ACTA ARITHMETICA
LXVIII.1 (1994)

On $x^3 + y^3 + z^3 = 3\mu xyz$ and Jacobi polynomials

by

Kaori Ota (Tokyo)

We consider the elliptic curve given by

$$x^3 + y^3 + z^3 = 3\mu xyz$$

over various fields. Theorem 1 gives the connection between an invariant differential form ω on this curve and Jacobi polynomials with some arguments. More precisely, Jacobi polynomials are given by coefficients of the power series expansion of ω at a basepoint with respect to some local parameter. This is quite analogous to the Jacobi quartic case (cf. [8]), where Legendre polynomials appear. We denote polynomials appearing as coefficients of ω by B_n.

As holomorphic differential 1-forms are unique up to constants, we obtain congruences for B_n by using the Cartier operator for complete irreducible smooth algebraic curves over algebraically closed fields of positive characteristic (Theorem 3). From the characteristic polynomial of the Frobenius map together with Honda theory, we obtain congruences for B_n modulo higher powers (Theorem 4). Also finding the special element for a formal group associated with some part of ω gives Theorem 5 (cf. [5]).

Theorems 1 and 2 are given in Section 1, whereas Theorems 3–5, concerning congruences for B_n, are in Section 2.

1. Let K be a field of characteristic different from 3 and $\mu \in \overline{K}$, the algebraic closure of K, and let E_μ be the curve in $\mathbb{P}^2(\overline{K})$ given by

$$x^3 + y^3 + z^3 - 3\mu xyz = 0. \tag{1.1}$$

E_μ is non-singular and gives an elliptic curve if $\mu^3 \neq 1$. Here we take $O = [0, -1, 1]$ as the origin for E_μ. Then

$$\omega = \frac{dx}{y^2 - \mu x}$$

is a holomorphic differential 1-form and thus is an invariant differential form on E_μ. x is a local parameter at O. In the affine space $z=1$, (1.1) becomes

(1.2)
$$x^3+y^3+1-3\mu xy=0.$$

The hypergeometric function ${}_2F_1$ is defined by

$${}_2F_1\left(\begin{matrix}\alpha\,,\,\beta\\ \gamma\end{matrix}\;;X\right)=\sum_{n=0}^{\infty}\frac{(\alpha)_n(\beta)_n}{(\gamma)_n n!}X^n,$$

where $(\theta)_n=\theta(\theta+1)\ldots(\theta+n-1)$ for $n>0$ and $(\theta)_0=1$.

THEOREM 1. *Let E_μ be defined over $K=\mathbb{Q}(\mu)$ with $\mu\in\mathbb{C}$, $\mu^3\neq 1$, and let ω have the power series expansion at O with respect to x as*

$$\omega=\sum_{n=0}^{\infty}b_n x^n\,dx.$$

Then

$$\begin{cases} b_{3n}=\gamma_n\cdot{}_2F_1\left(\begin{matrix}-n\,,\,n+\frac{2}{3}\\ \frac{2}{3}\end{matrix}\;;\mu^3\right) & \textit{with } \gamma_n=\dfrac{(-1)^n(\frac{2}{3})_n}{n!},\\ b_{3n+1}=\tau_n\cdot\mu\cdot{}_2F_1\left(\begin{matrix}-n\,,\,n+\frac{4}{3}\\ \frac{4}{3}\end{matrix}\;;\mu^3\right) & \textit{with } \tau_n=\dfrac{(-1)^{n+1}(\frac{4}{3})_n}{n!},\\ b_{3n+2}=0 \quad \textit{for any } n\geq 0. \end{cases}$$

Proof. Set

$$f=\frac{1}{y^2-\mu x},\qquad\text{so}\qquad y^2=\mu x+\frac{1}{f}.$$

Then from (1.2) we have

$$y=\frac{-(1+x^3)f}{1-2\mu xf}.$$

Hence

$$\left(\frac{-(1+x^3)f}{1-2\mu xf}\right)^2=\mu x+\frac{1}{f},$$

from which we get

(1.3)
$$\{1+2x^3(1-2\mu^3)+x^6\}\,f^3=-3\mu xf+1.$$

We now solve (1.3) for f. Let $f(x)=\sum_{n=0}^{\infty}b_n x^n$. Then we know that $b_0=f(0)=1$ and from (1.3),

$$\sum_{n=0}^{\infty}\Big(\sum_{i+j+k=n}b_ib_jb_k\Big)x^n+2(1-2\mu^3)\sum_{n=0}^{\infty}\Big(\sum_{i+j+k=n}b_ib_jb_k\Big)x^{n+3}$$
$$+\sum_{n=0}^{\infty}\Big(\sum_{i+j+k=n}b_ib_jb_k\Big)x^{n+6}=-3\mu\sum_{n=0}^{\infty}b_nx^{n+1}+1.$$

By comparing the coefficients of x^n in both sides, we can determine b_n for any $n \geq 0$ inductively. Thus (1.3) together with $b_0 = 1$ determines f completely.

