ACTA ARITHMETICA
XCIV.2 (2000)

θ-congruent numbers and elliptic curves

by

Makiko Kan (Tokyo)

1. Introduction. A natural number is called a *congruent number* if it is the area of a right triangle with rational sides. It is well known that a natural number is congruent if and only if the corresponding elliptic curve has infinitely many rational points. There have been several interesting and remarkable results about congruent numbers. For example, all natural numbers that are $\equiv 5, 6$ or $7 \pmod 8$ are congruent provided that the weak Birch–Swinnerton-Dyer conjecture holds true.

In [6] Fujiwara extended the concept of congruent numbers by considering general (not necessarily right) triangles with rational sides. Let θ be a real number with $0 < \theta < \pi$. In what follows, we call a triangle with rational sides and an angle θ a *rational θ-triangle.* We note here that, for such a triangle, $\cos\theta$ is necessarily rational. A rational $\cos\theta$ can be written as $\cos\theta = s/r,\ r, s \in \mathbb{Z}$, $\gcd(r, s) = 1$, $r > 0$. We denote $\sqrt{r^2 - s^2}$ by α_θ, which is a rational or a quadratic real uniquely determined by θ.

θ-congruent numbers are defined as follows. Throughout our paper, θ is always assumed to be $0 < \theta < \pi$ and $\cos\theta \in \mathbb{Q}$.

Definition. A natural number n is *θ-congruent* if $n\alpha_\theta$ is the area of a rational θ-triangle.

θ-congruent numbers for $\theta = \pi/2$ are nothing but ordinary congruent numbers, since $\alpha_{\pi/2} = 1$. Let $E_{n,\theta}$ be an elliptic curve defined by $y^2 = x(x + (r + s)n)(x - (r - s)n)$, where r and s are determined by θ as above.

Theorem (Fujiwara, [6]). *Let n be any natural number. Then*

(1) *n is θ-congruent if and only if $E_{n,\theta}$ has a rational point of order greater than* 2.

(2) *For $n \neq 1, 2, 3, 6$, n is θ-congruent if and only if $E_{n,\theta}$ has a positive $\mathbb{Q}$-rank.*

2000 *Mathematics Subject Classification*: 11G05, 11G18.

From this theorem, rational points on $E_{n,\theta}$ give us important information on θ-congruent numbers. In this vein, primes $\equiv 5,7,19 \pmod{24}$ are shown to be not $\pi/3$-congruent (Fujiwara, [6]). Our main results are the following.

LEMMA. *A square-free natural number n is θ-congruent if and only if n is the square-free part of $pq(p+q)(2rq+p(r-s))$, where p,q are natural numbers with* $\gcd(p,q)=1$.

REMARK. Fujiwara [6] showed that the following result (Thm. 2.1 of [9]) on $\pi/2$-congruent numbers can be easily derived from the above lemma: the numbers $\frac{1}{2}m_1m_2(m_1^2+m_2^2)$ for integers $m_1m_2>1$, $\gcd(m_1,m_2)=1$ are $\pi/2$-congruent. Using the above lemma, he also showed in [6] that, for any θ, there are infinitely many θ-congruent numbers in each residue class modulo 8, which is a generalization of a result in Theorem 3 of [3].

THEOREM. *Suppose that p is a prime. Then p is not $2\pi/3$-congruent if $p \equiv 7,11,13 \pmod{24}$ and is $2\pi/3$-congruent if $p\equiv 23 \pmod{24}$.*

So far as sufficient conditions for congruence are concerned, it has been proved, by analytic methods, that primes $n \equiv 5,6,7 \pmod 8$ are $\pi/2$-congruent ([1, 2, 6]). $\pi/2$-congruent numbers are relatively easier to handle since $E_{n,\pi/2}$ has complex multiplication, whereas $E_{n,\pi/3}$ and $E_{n,2\pi/3}$ do not. However, for $\theta=\pi/3$ or $2\pi/3$, we can make a reasonable conjecture based on existing conjectures and computer calculation. For instance, Cassels proved that $\dim_2 Ш(E/\mathbb{Q})[2]$ is even for any elliptic curve $E/\mathbb{Q}$ provided that the 2-primary part of $Ш(E/\mathbb{Q})$ is finite. Since $Ш(E/\mathbb{Q})$ is conjectured to be finite, the proposition of Section 2, the Birch–Swinnerton-Dyer conjecture and computer calculation lead us to the following conjecture.

