ACTA ARITHMETICA
158.3 (2013)

Optimal curves differing by a 3-isogeny

by

DONGHO BYEON and DONGGEON YHEE (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 examples where they differ. For example, $E_0 = X_0(11)$ and $E_1 = X_1(11)$ differ by a 5-isogeny. Stein and Watkins [SW] have made a precise conjecture about when E_0 and E_1 differ by a 2-isogeny or a 3-isogeny, based on numerical observations. For the 3-isogeny case, the conjecture is 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 the following statements are equivalent:*

(A) *There is an elliptic curve $E \in \mathcal{C}$ given by $E : y^2 + axy + y = x^3$ with discriminant $a^3 - 27 = (a-3)(a^2+3a+9)$, where a is an integer such that no prime factors of $a-3$ are congruent to 1 modulo 6 and a^2+3a+9 is a power of a prime number.*

(B) *E_0 and E_1 differ by a 3-isogeny.*

REMARK. This conjecture has to be modified because (B) does not imply (A) in general. For example, let $\mathcal{C}$ be the isogeny class consisting of the two elliptic curves $396C1$ and $396C2$ in Cremona's table. Then $E_0 = 396C1$ and $E_1 = 396C2$ differ by a 3-isogeny, but (A) is not true in this case.

In this paper, we prove the following theorem.

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

DOI: 10.4064/aa158-3-2

Theorem 1.1. *Let* (A) *and* (B) *be as in the Conjecture.*

(i) (A) *implies* (B).
(ii) *If* N *is square-free and* $3 \nmid N$, *then* (B) *implies* (A).

2. Preliminaries

2.1. For $i = 0, 1$, let E_i be the $X_i(N)$-optimal curve of an isogeny class $\mathcal{C}$ of elliptic curves of conductor N. Stein and Watkins [SW] conjectured that E_0 and E_1 differ by a 3-isogeny if and only if there is an elliptic curve $E \in \mathcal{C}$ parametrised by

$$c_4 = (n+3)(n^3 + 9n^2 + 27n + 3)$$

and

$$c_6 = -(n^6 + 18n^5 + 135n^4 + 504n^3 + 891n^2 + 486n - 27)$$

with the discriminant being $n(n^2+9n+27)$, where n is an integer such that no prime factors of n are congruent to 1 modulo 6 and $n^2 + 9n + 27$ is a power of a prime number.

Let E be an elliptic curve defined over $\mathbb{Q}$ with a rational torsion point of order 3. As a minimal model for E, we can take

$$E : y^2 + axy + by = x^3 \tag{1}$$

with $a, b \in \mathbb{Z}$, $b > 0$ such that neither $q \mid a$ nor $q^3 \mid b$ for any prime number q. The discriminant of E is

$$\Delta = b^3(a^3 - 27b)$$

and $T = \{(0,0), (0,-b), \infty\}$ is the torsion group of order 3. If we take $b = 1$ and put $n = a - 3$ in (1), then we obtain the curve in (A) of the Conjecture.

There is an isogeny defined over $\mathbb{Q}$ of degree 3 from E to the quotient curve E' of E by T and the curve E' is given by a model

$$E' : y^2 + axy + by = x^3 - 5abx - a^3b - 7b^2$$

with discriminant

$$\Delta' = b(a^3 - 27b)^3.$$

Hadano [Ha] obtained the following theorem.

Theorem 2.1 (Hadano). *The quotient curve* E' *of an elliptic curve* $E : y^2+axy+by = x^3$ *by* $T = \{(0,0), (0,-b), \infty\}$ *has a rational point of order* 3 *if and only if* b *is a cubic number* t^3 *with* $t > 0$. *Moreover the curve* E' *is given by*

$$E' : y^2 + (a+6t)xy + (a^2 + 3at + 9t^2)ty = x^3.$$

2.2. Let $\mathcal{C}$ be an isogeny class of elliptic curves defined over $\mathbb{Q}$. For any $E \in \mathcal{C}$, we 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 extension $E_{\mathbb{Z}} \to E'_{\mathbb{Z}}$ to Néron models is étale. Equivalently, π is étale if $\ker \pi$ is an étale group scheme. So one can show that an isogeny $\pi : E \to E'$ is étale when $\ker \pi \simeq \mathbb{Z}/l\mathbb{Z}$ and E has good reduction at l for an odd prime l. If $\pi : E \to E'$ is an isogeny over $\mathbb{Q}$, then $\pi^*(\omega_{E'}) = n\omega_E$ for some nonzero integer n. The isogeny π is étale if and only if $n = \pm 1$.

