isogenies of elliptic curves over $\mathbb{Q}$, together with the number of $\overline{\mathbb{Q}}$-isomorphism classes having a cyclic isogeny of each degree, were determined by Mazur [5] and Kenku [2, 3, 4].

Let K be a number field. If there exists a K-rational cyclic isogeny $\phi : E \to E'$ of degree n, this means that $\operatorname{Ker}\phi$ is $\operatorname{Gal}(\overline{K}/K)$-invariant cyclic group of order n and we will say that E/K has an n-isogeny. Denote by $Y_0(n)$ the affine curve whose K-rational points classify $\overline{K}$-isomorphism classes of pairs (E, C), where E/K is an elliptic curve and C is a cyclic ($\operatorname{Gal}(\overline{K}/K)$-invariant) subgroup of E. Let $X_0(n)$ be the compactification of $Y_0(n)$, obtained by adding the cusps.

Our goal in this paper is to study the number of elliptic curves with a n-isogeny over fixed number fields, where n is an integer such that the modular curve $X_0(n)$ is of a genus 1. Let S be the set of n-s such that $X_0(n)$ is of genus 1:

$$S = \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}. \tag{1}$$

The reason we choose only n such that $X_0(n)$ is of genus 1 is because in fact only this case is interesting: if $X_0(n)$ is of genus 0, then $\#Y_0(n)(K)$ will be infinite over any number field (here one implicitly uses the fact that $X_0(n)$ has at least one rational cusp together with the fact that the number of cusps is finite), while if $X_0(n)$ is of genus ≥ 2, then by Faltings' theorem it follows that $\#Y_0(n)(K)$ will be finite over any number field.

For all of the $n \in S$, $\#Y_0(n)(\mathbb{Q})$ is finite (and in some cases 0).

The second author showed [7] that if K is of prime degree (over $\mathbb{Q}$), then in all but finitely many explicitly listed cases, it holds that either $\#Y_0(n)(\mathbb{Q}) = \#Y_0(n)(K)$ or $\#Y_0(n)(K) = \infty$. The same was also shown for the modular curves $Y_1(n)$ (which parameterize isomorphism classes of elliptic curves together with a point of order n) of genus 1. On the other hand, it is shown in [6] that there exist infinitely many

2010 *Mathematics Subject Classification.* 11G05, 11G18, 11R16, 14H52.
Key words and phrases. Elliptic curves, Mordell-Weil group, isogenies.

quartic fields K such that $\#Y_1(n)(\mathbb{Q}) \neq \#Y_1(n)(K) < \infty$. In this paper we show a similar result for the curves $Y_0(n)$, where n is such that there exists a quadratic field such that $\#Y_0(n)(\mathbb{Q}) \neq \#Y_0(n)(K) < \infty$. We denote this set by T;

$$T = \{14, 15, 20, 21, 27, 49\}.$$

More explicitly, we show that there exists infinitely many quartic fields K such that $\#Y_0(n)(\mathbb{Q}) \neq \#Y_0(n)(K) < \infty$ for $n = 14, 15, 20, 21, 49$. For $n = 27$ we show that there are infinitely many sextic fields such that $\#Y_0(n)(\mathbb{Q}) \neq \#Y_0(n)(K) < \infty$.

The results for $n = 14, 15, 20, 21, 49$ are obtained essentially by 2-isogeny descent (see [9, Proposition 4.9, p.302.]) and following the general strategy of [6]. The main idea is to prove that, in an explicitly given family of number fields, the rank of the $X_0(n)(K)$ equals zero for each number field K, and that the number of non-cuspidal torsion points over K is greater than $\#X_0(n)(\mathbb{Q})_{tors}$. The case $n = 27$ cannot be handled by 2-isogeny descent (at least not over $\mathbb{Q}$) since it does not possess a 2-torsion point. We circumvent this problem by using the fact that $X_0(27)$ is an elliptic curve with j-invariant 0 and prove a general result about ranks of such elliptic curves over cubic extensions of number fields containing ζ_3, where ζ_3 is a primitive third root of unity.

2. The cases $n = 14, 15, 20, 21, 49$

As mentioned in the introduction, proving that $\operatorname{rank}(X_0(n)(K)) = 0$ is done by using 2-isogeny-descent groups. Let $X = X_0(n)$, ϕ a 2-isogeny from X to X', and ψ is its dual isogeny and $S_\psi(X)$ and $S_\phi(X')$ be the corresponding 2-isogeny-Selmer groups. Then

$$\operatorname{rank}(X(K)) \leq \log_2(|S_\psi(X)| \cdot |S_\phi(X')|) - 2.$$

For details, see [9, Chapter X].

We will also use, without mention, the well-known fact that if $L = K(\sqrt{d})$ is a quadratic extension of K, then

$$\operatorname{rank}(E(L)) = \operatorname{rank}(E(K)) + \operatorname{rank}(E^d(K))$$

where E^d is the quadratic twist of E by d.

Theorem 1. *Let p be a prime satisfying $p \equiv 3 \pmod 8$ and $\left(\frac{7}{p}\right) = -1$. Then,* $\operatorname{rank}(X_0^{(p)}(14)(\mathbb{Q})) = \operatorname{rank}(X_0^{(-7p)}(14)(\mathbb{Q})) = 0$.

Proof. From [6, Theorem 3] and the fact that the curves $X_0(14)$ and $X_1(14)$ are isogenous, it directly follows the statement of the theorem (isogenous curves have the same rank). □

Corollary 2. *There exist infinitely many primes p such that for $K = \mathbb{Q}(\sqrt{-7}, \sqrt{p})$,* $\operatorname{rank}(X_0(14)(K)) = 0$.

