Algorithmic construction of Shimura - Taniyama - Weil parametrization of elliptic curves over the rationals

H. Gopalakrishna Gadiyar and R. Padma
Department of Mathematics
School of Advanced Sciences
V.I.T. University, Vellore 632014 INDIA
E-mail: gadiyar@vit.ac.in, rpadma@vit.ac.in

Abstract
In this note we give an algorithm to explicitly construct the modular parametrization of an elliptic curve over the rationals given the Weierstrass function $\wp(z)$.

MSC2010: 11B68, 11F03, 11S40, 14H52, 14L05, 33E05

1 Introduction
We state a straightforward algorithm to construct the modular parametrization of elliptic curves over the rational numbers. The algorithm is implicit in the papers of Honda [5], Clarke [2], Goldfeld [3] and Buchstaber and Bunkova [11] described below. It consists of the following steps:

2 The algorithm
Step 1. Given the equation of the elliptic curve

$$E : y^2 = 4x^3 - g_2x - g_3$$  \hspace{1cm} (1)

over $\mathbb{Q}$, we have the parametrization $x = \wp(z; g_2, g_3), y = \wp'(z; g_2, g_3)$. 
Step 2. The formal exponential $f_E(T)$ of the formal group corresponding to this curve has been constructed explicitly by Buchstaber and Bunkova.

$$f_E(T) = -2 \frac{\wp(T; g_2, g_3)}{\wp'(T; g_2, g_3)}$$  \hfill (2)

Step 3. As $f_{E}(f_{L}(T)) = f_{L}(f_{E}(T)) = T$ the formal logarithm $f_{L}(T)$ is got from $f_{E}(T)$ by Lagrange inversion. $f_{L}(T)$ is related to the $L$-series of the elliptic curve. This is implicit in the work of Honda and Clarke. If

$$f_{L}(T) = \sum_{n=1}^{\infty} \frac{a(n)}{n} T^n$$  \hfill (3)

then

$$L_{E}(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}. \hfill (4)$$

and vice-versa.

Step 4. Goldfeld explicitly gives the modular parametrization as

$$x = \alpha(z) = \wp(F(z)) = \wp \left( \sum_{n=1}^{\infty} \frac{a(n)}{n} e^{2\pi i n z} \right) \hfill (5)$$

and

$$y = \beta(z) = \wp'(F(z)) = \wp' \left( \sum_{n=1}^{\infty} \frac{a(n)}{n} e^{2\pi i n z} \right). \hfill (6)$$

3 Formal group law

A commutative one dimensional formal group law over a ring $A$ is a formal power series \cite[17]{[4], [7]}

$$F(t_1, t_2) = t_1 + t_2 + \sum_{i,j \geq 1} a_{i,j} t_1^i t_2^j$$ \hfill (7)

such that the following conditions hold:

$$F(t, 0) = t, F(t_1, t_2) = F(t_2, t_1)$$

and

$$F(t_1, F(t_2, t_3)) = F(F(t_1, t_2), t_3)$$
The formal group $F$, the formal exponential $f_E$ and the formal logarithm $f_L$ are connected by the relations

$$F(t_1, t_2) = f_E(f_L(t_1) + f_L(t_2))$$  \hspace{1cm} (8)

and

$$f_E(f_L(T)) = f_L(f_E(T)) = T.$$  \hspace{1cm} (9)

### 4 Elliptic Curve and its formal group

Let $E$ be an elliptic curve $E : y^2 = 4x^3 - g_2x - g_3$ over $Q$. Let $L = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ be the lattice spanned by the two fundamental periods $\omega_1, \omega_2$ such that

$$g_2 = g_2(L) = 60 \sum_{l \in L - \{0\}} \frac{1}{l^4}$$  \hspace{1cm} (10)

and

$$g_3 = g_3(L) = 140 \sum_{l \in L - \{0\}} \frac{1}{l^6}.$$  \hspace{1cm} (11)

We have the Weierstrass parametrization $x = \wp(z), y = \wp'(z)$ where $\wp(z)$ the Weierstrass $\wp$- function

$$\wp(z) = \frac{1}{z^2} + 2 \sum_{n \geq 1} G_{2n+2(E, \omega)} \frac{z^{2n}}{(2n)!}.$$  \hspace{1cm} (12)

Here

$$G_k = \frac{(-1)^k(k-1)!}{2} \sum_{l \in L - \{0\}} \frac{1}{l^k}$$  \hspace{1cm} (13)

for $k \geq 4$. Note that $G_k = 0$ whenever $k$ is an odd integer. Also all the $G_k$’s can be got in terms of $g_2$ and $g_3$.

The Bernoulli-Hurwitz numbers have been defined by Katz[6] as follows. If $E$ is an elliptic curve given by (1), then

$$BH_k = 2kG_k$$  \hspace{1cm} (14)

for $k \geq 4$; $= 0$ if $k$ is odd.

