Bull. Aust. Math. Soc. **92** (2015), 44–51
doi:10.1017/S0004972715000295

FORMAL GROUPS AND INVARIANT DIFFERENTIALS OF ELLIPTIC CURVES

MOHAMMAD SADEK

(Received 6 October 2014; accepted 7 March 2015; first published online 4 May 2015)

Abstract

In this paper, we find a power series expansion of the invariant differential ω_E of an elliptic curve E defined over $\mathbb{Q}$, where E is described by certain families of Weierstrass equations. In addition, we derive several congruence relations satisfied by the trace of the Frobenius endomorphism of E.

2010 *Mathematics subject classification*: primary 14H52.

Keywords and phrases: elliptic curves, formal groups, invariant differentials.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ described by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

Choosing a local parameter $z = -x/y$ for E at its origin O_E, one can associate to E a power series $w(z) = \sum_{n=0}^{\infty} s_i z^i \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\![z]\!]$. Consequently, there are Laurent series expansions for the coordinates $x(z)$ and $y(z)$ from which one obtains power series expansions for several arithmetic objects attached to E, including the invariant differential ω_E, the formal logarithm $\log_E(z) = \int \omega_E(z)$ and the formal group law associated to E over $\mathbb{Z}$ given by $F(X, Y) = \log_E^{-1}(\log_E(X) + \log_E(Y))$.

Honda [5] found an interesting link between the L-series $L(s) = \sum_{n=1}^{\infty} c_n n^{-s}$ of an elliptic curve E and the formal group associated to E. If one sets $g(x) = \sum_{n=1}^{\infty} n^{-1} c_n x^n$, then $G(X, Y) = g^{-1}(g(X) + g(Y))$ is a formal group over $\mathbb{Z}$; moreover, $G(X, Y)$ is isomorphic to the formal group law $F(X, Y)$ associated to E over $\mathbb{Z}$. The isomorphism between these formal groups is made explicit to produce Atkin–Swinnerton-Dyer congruence relations. These congruence relations connect the coefficients of the L-series and the coefficients of the power series expansion of the invariant differential ω_E. The modularity of elliptic curves E defined over $\mathbb{Q}$ implies the existence of a set of congruence relations between the coefficients of the modular form attached to E and the coefficients of the power series expansion of ω_E.

The above discussion indicates that explicit formulas for the coefficients of the power series of ω_E will provide us with information about formal groups, L-series and modular forms associated to elliptic curves. There are few explicit descriptions for the power series expansion of ω_E of a certain elliptic curve E. To give one example, the expansion of ω_E can be found in [3] when E has a rational 2-torsion point, that is, E is described by a Weierstrass equation of the form $y^2 = x^3 + a_2x^2 + a_4x$. There, it is shown that $\omega_E = \sum_{n=0}^{\infty} P_n(a_2/\sqrt{\Delta})(\sqrt{\Delta})^n z^{2n}\,dz$, where P_n is the nth Legendre polynomial and Δ is the discriminant $\Delta = a_2^2 - a_4$. This enables the authors to find explicit congruence relations satisfied by Legendre polynomials using Atkin–Swinnerton-Dyer congruences and sharper congruences using other techniques when E has complex multiplication. Recently, Yasuda [11] found an explicit t-expansion of ω_E for the elliptic curve $E : y^2 = 4(x^3 + Ax + B)$, where $t = -2x/y$.

Further combinatorial quantities appear as coefficients of invariant differentials. For example, in [8], the integers $(-1)^m \sum_k \binom{m}{k}^3$ turn out to be the coefficients of the holomorphic differential form of a model of a $K3$-surface. Again, in [9], the Apéry numbers, $\sum_k \binom{n}{k}^2\binom{n+k}{k}$, which were used in Apéry's proof of the irrationality of $\zeta(2)$ and $\zeta(3)$, also appear as the coefficients of the holomorphic differential form of a model of a $K3$-surface.