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

2.3. As representatives of the cusps of $X_0(N)$, we use the rational numbers x/d where $d \mid N$, $d > 0$ and $(x, d) = 1$ with x taken modulo $(d, N/d)$. We say that such a cusp x/d is of *level* d, and we know that the cusp is defined over $\mathbb{Q}(\zeta_m)$, where $m = (d, N/d)$. Let (P_d) denote the divisor on $X_0(N)$ defined as the sum of all the cusps of level d (each with multiplicity one). Then (P_d) is invariant under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and the $\mathbb{Q}$-rational cuspidal subgroup $C(N)$ of $J_0(N)$ is generated by the divisor classes of all divisors of the kind

$$\phi((d, N/d))(P_1) - (P_d),$$

as d runs through the positive divisors of N.

Let f be the newform associated with the elliptic curve E of conductor N, and for each positive $d \mid N$, let $w_d = \pm 1$ be such that $W_d f = w_d f$, where W_d is the Atkin–Lehner involution. Let G be the product of those primes such that $w_p = 1$. Define a divisor Q supported on the cusps of $X_0(N)$ by

$$Q := \sum_{d \mid (N/G)} w_d (P_{dG}).$$

Let $r = \prod_{p \mid G}(p^2 - 1) \prod_{p \mid (N/G)}(p - 1)$, $h = (r, 24)$, and $n = r/h$.

Dummigan [Du] proved the following theorem under an additional condition, and later Byeon and Yhee [BY] proved it unconditionally.

THEOREM 2.3 (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 P of order l. Furthermore the image of P*

under the injective map from E_0 *to* $J_0(N)$ *induced by a parametrization* $\phi_0 : X_0(N) \to E_0$ *is* $(2n/l)[Q]$.

REMARK. Vatsal [Va] also proved that if there is an elliptic curve $E \in \mathcal{C}$ of conductor N defined over $\mathbb{Q}$ with a rational point of order l such that $l^2 \nmid N$, then $E_0 \in \mathcal{C}$ has a rational point P of order l, without explicit description of the point P.

2.4. For a prime p, $X_0(N)$ and its Jacobian $J_0(N)$ are also defined over $\mathbb{Q}_p$. When $p \nmid N$, $J_0(N)$ has good reduction modulo p. When $p \mid N$, the special fibre $J_0(N)_{\mathbb{F}_p}$ in the Néron model $J_0(N)$ over $\mathbb{Z}_p$ is the extension of a finite étale group scheme $\Phi_{N,p}$ by the connected component of identity $J_0(N)^0_{\mathbb{F}_p}$. The finite group $\Phi_{N,p}$ is called the *group of components* of the special fibre of the Néron model $J_0(N)$ over $\mathbb{Z}_p$.

Let $M \geq 1$ be a positive integer and let $p \geq 5$ be a prime such that $p \nmid M$. Consider the modular curve $X_0(Mp)$ over $\mathbb{Q}_p$. The model of the reduction modulo p of $X_0(Mp)$ consists of two irreducible components C_0 and C_1, each a copy of the modular curve $X_0(N)_{\mathbb{F}_p}$, glued together at the supersingular points. For each supersingular point x, let $e(x) = \frac{1}{2}|\mathrm{Aut}(x)|$. A regular minimal model of $X_0(Mp)$ may be obtained by replacing each supersingular point x with $e(x) > 1$ by a chain of $e(x) - 1$ copies of the projective line $\mathbb{P}^1$. Label these additional components by $C_2, \ldots, C_n$. For cusps of $X_0(Mp)$, we have $P_d \in C_0$ and $P_{dp} \in C_1$, where $d \mid M$.