CONJECTURE. *Let p be a prime number greater than 3. If $p \equiv 11, 13, 17, 23 \pmod{24}$, then p is $\pi/3$-congruent. If $p\equiv 5,17,19,23 \pmod{24}$, then p is $2\pi/3$-congruent.*

The second part of our theorem constitutes a partial answer to the above conjecture.

2. Proofs of the Lemma and of the first part of the Theorem

Proof of the Lemma. Consider the isogenous elliptic curve $E^*_{n,\theta} : ny^2 = x(x+1)(2rx+r-s)$ of $E_{n,\theta}$ given by the $\mathbb{Q}$-isomorphism

$$(x,y) \mapsto \left(\frac{x-(r-s)n}{2rn}, \frac{y}{2rn^2}\right).$$

By Fujiwara's theorem n is θ-congruent if and only if $E^*_{n,\theta}$ has a rational point (x,y) of order greater than 2, for which we can assume $x>0$. (If not, add 2-torsion point $(-1,0)$.) Put $x=p/q$ with $p,q\in\mathbb{N}$, $\gcd(p,q)=1$. Then it is easily checked that $n \equiv pq(p+q)(2rq+p(r-s)) \pmod{\mathbb{Q}^{*2}}$. ■

Examples. (1) Taking $p = 1$, $q = 1$ and $\theta = \pi/2$, we obtain a $\pi/2$-congruent number 6. In fact, 6 is the area of a right triangle with sides $3, 4$ and 5.

(2) Put $p = 61991193600 = 2^{10} \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 17^2 \cdot 19$, $q = 18357811081 = 157^2 \cdot 863^2$ and $\theta = 2\pi/3$. Then 19 is $2\pi/3$-congruent by the Lemma. In fact, $19\sqrt{3}$ is the area of a $2\pi/3$-triangle with sides $544/105$, $1995/136$ and $254659/14280$.

Here we restrict our attention to special cases $\theta = \pi/3$ and $2\pi/3$, and will try to prove the first part of the main theorem. First we prove the next proposition.

Proposition. *Let p be a prime greater than 3 and $Ш(E/\mathbb{Q})$ be the Shafarevich–Tate group of E over $\mathbb{Q}$. Then*

$$\operatorname{rank} E_{p,\pi/3}(\mathbb{Q}) + \dim_2 Ш(E_{p,\pi/3}/\mathbb{Q})[2] = \begin{cases} 0 & \text{for } p \equiv 5, 7, 19 \pmod{24}, \\ 1 & \text{for } p \equiv 11, 13, 17, 23 \pmod{24}, \\ 2 & \text{for } p \equiv 1 \pmod{24}, \end{cases}$$

$$\operatorname{rank} E_{p,2\pi/3}(\mathbb{Q}) + \dim_2 Ш(E_{p,2\pi/3}/\mathbb{Q})[2] = \begin{cases} 0 & \text{for } p \equiv 7, 11 \pmod{24}, \\ 1 & \text{for } p \equiv 5, 17, 19, 23 \pmod{24}, \\ 2 & \text{for } p \equiv 1, 13 \pmod{24}, \end{cases}$$

where $Ш(E/\mathbb{Q})$ is the Shafarevich–Tate group of E over $\mathbb{Q}$. Furthermore the rank of $E_{p,2\pi/3}(\mathbb{Q})$ vanishes if p is congruent modulo 24 to 13.

