References

[1] E. S. Barnes, *The complete enumeration of extreme senary forms*, Philos. Trans. Roy. Soc., London, Ser. A, 249 (1957), pp. 461–506.
[2] H. F. Blichfeldt, *The minimum values of positive quadratic forms in six, seven and eight variables*, Math. Zeitschr. 39 (1935), pp. 1–15.
[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, first edition, Oxford 1938.
[4] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. 11 (1877), pp. 242–292.
[5] R. A. Rankin, *On the minimal points of perfect quadratic forms*, Math. Zeitschr. 84 (1964), 228–232.
[6] G. Voronoi, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. Reine Angew. Math. 133 (1908), pp. 97–178.

UNIVERSITY COLLEGE
London, England

Received on 15. 9. 1969

ACTA ARITHMETICA
XVIII (1971)

Some elliptic function identities

by

J. W. S. Cassels (Cambridge)

Harold Davenport in memoriam

0. Introduction. In the course of some calculations about elliptic curves defined over finite fields I was led to identities about the coefficients of classical elliptic functions. These appear to be new, although they are entirely in the spirit of 19th century analysis. In this introduction I shall first enunciate the complex function identities and then describe the application to finite fields. The proofs will be given in the remainder of the paper.

I am grateful to Mr. A. D. McGettrick for some useful discussions and in particular for his contribution to § 6.

As we shall want to specialize mod p later, we must be rather more pedantic in the discussion of the complex function identities than would otherwise be appropriate.

Let x, A, B be independent indeterminates over some field k of characteristic 0 and define y by

$$y^2 = x^3+Ax+B. \tag{0.1}$$

We regard y as a formal series in $x^{-1/2}$:

$$y = x^{3/2}\{1+Ax^{-2}+Bx^{-3}\}^{1/2} = x^{3/2}\Big\{1+\sum_{j>0}\binom{\frac{1}{2}}{j}(Ax^{-2}+Bx^{-3})^j\Big\}. \tag{0.2}$$

There is a sequence of polynomials

$$L_j\in k[x, y, A, B] \tag{0.3}$$

uniquely defined by the properties

$$L_0 = 1, \quad L_1 = 0, \tag{0.4}$$

and

$$\sum_{j=0}^{r}\binom{r}{j} L_j x^{(r-j)/2} = O(1) \quad (r = 2, 3, \ldots) \tag{0.5}$$

where $O(1)$ denotes an element of $k[x^{1/2}, y, A, B]$ whose formal expansion contains no negative powers of $x^{-1/2}$. Indeed it is readily verified by induction that (0.4) together with (0.5) for $r \leqslant s$ defines the L_r $(r < s)$ uniquely and L_s up to an element of $k[A, B]$.

Now let k be the field C of complexes and let $A, B \in C$ satisfy

(0.6) $$4A^3+27B^2 \neq 0.$$

Then (0.1) defines an elliptic curve which is parametrized by the Weierstrass doubly-periodic functions, say

(0.7) $$x = \wp(z), \quad y = -2\wp'(z)$$

where

(0.8) $$dz = -dx/2y$$

and

(0.9) $$\begin{cases} x = z^{-2}+o(1), \\ y = z^{-3}+o(1), \end{cases} \quad (z \to 0).$$

We also require the Weierstrass zeta-function $\zeta(z)$ determined by

(0.10) $$\begin{cases} \dfrac{d\zeta(z)}{dz} = -x(z), \\ \zeta(z) = z^{-1}+o(1). \end{cases}$$

For any period ω of $\wp$ there is the constant $\eta(\omega)$ defined by

(0.11) $$\eta(\omega) = \zeta(z+\omega)-\zeta(z).$$

Clearly $\eta(\omega)$ depends linearly on ω.