Let $L = \bigoplus_{i=0}^n \mathbb{Z}[C_i]$ be the free abelian group generated by these components. Let $\iota : L \to L$ be the map defined by $\iota([C_i]) = \sum_{j=0}^n (C_i \cdot C_j)[C_j]$. Let $\deg : L \to \mathbb{Z}$ be the degree map. Then $\Phi_{Mp,p} = \ker(\deg)/\mathrm{im}(\iota)$. The component group $\Phi_{Mp,p}$ contains a canonical cyclic subgroup generated by the image $(0) - (\infty)$ in $\Phi_{Mp,p}$ of $C_0 - C_1 \in L$. The order of $(0) - (\infty)$ in $\Phi_{Mp,p}$ is precisely computed in [Ed], [Ma, Appendix].

THEOREM 2.4 (Mazur and Rapoport). *Let* $N = Mp = q_1 \cdots q_s p$ *be a positive square-free integer, where* $p \geq 5$ *and* q_i *are different prime integers. Then the order of* $(0) - (\infty)$ *in* $\Phi_{Mp,p}$ *is*

$$\frac{p-1}{\alpha} \prod_{i=1}^{s} (q_i + 1),$$

where $\alpha = 2, 4, 6,$ *or* 12.

3. Proof of Theorem 1.1

LEMMA 3.1. *Let* $E : y^2 + axy + by = x^3$ *be an elliptic curve, where* a, b *are integers such that* $(a, b) = 1$. *Let* $p \nmid 3$ *be a prime number such that* $p \mid \Delta = b^3(a^3 - 27b)$.

(i) *If* $p \mid b$, *then* $w_p = -1$.
(ii) *If* $p \mid a^3 - 27b$ *and* $p \equiv 1 \pmod 3$, *then* $w_p = -1$.
(iii) *If* $p \mid a^3 - 27b$ *and* $p \equiv -1 \pmod 3$, *then* $w_p = 1$.

Proof. Since $c_4 := a(a^3 - 24b)$, E has multiplicative reduction at p for every prime factor $p \neq 3$ of Δ. For every prime factor p of b, E has a split multiplicative reduction at p, so $w_p = -1$. For every prime factor $p \equiv -1 \pmod 3$ of $a^3 - 27b$, E has a nonsplit multiplicative reduction at p, so $w_p = 1$, and for every prime factor $p \equiv 1 \pmod 3$ of $a^3 - 27b$, E has a split multiplicative reduction at p, so $w_p = -1$ because the slopes of the tangent lines at the node $(-a^2/9, a^3/27) \in E(\mathbb{F}_p)$ are $(-3a \pm a\sqrt{-3})/6$ when $p \neq 2$. Similarly we can show that $w_2 = 1$ if $2 \mid a^3 - 27b$. ∎

Lemma 3.2. *If* $E : y^2 + axy + y = x^3$ *is an elliptic curve with discriminant* $a^3 - 27 = (a-3)(a^2+3a+9)$, *where a is an integer such that no prime factors of $a - 3$ are congruent to 1 modulo 6 and $a^2 + 3a + 9$ is a power of a prime number, then the conductor N of E is a square-free integer such that $3 \nmid N$ except $a = -6, -3, 0$ and there is only one prime divisor p of N such that $w_p = -1$.*

Proof. Suppose that E is as in the statement and $a^2 + 3a + 9$ is a power of a prime number p.

If $3 \mid a$, then $a^2 + 3a + 9$ must be a power of 3. So $a = -6, -3, 0$ and we have the following table:

a	E	N	w_p
-6	$27A4$	$27 = 3^3$	$w_3 = -1$
-3	$54A3$	$54 = 2 \cdot 3^3$	$w_2 = 1,\ w_3 = -1$
0	$27A3$	$27 = 3^3$	$w_3 = -1$

where $27A4$, $54A3$, $27A3$ are in Cremona's table.