In this paper, we derive explicit formulas for the z-power series expansions of the invariant differentials of elliptic curves described by the two special Weierstrass equations $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$ and $y^2 + a_3y = x^3 + a_6$. We find a power series solution to the functional equation satisfied by $w(z)$ and use this to write a z-power series expansion for ω_E. Several combinatorial numbers appear as coefficients of these power series. These numbers include the sums

$$\sum_{m=\lfloor n/2\rfloor}^{n} \sum_{k=0}^{\lfloor m/2\rfloor} \sum_{r=0}^{n-m-k} \binom{m}{k}\binom{m-k}{k}\binom{m-2k}{r}\binom{k}{n-m-k-r}$$

and

$$\sum_{k=\lfloor (n-1)/2\rfloor}^{n-1} \binom{n+k-1}{k}\binom{k}{n-k-1}.$$

Thus, we have families of congruence relations satisfied by the coefficients of the modular forms of these elliptic curves and an explicit description of the formal logarithms of the formal groups associated to them.

It is worth mentioning that although one can find the power series $w(z)$ for any Weierstrass equation, it is not usually easy to use it to obtain simple formulas for the invariant differential when $a_i \neq 0$ for every i. The two families of Weierstrass equations that we treat are broad enough to include many interesting examples, such as elliptic curves with nontrivial rational points.

https://doi.org/10.1017/S0004972715000295 Published online by Cambridge University Press

2. Formal groups of elliptic curves

Let E be an elliptic curve defined over the rational field $\mathbb{Q}$. Assume that E is described by the following Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

We furthermore assume that the Weierstrass equation is globally minimal. Let A be the local ring of functions defined at the origin O_E and $\widehat{A}$ the completion of A at its maximal ideal. Then $\widehat{A}$ is isomorphic to the power series ring $\mathbb{Q}[\![z]\!]$, where z is a parameter at the origin. This parameter can be used to express the Weierstrass coordinates as formal power series in z. More explicitly, we set

$$z = -\frac{x}{y} \quad \text{and} \quad w = -\frac{1}{y}.$$

Now z is a parameter at the origin $(z, w) = (0, 0)$. The Weierstrass equation for E becomes

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3.$$

By substituting the equation into itself recursively, we can write w as a power series in z:

$$w(z) = \sum_{i\geq 0} s_iz^i \in \mathbb{Z}[a_1, \ldots, a_6][\![z]\!],$$

where $s_0 = s_1 = s_2 = 0$, $s_3 = 1$ and, for $n \geq 4$,

$$s_n = a_1s_{n-1} + a_2s_{n-2} + a_3 \sum_{k+l=n} s_ks_l + a_4 \sum_{k+l=n-1} s_ks_l + a_6 \sum_{k+l+m=n} s_ks_ls_m. \tag{2.1}$$

For details, the reader can consult [1] and [7, Ch. IV]. Formal series expressions for x and y can then be deduced from $x(z) = z/w(z)$ and $y(z) = -1/w(z)$. Therefore, the pair $(x(z), y(z))$ is a formal solution to the Weierstrass equation of E.

The invariant differential ω_E of E can be expressed as a formal power series in z:

$$\omega_E = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} = \sum_{n=1}^{\infty} b(n)z^{n-1}\,dz, \quad b(n) \in \mathbb{Z},\ b(1) = 1.$$

Let p be a prime of good reduction for E. The trace of the Frobenius endomorphism modulo p is $t_p = 1 + p - \#E(\mathbb{F}_p)$. The following congruences are the Atkin–Swinnerton-Dyer congruences modulo a prime of good reduction (see [4]).

Corollary 2.1. *If E has good reduction modulo p, then:*

(a) $b(p) \equiv t_p \pmod{p}$;

(b) $b(np) \equiv b(n)\,b(p) \pmod{p}$ *if* $p \nmid n$;

(c) $b(np) - t_p\,b(n) + p\,b(n/p) \equiv 0 \pmod{p^s}$ *if* $n \equiv 0 \pmod{p^{s-1}}$, $s \geq 1$.

https://doi.org/10.1017/S0004972715000295 Published online by Cambridge University Press

3. The elliptic curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$

In this section, we consider elliptic curves over $\mathbb{Q}$ given by the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$, where $a_i \in \mathbb{Z}$. Any elliptic curve with a nontrivial torsion point can be described by such a Weierstrass equation.

