ACTA ARITHMETICA
165.4 (2014)

Optimal curves differing by a 5-isogeny

by

Dongho Byeon and Taekyung Kim (Seoul)

1. Introduction. For a positive integer N, let $X_1(N) = \mathbb{H}^*/\Gamma_1(N)$ and $X_0(N) = \mathbb{H}^*/\Gamma_0(N)$ denote the usual modular curves. Let $\mathcal{C}$ denote an isogeny class of elliptic curves defined over $\mathbb{Q}$ of conductor N. For $i = 0, 1$, there is a unique curve $E_i \in \mathcal{C}$ and a parametrization $\phi_i : X_i(N) \to E_i$ such that for any $E \in \mathcal{C}$ and parametrization $\phi_i' : X_i(N) \to E$, there is an isogeny $\pi_i : E_i \to E$ such that $\pi_i \circ \phi_i = \phi_i'$. For $i = 0, 1$, the curve E_i is called the $X_i(N)$-*optimal curve*.

It seems that for most isogeny classes $\mathcal{C}$, E_0 and E_1 are the same. However, there are also several examples of isogeny classes with non-isomorphic optimal curves. For example, $E_0 = X_0(11)$ and $E_1 = X_1(11)$ differ by a 5-isogeny. Based on numerical observations, Stein and Watkins [SW] made a precise conjecture on the classification of isogeny classes with non-isomorphic optimal curves. According to those authors, in any isogeny class $\mathcal{C}$, the optimal curves E_0 and E_1 are only isogenous by an isogeny of degree 1, 2, 3, 4, or 5. For the 5-isogeny case, they made the following

Conjecture (Stein and Watkins). *For $i = 0, 1$, let E_i be the $X_i(N)$-optimal curve of an isogeny class $\mathcal{C}$ of elliptic curves defined over $\mathbb{Q}$ of conductor N. Then E_0 and E_1 differ by a 5-isogeny if and only if $E_0 = X_0(11)$ and $E_1 = X_1(11)$.*

Remark. This conjecture needs to be modified as in the case of 3-isogeny (cf. [BY2]) because there is a counterexample when N is not square-free or $5 \mid N$. For example, assuming Stevens's conjecture [St, Conjecture 2.4]), consider the isogeny class '33825be' in Cremona's database of elliptic curves [Cr]. In this case, the curves '33825be1' and '33825be3' are $X_0(33825)$- and $X_1(33825)$-optimal, respectively.

In [BY2], Byeon and Yhee proved that the conjecture of Stein and Watkins is true for the case of 3-isogeny if N is square-free and $3 \nmid N$.

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 14K02.
Key words and phrases: elliptic curves, optimal curves, isogeny.

DOI: 10.4064/aa165-4-5

(There is an error in the proof of (ii) of Theorem 1.1 in [BY2]. However this error can be amended by using Proposition 4.1 below. For details, see Remark in §4.) In this paper, we prove that the conjecture of Stein and Watkins is true for the case of 5-isogeny if N is square-free and $5 \nmid N$:

THEOREM 1.1. *For $i = 0, 1$, let E_i be the $X_i(N)$-optimal curve of an isogeny class $\mathcal{C}$ of elliptic curves defined over $\mathbb{Q}$ of conductor N. Suppose that N is square-free and $5 \nmid N$. Then E_0 and E_1 differ by a 5-isogeny if and only if $E_0 = X_0(11)$ and $E_1 = X_1(11)$.*

2. Preliminaries. Let $\mathcal{C}$ be an isogeny class of elliptic curves defined over $\mathbb{Q}$. For any $E \in \mathcal{C}$, let $E_{\mathbb{Z}}$ be the Néron model over $\mathbb{Z}$ and ω_E a Néron differential on E. Let $\pi : E \to E'$ be an isogeny with $E, E' \in \mathcal{C}$. We say that π is *étale* if the extended morphism $E_{\mathbb{Z}} \to E'_{\mathbb{Z}}$ between Néron models is étale. Equivalently, π is étale if $\ker \pi$ is an étale group scheme. We need the following facts about étale isogenies (cf. [Va]):