Proof. This is a direct consequence of Dirichlet's theorem on arithmetic progressions applied on primes that satisfy conditions of Theorem 1. □

Theorem 3. *Let p be a prime satisfying $p \equiv 5 \pmod 8$, $p \equiv 2 \pmod 3$ and $\left(\frac{p}{5}\right) = -1$. Then,* $\operatorname{rank}(X_0^{(p)}(15)(\mathbb{Q})) = \operatorname{rank}(X_0^{(-p)}(15)(\mathbb{Q})) = 0$.

Proof. From [10] we know that the explicit model of $X_0(15)$ is

$$y^2 + xy + y = x^3 + x^2 - 10x - 10. \tag{2}$$

In order to prove the theorem, we shall use a method of descent via 2-isogenies. Therefore, we need to transform (2) from the Weierstrass form into the form $y^2 = x^3 + ax^2 + bx$, suitable for the application of this method. We calculate $b_2 = a_1^2 + 4a_2 = 5, b_4 = a_1a_3 + 2a_4 = -19$ and $b_6 = a_3^2 + 4a_6 = -39$, so x_0 is a root of $x^3 + 5x^2 - 152x - 624 = 0$. It is easy to check that $x_0 = 12$ satisfies the latter equation. Therefore, $a = 3x_0 + b_2 = 41$, $b = (a + b_2)x_0 + 8b_4 = 400$. Finally, we obtain the following curves (we write $E(n)$ instead of $X_0^{(n)}(15)(\mathbb{Q})$ and $E'(n)$ for the curve 2-isogenous to $E(n)$):

$$\begin{aligned} E(p) : y^2 &= x^3 + 41px^2 + 400p^2x, \\ E'(p) : y^2 &= x^3 - 82px^2 + 81p^2x, \\ E(-p) : y^2 &= x^3 - 41px^2 + 400p^2x, \\ E'(-p) : y^2 &= x^3 + 82px^2 + 81p^2x. \end{aligned}$$

Let us examine the size of the associated ϕ-Selmer groups for each of these curves.

1. $E(p) : y^2 = x^3 + 41px^2 + 400p^2x$

   We have to examine the solvability of the quartic (torsor) $N^2 = b_1M^4 + 41pM^2e^2 + b_2e^4$ with $b_1b_2 = 400p^2$, respecting $\gcd(M, e) = 1$ and assuming without loss of generality that b_1 is square-free. Thus,

   $$b_1 \in \{\pm 1,\ \pm 2,\ \pm 5,\ \pm 10,\ \pm p,\ \pm 2p,\ \pm 5p,\ \pm 10p\}.$$

   An obvious solution is $b_1 = 1$, but $b_1 = -p$ is also a solution; namely in this case we have $(M, e, N) = (5, 1, 0)$. Let us now check other possible values of b_1.

   1.1. $b_1 = -1$

   The torsor becomes $N^2 = -M^4 + 41pM^2e^2 - 400p^2e^4$. Reducing modulo 3 and noticing that $p \equiv 2 \pmod 3$ we get $N^2 \equiv -M^4 + M^2e^2 - e^4 \equiv 2 \pmod 3$, which is not a quadratic residue modulo 3. Therefore, $-1 \notin S_\psi(E(p))$.

   1.2. $b_1 = 2$

   We get the equation

   $$N^2 = 2M^4 + 41pM^2e^2 + 200p^2e^4. \tag{3}$$

   When e is even and M is odd, the right hand side of (3) is congruent to 2 modulo 4, and that is a contradiction with the left hand side. If both M and e are odd, then $N^2 \equiv 2 + p \equiv 7 \pmod 8$, and that is not possible. We are left with the case when M is even and e odd. Then, N is also even so we can take $M = 2t, N = 2N'$ and transform (3) into $N'^2 = 8t^4 + 41pt^2e^2 + 50p^2e^4$. Reducing modulo 4 we get $N'^2 = pt^2 + 2p^2 \equiv 2, 3 \pmod 4$, but that is impossible, so $2 \notin S_\psi(E(p))$.

   1.3. $b_1 = 2p$

   The equation is

   $$N^2 = p(2M^4 + 41M^2e^2 + 200e^4). \tag{4}$$

When e is even and M is odd, the right hand side of (4) is congruent to 2 modulo 4. Taking both M and e odd, the right hand side is congruent to $3p$ modulo 4, or 3 modulo 4 which is not a quadratic residue modulo 4. If M is even and e odd, we can take $M = 2t$. Then, $N^2 = p(32t^4 + 164t^2e^2 + 200e^4)$. By taking $N = 2N'$ and dividing by four, we get $N'^2 = p(8t^4 + 41t^2e^2 + 50e^4)$, which gives $N'^2 \equiv p(2 + t^2) \equiv 2, 6, 7 \pmod 8$, and that is impossible, which implies $2p \notin S_\psi(E(p))$.

1.4. $b_1 = -5$

In this case the torsor is $N^2 = -5M^4 + 41pM^2e^2 - 80p^2e^4$. Here we will observe reduction modulo 5 because the right hand side is congruent to pM^2e^2 modulo 5. Since the left hand side is a square and $\left(\frac{p}{5}\right) = -1$, the only possible options are either $5|M$ or $5|e$. In both cases we get $5|N$, so the left hand side is divisible not just by 5, but by 25. Therefore, the right hand side also needs to be divisible by 25. If $5|e$, then because the right hand side is divisible by 25, it follows that $5|M^4$, or $5|M$, and that is impossible because of $\gcd(M, e) = 1$. The case $5|M$ is proved analogously. Thus, $-5 \notin S_\psi(E(p))$.

1.5. $b_1 = 5$

The torsor becomes $N^2 = 5M^4 + 41pM^2e^2 + 80p^2e^4$. Concluding along the same lines as in the case $b_1 = -5$ we get $5 \notin S_\psi(E(p))$.