Set

$$(1.4)\qquad g(x) = \frac{1}{\sqrt{S}}\left\{\left(\frac{\sqrt{S}+x^3+1}{2}\right)^{1/3} - \mu x\left(\frac{2}{\sqrt{S}+x^3+1}\right)^{1/3}\right\},$$

where $S = 1+2x^3(1-2\mu^3)+x^6$. As S takes 1 as x tends to 0, we take principal values $|\mathrm{Im}(\log z)| < \pi$ for the logarithm in $\sqrt{S}$, and also in $((\sqrt{S}+x^3+1)/2)^{1/3}$ and $(2/(\sqrt{S}+x^3+1))^{1/3}$, for $(\sqrt{S}+x^3+1)/2$ and $2/(\sqrt{S}+x^3+1)$ both take 1 as x tends to 0. With this choice, g is an analytic function around $x = 0$. We have

$$\begin{aligned} Sg^3 &= \frac{1}{\sqrt{S}}\left\{\left(\frac{X}{2}\right)^{1/3} - \mu x\left(\frac{2}{X}\right)^{1/3}\right\}^3 \qquad \text{with } X = \sqrt{S}+x^3+1 \\ &= -3\mu x g + 1. \end{aligned}$$

Since $g(0) = 1$, we get $g = f$ around $x = 0$.

Now g has the following power series expansion near 0 (cf. (16) on p. 170 and (29) on p. 172 of [1]):

$$\frac{1}{\sqrt{S}}\left(\frac{\sqrt{S}+x^3+1}{2}\right)^{1/3} = \sum_{n=0}^{\infty} \frac{(\frac{2}{3})_n \cdot {}_2F_1\left(\begin{matrix} -n, n+\frac{2}{3} \\ \frac{2}{3} \end{matrix}; \mu^3\right)}{n!}(-x)^{3n},$$

$$\frac{1}{\sqrt{S}}\left(\frac{2}{\sqrt{S}+x^3+1}\right)^{1/3} = \sum_{n=0}^{\infty} \frac{(\frac{4}{3})_n \cdot {}_2F_1\left(\begin{matrix} -n, n+\frac{4}{3} \\ \frac{4}{3} \end{matrix}; \mu^3\right)}{n!}(-x)^{3n},$$

and by (1.4) we have

$$\begin{aligned} g(x) = \sum_{n=0}^{\infty} \gamma_n \cdot {}_2F_1\left(\begin{matrix} -n, n+\frac{2}{3} \\ \frac{2}{3} \end{matrix}; \mu^3\right)x^{3n} \\ + \sum_{n=0}^{\infty} \tau_n \cdot \mu \cdot {}_2F_1\left(\begin{matrix} -n, n+\frac{4}{3} \\ \frac{4}{3} \end{matrix}; \mu^3\right)x^{3n+1}, \end{aligned}$$

from which the theorem follows. ∎

Remarks. 1. For a non-negative integer $n, j > 0$ and $i - j > -1$, set

$$G_n(i,j,x) = {}_2F_1\left(\begin{matrix} -n\,,\ i+n \\ j \end{matrix}; x\right).$$

G_n is called the *Jacobi polynomial*. It satisfies the following second order differential equation:

$$(1.5)\qquad x(1-x)G_n'' + (j-(i+1)x)G_n' + (i+n)nG_n = 0.$$

It is known that G_n is the unique entire rational solution. Furthermore, $\{G_n(i,j,\cdot)\}_{n\in\mathbb{N}\cup\{0\}}$ form an orthonormal system of polynomials in [0,1] with respect to the inner product

$$\langle f,g\rangle=\int_0^1 f(x)g(x)x^{j-1}(1-x)^{i-j}\,dx$$

(cf. [2]). Legendre polynomials are Jacobi polynomials:

$$P_n(x)=G_n\left(1,1,\frac{1-x}{2}\right)={}_2F_1\left(\begin{matrix}n+1,-n\\1\end{matrix};\frac{1-x}{2}\right).$$

P_n are also defined as

$$\begin{cases} P_{2n}(x)=\dfrac{(-1)^n(\frac12)_n}{n!}\cdot{}_2F_1\left(\begin{matrix}-n,n+\frac12\\ \frac12\end{matrix};x^2\right),\\ P_{2n+1}(x)=\dfrac{(-1)^n(\frac32)_n}{n!}\,x\cdot{}_2F_1\left(\begin{matrix}-n,n+\frac32\\ \frac32\end{matrix};x^2\right).\end{cases}$$

