JOURNAL OF NUMBER THEORY 38, 265–286 (1991)

Supercongruences of Atkin and Swinnerton-Dyer Type for Legendre Polynomials

M. J. COSTER

C.W.I., Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

AND

L. VAN HAMME

Faculty of Applied Sciences, Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Brussel, Belgium

Communicated by Hans Zassenhaus

Received August 24, 1989; revised April 4, 1990

In this paper we prove some generalisations of congruences of Atkin and Swinnerton-Dyer type. This is done in the form of congruences for numbers $P_n(A/\sqrt{\Delta})$, where $P_n(t)$ are the orthogonal polynomials of Legendre. The proofs are based on complex multiplication of elliptic functions.

1. INTRODUCTION

This paper deals with so-called "supercongruences" for Legendre polynomials. We first explain what we mean by a supercongruence. Let p be an odd prime and consider the elliptic curve

$$\mathscr{E} : y^2 = x(x^2 + Ax + B),$$

where $A, B \in \mathbb{Z}_p$ (the ring of p-adic integers). If we choose $t = x/y$ as a local parameter, a short calculation (given in the beginning of the proof of Theorem 1 below) shows that the holomorphic form on the curve $\mathscr{E}$ takes the form

$$-\frac{dx}{2y} = (1 - 2At + \Delta t^4)^{-1/2}\, dt = \sum_{k=0}^{\infty} P_k\left(\frac{A}{\sqrt{\Delta}}\right) \cdot (\sqrt{\Delta})^k \cdot t^{2k}\, dt, \qquad (1)$$

where $P_n(t)$ is a Legendre polynomial and $\Delta = A^2 - 4B$. When the curve $\mathscr{E}$ has ordinary reduction over $\mathbb{F}_p$ (the field with p elements), the theory of

0022-314X/91 $3.00

formal groups (cf. [19, pp. 441–446] predicts a congruence of the Atkin–Swinnerton-Dyer type

$$c_{1/2(mp^r-1)} - (p+1-N_p)\cdot c_{1/2(mp^{r-1}-1)} + p\cdot c_{1/2(mp^{r-2}-1)} \equiv 0 \bmod p^r, \quad (2)$$

for any positive integer r and positive odd integer m, where we denote

$$c_n = \sqrt{\Delta}^n \cdot P_n\left(\frac{A}{\sqrt{\Delta}}\right),$$

and where N_p denotes the number of projective points on $\mathscr{E}$ over $\mathbb{F}_p$. As usual $P_n(t)=0$ if n is not a positive integer. We consider this congruence and all other congruences in this paper as a congruence in $\mathbb{Z}_p$ (the ring of p-adic integers). Assuming for the moment that the limit of $\{c_{1/2(mp^r-1)}/c_{1/2(mp^{r-1}-1)}\}_{r=1}^{\infty}$ by $\bar{\pi}$, we deduce from (2) that $\bar{\pi}$ is the root of

$$X^2 - (p+1-N_p)X + p = 0$$

for which $|\bar{\pi}|_p = 1$ (here is $|\cdot|_p$ the usual valuation on $\mathbb{Z}_p$). In this way one can write congruence (2) in the form

$$P_{1/2(mp^r-1)}\left(\frac{A}{\sqrt{\Delta}}\right) \equiv \sqrt{-mp^{r-1}\cdot(p-1)/2}\cdot\pi\cdot P_{1/2(mp^{r-1}-1)}\left(\frac{A}{\sqrt{\Delta}}\right) \bmod p^r, \quad (3)$$

(see [12, 13]).

The main point of this paper is that if the curve $\mathscr{E}$ has complex multiplication congruence (3) can be changed into a congruence mod p^{2r}. The existence of the limit can be deduced from Atkin and Swinnerton-Dyer, but it follows also from the supercongruence (5) which we prove. We call such congruences supercongruences (cf. [12, 13]). Many of such supercongruences have been proved during the last years. We mention [12, 5–7, 10, 11, 17], etc.

If K is an algebraic extension of $\mathbb{Q}$, we denote by $|\cdot|_p$ the valuation on K which extends the usual valuation on $\mathbb{Q}$. We denote by $\mathbb{Q}_p$ the field of p-adic numbers. We have the following theorem.

THEOREM 1. *Let p be an odd prime. Let d be a square-free positive integer such that $(-d/p)=1$ (here $(\cdot/\cdot)$ is the Legendre symbol). Let K be an algebraic numberfield such that $\sqrt{(-d)}\in K$ and $K\subset\mathbb{Q}_p$. Consider the elliptic curve*

$$\mathscr{E}: Y^2 = X(X^2+AX+B) \qquad \text{with} \quad A, B\in K \quad \text{and} \quad |A|_p = |A^2-4B|_p = 1. \quad (4)$$

Let $\Delta = A^2-4B$. Let ω and ω' be a basis of periods of $\mathscr{E}$ and suppose that $\tau=\omega'/\omega\in\mathbb{Q}(\sqrt{-d})$ (which implies that the curve has complex multiplica-

tion), τ *has positive imaginary part, and* $A = 3\mathscr{P}(\frac{1}{2}\omega)$, $\sqrt{\Delta} = \mathscr{P}(\frac{1}{2}\omega' + \frac{1}{2}\omega) - \mathscr{P}(\frac{1}{2}\omega')$, *where* $\mathscr{P}(z)$ *is the Weierstrass* $\mathscr{P}$*-function. Let* $\pi, \bar{\pi} \in \mathbb{Q}(\sqrt{-d})$ *such that* $\pi\bar{\pi} = p$, $|\pi|_p = 1/p$ *and* $|\bar{\pi}|_p = 1$. *Suppose that* $\pi = u_1 + v_1\tau$ *and* $\pi\tau = u_2 + v_2\tau$ *with* u_1, v_1, u_2, v_2 *integers and* v_1 *even. Then we have*

$$P_{1/2(mp^r-1)}\left(\frac{A}{\sqrt{\Delta}}\right) \equiv \varepsilon^{mp^{r-1}} \cdot \bar{\pi} \cdot P_{1/2(mp^{r-1}-1)}\left(\frac{A}{\sqrt{\Delta}}\right) \bmod \pi^{2r}, \tag{5}$$

where m *and* r *are positive integers, with* m *odd and*

$$\varepsilon = i^{-u_2v_2 + v_2 + p - 2}. \tag{6}$$

Here $i = \sqrt{-1}$.

The conditions $A = 3\mathscr{P}(\frac{1}{2}\omega)$ and v_1 even look arbitrary; however, these conditions are necessary to obtain a 2-torsion point in $(0, 0)$, which will be fixed by the Frobenius endomorphism $[\pi]$.

The proof of the theorem is based on complex multiplication of Jacobian elliptic functions.

By comparing congruences (3) and (5) we derive another expression for ε. If we put $m = r = 1$ in these congruences then we get

$$\varepsilon \equiv -\frac{N_p - 1}{\bar{\pi}} \cdot \Delta^{-1/4(p-1)} \bmod p.$$

Note that ε depends on the choice of $\sqrt{\Delta}$.

We first give two special cases of the theorem. In both examples the period lattice is of the form $\{m\alpha + ni\alpha : m, n \in \mathbb{Z}, i = \sqrt{(-1)}, \alpha \in \mathbb{R}\}$ but the choice of ω and ω' is different.

EXAMPLE 1. Let $\mathscr{E}$: $Y^2 = X(X^2 - 4)$. We can choose periods ω and ω' such that $\mathscr{P}(\frac{1}{2}\omega) = 0$, $\mathscr{P}(\frac{1}{2}\omega + \frac{1}{2}\omega') - \mathscr{P}(\frac{1}{2}\omega') = -4$ and $\omega'/\omega = \tau = -\frac{1}{2} + \frac{1}{2}i$. (If $\psi = \Gamma^2(\frac{1}{4})/4\sqrt{\pi}$, then $\omega = (1 + i) \cdot \psi$, $\omega' = \tau\omega = -\psi$ and $\mathscr{P}(\frac{1}{2}\omega') = 2$ and $\mathscr{P}(\frac{1}{2}\omega + \frac{1}{2}\omega') = -2$ (cf. [1, p. 658]).) Let $p \equiv 1 \bmod 4$ be a prime. Then p can be written as $p = a^2 + b^2$, with $a, b \in \mathbb{Z}$. Let $a \equiv 1 \bmod 4$. Let i be a p-adic integer such that $i^2 = -1$. Fix the sign of bi such that $a \equiv bi \bmod p$. Let $\pi = a - bi$. Then we have $\pi = (a - b) - 2b\tau$ and $\pi\tau = b + (a + b)\tau$. Hence $\varepsilon = i^{v_2(1-u_2)+p-2} = 1$. Since $P_{2n}(0) = (-4)^{-n} \cdot \binom{2n}{n}$ we derive the congruence

$$\binom{\frac{1}{2}(mp^r - 1)}{\frac{1}{4}(mp^r - 1)} \equiv (-4)^{1/4mp^{r-1}(p-1)} \cdot (a + bi) \cdot \binom{\frac{1}{2}(mp^{r-1} - 1}{\frac{1}{4}(mp^{r-1} - 1)} \bmod p^{2r}.$$

This congruence has been proved in several other ways. (Cf. [12].)