- If $\pi : E' \to E$ is any isogeny over $\mathbb{Q}$, then we have $\pi^*(\omega_E) = n_\pi \omega_{E'}$ for some non-zero $n_\pi \in \mathbb{Z}$. Moreover, the isogeny π is étale if and only if $n_\pi = \pm 1$.
- If π is any isogeny of prime degree, then precisely one of π or its dual isogeny $\hat{\pi}$ is étale.
- The composition of two étale isogenies is also étale.
- Any étale isogeny is necessarily cyclic.
- Let E be an elliptic curve over $\mathbb{Q}$ which admits a cyclic l-isogeny $E \to E'$, for an odd prime l. Then it is étale if and only if its kernel is isomorphic to $\mathbb{Z}/l\mathbb{Z}$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module.

Stevens [St] proved that in every isogeny class $\mathcal{C}$ of elliptic curves defined over $\mathbb{Q}$, there exists a unique curve $E_{\min} \in \mathcal{C}$ such that for every $E \in \mathcal{C}$, there is an étale isogeny $\pi : E_{\min} \to E$. The curve $E_{\min}$ is called the *minimal curve* in $\mathcal{C}$. Stevens conjectured that $E_{\min} = E_1$ and Vatsal [Va] proved the following theorem.

THEOREM 2.1 (Vatsal). *Suppose that the isogeny class $\mathcal{C}$ consists of semi-stable curves. Then the étale isogeny $\pi : E_{\min} \to E_1$ has degree a power of two.*

Dummigan [Du] proved the following theorem under a certain condition and later Byeon and Yhee [BY1] proved that it is in fact unconditionally true.

THEOREM 2.2 (Dummigan). *Let $E \in \mathcal{C}$ be an elliptic curve defined over $\mathbb{Q}$ of square-free conductor N with a rational point of order $l \nmid N$. Then $E_0 \in \mathcal{C}$ has a rational point of order l.*

3. Hadano's conjecture. Let E be a rational elliptic curve of conductor N having a rational torsion point of order n, and p be a prime dividing n. In [Ha], Hadano investigated whether the p-isogenous curve E' to E has a rational torsion point of order n again. In this paper, we need the case when $n = p = 5$. For this case, Hadano's work can be restated as follows.

When a rational elliptic curve E has a rational 5-torsion point, we can take a Weierstrass equation for E:

$$E : y^2 + (v - u)xy - uv^2y = x^3 - uvx^2 \tag{1}$$

where $u, v \in \mathbb{Z}$ with $(u, v) = 1$ and $u > 0$. Note that the discriminant Δ of E is given by

$$\Delta = u^5v^5(u^2 - 11uv - v^2)$$

and the torsion group is $T = \{\infty, (0, 0), (uv, u^2v), (uv, 0), (0, uv^2)\}$.

Lemma 3.1. *The Weierstrass equation of the form* (1) *with* $u, v \in \mathbb{Z}$, $(u, v) = 1$, *and* $u > 0$ *is minimal.*

Proof. We only need to check the minimality of (1) for primes dividing $\Delta = u^5v^5(u^2 - 11uv - v^2)$. For primes p dividing uv, we can obtain minimality by simply looking at the order of the constant c_4: indeed, $\operatorname{ord}_p c_4 = 0$. Suppose that a prime p divides $u^2 - 11uv - v^2$, and assume $\operatorname{ord}_p \Delta = \operatorname{ord}_p(u^2 - 11uv - v^2) \geq 12$. Note that in this case p can divide neither u nor v, as $(u, v) = 1$. Since $c_4 = u^4 - 12u^3v + 14u^2v^2 + 12uv^3 + v^4$, by dividing c_4 by $u^2 - 11uv - v^2$ we have

$$c_4 = (u^2 - 11uv - v^2)(-4u^2 - uv - v^2) + 5u^3(u - 11v).$$

If $p \mid c_4$, then we must have $p = 5$ or $p \mid (u - 11v)$ (or both). If $p \mid (u - 11v)$, then since $u^2 - 11uv - v^2 = (u - 11v)u - v^2$, we must have $p \mid v$, a contradiction. Thus, in any remaining cases, we have $\operatorname{ord}_p c_4 \leq 1$, and hence the equation is minimal at p. ∎

Let E' be an elliptic curve defined by $E' = E/T$. Then E' is given by a model

$$\begin{aligned} E' : y^2 + (v - u)xy - uv^2y = x^3 - uvx^2 &+ (5uv^3 - 10u^2v^2 - 5u^3v)x \\ &+ (uv^5 - 15u^2v^4 + 5u^3v^3 - 10u^4v^2 - u^5v) \end{aligned} \tag{2}$$

with discriminant $\Delta' = uv(u^2 - 11uv - v^2)^5$.