P_n satisfies the following differential equation:

$$(1-x^2)P_n''-2xP_n'+n(n+1)P_n=0. \tag{1.6}$$

These Legendre polynomials appear as coefficients of the power series expansion of the invariant differential

$$\omega=\frac{dx}{y}=\frac{dx}{\sqrt{1-2\varrho x^2+x^4}}=\sum_{n=0}^{\infty}P_n(\varrho)x^{2n}dx$$

for the Jacobi quartic $y^2=1-2\varrho x^2+x^4$ (cf. [8]). Theorem 1 gives an analogous result. Thus we define polynomials B_n by

$$\begin{cases} B_{3n}(x)=\dfrac{(-1)^n(\frac23)_n}{n!}\cdot{}_2F_1\left(\begin{matrix}-n,n+\frac23\\ \frac23\end{matrix};x^3\right)=\gamma_nG_n(\tfrac23,\tfrac23,x^3),\\ B_{3n+1}(x)=\dfrac{(-1)^{n+1}(\frac43)_n}{n!}\,x\cdot{}_2F_1\left(\begin{matrix}-n,n+\frac43\\ \frac43\end{matrix};x^3\right)=\tau_n\,x\,G_n(\tfrac43,\tfrac43,x^3),\\ B_{3n+2}(x)=0\quad\text{for } n\ge 0.\end{cases}$$

(We need the last definition only to simplify our statements.) The first few polynomials are

$$\begin{gathered} B_0(x)=1,\quad B_1(x)=-x,\quad B_2(x)=0,\quad B_3(x)=-\tfrac23+\tfrac53x^3,\\ B_4(x)=\tfrac43x-\tfrac73x^4,\quad B_5(x)=0,\quad B_6(x)=\tfrac59-\tfrac{40}{9}x^3+\tfrac{44}{9}x^6.\end{gathered}$$

From the differential equation (1.5) for G_n, we can find the differential equation for B_m with $m\not\equiv 2 \pmod 3$:

$$(1-x^3)B_m''-3x^2B_m'+m(m+2)xB_m=0.$$

(For $m \equiv 2 \pmod 3$), this equation does not have a polynomial solution.) Notice the similarity of this to (1.6).

From the identity (cf. (16) on p. 170 of [1])

$$(1.7)\qquad \binom{n+\alpha}{n}\cdot {}_2F_1\left(\begin{matrix}-n, n+\alpha+\beta+1\\ \alpha+1\end{matrix};\frac{1-x}{2}\right) = (-1)^n\binom{n+\beta}{n}\cdot {}_2F_1\left(\begin{matrix}-n, n+\alpha+\beta+1\\ \beta+1\end{matrix};\frac{1+x}{2}\right),$$

by taking $(\alpha,\beta)=(-\frac{1}{3},0)$ and also $(\alpha,\beta)=(\frac{1}{3},0)$ we obtain a simpler expression for B_n:

$$\begin{cases} B_{3n}(x) = {}_2F_1\left(\begin{matrix}-n, n+\frac{2}{3}\\ 1\end{matrix}; 1-x^3\right) = G_n(\frac{2}{3},1,1-x^3),\\ B_{3n+1}(x) = -x\cdot {}_2F_1\left(\begin{matrix}-n, n+\frac{4}{3}\\ 1\end{matrix}; 1-x^3\right) = -x\,G_n(\frac{4}{3},1,1-x^3).\end{cases}$$

2. For any $n \ge 0$,

$$B_n(x)\in \mathbb{Z}[1/3][x] \quad\text{and}\quad \deg B_n(x)=n \quad \text{if } n\not\equiv 2 \pmod 3.$$

The assertion on the degree of B_n is clear from the expressions for b_n in Theorem 1. So we only have to show that B_n has coefficients in $\mathbb{Z}[1/3]$.

From (1.2), by setting $Y=y+1$ we have

$$\begin{aligned} Y &= -\mu x+\mu xY+Y^2-\tfrac{1}{3}x^3-\tfrac{1}{3}Y^3\\ &= -\mu x+\mu x(-\mu x+\mu xY-\tfrac{1}{3}x^3+Y^2-\tfrac{1}{3}Y^3)\\ &\quad +(-\mu x+\mu xY-\tfrac{1}{3}x^3+Y^2-\tfrac{1}{3}Y^3)^2-\tfrac{1}{3}x^3-\tfrac{1}{3}Y^3\\ &= -\mu x+\ldots\in\mathbb{Z}[1/3][\mu][[x]].\end{aligned}$$

So

$$\omega=\frac{dx}{y^2-\mu x}=\frac{dx}{Y^2-2Y+1-\mu x}=\frac{dx}{1+\mu x+\ldots}\in\mathbb{Z}[1/3][\mu][[x]]\,dx.$$

Hence $B_n(\mu)\in\mathbb{Z}[1/3][\mu]$.

The following theorem gives an analogous statement to Theorem 4.1 on p. 140 of [7]. This may be known but it does not seem to appear anywhere in the literature.