Proof. First we notice the following: If $\theta = \pi/3$ or $2\pi/3$, then $E_{p,\theta}(\mathbb{Q})$ has $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as the torsion subgroup. This is immediately verified by the well known facts ([10], for instance Mazur's theorem (Thm. 7.5, p. 223)) and by the duplication formula.

Assume first that θ is $2\pi/3$. Let ϕ be the two-isogeny of $E_{p,2\pi/3}$ defined by

$$\phi((x, y)) = \left(\frac{y^2}{x^2}, \frac{-(x^2 + 3p^2)y}{x^2}\right),$$

and let $E'_{p,2\pi/3} : y^2 = x^3 + 4px^2 + 16p^2x$ be the isogenous elliptic curve given by ϕ. Then, by the well known fact (Prop. 4.9, p. 302, [10]), the ϕ-Selmer group over $\mathbb{Q}$ satisfies

$$S^{(\phi)}(E_{p,2\pi/3}/\mathbb{Q}) \cong \{d \in \{\pm1, \pm2, \pm3, \pm6, \pm p, \pm 2p, \pm 3p, \pm 6p\} : C_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \in \{\infty, 2, 3, p\}\},$$

where C_d is a curve given by $dw^2 = d^2 + 4pdz^2 + 16p^2z^4$. We now check the solubility of C_d in each local field and shall determine $S^{(\phi)}(E_{p,2\pi/3}/\mathbb{Q})$.

Suppose that d is negative and that $C_d(\mathbb{R}) \neq \emptyset$. Then the left hand side of C_d is negative, whereas the right hand side is not. It follows that C_d has no solution in $\mathbb{R}$. Suppose next that $d = 2k$ with $k = 1, 3, p, 3p$ and that $C_{2k}(\mathbb{Q}_2) \neq \emptyset$. Take the valuation v_2 at 2 of both sides. Then $v_2(\mathrm{LHS})$ is odd, while $v_2(\mathrm{RHS})$ is even, a contradiction. A similar argument tells us that C_3 and C_{3p} do not have $\mathbb{Q}_3$-solutions. We now investigate the last possible candidate $d = p$:

$$C_p : \quad w^2 = p + 4pz^2 + 16pz^4.$$

Suppose that $(w, z) \in C_p(\mathbb{Q}_p)$. If $v_p(w) \leq 0$, then $v_p(\mathrm{LHS}) = v_p(w^2)$ is even, while $v_p(\mathrm{RHS}) = v_p(16pz^4)$ is odd. Thus we can set $v_p(w) > 0$ and $v_p(z) \geq 0$. Replacing w by pw, we obtain $pw^2 = 1+4z^2+16z^4$, and $v_p(z) = 0$. Then $pw^2 = (1 + 2z^2)^2 + 12z^4$, and so p is congruent modulo 3 to 1.

Conversely, if p is congruent modulo 3 to 1, then the primitive third root z_0 of unity modulo p exists in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. In particular $z_0^4 + z_0^2 + 1 \equiv z_0 + z_0^2 + 1 \equiv 0 \pmod{p}$. Replacing z by $z/2$ in C_p yields $C_p : pw^2 = z^4 + z^2 + 1$. Hensel's lemma now assures a solution in $\mathbb{Q}_p$, since $\frac{d}{dz}(z^4 + z^2 + 1)\big|_{z=z_0} \not\equiv 0 \pmod{p}$. We thus conclude that C_p is soluble in $\mathbb{Q}_p$ if and only if p is congruent modulo 3 to 1.