1.6. $b_1 = 10$

The torsor is

$$N^2 = 10M^4 + 41pM^2e^2 + 40p^2e^4. \tag{5}$$

In this case we observe the parity of M and e. When e is even and M odd, N^2 is congruent to 2 modulo 4, and if both of them are odd, then $N^2 \equiv p + 2 \equiv 3 \pmod 4$. The remaining case is when M is even and e odd; let us assume that $M = 2t$. The equation (5) becomes $N^2 = 160t^4 + 164pt^2e^2 + 40p^2e^4$. Taking $N = 2N'$ and dividing by four, we get $N'^2 = 40t^4 + 41pt^2e^2 + 10p^2e^4$, which gives $N'^2 \equiv p(t^2 + 2p) \equiv 2, 3 \pmod 4$, and that is impossible. Therefore, $10 \notin S_\psi(E(p))$.

1.6. $b_1 = 10p$

We examine the equation $N^2 = p(10M^4+41M^2e^2+40e^4)$. Concluding as in the case $b_1 = 10$, we get $N^2 \equiv 2p \equiv 2 \pmod 4$ for e even and M odd, and $N^2 \equiv 3p \equiv 3 \pmod 4$ for both e and M odd. Taking e odd, $M = 2t$ and $N = 2N'$ we get $N'^2 \equiv p(2 + t^2) \equiv 2, 3 \pmod 4$ which implies that $10p \notin S_\psi(E(p))$.

Since $S_\psi(E(p))$ is a group, we have $p,\ -2p,\ -2,\ 5p,\ -5p,\ -10p,\ -10 \notin S_\psi(E(p))$. Namely, if for example $5p \in S_\psi(E(p))$, then because $-p \in S_\psi(E(p))$ we would have $-p \cdot 5p = -5 \in S_\psi(E(p))$, which we have showed that was not true. It follows that $\#S_\psi(E(p)) = 2$.

2. $E'(p) : y^2 = x^3 - 82px^2 + 81p^2x$

   Observing the torsor $N^2 = b_1M^4 - 82pM^2e^2 + b_2e^4$ with $b_1b_2 = 81p^2$ it easily follows that $b_1 = 1$ and $b_1 = p$ give the solutions $(1, 0, 1)$ and $(1, 1, 0)$. Negative values are not possible because in that case the right hand side of the torsor is negative and cannot be a square. There is only one case to observe, $b_1 = 3$ (eliminating this case automatically eliminates the case $b_1 = 3p$ because $S_\phi(E'(p))$ is a group). Reducing the torsor $N^2 = 3M^4 - 82pM^2e^2 + 27p^2e^4$ modulo p, we get $N^2 \equiv 3M^4 \pmod p$. Because of $p \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 4$ it follows that $\left(\frac{3}{p}\right) = -1$ which implies $p|M$ and $p|N$. Taking $M = pt$ and $N = pk$ yields $k^2 = 3p^2t^4 - 82pt^2e^2 + 27e^4$, which reduced modulo p once more gives $k^2 \equiv 27e^4 \pmod p$. M and e are coprime so e cannot be divisible by p and 3 is not a quadratic residue modulo p. Hence $3 \notin S_\phi(E'(p))$ and $3p \notin S_\phi(E'(p))$, which implies $\#S_\phi(E'(p)) = 2$ and $\operatorname{rank}(X_0^{(p)}(15)(\mathbb{Q})) = 0$.
3. $E(-p) : y^2 = x^3 - 41px^2 + 400p^2x$

   The torsor is $N^2 = b_1M^4 - 41pM^2e^2 + b_2e^4$ with $b_1b_2 = 400p^2$. Possible values for b_1 are $\{1, 2, 5, p, 2p, 5p, 10p, 10\}$ (for negative values the right hand side is negative). Except $b_1 = 1$, $b_1 = p$ is also an element of $S_\psi(E(-p))$, because in that case $(M, e, N) = (5, 1, 0)$ is a solution. Let us show that other values of b_1 do not give solutions.

   3.1. $b_1 = 2$

   The torsor is $N^2 = 2M^4 - 41pM^2e^2 + 200p^2e^4$. When e is even and M odd, then $N^2 \equiv 2 \pmod 4$ and when both M and e are odd, $N^2 \equiv 2 - p \equiv 5 \pmod 8$. If e is odd, $M = 2t$ and $N = 2N'$ we get $N'^2 \equiv 2p^2 - pt^2 \equiv 2, 5, 6 \pmod 8$ which implies that $2 \notin S_\psi(E(-p))$.

   3.2. $b_1 = 5p$

   The torsor is $N^2 = p(5M^4 - 41M^2e^2 + 80e^4)$. Reducing modulo 5 we get $N^2 \equiv 4pM^2e^2 \pmod 5$, which implies that either $5|M$ or $5|e$. Namely, because of $\left(\frac{p}{5}\right) = -1$ it follows that $\left(\frac{4p}{5}\right) = -1$. In both cases we get that the left hand side is divisible by 25, so the same must hold for the right hand side, and that is possible only if both M and e are divisible by 5. This is a contradiction, so $5p \notin S_\psi(E(-p))$.

   3.3. $b_1 = 10$

   The torsor is $N^2 = 10M^4 - 41pM^2e^2 + 40p^2e^4$. Reducing modulo 4 and modulo 8 easily eliminates the cases when e is even and M odd, and when both M and e are odd. If e is odd, $M = 2t$ and $N' = 2N$ then $N'^2 = 40t^4 - 41pt^2e^2 + 10p^2e^4 \equiv 2p^2 - pt^2 \equiv 2, 5, 6 \pmod 8$, so $10 \notin S_\psi(E(-p))$.

   The values $2p,\ 5,\ 10p \notin S_\psi(E(-p))$ as well, therefore $\#S_\psi(E(-p)) = 2$.
4. $E'(-p) : y^2 = x^3 + 82px^2 + 81p^2x$

   We examine the quartic $N^2 = b_1M^4 + 82pM^2e^2 + b_2e^4$ with $b_1b_2 = 81p^2$.

The value of b_1 can be one of $\{\pm 1,\ \pm 3,\ \pm p,\ \pm 3p\}$, and for $b_1 = 1$ and $b_1 = -p$ there are solutions $(M, e, N) = (1, 0, 1)$ and $(M, e, N) = (1, 1, 0)$.