THEOREM 2. *Let K be a finite field of characteristic $p\neq 3$. Set*

$$H(t)=\begin{cases}\displaystyle\sum_{n=0}^{(p-1)/3}\frac{(\frac{1}{3})_n(\frac{1}{3})_n}{(\frac{2}{3})_n n!}t^{3n} & \text{if } p\equiv 1 \pmod 3,\\ \displaystyle t\sum_{n=0}^{(p-2)/3}\frac{(\frac{2}{3})_n(\frac{2}{3})_n}{(\frac{4}{3})_n n!}t^{3n} & \text{if } p\equiv 2 \pmod 3.\end{cases}$$

Then

1. *For* $\mu \in \overline{K}$ *with* $\mu^3 \neq 1$, E_μ *is supersingular if and only if* $H(\mu) = 0$.
2. $H(t)$ *has distinct roots in* $\overline{K}$.

Proof. 1. Set

$$h = x^3 + y^3 + z^3 - 3\mu xyz. \tag{1.8}$$

Then

$$\begin{aligned} E_\mu \text{ is supersingular } &\Leftrightarrow \text{the Hasse invariant} = 0 \\ &\Leftrightarrow \text{the coefficient of } (xyz)^{p-1} \text{ in } h^{p-1} = 0 \end{aligned}$$

(cf. Proposition 4.21 on p. 332 of [3]).

(a) For $p \equiv 1 \pmod 3$, write $p = 3k+1$. Then the coefficient of $(xyz)^{p-1}$ in h^{p-1} is

$$\sum_{n=0}^{k} \binom{3k}{k-n}\binom{2k+n}{k-n}\binom{k+2n}{k-n}(-3)^{3n}\mu^{3n}.$$

Hence it suffices to find an integer $c_k \not\equiv 0 \pmod p$ independent of n satisfying

$$\binom{3k}{k-n}\binom{2k+n}{k-n}\binom{k+2n}{k-n}(-3)^{3n} \equiv c_k \frac{(\frac{1}{3})_n(\frac{1}{3})_n}{(\frac{2}{3})_n n!} \pmod p.$$

Now

$$\begin{aligned} (k-n)! \cdot 3^{k-n} &= (3k-3n)(3k-3(n+1))\ldots(3k-3(k-1)) \\ &\equiv (-1-3n)(-1-3(n+1))\ldots(-1-3(k-1)) \pmod p \\ &\equiv (-1)^{k-n}(3n+1)(3n+4)\ldots(3k-2) \pmod p. \end{aligned}$$

Hence

$$(k-n)! \equiv \frac{(-1)^{k-n}\{1\cdot 4\cdot 7\cdot \ldots \cdot (3k-2)\}}{3^{k-n}\{1\cdot 4\cdot 7\cdot \ldots \cdot (3n-2)\}} \pmod p.$$

So

$$\begin{aligned} \binom{3k}{k-n}\binom{2k+n}{k-n}\binom{k+2n}{k-n}(-3)^{3n} &= \frac{(3k)!(-3)^{3n}}{\{(k-n)!\}^3(3n)!} \\ &\equiv \frac{(3k)!3^{3(k-n)}\{1\cdot 4\cdot \ldots \cdot (3n-2)\}^3(-3)^{3n}}{(-1)^{3(k-n)}\{1\cdot 4\cdot 7\cdot \ldots \cdot (3k-2)\}^3(3n)!} \pmod p \\ &\equiv \frac{-1}{\{1\cdot 4\cdot \ldots \cdot (3k-2)\}^3}\frac{(\frac{1}{3})_n(\frac{1}{3})_n}{(\frac{2}{3})_n n!} \pmod p, \end{aligned}$$

as k is even, $(3k)! \equiv -1$ and $3^{3k} \equiv 1 \pmod p$. Thus we take

$$c_k = \frac{-1}{\{1\cdot 4\cdot \ldots \cdot (3k-2)\}^3}.$$

(b) For $p \equiv 2 \pmod 3$, write $p=3k+2$. Then the coefficient of $(xyz)^{p-1}$ in h^{p-1} is

$$\mu\sum_{n=0}^{k}\binom{3k+1}{k-n}\binom{2k+n+1}{k-n}\binom{k+2n+1}{k-n}(-3)^{3n+1}\mu^{3n}.$$

Now

$$\begin{aligned}(k-n)!\cdot 3^{k-n} &= (3k-3n)(3k-3(n+1))\dots(3k-3(k-1))\\ &\equiv (-1)^{k-n}(3n+2)(3n+5)\dots(3k-1) \pmod p.\end{aligned}$$

Hence

$$(k-n)! \equiv \frac{(-1)^{k-n}\{2\cdot 5\cdot\ldots\cdot(3k-1)\}}{3^{k-n}\{2\cdot 5\cdot\ldots\cdot(3n-1)\}} \pmod p.$$