We shall be concerned with the sequence of functions

(0.12) $$R_r(z) = \sum_{j=0}^{r} \binom{r}{j} L_j\big(x(z), y(z)\big)\big(\zeta(z)\big)^{r-j} \quad (r = 0, 1, 2, \ldots),$$

so

(0.13) $$R_0(z) = 1; \quad R_1(z) = \zeta(z).$$

Clearly $R_r(z)$ is a regular function of z except possibly at the period points. We investigate its behaviour there. Consider first the neighbourhood of $z = 0$ and write temporarily

(0.14) $$\zeta(z) = x^{1/2}(z)+\theta(z),$$

so

(0.15) $$\theta(z) = O(z^3) = O(x^{-3/2}).$$

On substituting (0.14) in (0.12) and rearranging we have

$$R_r(z) = \sum_{j=0}^{r}\binom{r}{j}\theta^{r-j}\sum_{l=0}^{j}\binom{j}{l}L_j(x, y)x^{(j-l)/2} = \sum_{j=0}^{r}\binom{r}{j}\theta^{r-j}A_j$$

(say), where

$$A_0 = 1, \quad A_1 = x^{1/2},$$
$$A_l = O(1) \quad (l \geqslant 2)$$

by (0.5). Hence

(0.16) $$R_r(z) = O(1) \quad (r \geqslant 2;\ z \to 0)$$

by (0.15).

If ω is any period and $\eta = \eta(\omega)$, then

(0.17) $$R_r(z+\omega) = \sum_{j=0}^{r}\binom{r}{j}L_j(x, y)(\zeta+\eta)^{r-j} = \sum_{j=0}^{r}\binom{r}{j}\eta^j R_{r-j}(z);$$

and so

(0.18) $$R_r(z+\omega) = r\eta^{r-1}z^{-1}+O(1)$$

by (0.10), (0.13) and (0.16). Hence $R_r(z)$ has simple poles at the periods ω with residue

(0.19) $$r\big(\eta(\omega)\big)^{r-1}$$

and no other singularities. This property defines $R_r(z)$ up to an additive constant: the appropriate additive constant for our purposes is determined by the definition in terms of the L_j.

Let u be a new variable and define the formal Laurent series $F(u, z)$ by

(0.20) $$uzF(u, z) = \sum_{j=0}^{\infty} zR_j(z)u^j/j!,$$

where the right-hand side is a formal double power series in the variables u, z. Our identity is

THEOREM 1.

(0.21) $$F(u, z) = F(z, u).$$

We postpone the proof of Theorem 1 to § 2 and now explain briefly its relevance to elliptic curves defined over finite fields.

1. Consider

(1.1) $$y^2 = x^3+Ax+B$$

as the equation of an elliptic curve $\mathscr{C}$ over the field $\boldsymbol{F} = \boldsymbol{F}_p$ of p elements and suppose that the Hasse invariant H is non-zero. Then there are precisely $p-1$ points on $\mathscr{C}$ of exact order p defined over the algebraic closure $\overline{\boldsymbol{F}}$ of $\boldsymbol{F}$. Further, there is a uniquely defined isogeny ϕ of $\mathscr{C}$ into itself

(1.2) $$\mathscr{C} \xrightarrow{\phi} \mathscr{C}$$

of degree p with kernel the points of order p. Let $\mathfrak{X} = (X, Y)$ and $\mathfrak{x} = (x, y) = \phi\mathfrak{X}$ be generic points of $\mathscr{C}$. Then the function field $\overline{F}(\mathfrak{X})$ is an Artin–Schreier extension of $\overline{F}(\mathfrak{x})$ which can be given explicitly as follows (Deuring [1]). Let

$$(1.3)\qquad (x^3+Ax+B)^{(p-1)/2} = \sum_j \lambda_j x^{3(p-1)/2-j}.$$

Then

$$(1.4)\qquad \overline{F}(\mathfrak{X}) = \overline{F}(\mathfrak{x})(g)$$

where

$$(1.5)\qquad g^p - Hg = y\sum_{j=0}^{(p-3)/2} \lambda_j x^{(p-3)/2-j}$$

and the Hasse invariant H is

$$(1.6)\qquad H = \lambda_{(p-1)/2}.$$

The automorphisms of $\overline{F}(\mathfrak{X})/\overline{F}(\mathfrak{x})$ are thus of the type

$$(1.7)\qquad g \to g+\mathfrak{H}$$

where

$$(1.8)\qquad \mathfrak{H}^{p-1} = H.$$

On the other hand, the automorphisms of $\overline{F}(\mathfrak{X})/\overline{F}(\mathfrak{x})$ are clearly

$$(1.9)\qquad \mathfrak{X} \to \mathfrak{X}+\mathfrak{d},$$

where $\mathfrak{d}$ is a p-division point. The problem that started the present investigation is to find an explicit expression for the $\mathfrak{d} = \mathfrak{d}(\mathfrak{H})$ such that

$$(1.10)\qquad g(\mathfrak{X}+\mathfrak{d}) = g(\mathfrak{X})+\mathfrak{H},$$

where $\mathfrak{H}$ is a given solution of (1.8).