Similarly $p \equiv 1 \pmod{3}$ suffices to yield a solution of C_p in the local field $\mathbb{Q}_3$, while $p \equiv 1, 3$, or $5 \pmod{8}$ suffices for $\mathbb{Q}_2$. To sum up all,

$$S^{(\phi)}(E_{p,2\pi/3}/\mathbb{Q}) = \begin{cases} \{1\} & \text{for } p \equiv 5, 7, 11, 17, 23 \pmod{24}, \\ \{1, p\} & \text{for } p \equiv 1, 13, 19 \pmod{24}. \end{cases}$$

We can show similarly

$$S^{(\widehat{\phi})}(E'_{p,2\pi/3}/\mathbb{Q}) = \begin{cases} \{1, -3, -p, 3p\} & \text{for } p \equiv 7, 11, 19 \pmod{24}, \\ \{\pm 1, \pm 3, \pm p, \pm 3p\} & \text{for } p \equiv 1, 5, 13, 17, 23 \pmod{24}. \end{cases}$$

By the next 3 exact sequences

$$0 \to E'_{p,2\pi/3}(\mathbb{Q})/\phi(E_{p,2\pi/3}(\mathbb{Q})) \to S^{(\phi)}(E_{p,2\pi/3}/\mathbb{Q}) \to \text{Ш}(E_{p,2\pi/3}/\mathbb{Q})[\phi] \to 0,$$

$$0 \to \frac{E'_{p,2\pi/3}(\mathbb{Q})[\widehat{\phi}]}{\phi(E_{p,2\pi/3}(\mathbb{Q})[2])} \to \frac{E'_{p,2\pi/3}(\mathbb{Q})}{\phi(E_{p,2\pi/3}(\mathbb{Q}))} \xrightarrow{\widehat{\phi}} \frac{E_{p,2\pi/3}(\mathbb{Q})}{2E_{p,2\pi/3}(\mathbb{Q})} \to \frac{E_{p,2\pi/3}(\mathbb{Q})}{\widehat{\phi}(E'_{p,2\pi/3}(\mathbb{Q}))} \to 0,$$

$$0 \to \text{Ш}(E_{p,2\pi/3}/\mathbb{Q})[\phi] \to \text{Ш}(E_{p,2\pi/3}/\mathbb{Q})[2] \to \text{Ш}(E_{p,2\pi/3}/\mathbb{Q})[\widehat{\phi}] \to 0,$$

we have

$$\operatorname{rank} E_{p,2\pi/3}(\mathbb{Q}) + \dim_2 \text{Ш}(E_{p,2\pi/3}/\mathbb{Q})[2] = \begin{cases} 0 & \text{for } p \equiv 7, 11 \pmod{24}, \\ 1 & \text{for } p \equiv 5, 17, 19, 23 \pmod{24}, \\ 2 & \text{for } p \equiv 1, 13 \pmod{24}. \end{cases}$$

A similar argument gives us the result for $\theta = \pi/3$ and we have

$$\operatorname{rank} E_{p,\pi/3}(\mathbb{Q}) + \dim_2 Ш(E_{p,\pi/3}/\mathbb{Q})[2] = \begin{cases} 0 & \text{for } p \equiv 5, 7, 19 \pmod{24}, \\ 1 & \text{for } p \equiv 11, 13, 17, 23 \pmod{24}, \\ 2 & \text{for } p \equiv 1 \pmod{24}. \end{cases}$$

Note that necessary information for $p \equiv 13 \pmod{24}$, $\theta = 2\pi/3$ is missing above. For this case, we need to replace x by $x - p$ in $E_{p,2\pi/3}$, and to check that $C_d(\mathbb{Q})$ and $C'_d(\mathbb{Q})$ are empty for $d = \pm1, \pm2, \pm3, \pm6, \pm p, \pm2p, \pm3p, \pm6p$, where $C_d : dw^2 = d^2 + 10pdz^2 + 9p^2z^4$, $C'_d : dw^2 = d^2 - 5pdz^2 + 4p^2z^4$.