Lemma 3.2. *The Weierstrass equation* (2) *with* $u, v \in \mathbb{Z}$, $(u, v) = 1$, *and* $u > 0$ *is minimal, possibly outside of the prime* $p = 5$.

Proof. As in Lemma 3.1, we only need to consider the primes p dividing $\Delta' = uv(u^2 - 11uv - v^2)^5$. If p divides uv, then the c_4-invariant c_4' of the equation (2) has order 0 at p. So suppose that p divides $u^2 - 11uv - v^2$.

In order to show minimality, we can also assume $\mathrm{ord}_p(u^2-11uv-v^2)\geq 3$. Note that in this case we have neither $p\,|\,u$ nor $p\,|\,v$. Since

$$\begin{aligned} c_4' &= u^4+228u^3v+494u^2v^2-228uv^3+v^4 \\ &= (u^2-11uv-v^2)(-3124u^2+239uv-v^2)+5^5u^3(u-11v), \end{aligned}$$

and since $u^2-11uv-v^2=(u-11v)u-v^2$, we must have $p=5$ and $p\nmid(u-11v)$. ∎

Note that when equation (2) is not minimal modulo $p=5$, the minimal discriminant of the equation is exactly $\Delta'/5^{12}$. For E' to have a rational point of order 5 again, the equation must be transformed into the form

$$E' : y^2+(V-U)xy-UV^2y=x^3-UVx^2 \tag{3}$$

for some $U,V\in\mathbb{Z}$ with $(U,V)=1$ and $U>0$. Since (2) and (3) must define the same curve, we can compare their discriminants and c_4-invariants. Since (3) is minimal (Lemma 3.1), we have

$$uv(u^2-11uv-v^2)^5=5^{12k}U^5V^5(U^2-11UV-V^2) \tag{4}$$

and

$$\begin{aligned} &v^4-228uv^3+494u^2v^2+228u^3v+u^4 \\ &\qquad\qquad = 5^{4k}(V^4+12UV^3+14U^2V^2-12U^3V+U^4), \end{aligned} \tag{5}$$

for some $k\in\{0,1\}$ chosen according to whether equation (2) is minimal or not.

Let

$$r=\frac{u^2-11uv-v^2}{UV}\in\mathbb{Q}.$$

Then

$$\begin{aligned} UVr &= u^2-11uv-v^2, \\ uvr^5 &= 5^{12k}(U^2-11UV-V^2). \end{aligned} \tag{6}$$

Set $s=v/u\in\mathbb{Q}$. If we write $f(x,y)=x^2-11xy-y^2$, then the right hand side of (5) can be written as $5^{4k}(f(U,V)^2+10UVf(U,V)+5U^2V^2)$. We divide both sides of (5) by u^4 and consider the formulae (6) to obtain

$$\begin{aligned} &s^4-228s^3+494s^2+228s+1 \\ &\qquad = \frac{5^{4k}(f(U,V)^2+10UVf(U,V)+5U^2V^2)}{u^4} \\ &\qquad = \frac{r^2 5^{24k}(f(U,V)^2+10UVf(U,V)+5U^2V^2)}{5^{20k}r^2u^4} \end{aligned} \tag{7}$$

$$= \frac{u^2v^2r^{12} + 10 \cdot 5^{12k} uvf(u,v)r^6 + 5 \cdot 5^{24k} f(u,v)^2}{5^{20k} r^2 u^4}$$
$$= \frac{s^2r^{12} + 2 \cdot 5^{12k+1}(s - 11s^2 - s^3)r^6 + 5^{24k+1}(1 - 22s + 119s^2 + 22s^3 + s^4)}{5^{20k} r^2}.$$