So for $k>0$,

$$\begin{aligned}&\binom{3k+1}{k-n}\binom{2k+n+1}{k-n}\binom{k+2n+1}{k-n}(-3)^{3n+1}\\ &\quad= \frac{(3k+1)!\,(-3)^{3n+1}}{\{(k-n)!\}^3(3n+1)!}\\ &\quad\equiv \frac{-(-3)^{3n+1}3^{3(k-n)}\{2\cdot 5\cdot\ldots\cdot(3n-1)\}^3}{(-1)^{3(k-n)}\{2\cdot 5\cdot\ldots\cdot(3k-1)\}^3\,(3n+1)!} \pmod p\\ &\quad\equiv \frac{-1}{\{2\cdot 5\cdot\ldots\cdot(3k-1)\}^3}\,\frac{(\frac{2}{3})_n(\frac{2}{3})_n}{(\frac{4}{3})_n n!} \pmod p,\end{aligned}$$

as k is odd, $(3k+1)! \equiv -1$ and $3^{3k+1} \equiv 1 \pmod p$.

So for $k>0$, we take

$$c_k = \frac{-1}{\{2\cdot 5\cdot\ldots\cdot(3k-1)\}^3}.$$

For $k=0$, i.e. for $p=2$, the coefficient of xyz in h is -3μ. Hence E_μ is supersingular if and only if $H(\mu)=\mu\neq 0$.

2. In both cases $p\equiv 1$ and $2 \pmod 3$, H satisfies the following differential equation:

$$(1.9)\qquad (1-t^3)H''-3t^2H'-tH=0.$$

This can be checked by direct computation.

Suppose that H has a multiple root $t=\mu_0$. Then $H(\mu_0)=H'(\mu_0)=0$. Hence $(1-\mu_0^3)H''(\mu_0)=0$. So if $\mu_0^3\neq 1$, then $H''(\mu_0)=0$. By taking the derivative of (1.9), we can show that $H'''(\mu_0)=0$ if $\mu_0^3\neq 1$. By repeating this process, we arrive at $H^{(n)}(\mu_0)=0$ for any $n\geq 0$, which is a contradiction. Hence we only have to show that

$$H(\mu)\neq 0 \quad \text{for } \mu^3=1.$$

Suppose that $p = 3k+1$. Then $k \equiv -\frac{1}{3} \pmod{p}$, so for $\mu^3 = 1$

$$\begin{aligned} H(\mu) &\equiv {}_2F_1\left(\begin{matrix} -k, k+\frac{2}{3} \\ \frac{2}{3} \end{matrix}\,;1\right) \pmod{p} \\ &= G_k(2/3, 2/3, 1). \end{aligned}$$

But from the proof of Theorem 1, we have the identity

$$\frac{1}{\sqrt{S}}\left(\frac{\sqrt{S}+x^3+1}{2}\right)^{1/3} = \sum_{n=0}^{\infty} \gamma_n G_n(2/3, 2/3, \mu^3) x^{3n}$$

with $S = 1 + 2x^3(1-2\mu^3) + x^6$.

For $\mu^3 = 1$, we have $S = (1-x^3)^2$. Hence

$$\frac{1}{1-x^3} = \sum_{n=0}^{\infty} x^{3n} = \sum_{n=0}^{\infty} \gamma_n G_n(2/3, 2/3, 1) x^{3n}.$$

So

$$\gamma_n G_n(2/3, 2/3, 1) = 1 \quad \text{for any } n \geq 0,$$

from which we get

$$G_k(2/3, 2/3, 1) = \frac{1}{\gamma_k} \not\equiv 0 \pmod{p}.$$

(Or we can use the identity (1.7) for $(\alpha, \beta) = (-1/3, 0)$ by substituting $x = -1$.)

Similarly for $p = 3k+2$,

$$\begin{aligned} H(\mu) &\equiv \mu \cdot {}_2F_1\left(\begin{matrix} -k, k+\frac{4}{3} \\ \frac{4}{3} \end{matrix}\,;1\right) \pmod{p} \\ &= \mu G_k(4/3, 4/3, 1). \end{aligned}$$

Since

$$\frac{1}{\sqrt{S}}\left(\frac{2}{\sqrt{S}+x^3+1}\right)^{1/3} = -\sum_{n=0}^{\infty} \tau_n G_n(4/3, 4/3, \mu^3) x^{3n},$$

we get

$$\frac{1}{1-x^3} = \sum_{n=0}^{\infty} x^{3n} = -\sum_{n=0}^{\infty} \tau_n G_n(4/3, 4/3, 1) x^{3n}.$$

Hence

$$\mu G_k(4/3, 4/3, 1) = \frac{-\mu}{\tau_k} \not\equiv 0 \pmod{p}.$$

(Or we can use the identity (1.7) for $(\alpha, \beta) = (1/3, 0)$ by substituting $x = -1$ as before.) ∎