Suppose that p is congruent modulo 24 to 13 and that C_p has a rational solution $(w, z) = (l/k, e/M) \in \mathbb{Q}^2$ where $l, k, e, M \in \mathbb{Z}\backslash\{0\}$, $\gcd(M, e) = \gcd(k, l) = 1$. Replacing lM^2/k by an integer N (k must divide M^2 here), we can reduce the problem to proving the non-existence of integral solutions (M, e, N) of $pN^2 = M^4 + 10M^2e^2 + 9e^4 = (M^2 + e^2)(M^2 + 9e^2)$ with $\gcd(M, e) = \gcd(N, e) = \gcd(M, N) = 1$. There are 4 cases to consider:

$$\text{(a)} \begin{cases} M^2 + e^2 = pS^2, \\ M^2 + 9e^2 = T^2, \end{cases} \qquad \text{(b)} \begin{cases} M^2 + e^2 = S^2, \\ M^2 + 9e^2 = pT^2, \end{cases}$$

$$\gcd(S, T) = 1, \ N = ST, \qquad \gcd(S, T) = 1, \ N = ST,$$

$$\text{(c)} \begin{cases} M^2 + e^2 = 2pS^2, \\ M^2 + 9e^2 = 2T^2, \end{cases} \qquad \text{(d)} \begin{cases} M^2 + e^2 = 2S^2, \\ M^2 + 9e^2 = 2pT^2, \end{cases}$$

$$\gcd(S, T) = 1, \ N = 2ST, \qquad \gcd(S, T) = 1, \ N = 2ST.$$

(c) is insoluble modulo 3. (a), (b) and (d) are also insoluble modulo 24. Therefore C_p has no rational solution.

Similarly we obtain $C_d(\mathbb{Q}) = \emptyset$ and $C'_d(\mathbb{Q}) = \emptyset$ for all $d = \pm1, \pm2, \pm3, \pm6, \pm p, \pm2p, \pm3p, \pm6p$. Thus the rank of $E_{p,2\pi/3}(\mathbb{Q})$ is zero when p is congruent modulo 24 to 13. This completes our proof. ■

The same argument tells us that the $\mathbb{Q}$-rank of $E_{n,\theta}$ is 0 when n is $1, 2$ or 3 and $\theta = \pi/3$ or $2\pi/3$. However 1 is $\pi/3$-congruent, as $E_{1,\pi/3}(\mathbb{Q})$ has a rational point of order 8.

From the proposition, we obtain the following corollary, first half of which was first proved in [6].

Corollary. *Let p be a prime. If $p \equiv 5, 7, 19 \pmod{24}$, then p is not $\pi/3$-congruent. If $p \equiv 7, 11, 13 \pmod{24}$, then p is not $2\pi/3$-congruent.*

3. Proof of the second part of the Theorem. In the last section we showed the first half of our main theorem. In this section, we prove the remaining part.

Remark. The *n-twist* of an elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$ is defined as $E^{(n)} : ny^2 = x^3 + ax^2 + bx + c$, which is isomorphic to E over $\mathbb{Q}(\sqrt{n})$. We usually identify all isomorphic elliptic curves over $\mathbb{Q}$. In our case, $E_{p,2\pi/3}$ is the $(-p)$-twist of $E_{1,\pi/3}$.

Let us quote a theorem of B. J. Birch [1], which deals with Heegner points, a special kind of non-trivial rational points.

Theorem (Birch, [1]). *Let p be a prime congruent modulo* 4 *to* 3 *and suppose that $p = 96T^2 - S^2$ is soluble with $T, S \in \mathbb{Z}$. Then, for almost all p, the $(-p)$-twist $E^{(-p)}$ of the elliptic curve $E : Y^2 = (X-1)(X^2-4)$ has a rational point of infinite order.*

Proof of the second part of the Theorem. Assume that p is a prime congruent modulo 24 to 23. Then p splits in $\mathbb{Q}(\sqrt{6})$ and there exist integers S and T satisfying $S^2 - 6T^2 = -p$. (Note that $\mathbb{Q}(\sqrt{6})$ is a PID.) If T were odd, $S^2 - 6T^2 \not\equiv -p \pmod 8$, and thus $S^2 - 24T^2 = -p$ is soluble in $\mathbb{Z}$. By multiplying the fundamental unit $5 + 2\sqrt{6}$ of $\mathbb{Q}(\sqrt{6})$, we can assume T to be even, again, without loss of generality. Therefore $S^2 - 96T^2 = -p$ is soluble in integers.