4.1. $b_1 = 3$

The torsor is $N^2 = 3M^4 + 82pM^2e^2 + 27p^2e^4$. Combining reduction modulo p and the fact that $\left(\frac{3}{p}\right) = -1$ (proved while examining the ϕ-Selmer group of $E'(p)$), we get $p|M$ and $p|N$. However, reducing the torsor modulo p once more, this implies $\left(\frac{3}{p}\right) = 1$, which is a contradiction. Thus, $3 \notin S_\phi(E'(-p))$.

4.2. $b_1 = -1$

The equation to observe is $N^2 = -M^4 + 82pM^2e^2 - 81p^2e^4$. When e is even and M odd, $N^2 \equiv -M^4 \equiv 7 \pmod 8$ which is not possible. Similarly, when M is even and e odd we get $N^2 \equiv -p^2e^4 \equiv 7 \pmod 8$. When both of them are odd, we can take $M^2 = 8a + 1, p = 8b + 5$ and $e^2 = 8c + 1$, so the torsor becomes $N^2 = -64a^2 + 9216abc + 1152ab + 5760ac + 704a - 69632b^2c^2 - 17408b^2c - 1088b^2 - 87040bc^2 - 20608bc - 1216b - 27200c^2 - 6080c - 336$. Observing congruences modulo 64 we have $N^2 \equiv 48 \pmod{64}$ and this is impossible, hence $-1 \notin S_\phi(E'(-p))$.

4.3. $b_1 = 3p$

In this final case, the torsor is $N^2 = p(3M^4 + 82M^2e^2 + 27e^4)$. The cases when M is even and e odd, and vice versa give $N^2 \equiv 7 \pmod 8$. If both M and e are odd, then putting $M^2 = 8a + 1, e^2 = 8b + 1$ gives $N^2 \equiv p\left(8 + 64(3a^2 + 2ab + a + 3b^2 + b)\right) \equiv 40 \pmod{64}$, which is not possible, so $3p \notin S_\phi(E'(-p))$.

Other possible values of b_1 $(-3p,\ p,\ -3)$ are also not in $S_\phi(E'(-p))$ because $S_\phi(E'(-p))$ is a group, therefore $\#S_\phi(E'(-p)) = 2$. Since $\#S_\psi(E(-p)) = 2$ as well, we conclude that $\operatorname{rank}(X_0^{(-p)}(15)(\mathbb{Q})) = 0$.

□

We prove the following corollary similarly as Corollary 2:

Corollary 4. *There exist infinitely many primes p such that for $K = \mathbb{Q}(i, \sqrt{p})$, $\operatorname{rank}(X_0(15)(K)) = 0$.*

The next corollary is a direct consequence of the Theorem 3 and the fact that $X_0(15)$ and $X_1(15)$ are isogenous:

Corollary 5. *Le p be a prime such that $p \equiv 5 \pmod 8$ and $p \equiv 2 \pmod 3$. Then $\operatorname{rank}(X_1(15)(\mathbb{Q}(i, \sqrt{p}))) = 0$.*

Theorem 6. *Let p be a prime satisfying $p \equiv 3 \pmod 4$, and $\left(\frac{p}{5}\right) = -1$. Then, $\operatorname{rank}(X_0^{(p)}(20)(\mathbb{Q})) = \operatorname{rank}(X_0^{(-p)}(20)(\mathbb{Q})) = 0$.*

Proof. The explicit model of $X_0(20)$ is $y^2 = (x+1)(x^2+4)$ from which we easily obtain curves to observe:

$$E(p) : y^2 = x^3 - 2px^2 + 5p^2x, \tag{6}$$

$$E'(p) : y^2 = x^3 + px^2 - p^2x, \tag{7}$$

$$E(-p) : y^2 = x^3 + 2px^2 + 5p^2x, \tag{8}$$

$$E'(-p) : y^2 = x^3 - px^2 - p^2x. \tag{9}$$

Here we made some simple transformations to obtain curves in such forms. Namely, to get $E(p)$ from the explicit model we use the substitution $x \mapsto x-1$. Furthermore, $E'(p)$ and $E'(-p)$ are simplified by dividing their coefficients a and b (in the short Weierstrass form) with u^2 and u^4 respectively.

1. $E(p) : y^2 = x^3 - 2px^2 + 5p^2x$

   The torsor is in this case $N^2 = b_1M^4 - 8pM^2e^2 + b_2e^4$ where $b_1b_2 = 5p^2$. It is obvious that $1, 5 \in S_\psi(E(p))$ and that negative values of b_1 imply negative value of the right hand side of the torsor. By observing congruences modulo powers of 2 (similarly as in the cases 1.2. and 3.3. of the proof of Theorem 3) and respecting the assumption $p \equiv 3 \pmod 4$, it easily follows that $p \notin S_\psi(E(p))$. Since $S_\psi(E(p))$ is a group; $5p \notin S_\psi(E(p))$ as well, so $\#S_\psi(E(p)) = 2$.
2. $E'(p) : y^2 = x^3 + px^2 - p^2x$

   The torsor is $N^2 = b_1M^4 + 16pM^2e^2 + b_2e^4$, $b_1b_2 = -p^2$. For $b_1 = -1$ and $b_1 = 1$ the torsor has integer solutions, and for other values of b_1 not. Namely, the case $b_1 = p$ is eliminated reducing modulo 5, because of $\left(\frac{p}{5}\right) = -1$, and the case $b_1 = -p$ is eliminated using the fact that $S_\phi(E'(p))$ is a group, so $\#S_\phi(E'(p)) = 2$ and $\operatorname{rank}(X_0^{(p)}(20)(\mathbb{Q})) = 0$.
3. $E(-p) : y^2 = x^3 + 2px^2 + 5p^2x$

   The torsor is $N^2 = b_1M^4 + 8pM^2e^2 + b_2e^4$, $b_1b_2 = 5p^2$, so $1, 5 \in S_\psi(E(-p))$. For negative values of b_1 the right hand side is negative and cannot be a square, and the cases $b_1 = p$ is eliminated by reducing modulo powers of 2. Since $S_\psi(E(-p))$ is a group, it follows that $\#S_\psi(E(-p)) = 2$.
4. $E'(-p) : y^2 = x^3 - px^2 - p^2x$

   This case is dealt with exactly as the $E'(p)$ case, so we will skip it. It follows that $\operatorname{rank}(X_0^{(-p)}(20)(\mathbb{Q})) = 0$ and the statement is proved.