EXAMPLE 2. Let $\mathscr{E}$: $Y^2 = X(X^2 + 3X + 2)$. We can choose periods ω and ω' for this curve such that $\mathscr{P}(\frac{1}{2}\omega) = 1$ and $\omega'/\omega = \tau = i$. (If ψ has the

same meaning as in Example 1 then $\omega = \sqrt{2} \cdot \psi$, $\omega' = \tau\omega = i\sqrt{2} \cdot \psi$, and $\mathscr{P}(\frac{1}{2}\omega') = -1$ and $\mathscr{P}(\frac{1}{2}\omega + \frac{1}{2}\omega') = 0$.) Let p, a, b, and π as defined in Example 1. We derive that $\pi = a - b\tau$, $\pi\tau = b + a\tau$, and $\varepsilon = i^{-b} = (-1)^{1/4(p-1)}$. We denote

$$c_n = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k}.$$

The numbers c_n have been used for proving that $\log 2$ is irrational with measure of irrationality 4.622... (see [2]). Carlitz [9] proved for the numbers c_n the congruence

$$c_{1/2(p-1)} \equiv (-1)^{1/4(p-1)} \cdot 2a \bmod p.$$

Since $c_n = P_n(3)$, we have the supercongruence

$$c_{1/2(mp^r-1)} \equiv (-1)^{1/4(p-1)} \cdot (a + bi) \cdot c_{1/2(mp^{r-1}-1)} \bmod p^{2r}.$$

Another proof of this supercongruence in the case $m = r = 1$ has been given by van Hamme in [18]. In Section 4 we give some more examples of the Theorem, and we prove that there are only eight examples of supercongruences where A and B are rational and where congruence (5) can be replaced by a congruence in $\mathbb{Z}$ (congruence (48)).

2. Some Preliminaries

2.1. *The Theta Functions*

We need some properties of classical theta functions. Let τ be a complex number with a positive imaginary part. We write

$$q = e^{\pi i \tau}.$$

Hence $|q| < 1$. We define

$$\vartheta(z) = \sum_{n \in \mathbb{Z}} q^{n^2} \cdot e^{2n\pi i z}, \qquad \text{for any} \quad z \in \mathbb{C}. \tag{7}$$

$\vartheta(z)$ is an entire function (cf. [27, p. 463] or [24, p. 4]). It is easy to verify that

$$\vartheta(z+1) = \vartheta(z), \tag{8.1}$$

$$\vartheta(z+\tau) = q^{-1}e^{-2\pi i z}\vartheta(z), \tag{8.2}$$

$$\vartheta(-z) = \vartheta(z); \tag{8.3}$$

cf. [24, pp. 1, 2, 17]. We define

$$\vartheta_{00}(z) = \vartheta(z), \qquad (\vartheta_3(\pi z)) \tag{9.1}$$

$$\vartheta_{01}(z) = \vartheta(z + \tfrac{1}{2}), \qquad (\vartheta_4(\pi z)) \tag{9.2}$$

$$\vartheta_{10}(z) = M(z) \cdot \vartheta(z + \tfrac{1}{2}\tau), \qquad (\vartheta_2(\pi z)) \tag{9.3}$$

$$\vartheta_{11}(z) = -iM(z) \cdot \vartheta(z + \tfrac{1}{2} + \tfrac{1}{2}\tau), \qquad (\vartheta_1(\pi z)), \tag{9.4}$$

where $M(z) = q^{1/4}e^{\pi i z}$; cf. [27, p. 464]. We have used Weber's notation for the theta functions. The notation of Whittaker and Watson has been added between brackets. The notation used by Mumford corresponds to the notation of Whittaker and Watson, but Mumford denotes $\vartheta_{11}(z)$ with a minus-sign. The zeros of $\vartheta_{00}(z)$, $\vartheta_{01}(z)$, $\vartheta_{10}(z)$, and $\vartheta_{11}(z)$ are given in [24, p. 12].

$$\vartheta_{00}(z) = 0 \quad \text{if and only if} \quad z = (m + \tfrac{1}{2}) + (n + \tfrac{1}{2})\tau, \quad \text{for} \quad m, n \in \mathbb{Z}, \tag{10.1}$$

$$\vartheta_{01}(z) = 0 \quad \text{if and only if} \quad z = m + (n + \tfrac{1}{2})\tau, \quad \text{for} \quad m, n \in \mathbb{Z}, \tag{10.2}$$

$$\vartheta_{10}(z) = 0 \quad \text{if and only if} \quad z = (m + \tfrac{1}{2}) + n\tau, \quad \text{for} \quad m, n \in \mathbb{Z}, \tag{10.3}$$

$$\vartheta_{11}(z) = 0 \quad \text{if and only if} \quad z = m + n\tau, \quad \text{for} \quad m, n \in \mathbb{Z}. \tag{10.4}$$

We abbreviate the values $\vartheta_{00}(0)$, $\vartheta_{01}(0)$, and $\vartheta_{10}(0)$ to ϑ_{00}, ϑ_{01}, and ϑ_{10}, respectively. There is an important relation between these numbers, namely Jacobi's identity

$$\vartheta_{01}^4 + \vartheta_{10}^4 = \vartheta_{00}^4; \tag{11}$$

cf. [27, p. 469].

2.2. *The Function $S(z)$.*

We use thetafunctions to introduce a function which plays a central role in this paper and which is related to the Jacobian elliptic functions $sn(z)$, $cn(z)$, and $dn(z)$. For the precise relation we refer to [12] or [27]. We define $S(z)$ by

$$S(z) = \frac{\vartheta_{10}(z/\omega) \cdot \vartheta_{11}(z/\omega)}{\vartheta_{00}(z/\omega) \cdot \vartheta_{01}(z/\omega)}. \tag{13}$$

The properties of $S(z)$ which we use in this paper are formulated in the following lemmas.

LEMMA 2.1.

$$S(-z) = -S(z), \tag{14.1}$$

$$S(z + \tfrac{1}{2}\omega) = -S(z), \tag{14.2}$$

$$S(z + \tfrac{1}{2}\omega') = 1/S(z), \tag{14.3}$$

$$S(0) = S(\tfrac{1}{2}\omega) = 0, \tag{14.4}$$

$$S(z) \text{ has poles for } z = \tfrac{1}{2}\omega' \text{ and } z = \tfrac{1}{2}\omega + \tfrac{1}{2}\omega', \tag{14.5}$$

$$S(z) = S(\alpha) \quad \text{if and only if} \quad z = \alpha + m\omega + n\omega'$$
$$\text{or} \quad z = \tfrac{1}{2}\omega - \alpha + m\omega + n\omega', \quad \text{where} \quad \omega' = \omega\tau, \quad \text{and} \quad m, n \in \mathbb{Z}. \tag{14.6}$$

Proof. These properties follow immediately from the properties of the theta functions, cf. [24, p. 23]. ∎

COROLLARY 2.2. *$S(z)$ is an elliptic function with periods ω, ω' or order 2.*

Proof. This follows from Lemma 2.1. ∎

LEMMA 2.3.

$$[\mathscr{P}'(z)]^2 = 4 \cdot (\mathscr{P}(z) - \mathscr{P}(\tfrac{1}{2}\omega)) \cdot (\mathscr{P}(z) - \mathscr{P}(\tfrac{1}{2}\omega')) \cdot (\mathscr{P}(z) - \mathscr{P}(\tfrac{1}{2}(\omega + \omega'))) \tag{15.1}$$

$$S(z) = c \cdot \frac{\mathscr{P}(z) - \mathscr{P}(\tfrac{1}{2}\omega)}{\mathscr{P}'(z)}, \tag{15.2}$$

where

$$c^2 = 4(\mathscr{P}(\tfrac{1}{2}(\omega + \omega')) - \mathscr{P}(\tfrac{1}{2}\omega')). \tag{15.3}$$