As we saw in the above remark, the elliptic curve E in Birch's theorem is isomorphic over $\mathbb{Q}$ to $E_{1,\pi/3}$ of which $E_{p,2\pi/3}$ is the $(-p)$-twist. We only have to check whether our p is one of the exceptional primes in Birch's theorem or not. According to [1], exceptional primes are related to a map π from a model $X_0(24)$ to Fricke's quartic curve C_{24} ([1, 4]). For more details, we now review Fricke's work and apply it to our situation.

Let $\Gamma_0(24)$ be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ as usual, $\mathfrak{H}$ be the upper half plane, $\mathfrak{H}^*$ be its completion, and $F_0(24)$ be the fundamental domain for $\Gamma_0(24)$ whose cusps are $0, 1/12, 1/8, 1/6, 1/4, 1/3, 1/2, \infty$ there. Furthermore let j be a modular invariant of $\mathrm{SL}_2(\mathbb{Z})$ and $j_{24}(z) = j(24z)$. The functions j and j_{24} are known to satisfy an algebraic identity $F_{24}(j, j_{24}) = 0$, and the curve $J_{24} : F_{24}(u, v) = 0$ is a model of $X_0(24) = \mathfrak{H}^*/\Gamma_0(24)$ ([1, 5]). $(j,\, j_{24})$ is actually a holomorphic map from $X_0(24)$ to J_{24} and can be recognized as a map from $F_0(24)$ to J_{24}.

Here we must note that J_{24} has a singularity on the quadratic surd z for which there exists an element $z' \in F_0(24)$ such that z and z' are not equivalent by $\Gamma_0(24)$, whereas $(j(z), j_{24}(z)) = (j(z'), j_{24}(z'))$. Namely,

$$\frac{24az + 24b}{cz + d} = \frac{24Az + B}{24Cz + D}$$

holds for some integers $a, b, c, d, A, B, C, D \in \mathbb{Z}$, $ad - bc = AD - BC = 1$, not only $a = A$, $24b = B$, $c = 24C$, $d = D$. This implies that the matrix

$$M = \begin{pmatrix} 24A & B \\ 24C & D \end{pmatrix}^{-1} \begin{pmatrix} 24a & 24b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Q})$$

is elliptic on $F_0(24)$. It is a well known fact that any elliptic element M has the property $|\operatorname{tr} M| < 2$, thus here, we can verify that the discriminant $\Delta(z)$ of z must satisfy $\Delta(z) + 2304 = 576|\operatorname{tr} M|^2$, therefore $-2304 \le \Delta(z) < 0$.

On the other hand, Fricke introduces two modular functions $\tau(z)$ and $\sigma(z)$ where $\tau(z) \in \mathbb{Q}(j(z), j_{24}(z))$, $\tau(z)$ is symmetric in $j(z)$ and $j_{24}(z), \sigma(z)/(j(z) - j_{24}(z)) \in \mathbb{Q}(\tau(z))$, and $\sigma^2(z) = f(\tau(z)) = \tau^4(z) - 12\tau^3(z) + 32\tau^2(z) - 24\tau(z) + 4$ ([5], p. 459, [1]). Then we can define a map from $F_0(24)$ to Fricke's quartic $C_{24} : \sigma(z)^2 = f(\tau(z))$ by $z \mapsto (\tau(z), \sigma(z))$, where $\sigma(z) = \sqrt{f(\tau(z))}$ (any one of the two branches) if $|z| > \sqrt{6}/12$ or $|z| = \sqrt{6}/12$, $\operatorname{Re}(z) \ge 0$, and $\sigma(z) = -\sqrt{f(\tau(z))}$ otherwise. Then we obtain a commutative diagram