□

From Theorem 6 we easily prove the next corollary:

Corollary 7. *There exist infinitely many primes p such that for $K = \mathbb{Q}(i, \sqrt{p})$,* $\operatorname{rank}(X_0(20)(K)) = 0$.

Theorem 8. *Let p be a prime satisfying $p \equiv 1 \pmod 3$, $p \equiv 3 \pmod 4$, and $\left(\frac{p}{7}\right) = 1$. Then,* $\operatorname{rank}(X_0^{(p)}(21)(\mathbb{Q})) = \operatorname{rank}(X_0^{(-3p)}(21)(\mathbb{Q})) = 0$.

Proof. While transforming the explicit model of $X_0(21)$, $y^2 + xy = x^3 - 4x - 1$, into the form where $(0, 0)$ is a point of order 2, we are supposed to determine the

integer root of polynomial $x^3+x^2-64x-64$. The polynomial has three different rational roots, so we choose $x_0=8$. From this we get the curves:

$$\begin{aligned} E(p): y^2 &= x^3+25px^2+144p^2x,\\ E'(p): y^2 &= x^3-50px^2+49p^2x,\\ E(-3p): y^2 &= x^3-75px^2+1296p^2x,\\ E'(-3p): y^2 &= x^3+150px^2+441p^2x. \end{aligned}$$

1. $E(p): y^2=x^3+25px^2+144p^2x$

   As in the previous theorem, we see that the possible values of b_1 are $\{\pm1,\ \pm2,\ \pm3,\ \pm6,\ \pm p,\ \pm2p,\ \pm3p,\ \pm6p\}$. Obviously, $b_1=1$ gives an integer solution, but the value $b_1=-p$ also gives a family of integer solutions: $(M,e,N)=(4x,0,x)$. The remaining cases are eliminated as follows.

   1.1. $b_1=2$

   The torsor is $N^2=2M^4+25pM^2e^2+72p^2e^4$. Since the discriminant of the polynomial on the right hand side is a square, we can write it as

   $$N^2=(M^2+8pe^2)(2M^2+9pe^2). \tag{10}$$

   It easily follows that the greatest common divisor of the brackets on the right hand side of (10) is either 1 or 7. Therefore, only two systems of equations are possible:

   $$\begin{aligned} M^2+8pe^2 &= \square,\\ 2M^2+9pe^2 &= \square, \end{aligned}$$

   and

   $$\begin{aligned} M^2+8pe^2 &= 7\square,\\ 2M^2+9pe^2 &= 7\square. \end{aligned}$$

   Note that after reduction modulo 3, they become the same system. By using $p\equiv1 \pmod 3$, that system is easily eliminated. Namely, if $3\nmid M$, then in the second equation 2 should be a quadratic residue modulo 3, which is not true. If $3|M$, then $3\nmid e$, hence in the first equation we get that 2 needs to be be a quadratic residue modulo 3. We conclude $2\notin S_\psi(E(p))$, which combined with $-p\in S_\psi(E(p))$ gives $-2p\notin S_\psi(E(p))$.

   1.2. $b_1=3$

   The torsor is $N^2=3M^4+25pM^2e^2+48p^2e^4$. If M and e are both odd, then $N^2\equiv3+p\equiv2 \pmod 4$, which is impossible. If e is even and M is odd, then $N^2\equiv3 \pmod 4$, which is also impossible. We are left with the case when M is even and e is odd. If we denote $M=2t$, then N needs to be even as well, so we can take $N=2l$ and get $l^2=12t^2+25pt^2e^2+12p^2e^4$. If t is odd, then $l^2\equiv p\equiv3 \pmod 4$, so the only remaining case is when t is even. Let us denote $t=2t'$, $l=2l'$ (l also needs to be even) so we finally get $l'^2=48t'^2+25pt'^2e^2+3p^2e^4$, or equivalently $l'^2\equiv3(t'^2+1) \pmod 4$, which gives $l'^2\equiv2,3 \pmod 4$,

but neither of these two cases is possible. Thus, $3 \notin S_\psi(E(p))$, and consequently $-3p \notin S_\psi(E(p))$.

1.3. $b_1 = 6$

The torsor is $N^2 = 6M^4 + 25pM^2e^2 + 24p^2e^4$, so we get a factorization

$$N^2 = (3M^2 + 8pe^2)(2M^2 + 3pe^2). \tag{11}$$

The greatest common divisor of the factors on the right hand side is either 1, or p, or 7, or $7p$. Hence, we get systems of equations of the form

$$\begin{aligned} 3M^2 + 8pe^2 &= a\square, \\ 2M^2 + 3pe^2 &= a\square, \end{aligned}$$

where $a = \gcd(3M^2 + 8pe^2,\ 2M^2 + 3pe^2)$. All these systems become the same one after reducing modulo 3 and are easily eliminated by taking $p \equiv 1 \pmod 3$. If $3|M$, then $3 \nmid e$, so we get from the first equation that 2 has to be a quadratic residue modulo 3. If $3 \nmid M$, then we arrive to the same conclusion in the second equation. Therefore, $6 \notin S_\psi(E(p))$, and $-6p \notin S_\psi(E(p))$.