Proof. See (15.1) in [27, pp. 443–444]. For the proof of (15.2) and (15.3) let Λ be the lattice spanned by ω and ω'. $S(z)$ is an elliptic function with periods ω and ω'. Hence $S(z) \in \mathbb{C}(\mathscr{P}(z), \mathscr{P}'(z))$. $S(z)$ is an odd function and $S(z)\mathscr{P}'(z)$ is an even function. $S(z)$ has poles for $z \equiv \frac{1}{2}\omega' \bmod \Lambda$ and $z \equiv \frac{1}{2}\omega + \frac{1}{2}\omega' \bmod \Lambda$, and zeros for $z \in \Lambda$ and $z \equiv \frac{1}{2}\omega \bmod \Lambda$. Hence $S(z)\mathscr{P}'(z)$ has zeros of multiplicity 2 for $z \equiv \frac{1}{2}\omega \bmod \Lambda$ and poles for $z \in \Lambda$ of order 2. Hence $S(z)\mathscr{P}'(z) = c(\mathscr{P}(z) - \mathscr{P}(\frac{1}{2}\omega))$ for some $c \in \mathbb{C}$. Using (14.3) we find

$$c \cdot \frac{\mathscr{P}(z + \frac{1}{2}\omega') - \mathscr{P}(\frac{1}{2}\omega)}{\mathscr{P}'(z + \frac{1}{2}\omega')} = \frac{\mathscr{P}'(z)}{c \cdot (\mathscr{P}(z) - \mathscr{P}(\frac{1}{2}\omega))}. \tag{16}$$

We use the formulas for the addition of a half period (cf. [27, p. 444])

$$\mathscr{P}(z + \tfrac{1}{2}\omega') - \mathscr{P}(\tfrac{1}{2}\omega) = \frac{(\mathscr{P}(\frac{1}{2}\omega') - \mathscr{P}(\frac{1}{2}\omega)) \cdot (\mathscr{P}(z) - \mathscr{P}(\frac{1}{2}\omega + \frac{1}{2}\omega'))}{(\mathscr{P}(z) - \mathscr{P}(\frac{1}{2}\omega'))},$$

and

$$\mathscr{P}'(z + \tfrac{1}{2}\omega') = -\frac{(\mathscr{P}(\frac{1}{2}\omega') - \mathscr{P}(\frac{1}{2}\omega)) \cdot (\mathscr{P}(\frac{1}{2}\omega') - \mathscr{P}(\frac{1}{2}\omega + \frac{1}{2}\omega')) \cdot \mathscr{P}'(z)}{(\mathscr{P}(z) - \mathscr{P}(\frac{1}{2}\omega'))^2}.$$

TABLE I

$S(\frac{1}{4}(u\omega + v\omega'))$	$v \backslash u$	0	1	2	3
	1	i	1	$-i$	-1
	3	$-i$	1	i	-1

Hence we get

$$c^2 = \frac{\mathscr{P}'(z) \cdot \mathscr{P}'(z + \frac{1}{2}\omega')}{(\mathscr{P}(z) - \mathscr{P}(\frac{1}{2}\omega)) \cdot (\mathscr{P}(z + \frac{1}{2}\omega') - \mathscr{P}(\frac{1}{2}\omega))}$$
$$= 4(\mathscr{P}(\tfrac{1}{2}\omega + \tfrac{1}{2}\omega') - \mathscr{P}(\tfrac{1}{2}\omega')). \quad \blacksquare$$

The following lemma is very useful for the calculation of the number ε in formula (5).

LEMMA 2.4. *We have for any integers u, v with v odd*

$$S(\tfrac{1}{4}(u\omega' + v\omega'))/S(\tfrac{1}{4}\omega') = i^{-uv+v-1}.$$

Proof. Using properties of the theta function we obtain

$$S(\tfrac{1}{4}\omega') = \frac{\vartheta_{10}(\frac{1}{4}\tau) \cdot \vartheta_{11}(\frac{1}{4}\tau)}{\vartheta_{00}(\frac{1}{4}\tau) \cdot \vartheta_{01}(\frac{1}{4}\tau)} = -iq \cdot \frac{\vartheta(\frac{1}{2} + 3\tau/4)\,\vartheta(3\tau/4)}{\vartheta(\frac{1}{4}\tau)\,\vartheta(\frac{1}{2} + \frac{1}{4}\tau)} = i,$$

$$S(\tfrac{1}{4}\omega + \tfrac{1}{4}\omega') = \frac{\vartheta_{10}(\frac{1}{4} + \frac{1}{4}\tau) \cdot \vartheta_{11}(\frac{1}{4} + \frac{1}{4}\tau)}{\vartheta_{00}(\frac{1}{4}\tau + \frac{1}{4}) \cdot \vartheta_{01}(\frac{1}{4}\tau + \frac{1}{4})}$$
$$= -iq^{1/2} e^{1/2\pi i(\tau+1)} \cdot \frac{\vartheta(3/4 + 3\tau/4)\,\vartheta(\frac{1}{4} + 3\tau/4)}{\vartheta(\frac{1}{4} + \frac{1}{4}\tau)\,\vartheta(3/4 + \frac{1}{4}\tau)} = 1.$$

Using the relations of (14) we find the values of Table I. Equation (17) follows immediately. $\blacksquare$

3. SUPERCONGRUENCES

3.1. *The Main Theorem*

We deduce Theorem 1 from Theorem 3.1 below. The conditions (18) and (19) of this theorem may seem a little artificial but it becomes clear during the proof of Theorem 1 that they fit our needs exactly.

THEOREM 3.1. *Let p be an odd prime. Let K be a numberfield with a finite valuation $|\cdot|_v$ such that $|p|_v < 1$. Let $R = \{\alpha \in K : |\alpha|_v \leqslant 1\}$ and let $\pi \in K$ be such that $|\pi|_v = |p|_v$. Suppose that the formal powerseries*

$$z = \sum_{n=1}^{\infty} \frac{\lambda_n}{n} t^n \qquad \text{with} \quad \lambda_n \in R, \tag{18}$$

has an inverse $t = t(z)$ which satisfies

$$t(\pi z) = \eta t^p \cdot \frac{1 + \pi \cdot a(1/t)}{1 - \pi \cdot d(t)}, \tag{19}$$

where $\eta \in R$ and $a(t)$ and $d(t) \in R(t)$, both of degree $\leqslant p-1$ and $a(0) = d(0) = 0$. Then we have

$$\lambda_{mp^r} \equiv \eta^{mp^{r-1}} \cdot \frac{p}{\pi} \cdot \lambda_{mp^{r-1}} \bmod \pi^{2r} \qquad \text{for all positive integers } m, r. \tag{20}$$

Proof. We derive from (18)

$$\pi z = \sum_{n=1}^{\infty} \frac{\pi \lambda_n}{n} \cdot t^n(z) \tag{21}$$

and

$$\pi z = \sum_{m=1}^{\infty} \frac{\lambda_m}{m} \cdot t^m(\pi z). \tag{22}$$

The idea of the proof is to compare the coefficients of t^{mp^r} in (21) and (22). Equation (20) is a consequence of the equality of these coefficients. We need some preparations. We define $a_{k,n}$ as the coefficient of t^n in the power series of $t^k(\pi z)$, i.e.,

$$t^k(\pi z) = \sum_{n=k}^{\infty} a_{k,n} t^n(z). \tag{23}$$

We calculate these coefficients $a_{k,n}$ in the case that $n = mp^r$ and we show that the coefficients a_{k,mp^r} satisfy the inequality $|a_{k,mp^r}|_v \leqslant |kmp^{r+1}|_v$, except for a_{mp^{r-1},mp^r} which is congruent to $\eta^{mp^{r-1}} \bmod \pi^{2r}$. This will prove the theorem. We use three technical but straightforward lemmas.

LEMMA 3.2. *a_{kp^s,mp^r} is the coefficient of $t^{mp^r \; kp^s+1}$ in*

$$\eta^{kp^s} \sum_{i=0}^{kp^s} \sum_{j=0}^{\infty} \binom{kp^s}{i} \cdot \binom{kp^s + j - 1}{j} \cdot \pi^{i+j} \cdot a^i(1/t) \cdot d^j(t). \tag{24}$$

Proof. We have

$$t^{kp^s}(\pi z) = \eta^{kp^s} \cdot t^{kp^{s+1}} \cdot \left(\frac{1+\pi a(1/t)}{1-\pi d(t)}\right)^{kp^s}$$

$$= \eta^{kp^s} \cdot t^{kp^{s+1}} \cdot \left(\sum_{i=0}^{kp^s} \binom{kp^s}{i} \cdot \pi^i \cdot a^i(1/t)\right)$$

$$\cdot \left(\sum_{j=0}^{\infty} \binom{-kp^s}{j} \cdot (-\pi)^j \cdot d^j(t)\right).$$

Note that $(-1)^j \cdot \binom{-kp^s}{j} = \binom{kp^s+j-1}{j}$. The lemma follows immediately. ∎

LEMMA 3.3. *We have* $a_{mp^{r-1},mp^r} \equiv \eta^{mp^{r-1}} \bmod \pi^{2r}$.