$$\begin{tikzcd}
 & z \in F_0(24)\setminus\{z \in F_0(24) : (j(z), j_{24}(z)) \text{ is singular on } J_{24}\} \arrow[dl] \arrow[dr] & \\
\pi : J_{24}\setminus\{\text{singular points}\} \arrow[rr] & & C_{24} \\
(j(z), j_{24}(z)) \arrow[rr, mapsto] & & (\tau(z), \sigma(z))
\end{tikzcd}$$

and this induces a well defined map π from $J_{24}\setminus\{\text{singular points}\}$ to C_{24}.

By Birch's theorem ([1], Thm. 1), if $-p = S^2 - 96T^2$ has an integral solution (S, T), and if the map π is well defined at the point $\omega = (S + \sqrt{-p})/(48T) \in F_0(24)$ $(\Delta(\omega) = -p)$, then ω certainly yields a nontrivial rational point on our elliptic curve $E_{p,2\pi/3}$.

We have seen that π is well defined on $J_{24}\setminus\{\text{singular points}\}$ and this confirms our theorem for $p > 2304$.

For 42 primes $p \equiv 23 \pmod{24}$, $23 \le p < 2304$, computer calculation together with Theorem 7.3 of [7] assure that each elliptic curve $E^{(-p)}$ has positive Mordell–Weil rank. This completes our proof. ■

Example. 23 is $2\pi/3$-congruent. Indeed $23\sqrt{3}$ is the area of a $2\pi/3$-rational triangle with sides 14/5, 230/7 and 1202/35. 2039 is also $2\pi/3$-congruent, since $2039\sqrt{3}$ is the area of a $2\pi/3$-rational triangle with sides

$$\frac{891339311078695734731 98}{703114432715601500117 9}, \quad \frac{286730065661422291748079 62}{445669655539347867365 99}$$

and

$$\frac{2036193258877906366441529848343726435356779132 02}{3133567670331061034744344902646726065474502 21}.$$

Acknowledgements. I would like to express special thanks to Professor Masahiko Fujiwara for his heartful seminars and encouragement. In addition, I would like to thank Professor Akira Kaneko and Professor Takaaki Kagawa for their kind advice.

References

[1] B. J. Birch, *Elliptic curves and modular functions*, in: Symposia Math. IV (Roma, 1968/69), Academic Press, 1970, 27–32.

[2] —, *Heegner points of elliptic curves*, in: Symposia Math. XV (Roma, 1973), Academic Press, 1975, 441–445.

[3] J. S. Chahal, *On an identity of Desboves*, Proc. Japan Acad. Ser. A 60 (1984), 105–108.

[4] G. Frey, *Some aspects of the theory of elliptic curves over number fields*, Exposition. Math. 4 (1986), 35–66.

[5] R. Fricke, *Lehrbuch der Algebra III*, Braunschweig, 1928.

[6] M. Fujiwara, *θ-congruent numbers*, in: Number Theory, K. Győry, A. Pethő, and V. Sós (eds.), de Gruyter, 1997, 235–241.

[7] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), 225–320.

[8] P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z. 204 (1990), 45–68.

[9] P. Serf, *Congruent numbers and elliptic curves*, in: Computational Number Theory, A. Pethő *et al.* (eds.), de Gruyter, 1991, 227–238.

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

[11] A. Wiman, *Über den Rang von Kurven* $y^2 = x(x+a)(x+b)$, Acta Math. 76 (1944), 225–251.

Department of Mathematics
Ochanomizu University
Otsuka, Tokyo 112-8610, Japan
E-mail: kan@math.ocha.ac.jp

Received on 24.11.1998
and in revised form on 13.12.1999 (3516)