Remark. Let $\mathbb{Z}_p$ be the ring of p-adic integers. If we denote the coefficient of $(xyz)^{p-1}$ in h^{p-1} by $\Lambda(\mu)$, then for $p\neq 3$, as polynomials in $\mathbb{Z}_p[\mu]$,

$$\Lambda(\mu)\equiv B_{p-1}(\mu)\pmod p.$$

Proof. With c_k in the proof of Theorem 2, we have

$$\Lambda(\mu)\equiv\begin{cases} c_k\cdot {}_2F_1\left(\begin{matrix}-k,k+\frac{2}{3}\\ \frac{2}{3}\end{matrix};\mu^3\right)\pmod p & \text{for } p=3k+1,\\ c_k\cdot\mu\cdot {}_2F_1\left(\begin{matrix}-k,k+\frac{4}{3}\\ \frac{4}{3}\end{matrix};\mu^3\right)\pmod p & \text{for } p=3k+2>2.\end{cases}$$

Hence it suffices to show that

$$c_k\equiv\begin{cases}\gamma_k\pmod p & \text{for } p=3k+1,\\ \tau_k\pmod p & \text{for } p=3k+2.\end{cases}$$

For $p=3k+1$,

$$\begin{aligned}\gamma_k&=\frac{(-1)^k(\frac{2}{3})_k}{k!}=\frac{(-1)^k(3k)!}{3^{2k}(k!)^2\{1\cdot 4\cdot 7\cdot\ldots\cdot(3k-2)\}}\\ &\equiv\frac{-(-1)^k}{\{1\cdot 4\cdot 7\cdot\ldots\cdot(3k-2)\}^3}\equiv c_k\pmod p\end{aligned}$$

as k is even.

For $p=3k+2$ and $k>0$,

$$\begin{aligned}\tau_k&=\frac{(-1)^{k+1}(\frac{4}{3})_k}{k!}=\frac{(3k+1)!}{3^{2k}(k!)^2\{2\cdot 5\cdot\ldots\cdot(3k-1)\}}\\ &\equiv\frac{-1}{\{2\cdot 5\cdot\ldots\cdot(3k-1)\}^3}\equiv c_k\pmod p\end{aligned}$$

as k is odd.

For $p=2$,

$$\Lambda(\mu)=-3\mu\equiv B_1(\mu)\pmod 2.\ \blacksquare$$

2. In this section we obtain congruences for B_n by using the Cartier operator and Honda theory.

THEOREM 3. *Let p be a prime different from 3. For $m\geq 1$ and $n\geq 0$, as polynomials in $\mathbb{Z}_p[\mu]$ we have*

$$B_{mp^n-1}(\mu)\equiv B_{p-1}(\mu)B_{p-1}(\mu^p)\ldots B_{p-1}(\mu^{p^{n-1}})B_{m-1}(\mu^{p^n})\pmod p.$$

Proof. We proceed our proof as in [8]. We consider E_μ over $\overline{\mathbb{F}_p(\mu)}$ and let $\mathcal{C}$ be the Cartier operator (cf. [6]):

$$\mathcal{C}: H^0(E_\mu,\Omega^1)\to H^0(E_\mu,\Omega^1).$$

Let

$$\omega = \frac{dx}{y^2 - \mu x} = f dx.$$

Note that x is a local parameter at $O = [0, -1, 1]$. Then f can be written uniquely as $f = f_0^p + f_1^p x + \ldots + f_{p-1}^p x^{p-1}$. If we set $f_{p-1} = \sum_{n=0}^{\infty} a_n x^n$, then

$$(a_{k-1}(\mu))^p = B_{pk-1}(\mu) \quad \text{for any } k \geq 1. \tag{2.1}$$

Now

$$\mathcal{C}(\omega) = f_{p-1} dx = B_{p-1}^{1/p} f dx. \tag{2.2}$$

By comparing coefficients of x^{k-1} of f_{p-1} and $B_{p-1}^{1/p} f$, we get

$$a_{k-1} = B_{p-1}^{1/p} B_{k-1}.$$

Hence from (2.1),

$$B_{pk-1}(\mu) = B_{p-1}(\mu) B_{k-1}(\mu^p).$$

So for $m \geq 1$ and $n \geq 0$, we obtain

$$\begin{aligned} B_{mp^n-1}(\mu) &= B_{p-1}(\mu) B_{mp^{n-1}-1}(\mu^p) \\ &= B_{p-1}(\mu) B_{p-1}(\mu^p) B_{mp^{n-2}-1}(\mu^{p^2}) = \ldots \\ &= B_{p-1}(\mu) B_{p-1}(\mu^p) \ldots B_{p-1}(\mu^{p^{n-1}}) B_{m-1}(\mu^{p^n}). \ \blacksquare \end{aligned}$$