By multiplying both sides of (7) by $5^{20k}r^2$, we get the Diophantine equation

$$\begin{aligned} (8) \qquad & 5^{20k}r^2(s^4 - 228s^3 + 494s^2 + 228s + 1) \\ &= s^2r^{12} + 2 \cdot 5^{12k+1}(s - 11s^2 - s^3)r^6 + 5^{24k+1}(1 - 22s + 119s^2 + 22s^3 + s^4). \end{aligned}$$

Moreover, when $k = 0$, we get a simpler equation

$$\begin{aligned} &[-r^5s + 5r^4s - 15r^3s + 25r^2s - 25rs + s^2 + 11s - 1] \\ &\qquad \times [r^5s + 5r^4s + 15r^3s + 25r^2s + 25rs + s^2 + 11s - 1] \times [r^2 - 5] = 0. \end{aligned}$$

Since $r \in \mathbb{Q}$, we drop the last factor to get

$$\begin{aligned} &[s^2 - 1 - (r^5 - 5r^4 + 15r^3 - 25r^2 + 25r - 11)s] \\ &\qquad \times [s^2 - 1 + (r^5 + 5r^4 + 15r^3 + 25r^2 + 25r + 11)s] = 0, \end{aligned}$$

so if we make the substitution $r + 1 = t$ or $r - 1 = t$, the above equation is equivalent to

$$(9) \qquad s^2 + (t^4 + 5t^2 + 5)st = 1.$$

Unlike the case $k = 0$, when $k = 1$, we cannot reduce the equation (8) to a simpler one.

Hadano [Ha] only considered the case $k = 0$, and proved the following proposition. We slightly modify his result to cover all possible cases.

PROPOSITION 3.3 (Hadano). *If a rational elliptic curve E of conductor N has a rational point P of order 5 and $E' := E/\langle P \rangle$ has a rational point of order 5 again, then the Diophantine equation (8) has a rational solution in (r, s) (specifically, the Diophantine equation (9) has a rational solution in (s, t) when $k = 0$).*

We can observe that (9) has trivial solutions $(s, t) = (\pm 1, 0)$, and these correspond to the elliptic curves $E = X_1(11)$ and $E' = X_0(11)$. Based on this observation and Proposition 3.3, Hadano [Ha] conjectured the following.

CONJECTURE (Hadano). *The Diophantine equation (9) has only trivial solutions $(s, t) = (\pm 1, 0)$. In particular, if a rational elliptic curve E has a rational point P of order 5 and $E' := E/\langle P \rangle$ has a rational point of order 5 again, then $E' = X_0(11)$ and $E = X_1(11)$.*

Rubin and Silverberg [RS] considered some families of elliptic curves with constant mod-p representations. In particular, following Klein, they defined an elliptic curve B_u over $\mathbb{Q}(u)$ as follows:

$$B_u : y^2 = x^3 - \frac{u^{20} - 228u^{15} + 494u^{10} + 228u^5 + 1}{48}x + \frac{u^{30} + 522u^{25} - 10005u^{20} - 10005u^{10} - 522u^5 + 1}{864}.$$

The curve B_u has the property that $B_u[5] \cong (\mathbb{Z}/5\mathbb{Z}) \oplus \mu_5$ as $\mathrm{Gal}(\overline{\mathbb{Q}(u)}/\mathbb{Q}(u))$-module. Using this curve, we show:

Proposition 3.4. *Hadano's conjecture is not true.*

Proof. By substituting a special value $u \in \mathbb{Q}$, we get an elliptic curve defined over $\mathbb{Q}$ which has its full 5-torsion subgroup isomorphic to $(\mathbb{Z}/5\mathbb{Z}) \oplus \mu_5$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. Hence, at least in the case that B_u gives a semistable curve, we have a sequence of elliptic curves with étale isogenies

$$B_u/\mu_5 \to B_u \to B_u/(\mathbb{Z}/5\mathbb{Z}).$$

More concretely, if we substitute $u = 3$, then B_u becomes the semistable curve '185163a2' in Cremona's database, and we have

$$\text{'185163a1'} \to \text{'185163a2'} \to \text{'185163a3'},$$

where both arrows indicate étale isogenies. This sequence corresponds to the solution $s = -1/243$ and $t = -8/3$ of (9). So Hadano's conjecture is not true. ∎

Remark. In the case $k = 1$, we have the following example. Consider the elliptic curve B_u with $u = 2$. This gives a sequence

$$\text{'550k3'} \to \text{'550k2'} \to \text{'550k1'}.$$

This curve corresponds to the solution $(r, s) = (125/2, -1/32)$ of (8).