Let $z = -x/y$ to be a parameter at the origin and $w = -1/y$. According to (2.1), $w(z) = \sum_{n=0}^{\infty} s_n z^n$, where $s_0 = s_1 = s_2 = 0, s_3 = 1$ and

$$s_n = a_1 s_{n-1} + a_2 s_{n-2} + a_3 \sum_{k+l=n} s_k s_l + a_4 \sum_{k+l=n-1} s_k s_l.$$

The generating function $w(z)$ of the sequence $(s_n)_{n=0}^{\infty}$ satisfies the following functional equation:

$$w(z) = z^3 + a_1 z w(z) + a_2 z^2 w(z) + a_3 w(z)^2 + a_4 z w(z)^2.$$

The above equation is quadratic in $w(z)$. As a consequence,

$$w(z) = \frac{1 - a_1 z - a_2 z^2 - \sqrt{(1 - a_1 z - a_2 z^2)^2 - 4z^3(a_3 + a_4 z)}}{2(a_3 + a_4 z)}. \tag{3.1}$$

We chose the negative sign because the positive sign would force $w(z)$ to have a pole at $z = 0$. Recall that $x(z) = z/w(z)$ and $y(z) = -1/w(z)$. The invariant differential ω_E of E is given by

$$\omega_E = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} = \frac{\frac{dw}{dz}}{3z^2 + 2a_2zw + a_4w^2 + a_1w}\, dz. \tag{3.2}$$

We use Mathematica [10] to substitute (3.1) in the formula for ω_E to obtain

$$\omega_E = \frac{1}{\sqrt{1 - 2(a_1 + a_2 z)z + [(a_1 + a_2 z)^2 - 4(a_3 + a_4 z)z]z^2}}\, dz. \tag{3.3}$$

If $\phi(x)$ is a power series, we write $[x^n]\phi(x)$ for the coefficient of x^n in $\phi(x)$. Before we proceed to the main result of this section, we recall that the generalised central trinomial polynomials $T_n(x, y)$ are defined by

$$T_n(x, y) = [t^n](t^2 + xt + y)^n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k}\binom{n-k}{k} x^{n-2k} y^k$$

and have the generating function

$$\frac{1}{\sqrt{1 - 2xt + (x^2 - 4y)t^2}} = \sum_{n=0}^{\infty} T_n(x, y) t^n.$$

THEOREM 3.1. *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x, a_i \in \mathbb{Z}$, be an elliptic curve over $\mathbb{Q}$. Let $z = -x/y$ be a local parameter at O_E. The z-power series expansion of ω_E is given by $\sum_{n=0}^{\infty} b(n+1)z^n\, dz$, where $b(n+1)$ is*

$$\sum_{m=\lfloor n/2 \rfloor}^{n} \sum_{k=0}^{\lfloor m/2 \rfloor} \sum_{r=0}^{n-m-k} \binom{m}{k}\binom{m-k}{k}\binom{m-2k}{r}\binom{k}{n-m-k-r} a_1^{m-2k-r} a_2^r a_3^{2k-n+m+r} a_4^{n-m-k-r}.$$

https://doi.org/10.1017/S0004972715000295 Published online by Cambridge University Press

Proof. We compare the formula (3.3) for ω_E with the generating function of the generalised central trinomial polynomials. We conclude that