Proof. We apply Lemma 3.2 with $k=m$ and $s=r-1$. Then we need the coefficient of t^0 in expression (24). We define $b_{ij}=$ as the constant term in $a^i(1/t) \cdot d^j(t)$. We conclude that $b_{00}=1$, $b_{0j}=0$ for $j>0$ and $b_{i0}=0$ for $i>0$. Hence

$$a_{mp^{r-1},mp^r} = \eta^{mp^{r-1}} \cdot \left(1 + \sum_{i=1}^{mp^{r-1}} \sum_{j=1}^{\infty} \binom{mp^{r-1}}{i} \cdot \pi^i \cdot \binom{mp^{r-1}+j-1}{j} \cdot \pi^j \cdot b_{ij}\right).$$

Since $\binom{mp^{r-1}}{i}$ contains at least $r-i$ factors p and $\binom{kp^{r-1}+j-1}{j}$ contains at least $r-j$ factors, the terms in the sums over i and j vanish mod π^{2r}. ∎

LEMMA 3.4. *If* $kp^s \neq mp^{r-1}$ *then we have*

$$|a_{kp^s,mp^r}|_v \leqslant |kp^s \cdot mp^r \cdot p|_v.$$

(In other words

$$a_{kp^s,mp^r} \equiv 0 \bmod \pi^{r+s+1}.)$$

Proof. Define $\Delta = mp^{r-1} - kp^s$. Then $\Delta \neq 0$. We distinguish two cases:

(i) $\Delta > 0$,

(ii) $\Delta < 0$.

Case (i) We know that $\deg_t(a(1/t)) \leqslant 0$ and $\deg_t(d(t)) \leqslant p-1$. This implies that $\deg_t(a^i(1/t) \cdot d^j(t)) \leqslant j(p-1)$. Hence the terms in (24) contribute only to a_{kp^s,mp^r} if $j(p-1) \geqslant \Delta p$. This implies that $j \geqslant \Delta + 1$. It follows that $kp^s + j - 1 \geqslant mp^{r-1} > kp^s$ and $j! \cdot \binom{kp^s+j-1}{j}$ contains the factors mp^{r-1} and kp^s. Hence $\operatorname{ord}_p\binom{kp^s+j-1}{j} \geqslant r+s-1-\operatorname{ord}_p(j!) > r+s-1-\frac{1}{2}j$. Now we have $\operatorname{ord}_\pi(a_{kp^s,mp^r}) \geqslant \operatorname{ord}_\pi$ coef. of $t^{\Delta p}$ in

$$\left(\eta^{kp^s} \sum_{i=0}^{kp^s} \sum_{j=0}^{\infty} \binom{kp^s}{i} \cdot \binom{kp^s+j-1}{j} \cdot \pi^{i+j} \cdot a^i(1/t) \cdot d^j(t)\right)$$

$$\geqslant \min_{j \geqslant \Delta+1} \left(j + \operatorname{ord}_\pi \binom{kp^s+j-1}{j}\right) > \min_{j \geqslant \Delta+1} r+s-1+\frac{1}{2}j \geqslant r+s.$$

The proof of case (ii) is similar. ∎

Continuation of the proof of Theorem 3.1. The coefficients of t^{mp^r} in Eqs. (21) and (22) must be equal. Hence we have

$$\frac{\pi}{mp^r} \cdot \lambda_{mp^r} = \sum_{j=1}^{mp^r} \frac{1}{j} \cdot \lambda_j \cdot a_{j,mp^r}.$$

We split the sum on the right side in several subsums depending on the number of factors p in j,

$$\lambda_{mp^r} = \sum_{s=0}^{\infty} {\sum_{k=1}^{[mp^{r-s}]}}' \lambda_{kp^s} \cdot \frac{mp^r}{k\pi p^s} \cdot a_{kp^s,mp^r},$$

where $\sum'$ denotes the sum over all integers coprime to p. Note that $|mp^r/k\pi p^s|_v \leqslant |p|_v^{r-s-1}$. By Lemma 3.4 a_{kp^s,mp^r} contains $r+s+1$ factors π if $kp^s \neq mp^{r-1}$. Hence we find using Lemma 3.3

$$\lambda_{mp^r} \equiv \lambda_{mp^{r-1}} \cdot \frac{mp^r}{m\pi p^{r-1}} \cdot a_{mp^{r-1},mp^r} \equiv \eta^{mp^{r-1}} \cdot \bar{\pi} \cdot \lambda_{mp^{r-1}} \bmod \pi^{2r}. \quad \blacksquare$$

3.2. *Application to the Legendre Polynomials*

In this section we show how Theorem 3.1 can be used to find congruences involving Legendre polynomials. Let $\mathscr{E}$ be an elliptic curve with complex multiplication τ. Suppose τ is a root of

$$Rx^2 + Sx - T = 0, \qquad \text{for integers } R, S, T \text{ with } \quad \gcd(R, S, T) = 1.$$

We define $\operatorname{discr}(\tau) = D = 4RT - S^2$. Then the endomorphism ring of $\mathscr{E}$ denoted by $\operatorname{End}(\mathscr{E})$ is the order generated by 1 and $\frac{1}{2}(D + \sqrt{-D})$ (cf. [23, pp. 90–93]). Let $\alpha \in \operatorname{End}(\mathscr{E})$. Then $\alpha\tau = x + y\tau$ for some integers x and y. If $\alpha \in \operatorname{End}(\mathscr{E})$ then $S(\alpha z)$ is a rational function of $S(z)$ (since $S(z)$ is an elliptic function). In Lemma 3.6 below this rational function is given explicitely in the particular case that $\alpha = \pi$.

THEOREM 1. *Let p be an odd prime. Let d be a square-free positive integer such that $(-d/p) = 1$. Let K be an algebraic numberfield such that $\sqrt{(-d)} \in K$ and $K \subset \mathbb{Q}_p$. Consider the elliptic curve*

$$\mathscr{E} : Y^2 = X(X^2 + AX + B) \qquad \text{with} \quad A, B \in K \quad \text{and} \quad |A|_p = |A^2 - 4B|_p = 1. \tag{4}$$

Let $\Delta = A^2 - 4B$. Let ω and ω' be a basis of periods of $\mathscr{E}$ which satisfies

$$\tau = \omega'/\omega \in \mathbb{Q}(\sqrt{-d}) \qquad \text{and} \qquad \operatorname{Im}(\tau) > 0, \tag{25}$$

$$A = 3\mathscr{P}(\tfrac{1}{2}\omega) \tag{26}$$

and

$$\sqrt{\Delta} = \mathscr{P}(\tfrac{1}{2}\omega' + \tfrac{1}{2}\omega) - \mathscr{P}(\tfrac{1}{2}\omega') \tag{27}$$

Let $\pi, \bar{\pi} \in \mathbb{Q}(\sqrt{-d})$ *such that* $\pi\bar{\pi} = p$, $|\pi|_p = 1/p$ *and* $|\bar{\pi}|_p = 1$. *Suppose that*

$$\pi = u_1 + v_1\tau \qquad \text{with } u_1 \text{ and } v_1 \text{ integers and } v_1 \text{ even} \tag{28.1}$$

and

$$\pi\tau = u_2 + v_2\tau \qquad \text{with } u_2, v_2 \text{ integers.} \tag{28.2}$$

Then we have the following congruence between the values of the Legendre polynomial

$$P_{1/2(mp^{r-1})}\left(\frac{A}{\sqrt{\Delta}}\right) \equiv \varepsilon^{mp^{r-1}} \cdot \bar{\pi} \cdot P_{1/2(mp^{r-1}-1)}\left(\frac{A}{\sqrt{\Delta}}\right) \bmod \pi^{2r}, \tag{5}$$

where m and r are positive integers, with m odd and

$$\varepsilon = i^{-u_2v_2 + v_2 + p - 2}. \tag{6}$$

Proof. We construct local parameters t and z which satisfy Eqs. (18) and (19). $\mathscr{E}$ can be parametrised by the meromorphic functions

$$x = \mathscr{P}(z) - \mathscr{P}(\tfrac{1}{2}\omega) \qquad \text{and} \qquad y = -\tfrac{1}{2}\mathscr{P}'(z), \tag{30}$$

for $z \in \mathbb{C}$. Consider $t = x/y$. Using (15) we can express t in terms of z:

$$t = -2 \cdot \frac{\mathscr{P}(z) - \mathscr{P}(\tfrac{1}{2}\omega)}{\mathscr{P}'(z)} = -\frac{2}{c} \cdot S(z). \tag{31}$$

Note that $t(z) = z +$ higher order terms in z. We derive from (31) that

$$\frac{x^2}{t^2} = x \cdot (x^2 + Ax + B),$$

which implies that

$$x^2 + \left(A - \frac{1}{t^2}\right) \cdot x + B = 0 \tag{32.1}$$

and

$$x = -\frac{1}{2}A + \frac{1}{2t^2} \cdot (1 + \sqrt{(1 - 2At^2 + \Delta t^4)}),$$

where

$$\Delta = A^2 - 4B. \tag{32.2}$$

Differentiation of (32.1) gives

$$\frac{dx}{-2x} = \frac{dt}{t((A+2x)\cdot t^2 - 1)} = \frac{dt}{t\cdot\sqrt{(1-2At^2+\Delta t^4)}}.$$