THEOREM 4. *Let p be a prime different from* 3 *and $\mu \in \mathbb{Z}_p$. Let $\overline{E}_\mu$ be $E_\mu \bmod p$ and assume that $\overline{E}_\mu$ is non-singular* (*i.e.* $\mu^3 \not\equiv 1 \pmod p$)*. Let $\xi(x) = x^p$ be the Frobenius map and denote the trace of ξ acting on the Tate module by* $\mathrm{Tr}(\xi)$. *Then*:

1. $\mathrm{Tr}(\xi) \equiv B_{p-1}(\mu) \pmod p$.
2. *For $n \geq 1$ and $m \geq 1$,*

$$B_{mp^n-1}(\mu) - \mathrm{Tr}(\xi) B_{mp^{n-1}-1}(\mu) + p B_{mp^{n-2}-1}(\mu) \equiv 0 \pmod{p^n},$$

where we set $B_{mp^{n-2}-1}(\mu) = 0$ for $n = 1$.

In particular, for $m \geq 1$

$$B_{pm-1}(\mu) \equiv B_{p-1}(\mu) B_{m-1}(\mu) \pmod p.$$

Proof. Set

$$f(x) = \sum_{n=1}^{\infty} \frac{B_{n-1}(\mu)}{n} x^n$$

and consider the formal group F with f as its transformer:

$$F(x, y) = f^{-1}(f(x) + f(y))$$

(cf. [4] for terminology). Then F gives the formal group of E_μ by taking $O = [0, -1, 1]$ as the origin and x as a local parameter at O. Since the equation (1.1) defines a smooth group scheme over $\mathbb{Z}_p$ and its formal completion along the unit section is $\mathrm{Spf}(\mathbb{Z}_p[[x]])$, this F is p-integral. Let $\overline{F} = F \pmod p$. Since ξ satisfies the equation

$$X^2 - \mathrm{Tr}(\xi)X + p = 0,$$

the induced map $\overline{\xi}$ on $\overline{F}$ also satisfies the same equation (cf. Theorem 7.4 on p. 92 of [7]). Hence

$$\begin{aligned} 0 &= (\overline{\xi}^2 - \mathrm{Tr}(\xi)\overline{\xi} + p)(x) \\ &= \overline{F}((\overline{\xi}^2 - \mathrm{Tr}(\xi)\overline{\xi})(x), [p]_*(x)) \\ &= \overline{F}(\overline{F}(x^{p^2}, [-\mathrm{Tr}(\xi)]_*(x^p)), [p]_*(x)), \end{aligned}$$

where for any $u \in \mathbb{Z}_p$, $[u](x) = f^{-1}(uf(x))$ gives an endomorphism of F and $[u]_*(x) = [u](x) \pmod p$. Hence

$$f^{-1}(f(x^{p^2}) - \mathrm{Tr}(\xi)f(x^p) + pf(x)) \equiv 0 \pmod p.$$

From Lemma (4.2) in [4],

$$f(x^{p^2}) - \mathrm{Tr}(\xi)f(x^p) + pf(x) \equiv 0 \pmod p.$$

From this, we have

$$\sum_{n=1}^{\infty} \frac{B_{n-1}}{n} x^{p^2 n} - \mathrm{Tr}(\xi) \sum_{n=1}^{\infty} \frac{B_{n-1}}{n} x^{pn} + p \sum_{n=1}^{\infty} \frac{B_{n-1}}{n} x^n \equiv 0 \pmod p.$$

By taking the coefficient of $x^{p^n m}$, we have

$$\frac{B_{p^{n-2}m-1}}{p^{n-2}m} - \mathrm{Tr}(\xi)\frac{B_{p^{n-1}m-1}}{p^{n-1}m} + p\,\frac{B_{p^n m-1}}{p^n m} \equiv 0 \pmod p.$$

Hence

$$B_{mp^n-1} - \mathrm{Tr}(\xi)B_{mp^{n-1}-1} + pB_{mp^{n-2}-1} \equiv 0 \pmod{p^n},$$

which proves the second statement.

For the first statement, we have, mod p,

$$\begin{aligned} \mathrm{Tr}(\xi) &= \mathrm{Tr}(\xi \text{ acting on } H^1(\overline{E}_\mu, \mathcal{O}_{\overline{E}_\mu})) \\ &= \text{the coefficient of } (xyz)^{p-1} \text{ in } h^{p-1} = B_{p-1} \end{aligned}$$

(cf. (1.8) for h and Remark after Theorem 2). ∎

THEOREM 5. *Suppose that p is a prime with $p \equiv 1 \pmod 3$. Then for $m \not\equiv 0 \pmod 3$ and $n \ge 1$, as polynomials in $\mathbb{Z}_p[\mu]$,*

$$B_{p^n m}(\mu) \equiv B_{p^{n-1}m}(\mu^p) \pmod{p^n}.$$

Proof. The proof goes exactly as in [5]. Let $\mathbb{Q}_p$ be the field of p-adic numbers and $K = \mathbb{Q}_p(\mu)$, and consider the Gaussian valuation on K, i.e.