$$\omega_E = \sum_{m=0}^{\infty} T_m(a_1 + a_2 z, (a_3 + a_4 z)z) z^m \, dz.$$

Consequently,

$$\begin{aligned} &T_m(a_1 + a_2 z, (a_3 + a_4 z)z) \\ &\quad = \sum_{k=0}^{\lfloor m/2 \rfloor} \binom{m}{k}\binom{m-k}{k} (a_1 + a_2 z)^{m-2k} (a_3 + a_4 z)^k z^k \\ &\quad = \sum_{k=0}^{\lfloor m/2 \rfloor} \binom{m}{k}\binom{m-k}{k} \left(\sum_{i=0}^{m-2k} \binom{m-2k}{i} a_1^{m-2k-i} a_2^i z^i \right) \left(\sum_{j=0}^{k} \binom{k}{j} a_3^{k-j} a_4^j z^j \right) z^k \\ &\quad = \sum_{k=0}^{\lfloor m/2 \rfloor} \binom{m}{k}\binom{m-k}{k} \sum_{s=0}^{m-k} \left(\sum_{r=0}^{s} \binom{m-2k}{r}\binom{k}{s-r} a_1^{m-2k-r} a_2^r a_3^{k-s+r} a_4^{s-r} \right) z^{s+k}. \end{aligned}$$

For the third equality, we applied the formula for multiplying polynomials. Now,

$$\begin{aligned} b(n+1) &= [z^n]\, \omega_E = [z^n] \sum_{m=0}^{\infty} T_m(a_1 + a_2 z, (a_3 + a_4 z)z)\, z^m \\ &= [z^n] \sum_{m=0}^{\infty} \sum_{k=0}^{\lfloor m/2 \rfloor} \sum_{s=0}^{m-k} \sum_{r=0}^{s} \binom{m}{k}\binom{m-k}{k}\binom{m-2k}{r}\binom{k}{s-r} a_1^{m-2k-r} a_2^r a_3^{k-s+r} a_4^{s-r} z^{s+k+m}. \end{aligned}$$

That is, $b(n+1)$ is the sum of the coefficients for which $s + k + m = n$. Since $0 \le s \le m - k$, one has $n \le 2m$. Moreover, m cannot exceed n. It follows that $b(n+1)$ is

$$\sum_{m=\lfloor n/2 \rfloor}^{n} \sum_{k=0}^{\lfloor m/2 \rfloor} \sum_{r=0}^{n-m-k} \binom{m}{k}\binom{m-k}{k}\binom{m-2k}{r}\binom{k}{n-m-k-r} a_1^{m-2k-r} a_2^r a_3^{2k-n+m+r} a_4^{n-m-k-r}. \qquad \square$$

Using Theorem 3.1, one has the following explicit description of the z-power series expansion of ω_E for any elliptic curve $E/\mathbb{Q}$ described by $E : y^2 + a_3 y = x^3$:

$$\omega_E = \frac{1}{\sqrt{1 - 4a_3 z^3}}\, dz = \sum_{n=0}^{\infty} \binom{2n}{n} a_3^n z^{(3n+1)-1}\, dz.$$

Observing that the discriminant of E is $\Delta_E = -27a_3^4$, one uses Corollary 2.1 to obtain the following congruences.

Corollary 3.2. *Let $E/\mathbb{Q}$ be an elliptic curve defined by $y^2 + ay = x^3$ and p a prime such that $p \nmid 3a$ and let $t_p = 1 + p - \#E(\mathbb{F}_p)$. Then $t_p = 0$ for $p \equiv 2 \pmod 3$ and, for $p \equiv 1 \pmod 3$:*

https://doi.org/10.1017/S0004972715000295 Published online by Cambridge University Press

(a) $t_p \equiv \binom{2\left(\frac{p-1}{3}\right)}{\frac{p-1}{3}} a^{(p-1)/3} \pmod p$;

(b) $\binom{2\left(\frac{np-1}{3}\right)}{\frac{np-1}{3}} \equiv \binom{2\left(\frac{n-1}{3}\right)}{\frac{n-1}{3}} \binom{2\left(\frac{p-1}{3}\right)}{\frac{p-1}{3}} \pmod p$ *if* $n \equiv 1 \pmod 3$;

(c) $\binom{2\left(\frac{np-1}{3}\right)}{\frac{np-1}{3}} a^{(np-1)/3} - t_p \binom{2\left(\frac{n-1}{3}\right)}{\frac{n-1}{3}} a^{(n-1)/3} + p \binom{2\left(\frac{n/p-1}{3}\right)}{\frac{n/p-1}{3}} a^{(n/p-1)/3} \equiv 0 \pmod{p^s}$
if $n \equiv 0 \pmod{p^{s-1}}$, $s \geq 1$.