Hence

$$dz = -\frac{dx}{2y} = (1-2At^2+\Delta t^4)^{-1/2}\,dt = \sum_{k=0}^{\infty} P_k\left(\frac{A}{\sqrt{\Delta}}\right)\cdot(\sqrt{\Delta})^k\cdot t^{2k}\,dt.$$

Then z can be expressed as a function of t by

$$z = \sum_{k=0}^{\infty} \frac{1}{2k+1}\cdot P_k\left(\frac{A}{\sqrt{\Delta}}\right)\cdot(\sqrt{\Delta})^k\cdot t^{2k+1}. \tag{33}$$

We use Lemma 3.6. First we need some formulas. We derive the relation between the zeros of $\mathscr{P}'(z)$ and the coefficient B of (25) from (15.1), (25), and (30)

$$B = (\mathscr{P}(\tfrac{1}{2}\omega') - \mathscr{P}(\tfrac{1}{2}\omega))\cdot(\mathscr{P}(\tfrac{1}{2}(\omega+\omega')) - \mathscr{P}(\tfrac{1}{2}\omega)). \tag{34.1}$$

Combination of this formula and (26) gives

$$\Delta = (\mathscr{P}(\tfrac{1}{2}\omega') - \mathscr{P}(\tfrac{1}{2}(\omega+\omega')))^2. \tag{34.2}$$

Hence we have, using (15.3),

$$c^2 = 4\sqrt{\Delta}, \text{ for the proper choice of } \sqrt{\Delta}, \tag{35.1}$$

and

$$\sqrt{\Delta} = \mathscr{P}(\tfrac{1}{2}(\omega+\omega')) - \mathscr{P}(\tfrac{1}{2}\omega'). \tag{35.2}$$

LEMMA 3.6. *Let d, p, $\mathscr{E}$, π, $\bar{\pi}$, Δ, A, B, ω, ω', x, y satisfy the conditions of Theorem* 1. *Let $R = \{\alpha \in K : \mathrm{ord}_\pi(\alpha) \geqslant 0\}$. Then we have*

$$t(\pi z) = \eta\cdot\frac{A_1 t(z) + A_3 t^3(z) + \cdots + A_{p-2}t^{p-2}(z) + t^p(z)}{1 + D_2 t^2(z) + \cdots + D_{p-1}t^{p-1}(z)}, \tag{36}$$

where η, $A_1, A_3, \ldots, A_{p-2}$, $D_2, D_4, \ldots, D_{p-1} \in R$, $A_1, A_3, \ldots, A_{p-2}$, $D_2, D_4, \ldots, D_{p-1} \equiv 0 \bmod \pi$, *and*

$$\eta = \varepsilon\cdot\sqrt{\Delta^{1/2(p-1)}} \tag{37.1}$$

and

$$\varepsilon = i^{-u_2v_2+v_2+p-2}. \tag{37.2}$$

This lemma is proved after the proof of the theorem. We now apply Theorem 3.1. The role of formulas (18) and (19) is played by formulas (33) and (36). Congruence (20) now becomes

$$\sqrt{\Delta^{1/2(mp^r-1)}} \cdot P_{1/2(mp^r-1)}\left(\frac{A}{\sqrt{\Delta}}\right) \equiv \eta^{mp^{r-1}} \cdot \bar{\pi} \cdot \sqrt{\Delta^{1/2(mp^{r-1}-1)}} \cdot P_{1/2(mp^{r-1}-1)}\left(\frac{A}{\sqrt{\Delta}}\right) \bmod \pi^{2r}.$$

Dividing by $\sqrt{\Delta^{1/2(mp^r-1)}}$ and using (37.1) gives congruence (29.1). ∎

Proof of Lemma 3.6. The proof of this lemma is due to Weber (cf. [26, pp. 584–594]). Since this proof is scattered over several pages and uses properties of Jacobian elliptic functions, we give here a more compact proof. Let Λ be the lattice defined by ω and ω'. Consider

$$F(z) = S(z) \cdot \prod_{\alpha \in \mathscr{A}} \frac{(S(z) - S(\alpha))}{(1 - S(\alpha) \cdot S(z))},$$

where $\mathscr{A} = \{\alpha \in \mathbb{C} : \pi\alpha \equiv 0 \mod \Lambda, \ \alpha \not\equiv 0 \mod \Lambda, \ \alpha = \sigma\omega + \sigma'\omega' \text{ with } -\frac{1}{2} < \sigma, \sigma' < \frac{1}{2}\}$. Note that $|\mathscr{A}| = p - 1$. We show that if π satisfies (28) all zeros and poles of $S(\pi z)$ and $F(z)$ coincide. Note that

$$\{z \mid F(z) = 0\} = \{z \mid \pi z \equiv 0 \bmod \Lambda \text{ or } \pi(\tfrac{1}{2}\omega - z) \equiv 0 \bmod \Lambda\}.$$

Since v is even implies that $\frac{1}{2}\pi\omega \equiv \frac{1}{2}\omega \bmod \Lambda$, we have

$$\begin{aligned}\{z \mid F(z) = 0\} &= \{z \mid \pi z \equiv 0 \bmod \Lambda \text{ or } \pi z \equiv \tfrac{1}{2}\omega \bmod \Lambda\} \\ &= \{z \mid S(\pi z) = 0\}.\end{aligned}$$

The endomorphism $[\pi]$ permutes the torsion points on $\mathscr{E}$. Since $\frac{1}{2}\pi\omega \equiv \frac{1}{2}\omega \bmod \Lambda$ we have either $\frac{1}{2}\pi\omega' \equiv \frac{1}{2}\omega' \bmod \Lambda$ or $\frac{1}{2}\pi\omega' \equiv \frac{1}{2}(\omega + \omega') \bmod \Lambda$. Hence we have

$$\begin{aligned}\{z \mid F(z) = \infty\} &= \{z \mid S(z) = \infty \text{ or } S(z) = 1/S(\alpha)\} \\ &= \{z \mid S(z + \tfrac{1}{2}\omega') = 0 \text{ or } S(z + \tfrac{1}{2}\omega') = S(\alpha)\} \\ &= \{z \mid \pi(z + \tfrac{1}{2}\omega') \equiv 0 \bmod \Lambda \text{ or } \pi(z + \tfrac{1}{2}\omega') \equiv \tfrac{1}{2}\omega \bmod \Lambda\} \\ &= \{z \mid \pi z \equiv \tfrac{1}{2}\omega' \bmod \Lambda \text{ or } \pi z \equiv \tfrac{1}{2}(\omega + \omega') \bmod \Lambda\} \\ &= \{z \mid S(\pi z) = \infty\}.\end{aligned}$$

Since $F(z)$ and $S(\pi z)$ are both elliptic functions of the same order, we conclude that

$$S(\pi z) = \varepsilon \cdot S(z) \cdot \prod_{\alpha} \frac{S(z) - S(\alpha)}{1 - S(\alpha) \cdot S(z)} \qquad \text{for some } \varepsilon \in \mathbb{C}. \tag{38}$$

We calculate ε by putting $z = \frac{1}{4}\omega'$ in (38) and using Lema 2.4. Since the elements of $\mathscr{A}$ appears in pairs α and $-\alpha$ and since $S(-\alpha) = -S(\alpha)$ we have

$$\prod_{\alpha} \frac{S(\frac{1}{4}\omega') - S(\alpha)}{1 - S(\alpha) \cdot S(\frac{1}{4}\omega')} = \prod_{\alpha} \frac{i - S(\alpha)}{1 - iS(\alpha)} = i^{p-1}.$$

Hence we find

$$\varepsilon = \frac{S(\frac{1}{4}\pi\omega')}{S(\frac{1}{4}\omega')} \cdot i^{p-1} = i^{-xy+y+p-2},$$

where $\pi\tau = x + y\tau$. By combining (31.2) and (38) we find

$$\begin{aligned} t(\pi z) &= \varepsilon \cdot t(z) \cdot \prod_{\alpha \in \mathscr{A}} \frac{\frac{1}{2}ct(z) + S(\alpha)}{1 + \frac{1}{2}cS(\alpha) \cdot t(z)} \\ &= \varepsilon \left(\frac{1}{2}c\right)^{p-1} \cdot t(z) \cdot \prod_{\alpha} \frac{t(z) + 2S(\alpha)/c}{1 + \frac{1}{2}cS(\alpha) \cdot t(z)}. \end{aligned} \tag{39}$$