If $3 \nmid a$, then $3 \nmid a^3 - 27$ and for any prime divisor of N, E has multiplicative reduction. So the conductor N of E is a square-free integer such that $3 \nmid N$. Suppose that $a^2 + 3a + 9 = p^k$. Then k is odd unless $a = 5$, $p = 7$ and $a = -8$, $p = 7$. So $p \equiv 1 \pmod 3$. By Lemma 3.1, $w_p = -1$ and $w_q = 1$ for every $q \mid a - 3$. ∎

Now we can prove Theorem 1.1.

Proof of Theorem 1.1. (i) First we assume that $a \neq -6, -3, 0$. Let $E \in \mathcal{C}$ be an elliptic curve given by

$$E : y^2 + axy + y = x^3$$

with discriminant $\Delta = a^3 - 27 = (a-3)(a^2+3a+9)$, where a is an integer such that no prime factors of $a - 3$ are congruent to 1 modulo 6 and

$a^2+3a+9=p^r$ is a power of a prime integer p. Let $T=\{(0,0),(0,-1),\infty\}$ be the torsion group of order 3 in $E(\mathbb{Q})$.

By Theorem 2.1, the quotient curve E' of E by T has a rational point of order 3 and the equation of E' is

$$E' : y^2+(a+6)xy+(a^2+3a+9)y=x^3.$$

The discriminant of Δ' of E' is $\Delta'=(a^3-27)^3$, and $T'=\{(0,0),(0,-(a^2+3a+9),\infty\}$ is the torsion group of order 3 in $E'(\mathbb{Q})$. Since E' also has a rational point of order 3, we have the following étale 3-isogenies of elliptic curves:

$$E\to E'\to E''.$$

Since $(a+6)^3-(a-3)^3=3^3(a^2+3a+9)$, a^2+3a+9 cannot be a cube, by the case $n=3$ of Fermat's Last Theorem. So E'' has no rational points of order 3. Since $4x^3+a^2x+2ax+1=0$ has no rational solutions, E has no rational points of order 2 by the duplication formula.

Let $C(E)$ denote the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in the isogeny class $\mathcal{C}$ of E. For a prime p, let $C_p(E)$ be the number of $\mathbb{Q}$-isomorphism classes of elliptic curves p-power isogenous to E. Then we have the product formula

$$C(E)=\prod_p C_p(E).$$

Kenku [Ke] proved that $Y_0(N)(\mathbb{Q})=\mathbb{H}/\Gamma_0(N)(\mathbb{Q})$ is empty except for $N\le 10$, and $N=11$, 12, 13, 14, 15, 16, 17, 18, 19, 21, 25, 27, 37, 43, 67, and 163. This result implies that $C_3(E)\le 4$. (For details, see the table in the proof of Theorem 2 in [Ke].) If there is an étale 3-isogeny $E'''\to E$ with $E''' : y^2+Axy+B^3y=x^3$, then the discriminant $\Delta=a^3-3^3$ of E should be equal to $u^{-12}B^3(A^3-27B^3)^3$ for some $u\in\mathbb{Z}_{>0}$, which is impossible because $a\ne 0$. Since E'' has no rational points of order 3, we have $C_3(E)=3$. So Kenku's result above implies that $C_2(E)\le 2$ and $C_p(E)=1$ for any prime $p\ne 2,3$, because 9, 18 and 27 are the only multiples of 9 on Kenku's list. Since E has no rational points of order 2, there is no 2-isogenous curve of E and we have $C_2(E)=1$. By the above product formula we have $C(E)=3$. So the isogeny class $\mathcal{C}$ of E is

$$E\xrightarrow{3}E'\xrightarrow{3}E'',$$

where each arrow denotes an étale 3-isogeny. Thus E is $E_{\min}$ in $\mathcal{C}$.