As pointed out by the referee, the congruence in Corollary 3.2(b) holds modulo p^2 (see for example [2], where p-adic techniques are used to produce such congruence relations modulo higher powers of p). Investigating similar congruence relations modulo higher powers of p will be the subject of future work.

4. The elliptic curve $y^2 + a_3y = x^3 + a_6$

Finally, we consider the family of elliptic curves defined by $y^2 + a_3y = x^3 + a_6$, $a_i \in \mathbb{Z}$. We set $z = -x/y$ and $w(z) = -1/y = \sum_{n=0}^{\infty} s_n z^n$, where $s_0 = s_1 = s_2 = 0$, $s_3 = 1$ and

$$s_n = a_3 \sum_{k+l=n} s_k s_l + a_6 \sum_{k+l+m=n} s_k s_l s_m, \quad n \geq 4.$$

Now, $w(z)$ satisfies the functional equation $w(z) = z^3 + a_3 w(z)^2 + a_6 w(z)^3$, which can be rewritten as

$$v = z^3 = w(z)(1 - a_3 w(z) - a_6 w(z)^2) = \frac{w(z)}{1/(1 - a_3 w(z) - a_6 w(z)^2)}. \tag{4.1}$$

In order to find the power series expansion of ω_E, we will need the following lemma.

Lemma 4.1 (Lagrange inversion theorem). *Suppose that $u = u(x)$ is a power series in x satisfying $x = u/\phi(u)$, where $\phi(u)$ is a power series in u with a nonzero constant term. Then*

$$[x^n]u(x) = \frac{1}{n}[u^{n-1}]\phi^n(u).$$

Applying Lemma 4.1 to (4.1),

$$\begin{aligned}
[v^n]w(v) &= \frac{1}{n}[w^{n-1}]\left(\frac{1}{1 - a_3 w - a_6 w^2}\right)^n = \frac{1}{n}[w^{n-1}] \sum_{k=0}^{\infty} (-1)^k \binom{-n}{k} (a_3 + a_6 w)^k w^k \\
&= \frac{1}{n}[w^{n-1}] \sum_{k=0}^{\infty} \sum_{j=0}^{k} \binom{n+k-1}{k} \binom{k}{j} a_3^{k-j} a_6^j w^{j+k} \\
&= \frac{1}{n} \sum_{k=\lfloor (n-1)/2 \rfloor}^{n-1} \binom{n+k-1}{k} \binom{k}{n-k-1} a_3^{2k-n+1} a_6^{n-1-k}.
\end{aligned}$$

https://doi.org/10.1017/S0004972715000295 Published online by Cambridge University Press

THEOREM 4.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the Weierstrass equation $y^2 + a_3y = x^3 + a_6$. Let $z = -x/y$. The z-power series expansion of the invariant differential ω_E of E is given by*

$$\omega_E = \sum_{n=1}^{\infty}\Bigg(\sum_{k=\lfloor (n-1)/2\rfloor}^{n-1}\binom{n+k-1}{k}\binom{k}{n-k-1}a_3^{2k-n+1}a_6^{n-k-1}\Bigg)z^{(3n-2)-1}\,dz.$$

PROOF. By (3.2), the invariant differential of E is given by $\omega_E = (dw/dz)/(3z^2)\,dz$. The result now follows, as we have shown that

$$w(z) = \sum_{n=1}^{\infty}\Bigg(\frac{1}{n}\sum_{k=\lfloor (n-1)/2\rfloor}^{n-1}\binom{n+k-1}{k}\binom{k}{n-k-1}a_3^{2k-n+1}a_6^{n-k-1}\Bigg)z^{3n}. \qquad \square$$