Put $\eta = \varepsilon \cdot (\frac{1}{2}c)^{p-1}$. Hence

$$\eta = \varepsilon \cdot \sqrt{\Delta^{1/2(p-1)}} \tag{40}$$

by (35.1). We define

$$\begin{aligned} A(t) &= t(z) \cdot \prod_{\alpha \in \mathscr{A}} (t(z) + 2S(\alpha)/c) \\ &= A_1 t(z) + A_3 t^3(z) + \cdots + A_{p-2} t^{p-2}(z) + t^p(z) \end{aligned} \tag{41.1}$$

and

$$D(t) = \prod_{\alpha \in \mathscr{A}} (1 + \tfrac{1}{2}cS(\alpha) \cdot t(z)) = 1 + D_2 t^2(z) + \cdots + D_{p-1} t^{p-1}(z). \tag{41.2}$$

We now show that the coefficients A_{2k-1} and D_{2k} are elements of K. By estimating the values of these coefficients we show that they belong to R and vanish mod π, for $k = 1 \cdots \frac{1}{2}(p-1)$. From formula (33) we derive that $t(z)$ can be written as a power series of z with coefficients in K. Hence $t(\pi z)$ can be written as a power series of πz with coefficients in K. z can be

written as a power series of t with coefficients in K. Therefore $t(\pi z)$ can be written as a power series of t with coefficients in $K(\pi)=K$. Hence $A(t)$ and $D(t)$ are polynomials in $K[t]$. For the proof that the coefficients A_{2k-1} and D_{2k} vanish mod π, we consider the power series of $z(t)$ in (33) mod π and mod t^p. We derive

$$z(t) \equiv c_1 t + c_3 t^3 + \cdots + c_{p-2} t^{p-2} \bmod \pi, t^p, \tag{42.1}$$

where $c_{2j-1} \in R$, for $1 \leqslant j \leqslant (p-1)/2$. Similarly we express $t(z)$ in a power series in z mod π and mod z^p. We obtain

$$t(z) \equiv c'_1 z + c'_3 z^3 + \cdots + c'_{p-2} z^{p-2} \bmod \pi, z^p, \tag{42.2}$$

where $c'_{2j+1} \in R$. Hence for $t(\pi z)$ we have

$$t(\pi z) \equiv c''_1 z + c''_3 z^3 + \cdots + c''_{p-2} z^{p-2} \bmod \pi, z^p, \tag{42.3}$$

where $c''_{2j-1} = c'_{2j-1} \cdot \pi^{2j-1}$, which implies that $c''_{2j-1} \equiv 0 \bmod \pi$. Formulas (35.1), (40), and (41) imply that

$$(t\sqrt{\Delta})^p \cdot A(1/t\sqrt{\Delta}) = D(t), \tag{43}$$

$$D_{2j} = \Delta^j \cdot A_{p-2j} \qquad \text{for} \quad j = 1 \cdots \tfrac{1}{2}(p-1), \tag{44}$$

and

$$A(t) = \eta \cdot t(\pi z) \cdot D(t). \tag{45}$$

We define a function v and $v^{(n)}$ (which operates on power series and polynomials, respectively, and whose image is the largest valuation of the coefficients of the polynomial), as follows. Let $v_\pi(G(T)) = \min_i \operatorname{ord}_\pi(g_i)$ and $v_\pi^{(n)}(G(T)) = \min_{i \leqslant n} \operatorname{ord}_\pi(g_i)$ for $G(T) = \sum_i g_i T^i \in K[T]$. Then (43) implies that $v_\pi^{(p-1)}(t(\pi z(t))) = 1$. Since we have from (44) that $v_\pi(A(t)) = v_\pi(D(t))$. It follows from (45) that $v_\pi(A(t) - t^p) \geqslant 1 + v_\pi(A(t))$. This inequality holds for $v_\pi(A(t) - t^p) = 1$. ∎

4. Examples

4.1. *Examples with Rational j-Invariant*

In this section we treat all posible cases of elliptic curves of the form

$$\mathscr{E} : y^2 = x(x^2 + Ax + B) \qquad \text{with} \quad A, B \in \mathbb{Z}, \tag{46}$$

up to transformations on x and y of the form $x = \alpha^2 \cdot x'$ and $y = \alpha^3 \cdot y'$. These curves have complex multiplication. They are listed in Table II together with the related supercongruences. They are determined by the

TABLE II

Curve	τ	Weierstrass form	Δ	$A/\sqrt{\Delta}$	End($\mathscr{E}$)	Primes
$\mathscr{E}_{1a}$	i	$y^2 = x(x^2+3x+2)$	1	3	$\mathbb{Z}[i]$	$p \equiv 1 \bmod 4$
$\mathscr{E}_{1b}$	$\frac{1}{2}i$	$y^2 = x(x^2+6x+1)$	32	$3\sqrt{2}/4$	$\mathbb{Z}[2i]$	$p \equiv 1 \bmod 4$
$\mathscr{E}_{1c}$	$-\frac{1}{2}+\frac{1}{2}i$	$y^2 = x(x^2-4)$	16	0	$\mathbb{Z}[i]$	$p \equiv 1 \bmod 4$
$\mathscr{E}_2$	$\frac{1}{2}\sqrt{(-2)}$	$y^2 = x(x^2+4x+2)$	8	$\sqrt{2}$	$\mathbb{Z}[\sqrt{-2}]$	$p \equiv 1, 3 \bmod 8$
$\mathscr{E}_{3a}$	$-\frac{1}{4}+\frac{1}{4}\sqrt{(-3)}$	$y^2 = x(x^2+6x-3)$	48	$\frac{1}{2}\sqrt{3}$	$\mathbb{Z}[\sqrt{-3}]$	$p \equiv 1 \bmod 6$
$\mathscr{E}_{3b}$	$\frac{1}{2}+\frac{1}{2}\sqrt{(-3)}$	$y^2 = x(x^2-3x+3)$	-3	$\sqrt{(-3)}$	$\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{-3}]$	$p \equiv 1 \bmod 6$
$\mathscr{E}_{7a}$	$(-1+\sqrt{(-7)})/8$	$y^2 = x(x^2+42x-7)$	1792	$3\sqrt{7}/8$	$\mathbb{Z}[\sqrt{-7}]$	$p \equiv 1, 2, 4 \bmod 7$
$\mathscr{E}_{7b}$	$\frac{1}{2}+\frac{1}{2}\sqrt{(-7)}$	$y^2 = x(x^2-21x+112)$	-7	$3\sqrt{(-7)}$	$\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{-7}]$	$p \equiv 1, 2, 4 \bmod 7$

fact that the j-invariants $j(\tau)$ and $j(2\tau)$ are rational. Namely suppose that $\mathscr{E}$ has lattice $\Lambda=[\omega,\omega']$ with $\omega'/\omega=\tau$. Note that $A, B\in\mathbb{Z}$ implies that $j(\tau)\in\mathbb{Q}$. The condition that $\mathscr{E}$ has complex multiplication implies that $j(\tau)$ assume one of 13 well-known values; see [23, p. 133, Theorem 5 and 21, p. 233]. $\mathscr{E}$ has 2-torsion point $(0,0)$. This implies that $\mathscr{E}$ is isogenous to the elliptic curve

$$\mathscr{E}': y^2=x(x^2-2Ax+\Delta), \tag{47}$$

where $\Delta=A^2-4B$; cf. [21, pp. 91–96]. $\mathscr{E}$ has a lattice $[\omega_1,\omega_1']$ with $\omega_1'/\omega_1=2\tau$. Hence $j(2\tau)$ is equal to one of the 13 values mentioned above. We derive that modulo the subgroup $\Gamma(2)$ of the modular group $SL(2,\mathbb{Z})$ only eight values of τ satisfy these conditions These values are listed in Table II. In the first column we denote by $\mathscr{E}_{d\alpha}$ an elliptic curve with $\tau\in\mathbb{Q}(\sqrt{-d})$ and the letter α is used for distinguishing the elliptic curves with the same d.

In each of the cases in Table II congruence (4), which in our case is a congruence in $\mathbb{Q}(\sqrt{-d})$, gives a congruence $\mathbb{Z}$ in the following way. Let p be a prime which split in $\mathrm{End}(\mathscr{E})$. The form of this prime is indicated in the table. According to Theorem 1 we have

$$P_{1/2(mp^r-1)}\left(\frac{A}{\sqrt{\Delta}}\right)\equiv\varepsilon^{mp^{r-1}}\cdot\bar{\pi}\cdot P_{1/2(mp^{r-1}-1)}\left(\frac{A}{\sqrt{\Delta}}\right)\bmod\pi^{2r},$$

where ε has been defined in (37.2). We denote by c_n the rational integers

$$c_n=\sqrt{\Delta^n}\cdot P_n\left(\frac{A}{\sqrt{\Delta}}\right).$$

We choose π in such a way that $|\pi|_p=1/p$ and $|\bar{\pi}|_p=1$. By considering the congruence modulo p^{2r} instead of modulo π^{2r}, we obtain

$$c_{1/2(mp^r-1)}\equiv\eta^{mp^{r-1}}\cdot\bar{\pi}\cdot c_{1/2(mp^{r-1}-1)}\bmod p^{2r}, \tag{48}$$

where η is defined in (37.1). We now turn to the information given in Table III. We have written $\pi=a+b\sqrt{-d}$ and $\bar{\pi}=a-b\sqrt{-d}$. We list conditions on these numbers a and b. Then we list ε and η and finally we give an integer expression for c_n. These formulas can be found by writing $P_n(t)$ as a hypergeometric function $P_n(t)={}_2F_1(-n,n+1,1,(1-t)/2)$ and using the transformation formulas for hypergeometric functions (cf. [12, pp. 90–91]). We explain the column of ε. χ_π is the multiplicative character of order 4 [22, p. 122], i.e., $\chi_\pi(2)=i^k$ such that $2^{1/4(p-1)}\equiv i^k \bmod \pi$.