for $f(\mu)=\sum_{i=0}^{n} a_i\mu^i \in \mathbb{Q}_p[\mu]$,

$$\nu(f) \stackrel{\text{def}}{=} \min\{\nu_p(a_i) \mid 0 \le i \le n\}$$

with the p-adic valuation of $\mathbb{Q}_p$ normalized by $\nu_p(p)=1$. Let $\mathcal{O}$ and $\mathcal{P}$ be the valuation ring and the maximal ideal of K, respectively. Then there exists an endomorphism σ of K such that

$$\alpha^\sigma \equiv \alpha^p \pmod{\mathcal{P}} \quad \text{for any } \alpha \in \mathcal{O}.$$

In particular, for $f(\mu)$ in $\mathbb{Q}_p[\mu]$,

$$(f(\mu))^\sigma = f(\mu^p).$$

Set

$$\begin{aligned} g'(x) &= \sum_{n=0}^{\infty} B_{3n+1}(\mu)x^{3n} = B_1(\mu) + B_4(\mu)x^3 + \dots \\ &= -\frac{\mu}{\sqrt{S}}\left(\frac{2}{\sqrt{S}+x^3+1}\right)^{1/3}, \end{aligned}$$

where $S = 1+2x^3(1-2\mu^3)+x^6$. Then by changing a variable from x to t with $x^3 = t^3(1-\mu^3t^3)/(1-t^3)$, we get

$$g'(x)dx = \frac{-\mu}{1-\mu^3t^3}\,dt \stackrel{\text{set}}{=} r'(t)dt.$$

Then

$$r(t) = -\sum_{n=0}^{\infty} \frac{\mu^{3n+1}}{3n+1} t^{3n+1},$$

and r is of type $(-\mu, p-T)$ in the terminology of [4]. From the next little lemma the transformation from x to t is given by

$$x = t + \ldots \in \mathbb{Z}_p[\mu][[t]].$$

So the formal group with $g(x)$ as its transformer is also of type $(-\mu, p-T)$ (cf. Proposition 2.5 in [4]). Thus

$$pg(x) - g^\sigma(x^p) \equiv 0 \pmod{p},$$

where for $u(x)=\sum_{n=0}^{\infty}\lambda_n x^n$ in $K[[x]]$,

$$u^\sigma(x) = \sum_{n=0}^{\infty} \lambda_n^\sigma x^n.$$

Hence for $p \equiv 1 \pmod 3$ and for $m \equiv 1 \pmod 3$,

$$p\,\frac{B_{p^n m}(\mu)}{p^n m} - \frac{B_{p^{n-1}m}(\mu^p)}{p^{n-1}m} \equiv 0 \pmod{p}.$$

For $m \equiv 2 \pmod 3$, as $p^n m \equiv p^{n-1}m \equiv 2 \pmod 3$ we have

$$B_{p^n m} = B_{p^{n-1}m} = 0. \ \blacksquare$$

LEMMA. *There exists a power series*

$$x = \sum_{n=1}^{\infty} d_n t^n = t + \ldots \in \mathbb{Z}_p[a][[t]]$$

satisfying $x^3 = t^3(1 - at^3)/(1 - t^3)$.

Proof. Set

$$x = \sum_{n=1}^{\infty} d_n t^n.$$

Then we can determine the d_n inductively to make them satisfy the given equation. ∎

Acknowledgements. The author would like to thank N. Yui who introduced her to the subject. Thanks are also due to M. Ohta for useful conversations during the preparation of this paper.

References

[1] H. Bateman, *Higher Transcendental Functions*, Vol. 2, McGraw-Hill, 1953.
[2] R. Courant and D. Hilbert, *Methods of Mathematical Physics*, Vol. 1, Interscience, 1953.
[3] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Math. 52, Springer, 1977.
[4] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan 22 (1970), 213–246.
[5] —, *Two congruence properties of Legendre polynomials*, Osaka J. Math. 13 (1976), 131–133.
[6] J. P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, in: Œuvres, Vol. 1, 38, 501–530.
[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106, Springer, 1986.
[8] N. Yui, *Jacobi quartics*, *Legendre polynomials and formal groups*, in: Elliptic Curves and Modular Forms in Algebraic Topology, Lecture Notes in Math. 1326, Springer, 1988, 182–215.

DEPARTMENT OF MATHEMATICS
TSUDA COLLEGE
KODAIRA TOKYO, 187 JAPAN
E-mail: OTA@TSUDA.AC.JP

Received on 24.11.1993 (2525)