Now apply the Atkin–Swinnerton-Dyer congruences to the elliptic curve E defined over $\mathbb{Q}$ by the Weierstrass equation $y^2 + a_3y = x^3 + a_6$. If E has good reduction modulo p and $t_p = 1 + p - \#E(\mathbb{F}_p)$, we can use Hasse's bound, $|t_p| < 2\sqrt{p}$, to see that $t_p = 0$ if $p \equiv 2 \pmod 3$ and

$$t_p \equiv \sum_{k=\lfloor (p-1)/6\rfloor}^{(p-1)/3}\binom{\frac{p-1}{3}+k}{k}\binom{k}{\frac{p-1}{3}-k}a_3^{2k-((p-1)/3)}a_6^{((p-1)/3)-k} \pmod p \text{ if } p \equiv 1 \pmod 3.$$

REMARK 4.3. Given Theorems 3.1 and 4.2, the Atkin–Swinnerton-Dyer congruences can be used to produce a large number of congruence relations relating combinatorial objects to coefficients of modular forms, as well as congruences satisfied by the combinatorial objects themselves.

To give an example, consider elliptic curves with n-torsion points which can be parametrised by Tate's normal form. Specifically, an elliptic curve $E_n/\mathbb{Q}$ with a rational n-torsion point $(0, 0)$, where $n \geq 4$, is described by the Weierstrass equation

$$y^2 + (1-c)xy - by = x^3 - bx^2, \quad c, b \in \mathbb{Z}.$$

These explicit parametrisations are due to Kubert (see [6]). According to Theorem 3.1, the invariant differential of E_n is

$$\omega_{E_n} = \frac{dz}{\sqrt{1 - 2(1-c-bz)z + [(1-c-bz)^2 + 4bz]z^2}} = \sum_{n=1}^{\infty} b(n)z^{n-1}\,dz,$$

where

$$b(n) = \sum_{m=0}^{n-1}\sum_{k=0}^{\lfloor m/2\rfloor}\binom{m}{k}\binom{m-k}{k}\binom{m-2k}{n-m-k-1}(1-c)^{2m-n-k+1}(-b)^{n-m-1},$$

and one obtains congruence relations satisfied by $b(n)$ using Corollary 2.1.

Acknowledgement

I would like to thank the anonymous referee for his thorough reading of the article and many helpful suggestions to improve the manuscript.

https://doi.org/10.1017/S0004972715000295 Published online by Cambridge University Press

References

[1] A. Bluher, 'A leisurely introduction to formal groups and elliptic curves', 1997, available on-line at http://www.math.uiuc.edu/Algebraic-Number-Theory/0076/.
[2] M. Coster, 'Generalisation of a congruence of Gauss', *J. Number Theory* **29**(3) (1988), 300–310.
[3] M. J. Coster and L. Van Hamme, 'Supercongruences of Atkin and Swinnerton-Dyer type for Legendre polynomials', *J. Number Theory* **38** (1991), 265–286.
[4] M. Hazewinkel, 'Three lectures on formal groups', *Canad. Math. Soc. Conf. Proc.* **5** (1986), 51–67.
[5] T. Honda, 'Formal groups and zeta-functions', *Osaka J. Math.* **5**(2) (1968), 199–213.
[6] D. S. Kubert, 'Universal bounds on the torsion of elliptic curves', *Proc. Lond. Math. Soc.* (3) **33**(2) (1976), 193–237.
[7] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106 (Springer, New York, 1986).
[8] J. Stienstra, 'Formal groups and congruences for L-functions', *Amer. J. Math.* **109**(6) (1987), 1111–1127.
[9] J. Stienstra and F. Beukers, 'On the Picard–Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces', *Math. Ann.* **271** (1985), 269–304.
[10] Wolfram Research, *Mathematica*, ver. 5.0.
[11] S. Yasuda, 'Explicit t-expansions for the elliptic curve $E : y^2 = 4(x^3 + Ax + B)$', *Proc. Japan Acad. Ser. A Math. Sci.* **89**(9) (2013), 123–127.

MOHAMMAD SADEK, Department of Mathematics and Actuarial Science,
American University in Cairo, Egypt
e-mail: mmsadek@aucegypt.edu

https://doi.org/10.1017/S0004972715000295 Published online by Cambridge University Press