By Theorem 2.2, E is E_1 in $\mathcal{C}$. By Theorem 2.3, E'' cannot be E_0 in $\mathcal{C}$. To prove (i), it is enough to show that E cannot be E_0 in $\mathcal{C}$. Suppose it is. Let $\phi : X_0(N)\to E$ be the modular parametrization and $\psi : J_0(N)\to E$ be the induced homomorphism. Then the dual $\hat{\psi} : E\to J_0(N)$ is injective. Let $E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$, where $E^0(\mathbb{Q}_p)$ is the subgroup of points which have nonsingular reduction modulo p, and $\Phi_{N,p}$ be the component groups of E and $J_0(N)$ respectively. Let $\lambda : E(\mathbb{Q}) \to E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)$ and $\lambda' : J_0(N)(\mathbb{Q}) \to \Phi_{N,p}$ be their canonical reduction maps. Then we have the following commutative diagram:

$$\begin{tikzcd} E(\mathbb{Q})_{\mathrm{tors}} \arrow[r, "\lambda"] \arrow[d, "\hat{\psi}"] & E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p) \arrow[d, "\hat{\psi}'"] \\ J_0(N)(\mathbb{Q})_{\mathrm{tors}} \arrow[r, "\lambda'"] & \Phi_{N,p} \end{tikzcd} \tag{2}$$

where $\hat{\psi}'$ is the injective homomorphism induced by $\hat{\psi}$.

By Lemma 3.2, the conductor N of E is a square-free integer such that $3 \nmid N$ and there is only one prime divisor p of N such that $w_p = -1$. Write $N = Mp$, where $M = q_1 \cdots q_s$ and q_i are different primes. Then $q_i \mid a - 3$ and $q_i \equiv 2 \pmod 3$ for all $i = 1, \ldots, s$.

By Theorem 2.3, if E is E_0 in $\mathcal{C}$, then E has a point P of order 3 such that

$$\hat{\psi}(P) = \frac{2(p-1)}{3h} \prod_{i=1}^{s} (q_i^2 - 1)[(P_M) - (P_N)]$$

in $J_0(N)$, where $h = (r, 24)$ and $r = (p-1)\prod_{i=1}^{s}(q_i^2 - 1)(p-1)$. We note that $3 \mid h$. Since $P_M \in C_0$ and $P_N \in C_1$, $\lambda'((P_M) - (P_N)) = (0) - (\infty)$.

Theorem 2.4 and $3 \nmid \prod_{i=1}^{s}(q_i - 1)$ imply that

$$\lambda'(\hat{\psi}(P)) = \frac{2(p-1)}{3h} \prod_{i=1}^{s}(q_i + 1) \prod_{i=1}^{s}(q_i - 1)[(0) - (\infty)]$$

is not trivial in $\Phi_{N,p}$. So $P \in E$ has singular reduction modulo p. But the points $(0,0)$ and $(0,-1)$ in E have nonsingular reduction modulo p. Thus E cannot be E_0 in $\mathcal{C}$.

Finally we assume that $a = -6, -3$, or 0. If $a = -6$ ($E = 27A4$) or $a = 0$ ($E = 27A3$), then $E_0 = 27A1$ and $E_1 = 27A3$ differ by a 3-isogeny in the isogeny class $\mathcal{C}$ of E by [St, §7. Numerical evidence]. If $a = -3$ ($E = 54A3$), then $E_0 = 54A1$ and $E_1 = 54A3$ differ by a 3-isogeny in the isogeny class $\mathcal{C}$ of E by Cremona's table. So we complete the proof of (i).

(ii) Suppose that E_0 and E_1 differ by a 3-isogeny and the conductor N of these curves is a square-free integer such that $3 \nmid N$. By Theorem 2.2, there is an étale 3-isogeny from E_1 to E_0. So E_1 has a rational point of order 3, and as a minimal model for E_1 we can take

$$E_1 : y^2 + axy + by = x^3$$

with $a, b \in \mathbb{Z}$, $b > 0$. The discriminant of E_1 is

$$\Delta_1 = b^3(a^3 - 27b)$$

and $T_1 = \{(0,0), (0,-b), \infty\}$ is the torsion group of order 3 in $E_1(\mathbb{Q})$.