For $\mathscr{E}_{1b}$ we have $i^{1/2h}=\chi_\pi(2)$; see [22, p. 64, Ex. 26, 27].

For $\mathscr{E}_{3a}$ and $\mathscr{E}_{3b}$ we have $i^h=i^{1/2(p-1)}$.

For $\mathscr{E}_{7a}$ and $\mathscr{E}_{7b}$ we have $i^h=i^{+1/2(p-1)}$.

TABLE III

Curve	$A/\sqrt{\Delta}$	Conditions on a and b	ε	η	c_n
$\mathscr{E}_{1a}$	3	$a \equiv 1 \bmod 4$	$(-1)^{1/4(p-1)}$	$(-1)^{1/4(p-1)}$	$\sum_{k=0}^{n} \binom{n}{k} \cdot \binom{n+k}{k}$
$\mathscr{E}_{1b}$	$3\sqrt{2}/4$	$a \equiv 1 \bmod 4$	$\chi_\pi(2)$	$32^{1/4(p-1)} \cdot \chi_\pi(2)$	$\sum_{k=0}^{n} \binom{n}{k} \cdot \binom{2k}{k} \cdot 4^{n-k}$
$\mathscr{E}_{1c}$	0	$a \equiv 1 \bmod 4$	1	2^{p-1}	$\begin{cases} 0 \text{ if } n \text{ is odd} \\ (-1)^{1/2n} \cdot \binom{n}{1/2n} \end{cases}$
$\mathscr{E}_2$	$\sqrt{2}$	$a \equiv 1 \bmod 4$	i^{-b}	$i^b \cdot 8^{1/4(p-1)}$	$\sum_{k=0}^{[1/2n]} \binom{n}{k} \binom{2n-2k}{n} \cdot 2^{n-k} \cdot (-1)^k$
$\mathscr{E}_{3a}$	$\frac{1}{2}\sqrt{3}$	$a+b \equiv 1 \bmod 4$	$(-i)^{1/2(p-1)}$	$(-4\sqrt{-3})^{1/2(p-1)}$	$\sum_{k=0}^{[1/2n]} \binom{n}{2k} \binom{2k}{k} \cdot 6^n \cdot (-1/12)^k$
$\mathscr{E}_{3b}$	$\sqrt{(-3)}$	$a+b \equiv 1 \bmod 4$	1	$(\sqrt{-3})^{1/2(p-1)}$	$\sum_{k=0}^{[1/2n]} \binom{n}{2k} \binom{2k}{k} \cdot 3^{n-k} \cdot (-1)^n$
$\mathscr{E}_{7a}$	$3(\sqrt{7})/8$	$a+b \equiv 1 \bmod 4$	$i^{1/2(p-1)}$	$(16\sqrt{-7})^{1/2(p-1)}$	$\sum_{k=0}^{[1/2n]} \binom{n}{2k} \binom{2k}{k} \cdot 42^{n-2k} \cdot (-7)^k$
$\mathscr{E}_{7b}$	$3\sqrt{(-7)}$	$a+b \equiv 1 \bmod 4$	$(-1)^{1/2(p-1)}$	$(-\sqrt{-7})^{1/2(p-1)}$	$\sum_{k=0}^{[1/2n]} \binom{n}{2k} \binom{2k}{k} \cdot (-21)^{n-2k} \cdot 112^k$

4.2 *Examples with the j-Invariant in a Quadratic Field*

It can be shown that we have $A/\sqrt{\Delta} = 2\sqrt{(\sqrt{5}-2)}$ for $\tau_\alpha = (-1+\sqrt{(-5)})/6$ and $A/\sqrt{\Delta} = 2\sqrt{(-\sqrt{5}-2)}$ for $\tau_\beta = \frac{1}{2}(-1+\sqrt{(-5)})$. These results imply interesting supercongruences. We define the curves $\mathscr{E}_{5\alpha}$ and $\mathscr{E}_{5\beta}$ by

$$\mathscr{E}_{5\alpha} : y^2 = x(x^2+4x+2-\sqrt{5})$$

and

$$\mathscr{E}_{5\beta} : y^2 = x(x^2+4x+2+\sqrt{5}).$$

Let p be a prime such that $p = \pi\bar{\pi}$ with $\pi, \bar{\pi} \in \mathbb{Z}[\sqrt{-5}]$. Let $\pi = a + b\sqrt{-5}$. It can be verified easily that $p \equiv 1, 9 \bmod 20$. Note that $\sqrt{5} \in \mathbb{Z}_p$. Let $A_n = P_n(2\sqrt{(\sqrt{5}-2)})$ and $B_n = P_n(2\sqrt{(-\sqrt{5}-2)})$. It is not hard to prove that $\mathscr{A}(m, r) = A_{1/2(mp^r-1)}/A_{1/2(mp^{r-1}-1)} = C(m, r) + D(m, r)\sqrt{5}$ and $\mathscr{B}(m, r) = B_{1/2(mp^r-1)}/B_{1/2(mp^{r-1}-1)} = C(m, r) - D(m, r)\sqrt{5}$, for rationals $C(m, r)$ and $D(m, r)$. By the theorem we have the congruences

$$A_{1/2(mp^r-1)} \equiv \varepsilon_\alpha^{mp^{r-1}} \cdot \bar{\pi} \cdot A_{1/2(mp^{r-1}-1)} \bmod \pi^{2r}.$$

and

$$B_{1/2(mp^r-1)} \equiv \varepsilon_\beta^{mp^{r-1}} \cdot \bar{\pi} \cdot B_{1/2(mp^{r-1}-1)} \bmod \pi^{2r}.$$

We calculate that $\varepsilon_\alpha = i^b$ and $\varepsilon_\beta = (-i)^b$. Hence we have

(i) If b is even then $D(m, r) \equiv 0 \bmod p^{2r}$ and $C(m, r) \equiv \varepsilon_\alpha \cdot \bar{\pi} \bmod \pi^{2r}$.

(ii) If b is odd then $C(m, r) \equiv 0 \bmod p^{2r}$ and $D(m, r)\sqrt{5} \equiv \varepsilon_\beta^{mp^{r-1}} \cdot \bar{\pi} \bmod \pi^{2r}$.

Similar phenomena appear in the cases that $\tau_\beta = \frac{1}{2}(1+\sqrt{(-13)})$, $\frac{1}{2}(1+\sqrt{(-37)})$, $\frac{1}{2}(1+3i)$ $\frac{1}{2}(1+5i)$, $\frac{1}{2}\sqrt{-6}$, $\frac{1}{2}\sqrt{-10}$, $\frac{1}{2}\sqrt{-18}$, $\frac{1}{2}\sqrt{-22}$, and $\frac{1}{2}\sqrt{-58}$. The related supercongruences can be deduced from Table IVa and IVb.