1.4. $b_1 = p$

The torsor is $N^2 = pM^4 + 25pM^2e^2 + 144pe^4$. This case is eliminated by observing congruences modulo powers of 2, in the same manner as in case 1.2. Thus, $p \notin S_\psi(E(p))$, and $-1 \notin S_\psi(E(p))$.

1.5. $b_1 = 2p$

From the torsor $N^2 = 2pM^4 + 25pM^2e^2 + 72pe^4$, we obtain the appropriate factorization

$$N^2 = p(2M^2 + 9e^2)(M^2 + 8e^2). \tag{12}$$

By observing the factors on the right hand side of (12), we get the systems of the equations

$$\begin{aligned} 2M^2 + 9e^2 &= ap\square, \\ M^2 + 8e^2 &= a\square, \end{aligned}$$

and

$$\begin{aligned} 2M^2 + 9e^2 &= a\square, \\ M^2 + 8e^2 &= ap\square, \end{aligned}$$

where $a \in \{1, 7\}$. After reducing modulo 3 and taking $p \equiv 1 \pmod 3$, all these systems become the same. That system is easily eliminated by taking $3 \nmid M$ (first equation), or $3|M,\ 3 \nmid e$ (second equation). Thus, $2p \notin S_\psi(E(p))$, and $-2 \notin S_\psi(E(p))$.

1.6. $b_1 = 3p$

The torsor is $N^2 = 3pM^4 + 25pM^2e^2 + 48pe^4$, and this is equivalent to

$$(6M^2 + 25e^2)^2 - 49e^4 = 12p\square. \tag{13}$$

From the assumption $\left(\frac{p}{7}\right) = 1$ we conclude that the right hand side of (13) is either divisible by 7, or does not give a quadratic residue modulo 7. However, reduction modulo 7 leaves on the left hand side a square $(6M^2 + 25e^2)^2$, so it needs to hold

$$7 \mid 6M^2 + 25e^2. \tag{14}$$

Let us write the torsor as

$$N^2 = p(M^2 + 3e^2)(3M^2 + 16e^2).$$

Since $\gcd(M^2+3e^2,\ 3M^2+16e^2) \in \{1, 7\}$, and from (14) it follows that $7|M^2+3e^2$ and $7|3M^2+16e^2$, we conclude that $\gcd(M^2+3e^2,\ 3M^2+16e^2) = 7$. Thus, we observe the systems

$$\begin{aligned} M^2 + 3e^2 &= 7p\square, \\ 3M^2 + 16e^2 &= 7\square, \end{aligned}$$

and

$$\begin{aligned} M^2 + 3e^2 &= 7\square, \\ 3M^2 + 16e^2 &= 7p\square. \end{aligned}$$

With the assumption $p \equiv 3 \pmod 4$, both systems are eliminated reducing modulo powers of 2. Namely, if M is even, we get from the first equation of the first system that 3 needs to be a quadratic residue modulo 4, a contradiction. If M is odd, then the left hand side of the second equation is congruent 3 modulo 8, which is a contradiction with the right hand side. Let us focus now on the second system. If M is odd, then from the second equation of the second system we get that 3 has to be a quadratic residue modulo 4. If M is even, then e must be odd. When M is divisible by 4, then the left hand side of the first equation is congruent 3 modulo 8, which is a contradiction with the right hand side. If M is divisible by 2, but not by 4, then the left hand side of the second equation is congruent 12 modulo 16, but that is not true for the right hand side. Therefore, $3p \notin S_\psi(E(p))$, and $-3 \notin S_\psi(E(p))$.

1.7. $b_1 = 6p$

The torsor is $N^2 = 6pM^4 + 25pM^2e^2 + 24pe^4$, which gives

$$N^2 = p(3M^2 + 8e^2)(2M^2 + 3e^2).$$

This case is eliminated analogously as the case 1.5. Thus, $6p \notin S_\psi(E(p))$, and $-6 \notin S_\psi(E(p))$.

The analysis of the cases 1.1. - 1.7. eliminated all remaining possible values of b_1. Therefore, $\#S_\psi(E(p)) = 2$.

2. $E'(p) : y^2 = x^3 - 50px^2 + 49p^2x$

There are only four possible values of b_1 in this case: $\{1, 7, p, 7p\}$. For $b_1 = 1$ and $b_1 = p$ there are solutions $(1, 0, 1)$ and $(1, 1, 0)$, while the cases $b_1 = 7$ and $b_1 = 7p$ are eliminated reducing modulo 7, because of $\left(\frac{p}{7}\right) = 1$. We conclude that $\#S_\phi(E'(p)) = 2$ and consequentely $\operatorname{rank}(X_0^{(p)}(21)(\mathbb{Q})) = 0$.

3. $E(-3p) : y^2 = x^3 - 75px^2 + 1296p^2x$

   Except $b_1 = 1$, the value $b_1 = 3p$ also gives an integer solution $(M, e, N) = (4, 0, 1)$ of the associated torsor. Negative values of b_1 are eliminated immediately, so we are left with the cases $\{2, 3, 6, p, 2p, 6p\}$. $b_1 = 2$ and $b_1 = 2p$ yield a contradiction by observing congruences modulo 3, the latter additionally using the assumption $p \equiv 1 \pmod 3$. The case $b_1 = 3$ is eliminated reducing modulo powers of 2. Because $S_\psi(E(-3p))$ is a group, remaining cases fail as well. Thus, $\#S_\psi(E(-3p)) = 2$.
4. $E'(-3p) : y^2 = x^3 + 150px^2 + 441p^2x$

   The values $b_1 = 1$ and $b_1 = -3p$ give an integer solution of the associated torsor, the latter $(M, e, N) = (1, 1, 0)$. When $b_1 = -1$ or $b_1 = -7$, we get a contradiction modulo 3 for all p. For $b_1 = -p$ and $b_1 = -7p$ we additionally use the condition $p \equiv 1 \pmod 3$. The value $b_1 = -3$ is eliminated reducing modulo 32, and the values $b_1 = -21$ and $b_1 = -21p$ reducing modulo 7 and using the assumption $\left(\frac{p}{7}\right) = 1$. All other cases are eliminated by using the fact that $S_\phi(E'(-3p))$ is a group, which implies $\#S_\phi(E'(-3p)) = 2$ and finally $\mathrm{rank}(X_0^{(-3p)}(21)(\mathbb{Q})) = 0$.