By Theorem 2.3, E_0 also has a rational point of order 3. By Theorem 2.1, b is a cubic number t^3 with $t > 0$ and E_0 is given by

$$E_0 : y^2 + (a + 6t)xy + (a^2 + 3at + 9t^2)ty = x^3.$$

The discriminant of E_0 is

$$\Delta_0 = (a^2 + 3at + 9t^2)^3((a + 6t)^3 - 27(a^2 + 3at + 9t^2)t) = t^3(a^3 - 27t^3)^3$$

and $T_0 = \{(0,0), (0, -(a^2 + 3at + 9t^2)t), \infty\}$ is the torsion group of order 3 in $E_0(\mathbb{Q})$.

Consider again the commutative diagram (2). Let $P = (0,0)$ or $(0, -(a^2 + 3at + 9t^2)t)$ be the point of order 3 in E_0 and p be a prime divisor of $a^2+3at+9t^2$. Write $N = Mp_1 \cdots p_u p$ so that $w_q = 1$ for every prime divisor $q \mid M$, and $w_{p_i} = -1$ for every prime number p_i. We note that $w_p = -1$. By Theorem 2.3,

$$\begin{aligned}\hat{\psi}(P) &= \frac{2n}{3} \sum_{d|(N/M)} w_d(P_{dM}) \\ &= \frac{2n}{3} \sum_{p_{i_1} \cdots p_{i_v} |(N/Mp)} (-1)^v [(P_{p_{i_1} \cdots p_{i_v} M}) - (P_{pp_{i_1} \cdots p_{i_v} M})],\end{aligned}$$

where the number of summands is 2^u and if $u \ge 1$, we have $(-1)^v = 1$ for half of them, and $(-1)^v = -1$ for the other half. Since $P_{p_{i_1} \cdots p_{i_v} M} \in C_0$ and $P_{pp_{i_1} \cdots p_{i_v} M} \in C_1$ for any $p_{i_1} \cdots p_{i_v}$, we have

$$\lambda'((P_{p_{i_1} \cdots p_{i_v} M}) - (P_{pp_{i_1} \cdots p_{i_v} M})) = (0) - (\infty)$$

for any $p_{i_1} \cdots p_{i_v}$. Thus $\lambda'(\hat{\psi}(P))$ is trivial in $\Phi_{N,p}$ if $u \ge 1$. Since the point P in E_0 has singular reduction modulo p, $\lambda'(\hat{\psi}(P))$ is nontrivial in $\Phi_{N,p}$. So p is the only prime such that $w_p = -1$.

By Lemma 3.1, the elliptic curve E_1 in $\mathcal{C}$ is $E_1 : y^2 + axy + y = x^3$ with discriminant $a^3 - 27 = (a-3)(a^2 + 3a + 9)$, where a is an integer such that no prime factors of $a - 3$ are congruent to 1 modulo 6 and $a^2 + 3a + 9$ is a power of p. This completes the proof of (ii). ■

Example. Consider the elliptic curve $E : y^2 - 20xy + y^2 = x^3$ (8027a3 in Cremona's table) of conductor $8027 = 23 \cdot 349$ and the quotient curve E' : $y^2 - 14xy + 349y = x^3$ (8027a1 in Cremona's table) by $T = \{(0,0), (0,-1), \infty\}$. By Theorem 1.1 and its proof, we know that $E_0 = E'$, $E_1 = E$ and they differ by a 3-isogeny. Watkins [Wa] checked this example in another way.

Acknowledgements. The authors would like to thank the referee for his careful reading of the manuscript and for many valuable suggestions.

This work was supported by the Korea Research Foundation (KRF) grant funded by the Korea government (MEST) (No. 2010-0026473).

References

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

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

[Ed] B. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein"*, Astérisque 196–197 (1991), 159–170.

[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.

[Ma] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. 47 (1978), 33–186.

[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 subgroup of $J_0(N)$ and applications to elliptic curves*, J. Inst. Math. Jussieu 4 (2005), 281–316.

[Wa] M. Watkins, *Computing the modular degree of an elliptic curve*, Experiment. Math. 11 (2002), 487–502.

Dongho Byeon, Donggeon Yhee
Department of Mathematics
Seoul National University
Seoul, Korea
E-mail: dhbyeon@snu.ac.kr
dgyhee@gmail.com

Received on 15.2.2012
and in revised form on 27.8.2012 (6977)