4.3 *Tables IVa and IVb*

Tables IVa and IVb are due to Weber (see [26, pp. 113–114 and Table VI]). Nevertheless we give a review of his results because his notation is different from ours. We give, without proof, the connection between the two notations in the following lemma:

TABLE IVa

d	$f_1^{24}(\sqrt{(-d)})$	τ	$A/\sqrt{\Delta}$
2	64	$\frac{1}{2}\sqrt{(-2)}$	$\sqrt{2}$
4	512	$\frac{1}{2}i$	$3\sqrt{2}/4$
4	512	i	3
6	$(4+2\sqrt{2})^4$	$\sqrt{(-6)}/6$	$\sqrt{12}-\sqrt{6}$
6	$(4+2\sqrt{2})^4$	$\sqrt{(-6)}/2$	$\sqrt{12}+\sqrt{6}$
10	$(\frac{1}{2}(\sqrt{10}+\sqrt{5}))^{12}$	$\sqrt{(-10)}/10$	$3(\sqrt{10}-2\sqrt{2})$
10	$(\frac{1}{2}(\sqrt{10}+\sqrt{5}))^{12}$	$\sqrt{(-10)}/2$	$3(\sqrt{10}+2\sqrt{2})$
18	$4\cdot(2+\sqrt{6})^8$	$\sqrt{(-18)}/18$	$2(5-2\sqrt{6})\cdot\sqrt{(10\sqrt{6})}$
18	$4\cdot(2+\sqrt{6})^8$	$\sqrt{(-18)}/2$	$2(5+2\sqrt{6})\cdot\sqrt{(10\sqrt{6})}$
22	$64\cdot(1+\sqrt{2})^{12}$	$\sqrt{(-22)}/22$	$3\sqrt{22}\cdot(7+5\sqrt{2})$
22	$64\cdot(1+\sqrt{2})^{12}$	$\sqrt{(-22)}/2$	$3\sqrt{22}\cdot(-7+5\sqrt{2})$
58	$(5+\sqrt{29})^{12}/64$	$\sqrt{(-58)}/58$	$99(70+13\sqrt{29})\cdot\sqrt{2}$
58	$(5+\sqrt{29})^{12}/64$	$\sqrt{(-58)}/2$	$99(-70+13\sqrt{29})\cdot\sqrt{2}$

TABLE IVb

d	$f^{24}(\sqrt{(-d)})$	τ	$A/\sqrt{\Delta}$
1	64	$-\frac{1}{2}+\frac{1}{2}i$	0
3	256	$-\frac{1}{4}+\frac{1}{4}\sqrt{(-3)}$	$\frac{1}{2}\sqrt{3}$
3	256	$\frac{1}{2}+\frac{1}{2}\sqrt{(-3)}$	$\sqrt{(-3)}$
5	$(1+\sqrt{5})^6$	$(-1+\sqrt{(-5)})/6$	$2\sqrt{(\sqrt{5}-2)}$
5	$(1+\sqrt{5})^6$	$(1+\sqrt{(-5)})/2$	$2\sqrt{(-\sqrt{5}-2)}$
7	4096	$(-1+\sqrt{(-7)})/8$	$3\sqrt{7}/8$
7	4096	$(1+\sqrt{(-7)})/2$	$3\sqrt{(-7)}$
9	$4\cdot(1+\sqrt{3})^8$	$(-1+3i)/10$	$2\sqrt{(14\sqrt{3}-24)}$
9	$4\cdot(1+\sqrt{3})^8$	$(1+3i)/2$	$2\sqrt{(-14\sqrt{3}-24)}$
13	$(3+\sqrt{13})^6$	$(-1+\sqrt{(-13)})/14$	$6\sqrt{(5\sqrt{13}-18)}$
13	$(3+\sqrt{13})^6$	$(1+\sqrt{(-13)})/2$	$6\sqrt{(-5\sqrt{13}-18)}$
15	$16\cdot(1+\sqrt{5})^8$	$(-1+\sqrt{-15})/16$	$(7+\sqrt{5})\cdot\sqrt{3}/16$
15	$16\cdot(1+\sqrt{5})^8$	$(1+\sqrt{-15})/2$	$(16+7\sqrt{5})\cdot\sqrt{-3}$
25	$(1+\sqrt{5})^{24}/2^{18}$	$(-1+5i)/26$	$12(9-4\sqrt{5})\cdot 5^{1/4}$
25	$(1+\sqrt{5})^{24}/2^{18}$	$(1+5i)/2$	$-12(9+4\sqrt{5})\cdot(-5)^{1/4}$
37	$64\cdot(6+\sqrt{37})^6$	$(-1+\sqrt{(-37)})/38$	$42(\sqrt{37}-6)\sqrt{(\sqrt{37}-6)}$
37	$64\cdot(6+\sqrt{37})^6$	$(1+\sqrt{(-37)})/2$	$42(-\sqrt{37}-6)\sqrt{(-\sqrt{37}-6)}$

LEMMA 4.1. *Let* $f(\tau)$ *and* $f_1(\tau)$ *be Weber-functions* (*cf.* [26, *pp.* 113–114]). *With the notation* $F=f^{24}(\tau)$ *and* $F_1=f_1^{24}(\tau)$, *we have*

$$\text{(i)} \quad \frac{A}{\sqrt{\Delta}}\left(-\frac{1}{\tau}\right)=\sqrt{(1+64/F_1)},$$

$$\text{(ii)} \quad \frac{A}{\sqrt{\Delta}}\left(\frac{1}{2}\tau\right)=\sqrt{(1+F_1/64)},$$

$$\text{(iii)} \quad \frac{A}{\sqrt{\Delta}}\left(\frac{1}{1-\tau}\right)=\sqrt{(1-64/F)},$$

$$\text{(iv)} \quad \frac{A}{\sqrt{\Delta}}\left(\frac{1}{2}(\tau-1)\right)=\sqrt{(1-F/64)}.$$

Proof. See [12, p. 96].

ACKNOWLEDGMENTS

The authors thank F. Beukers and R. Tijdeman for reading an earlier version of the paper and for suggesting many improvements. We are grateful to the referee for his critical but constructive remarks.

REFERENCES

1. K. ABRAMOWITZ AND I. A. STEGUN, "Handbook of Mathematical Functions," Dover, New York, 1970.
2. K. ALLADI AND M. L. ROBINSON, On certain values of the logarithm, *in* "Lecture Notes," Vol. 751, pp. 1–9.
3. A. O. L. ATKIN AND H. P. F. SWINNERTON-DYER, Modular forms on noncongruence subgroups, *Proc. Sympos. Pure Math.* **19** (1971), 1–25.
4. W. E. H. BERWICK, Modular invariants expressible in terms of quadratic and cubic irrationals, *Proc. London Math. Soc.* **28** (1928), 53–69.
5. F. BEUKERS, Some congruences for the Apéry numbers, *J. Number Theory* **21** (1985), 141–150.
6. F. BEUKERS, Another congruence for the Apéry numbers, *J. Number Theory* **25** (1987), 201–210.
7. F. BEUKERS, Congruence properties of coefficients of solutions of Picard–Fuchs equations, *in* "Groupe d'étude, d'analyse ultramétrique" (G. Christol, Ed.), Paris VI, to appear.
8. F. BEUKERS AND J. STIENSTRA, On the Picard–Fuchs equation and the formal Brauer group of certain elliptic *K*3-surfaces, *Math. Ann.* **271** (1985), 293–304.
9. L. CARLITZ, Advanced problem 4628, *Amer. Math. Monthly* **62** (1955), 186; **63** (1956), 348–350.
10. S. CHOWLA, J. COWLES, AND M. COWLES, Congruence properties of Apéry numbers, *J. Number Theory* **12** (1980), 188–190.
11. S. CHOWLA, B. DWORK, AND R. J. EVANS, On the mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$, *J. Number Theory* **24** (1986), 188–196.

12. M. J. COSTER, "Supercongruences," Thesis, Univ. of Leiden, Holland, 1988.
13. M. J. COSTER, Supercongruences, *in* "Proceedings Conference on *p*-Adic Analysis, Trento, Italy, 1989," to appear.
14. G. EISENSTEIN, "Mathematische Werke, Band I," Chelsea, New York, 1975.
15. C. F. GAUSS, "Arithmetische Untersuchungen (Disquisitiones Arithmeticae)," Chelsea, New York, 1965.
16. I. GESSEL, Some congruences for Apéry numbers, *J. Number Theory* **14** (1982), 362–368.
17. L. VAN HAMME, The *p*-adic gamma function and congruences of Atkin and Swinnerton-Dyer, *in* "Groupe d'étude d'analyse ultramétrique," 9e année 81/82, Fasc. 3 no. J17-6p. Paris, 1982.
18. L. VAN HAMME, Proof of a conjecture of Beukers on Apéry numbers, *in* "Proceedings of the Conference of *p*-adic Analysis, Hengelhoef, Belgium, 1986," pp. 189–195, 1986.
19. M. HAZEWINKEL, "Formal Groups and Applications," Academic Press, New York, 1978.
20. A. HURWITZ AND R. COURANT, "Functionentheorie," 4th ed., Springer-Verlag, Berlin, 1964.
21. D. HUSEMÖLLER, "Elliptic Curves," Springer-Verlag, New York, 1987.
22. K. IRELAND AND M. ROSEN, "A Classical Introduction to Modern Number Theory," Springer-Verlag, New York, 1982.
23. S. LANG, "Elliptic Curves," Addison-Wesley, Reading, MA, 1973.
24. D. MUMFORD, "Tata Lectures on Theta 1, Progress, in Math.," Vol. 28, Birkhäuser, Boston, 1983.
25. J. H. SILVERMAN, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1986.
26. H. WEBER, "Lehrbuch der Algebra, dritter Band," Vieweg, Braunschweig, 1908.
27. E. T. WHITTAKER AND G. N. WATSON, "A Course of Modern Analysis," 4th ed., Cambridge Univ. Press, London, 1940.