Clarke[2] defines the universal Bernoulli numbers by the formula

$$\frac{T}{f_E(T)} = \sum_{k \geq 0} \hat{B}_k \frac{T^k}{k!}.$$  \hspace{1cm} (15)
When \( f_E(t) = e^t - 1 \), we get the classical Bernoulli numbers \( B_k \).

For the elliptic curve \( E \) in the Weierstrass form, Buchstaber and Bunkova [1] have used the theory of solitons to make explicit constructions of formal group laws.

\[
F(t_1, t_2) = t_1 + t_2 - b \frac{2g_2 + 3g_3m}{4 - g_2m^2 - g_3m^3}
\]

is the formal group law of the elliptic curve \( E \), where for \( i = 1, 2 \), \((x_i, y_i) \in E\)

\[
t_i = -2 \frac{x_i}{y_i}, \quad s_i = -\frac{2}{y_i}, \quad \text{and}
\]

\[
m = \frac{s_1 - s_2}{t_1 - t_2}, \quad b = \frac{t_1s_2 - t_2s_1}{t_1 - t_2},
\]

and the function

\[
f_E(T) = -2 \frac{\wp(T; g_2, g_3)}{\wp'(T; g_2, g_3)}
\]

is the exponential of the formal group.

Hence the \( \hat{B}_k \) can be got in terms of the Bernoulli - Hurwitz numbers \( BH_k \) in the case of elliptic curves.

### 5 Formal logarithm and the \( L \)-series of an elliptic curve

The formal logarithm \( f_L(T) \) is got from \( f_E(T) \) by Lagrange inversion. If

\[
f_L(T) = \sum_{n=1}^{\infty} \frac{a(n)}{n} T^n
\]

denotes the formal logarithm of an elliptic curve \( E \), then the \( L \)-series of the elliptic curve is given by

\[
L_E(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}
\]

and vice-versa [5].

If we take \( f_E(T) = e^T - 1 \) in (15), we get the classical Bernoulli numbers \( B_k \) and the corresponding formal logarithm is \( f_L(T) = \log(1 + T) \) In this case one gets the Dirichlet \( (L-) \) series

\[
\eta(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \cdots = (1 - 2^{1-s}) \zeta(s),
\]
where \( \zeta(s) \) is the classical Riemann - zeta function.

The Shimura - Taniyama - Weil conjecture which is now known as the modularity theorem states that any elliptic curve over rational numbers is modular.

In [3], D. Goldfeld gives the modular parametrization of \( E \) as follows:

\[
\alpha(z) = \wp(F(z)) = \wp \left( \sum_{n=1}^{\infty} \frac{a(n)}{n} e^{2\pi inz} \right)
\]

(23)

and

\[
\beta(z) = \wp'(F(z)) = \wp' \left( \sum_{n=1}^{\infty} \frac{a(n)}{n} e^{2\pi inz} \right).
\]

(24)

where

\[
f(z) = \sum_{n=1}^{\infty} a(n)e^{2\pi inz}
\]

(25)

is a cusp form of weight 2 for \( \Gamma_0(N) \) and \( N \) is the conductor of the elliptic curve \( E \).

6 Conclusion

The Riemann zeta-function \( \zeta(s) \) has two fundamental representations.

\[
\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left( 1 - \frac{1}{p^s} \right)^{-1}, \text{ if } \text{Re. } s > 1.
\]

(26)

These we call the left hand and the right hand side. The left hand side is a sum over the integers and the right hand side is a product over primes. In recent times the \( p \)-adic approach which corresponds to the right hand side has been cultivated extensively. It is hoped that the present note will re-kindle an interest in an approach which relies on complex analysis.

7 Acknowledgements

We would like to thank Professors Arul Lakshminarayan (IIT, Madras), A. Sankaranarayanan (TIFR), K. Srinivas (IMSc, Chennai) for making available the papers and books used in this research.
References

[1] V. M. Buchstaber and E. Yu. Bunkova, Elliptic formal group laws, integral Hirzebruch genera and Krichever genera, arXiv:1010.0944v1

[2] Francis Clarke, The Universal von Staudt theorems, Trans. A. M. S., Volume 115, Number 2, October 1989.

[3] D. Goldfeld, Modular elliptic curves and Diophantine problems, Number Theory, Proceedings of the First Conference of the Canadian Number Theory Association held at the Banff Centre, Banff, Alberta, April 17-27, 1988, R. Mollin (Ed.), Walter de Gruyter Inc., 157 - 175.

[4] M. Hazewinkel, Formal groups and applications, Academic Press, 1978.

[5] T. Honda, Formal groups and zeta functions, Osaka J. Math. Vol.5, 1968, 199-213.

[6] Nicholas M. Katz, The congruences of Clausen - von Staudt and Kummer for Bernoulli-Hurwitz numbers, Math. Annalen, Vol. 216, 1975, 1-4.

[7] J. Silverman, The arithmetic of elliptic curves, GTM 106, Springer - Verlag, New York, 1985.