4. Proof of Theorem 1.1. Let f be the newform associated to an elliptic curve E of conductor N. Consider the case that N is square-free. For $d \mid N$, let W_d be the Atkin–Lehner involution and let $w_d = \pm 1$ be such that $W_d f = w_d f$ (cf. [AL]). We note that for primes $p \mid N$, $w_p = -1$ or $+1$ according as the multiplicative reduction at p is split or non-split, respectively.

Proposition 4.1. *Let E_0 be the $X_0(N)$-optimal curve of an isogeny class $\mathcal{C}$ of elliptic curves defined over $\mathbb{Q}$ of conductor N, and l be an odd prime. Suppose that N is square-free and $l \nmid N$. If $\mu_\ell \subset E_0[\ell]$, then there is only one prime $p \mid N$ such that $w_p = -1$.*

Proof. By [Va, Theorem 1.1], $\mu_\ell \subset E_0[l]$ must be contained in the Shimura subgroup $\Sigma(N)$ of $J_0(N)$. By [LO, Theorem 1], $\Sigma(N)$ is isomorphic to a subgroup of $\mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^\times, U)$, where U is the group of complex numbers of modulus 1. So μ_ℓ is isomorphic to a subgroup of $\mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})^\times, U)$

for a prime $p \mid N$ such that $p \equiv 1 \pmod{\ell}$. We know that $w_p = -1$ because $p \equiv 1 \pmod{\ell}$ implies that E_0 has split multiplicative reduction at p. By [LO, Theorem 3], W_p acts on μ_ℓ by multiplication by -1, and W_q acts trivially on μ_ℓ for primes $q \neq p$ and $q \mid N$. This implies that $w_p = -1$ and $w_q = 1$ for primes $q \neq p$ and $q \mid N$. ∎

Proof of Theorem 1.1. The $\mathbb{Q}$-isogeny class of $X_0(11)$ consists of three elliptic curves '11a1' $= X_0(11)$, '11a2' $= X_0(11)/(\mathbb{Z}/5\mathbb{Z})$ and '11a3' $= X_0(11)/\mu_5 = X_1(11)$ (cf. Cremona's database). So we have rational étale isogenies

$$\text{`11a3'} \to \text{`11a1'} \to \text{`11a2'}.$$

Hence $X_0(11)$- and $X_1(11)$-optimal curves differ by a 5-isogeny.

Now, let $\mathcal{C}$ be an isogeny class of elliptic curves over $\mathbb{Q}$ with a square-free conductor N which is not divisible by 5. Suppose that E_0 and E_1 differ by a 5-isogeny. (We can show that E_0 and E_1 cannot differ by an isogeny of degree $5n$, $n > 1$.) Then by Vatsal's theorem (Theorem 2.1), there is an étale rational 5-isogeny $E_1 \to E_0$. So E_1 contains a rational point of order 5. By Dummigan's theorem (Theorem 2.2), E_0 also contains a rational point of order 5, and by taking the quotient by the subgroup it generates, we can find another curve $E' \in \mathcal{C}$. We know that E' has no rational 5-torsion points (cf. [Ke]). So we have the following diagram of curves with étale 5-isogenies:

$$E_1 \to E_0 \to E'.$$

Since the dual isogeny of $E_1 \to E_0$ is not étale, the kernel of the dual isogeny equals $\mu_5 \subset E_0[5]$.