□

As in the other cases, Theorem 8 also implies the next corollary:

Corollary 9. *There exist infinitely many primes p such that for $K = \mathbb{Q}(\sqrt{-3}, \sqrt{p})$, $\mathrm{rank}(X_0(21)(K)) = 0$.*

Theorem 10. *Let p be a prime satisfying $p \equiv 1 \pmod 4$, and $\left(\frac{p}{7}\right) = -1$. Then, $\mathrm{rank}(X_0^{(p)}(49)(\mathbb{Q})) = \mathrm{rank}(X_0^{(-7p)}(49)(\mathbb{Q})) = 0$.*

Proof. An explicit model of $X_0(49)$ is $y^2 + xy = x^3 - x^2 - 2x - 1$. By transforming it into the form suitable for descent via 2-isogenies, we get the curves

$$\begin{aligned} E(p) : y^2 &= x^3 + 21px^2 + 112p^2x, \\ E'(p) : y^2 &= x^3 - 42px^2 - 7p^2x, \\ E(-7p) : y^2 &= x^3 - 147px^2 + 5488p^2x, \\ E'(-7p) : y^2 &= x^3 + 294px^2 - 343p^2x. \end{aligned}$$

By calculating its j-invariant (that is -3375), we notice that $E(p)$ has a complex multiplication with the ring of integers of $\mathbb{Q}(\sqrt{-7})$. Hence, the curves $E(p)$ and $E(-7p)$ are isogenous, so we will compute the rank just for the first of them.

1. $E(p) : y^2 = x^3 + 21px^2 + 112p^2x$

   The associated torsor has obvious integer solutions for $b_1 = 1$ and $b_1 = 7$. The values $b_1 = p$ and $b_1 = 2p$ can be easily eliminated by using the assumption $\left(\frac{p}{7}\right) = -1$, and the value $b_1 = 2$ by using $p \equiv 1 \pmod 4$. When b_1 is negative, the right hand side of the torsor is negative, which is impossible, and all other cases are eliminated by the group structure of $S_\psi(E(p))$. Thus, $\#S_\psi(E(p)) = 2$.
2. $E'(p) : y^2 = x^3 - 42px^2 - 7p^2x$

   There are integer solutions of the associated torsor for $b_1 = 1$ and $b_1 = 7$,

the case $b_1 = p$ fails because of $\left(\frac{p}{7}\right) = -1$ and the case $b_1 = -p$ because of $p \equiv 1 \pmod 4$. We conclude $\#S_\phi(E'(p)) = 2$ and $\operatorname{rank}(X_0^{(p)}(49)(\mathbb{Q})) = 0$. Since $E(p)$ and $E(-7p)$ are isogenous, $\operatorname{rank}(X_0^{(-7p)}(49)(\mathbb{Q})) = 0$ as well. □

Corollary 11. *There exist infinitely many primes p such that for $K = \mathbb{Q}(\sqrt{-7}, \sqrt{p})$, $\operatorname{rank}(X_0(49)(K)) = 0$.*

3. The case $n = 27$

Recall from [6] that $\mathbb{Q}(\sqrt{-3})$ is the only quadratic field K with the property that $\#Y_0(27)(\mathbb{Q}) \neq \#Y_0(27)(K) < \infty$. All three $\mathbb{Q}(\sqrt{-3})$-rational points on $Y_0(27)$ correspond to the same CM j-invariant, -12288000. We will construct infinitely many extensions F of K such that $\#Y_0(27)(\mathbb{Q}) \neq \#Y_0(27)(F) < \infty$. However, in this case we will not construct quadratic extensions of $\mathbb{Q}(\sqrt{-3})$, but instead cubic ones.

As $X_0(27)(\mathbb{Q}(\sqrt{-3})) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, one cannot use 2-isogeny descent in this case because $X_0(27)(\mathbb{Q}(\sqrt{-3}))$ has no 2-torsion. However, the existence of a 3-torsion point leads one to use the 3-Selmer group in place of the 2-isogeny-Selmer group. For simplicity denote $X = X_0(27)$; a short Weierstrass model for X is

$$X : y^2 = x^3 - 432$$

which can also be written (in projective coordinates) as

$$X' : x'^3 + y'^3 = z'^3.$$

A cubic twist C_n of X, where $n \in K^*/(K^*)^3$, can be written as

$$C_n : y^2 = x^3 - 432n^2$$

or as

$$C_n' : x'^3 + y'^3 = nz'^3.$$

Denote by $E(K)(n')$ the n-free part of $E(K)$, i.e. $E(K)/E(K)[n]$. Whereas in the previous section we used the fact that $\operatorname{rank}(E(F(\sqrt{d}))) = \operatorname{rank}(E(F)) + \operatorname{rank}(E^d(F))$, for any number field F, we will use the following lemma in this case.