Suppose that E_1 has Weierstrass model given by

$$y^2 + (v-u)xy - uv^2y = x^3 - uvx^2,$$

where $u, v \in \mathbb{Z}$ with $(u,v) = 1$. Since $w_p = -1$ for each prime p dividing uv, we must conclude that uv is divisible by *at most* one prime p, by Proposition 4.1. Suppose that $uv = \pm 1$. Invoking Hadano's considerations, our sequence of curves with étale isogenies $E_1 \to E_0 \to E'$ corresponds to finding a rational solution $(s,t) \in \mathbb{Q} \times \mathbb{Q}$ of equation (9) with the additional condition $s = v/u = \pm 1$. Since the polynomial equation $t^4 + 5t^2 + 5$ does not admit rational solutions, we must have $t = 1$ and this solution gives $E_0 = X_0(11)$ and $E_1 = X_1(11)$.

Now, it remains to deal with the case $uv = \pm p$ for some prime p. Hadano's Diophantine equation (9) in this case has the form

$$p^2 \pm p(t^4 + 5t^2 + 5)t = 1. \tag{10}$$

Changing this equation into a homogeneous form and viewing it modulo p, we easily deduce that it does not admit a rational solution in $t \in \mathbb{Q}$. This proves Theorem 1.1. ∎

REMARK. In the proof of (ii) of Theorem 1.1 in [BY2], to show that if E_0 and E_1 differ by a 3-isogeny, there is only one prime $p \mid N$ such that $w_p = -1$, we used the commutative diagram (see [BY2, (2), p. 225])

$$\begin{tikzcd} E(\mathbb{Q})_{\mathrm{tors}} \arrow[r, "\lambda"] \arrow[d, "\hat{\psi}"] & E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p) \arrow[d, "\hat{\psi}'"] \\ J_0(N)(\mathbb{Q})_{\mathrm{tors}} \arrow[r, "\lambda'"] & \Phi_{N,p} \end{tikzcd}$$

and injectivity of $\hat{\psi}'$. But we realize that $\hat{\psi}'$ is not generally injective, though $\hat{\psi}$ is. For example, consider the curve '155a1' in Cremona's database. When $N = 155 = 5 \cdot 31$ and $p = 5$, the component group $\Phi_{155,5}$ has order $3 \cdot 2^5$, which is easily obtained from Table 2 of the appendix in [Ma]. Meanwhile the Tamagawa number of '155a1' at $p = 5$ is 5, which shows that $\hat{\psi}'$ cannot be injective. However, using Proposition 4.1 and the fact that $\mu_3 \subset E_0$, we can show that there is only one prime $p \mid N$ such that $w_p = -1$.

Acknowledgments. The first author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2007694). The second author was supported by Global Ph.D Fellowship Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (grant number 2011-0007588).

References

[AL] A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(N)$*, Math. Ann. 185 (1970), 135–160.

[BY1] D. Byeon and D. Yhee, *Rational torsion on optimal curves and rank-one quadratic twists*, J. Number Theory 131 (2011), 552–560.

[BY2] D. Byeon and D. Yhee, *Optimal curves differing by a 3-isogeny*, Acta Arith. 158 (2013), 219–227.

[Cr] J. E. Cremona, *Elliptic curve data*, http://homepages.warwick.ac.uk/~masgaj/ftp/data/.

[Du] N. Dummigan, *Rational torsion on optimal curves*, Int. J. Number Theory 1 (2005), 513–531.

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

[Ke] M. Kenku, *On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class*, J. Number Theory 15 (1982), 199–202.

[LO] S. Ling and J. Oesterlé, *The Shimura subgroup of $J_0(N)$*, Astérisque 196-197 (1991), 171–203.

[Ma] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1978), 33–186.

[RS] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representaion*, in: Elliptic Curves, Modular Forms, and Fermat's Last Theorem, Int. Press, Cambridge, MA, 1995, 148–161.

[St] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. 98 (1989), 75–106.

[SW] W. Stein and M. Watkins, *A database of elliptic curves—first report*, in: Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002, 267–275.

[Va] V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves*, J. Inst. Math. Jussieu 4 (2005), 281–316.

Dongho Byeon, Taekyung Kim
Department of Mathematics
Seoul National University
Seoul, Korea
E-mail: dhbyeon@snu.ac.kr
taekyung@snu.ac.kr

Received on 27.9.2013
and in revised form on 1.7.2014 (7599)