Lemma 12. *Let C/K be an elliptic curve with j-invariant 0 over a number field K containing ζ_3. Let $F = K(\sqrt[3]{m})$, where m is a cubefree integer and denote by C_m and C_{m^2} cubic twists of C which become isomorphic to C over F. Then*

$$C(F)(3') \simeq C(K)(3') \oplus C_m(K)(3') \oplus C_{m^2}(K)(3').$$

In particular,

$$\operatorname{rank}(C(F)) = \operatorname{rank}(C(K)) + \operatorname{rank}(C_m(K)) + \operatorname{rank}(C_{m^2}(K)).$$

Proof. Let σ be a generator of $\operatorname{Gal}(F/K)$, defined by $\sigma(\sqrt[3]{m}) = \zeta_3 \sqrt[3]{m}$. Note that C, C_m and C_{m^2} are all isomorphic over F and that the points fixed by $\operatorname{Gal}(F/K)$ are isomorphic to $C(K)$, and

$$C_m(K) \simeq \{P \in C(F) : P^\sigma = \zeta_3^2 P, \overline{P} = P\},$$

(see [1]) and similarly,

$$C_{m^2}(K) \simeq \{P \in C(F) : P^\sigma = \zeta_3 P, \overline{P} = P\}.$$

Let $P \in C(F)$. Then

$$Q = P + P^\sigma + P^{\sigma^2} \in C(K), \tag{15}$$

$$Q' = P + \zeta_3 P^{\sigma} + \zeta_3^2 P^{\sigma^2} \in C_m(K), \tag{16}$$

$$Q'' = P + \zeta_3^2 P^{\sigma} + \zeta_3 P^{\sigma^2} \in C_{m^2}(K). \tag{17}$$

By adding (15), (16) and (17), we get

$$3P \in C(K) + C_m(K) + C_{m^2}(K).$$

Thus for any point $P \in C(F)$, $3P$ can be written as the sum of a point on $C(K)$, a point on $C_m(K)$ and a point on $C_{m^2}(K)$.

Now we prove the reverse: let $Q \in C(K)$, $Q' \in C_m(K)$ and $Q'' \in C_{m^2}(K)$ be all non-zero points. As all these curves are isomorphic over F, we can view Q' and Q'' as points on $C(F)$, by mapping them by the appropriate isomorphism.

We claim that points Q, Q' and Q'' are independent (one point cannot be written as a linear combination of the others) in $C(F)$ if and only if none of these points are annihilated by multiplication by 3.

Suppose

$$\alpha Q + \beta Q' + \gamma Q'' = 0. \tag{18}$$

Applying σ and σ^2 to this equation, one gets

$$\alpha Q + \zeta_3^2 \beta Q' + \zeta_3 \gamma Q'' = 0, \tag{19}$$

and

$$\alpha Q + \zeta_3 \beta Q' + \zeta_3^2 \gamma Q'' = 0. \tag{20}$$

Adding the 3 equations, one gets $3\alpha Q = 0$, which is, by assumption, true if and only if $\alpha = 0$. By multiplying equation (19) by ζ_3 and (20) by ζ_3^2 and then adding all the equations together, one gets $3\beta Q' = 0$. Hence $\beta = 0$. By the same argument, one concludes that $\gamma = 0$.

By what we have shown, it is an easy to see that the

$$C(F)(3') \simeq C(K)(3') \oplus C_m(K)(3') \oplus C_{m^2}(K)(3'),$$

as claimed. □

Remark 1. Note that a more highbrow (and shorter) way of stating the above result would be to decompose the $\mathbb{Q}(\zeta_3)$-linear representation $\mathbb{Q} \otimes C(F)$ of $\mathrm{Gal}(F/K)$ into the sum of its irreducible eigenspaces, but we felt that a more explicit proof was appropriate.

We are now ready to prove the following:

Theorem 13. *Let $p \equiv 2, 5 \pmod 9$ be a prime. Then*

$$\#Y_0(27)(\mathbb{Q}) \neq \#Y_0(27)(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{p})) < \infty.$$

Proof. From [6] we have

$$\#Y_0(27)(\mathbb{Q}) < \#Y_0(27)(\mathbb{Q}(\sqrt{-3}) \leq \#Y_0(27)(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{p})),$$

so we need to prove that $\#Y_0(27)(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{p})) < \infty$, or in other words that $\mathrm{rank}\left(X_0(27)(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{p}))\right) = 0$.

As already mentioned $X_0(27) = C_1$, and from Lemma 12 it follows that

$$\begin{aligned}\mathrm{rank}\left(X_0(27)(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{p}))\right) = \mathrm{rank}\left(C_1(\mathbb{Q}(\sqrt{-3}))\right) + \mathrm{rank}\left(C_p(\mathbb{Q}(\sqrt{-3}))\right) \\ + \mathrm{rank}\left(C_{p^2}(\mathbb{Q}(\sqrt{-3}))\right).\end{aligned}$$

Now one uses the fact that C_1, C_p and C_{p^2} are elliptic curves with complex multiplication by $\mathbb{Z}[\zeta_3]$, and it follows that they are ismorphic to their quadratic twists by -3. Now we have

$$\operatorname{rank}\left(X_0(27)(\mathbb{Q}(\sqrt{-3},\sqrt[3]{p}))\right) = 2\operatorname{rank}(C_1(\mathbb{Q})) + 2\operatorname{rank}(C_p(\mathbb{Q})) + 2\operatorname{rank}(C_{p^2}(\mathbb{Q})).$$

It is well known (and easily verifiable) that $\operatorname{rank}(C_1(\mathbb{Q})) = 0$. For the facts that $\operatorname{rank}(C_p(\mathbb{Q})) = 0$ and $\operatorname{rank}(C_{p^2}) = 0$, see [8, Theorem VIII]. □

References

[1] S. Dasgupta and J. Voight, *Heegner points and Sylvester's conjecture*, Arithmetic Geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, 2009, 91–102.

[2] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20.

[3] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239–244.

[4] M. A. Kenku, *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), 415–427.

[5] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[6] F. Najman, *Exceptional elliptic curves over quartic fields*, Int. J. Number Theory, **8** (2012), 1231–1246.

[7] F. Najman, *On the number of elliptic curves with prescribed isogeny or torsion group over number fields of prime degree*, Glasgow Math. J, to appear.

[8] E. S. Selmer, *The diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. **85** (1951), 203–362.

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

[10] Y. Yang, *Defining equations of modular curves*, Adv. Math. **204** (2006), 481–508.

Kumičićeva 20, 51000 Rijeka, Croatia
E-mail address: miljen.mikic@gmail.com

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail address: fnajman@math.hr