I was unable to find a satisfactory solution in general but obtained one which was good enough for computational purposes when the curve (1.1) and the isogeny (1.2) are the reductions of a curve and an isogeny defined over an imaginary quadratic number field K (say). The reduction will be modulo an ideal $\mathfrak{p}$ of K of norm p. To avoid extra notation we shall denote an element of K and its residue modulo $\mathfrak{p}$ by the same letter.

We define $C_j, D_j \in k$ $(j = 0, 1, 2, \ldots)$ as the coefficients in the expansions of the functions

$$\frac{1}{2!}R_2(z) = \frac{1}{2}\{\zeta^2(z)-x(z)\} = \sum_{j=0}^{\infty} C_j z^j,$$

$$\frac{1}{3!}R_3(z) = \frac{1}{6}\{\zeta^3(z)-3\zeta(z)x(z)+2y(z)\} = \sum_{j=0}^{\infty} D_j z^j$$

of the previous section. Then

THEOREM 2 [1]. *Suppose that ϕ is the reduction of an isogeny defined in characteristic 0. Then the coordinates $X(\mathfrak{H})$, $Y(\mathfrak{H})$ of the division point $\mathfrak{d} = \mathfrak{d}(\mathfrak{H})$ are*

$$X(\mathfrak{d}) = H^2\sum_{j=1}^{p-2} j!\,C_j\mathfrak{H}^{-j}, \qquad Y(\mathfrak{d}) = H^3\sum_{j=1}^{p-2} j!\,D_j\mathfrak{H}^{-j}.$$

It is, of course, implicit in the enunciation of Theorem 2 that C_j and D_j are integers for $\mathfrak{p}$ and so can be taken modulo $\mathfrak{p}$.

2. The complex case. In this section it is convenient to write $b_0 = 1$, $b_1 = 0$, and b_j for the constant term in $R_j(z)$ $(j > 1)$, so that

$$(2.1)\qquad \begin{cases} R_0 = b_0 = 1, \\ R_1 = z^{-1}+b_1+O(z) = z^{-1}+O(z), \\ R_j = b_j+O(z)\ \ (j>1). \end{cases}$$

For any period ω it follows from (0.17) that

$$(2.2)\qquad R_r(z+\omega) = r\eta^{r-1}z^{-1}+\sum_{j=0}^{r}\binom{r}{j} b_j\eta^{r-j}+O(z),$$

where

$$(2.3)\qquad \eta = \eta(\omega).$$

We shall now set up recurrence relations involving the $R_r(z)$ and their derivatives.

For $r \geqslant 0$, $s \geqslant 0$ consider

$$(2.4)\qquad I(r,s)(z) = R_r(z)R_s(z)+\frac{rs}{r+s-1}R'_{r+s-1}(z) - \sum_{j=0}^{r+s-1}\left\{s\binom{r}{j}+r\binom{s}{j}\right\}\frac{b_j}{r+s-j}R_{r+s-j}(z).$$

The only possible poles of $I(r,s)(z)$ are at the period points and it follows readily from (2.2) that $I(r,s)(z)$ is regular there too. Hence

$$(2.4')\qquad I(r,s)(z) = \text{constant}$$

by Liouville's theorem. But now by (0.17) we have

$$(2.5)\qquad I(r,s)(\omega+z) = \sum_t \eta^{r+s-t}J(r,s,t),$$

[1] See Corrigendum, p. 51.

where

(2.6) $$J(r,s,t) = J(r,s,t)(z)$$
$$= \sum_{j+k=t} \binom{r}{j}\binom{s}{k} R_j(z)R_k(z) + \frac{rs}{r+s-1}\binom{r+s-1}{t-1} R'_{t-1}(z) -$$
$$- \sum_{j+k=t} \left\{ s\binom{r}{j} + r\binom{s}{j} \right\} \frac{b_j}{r+s-j}\binom{r+s-j}{k} R_k(z)$$

is independent of ω. Since η takes infinitely many distinct values, it follows from (2.4′) that

(2.7) $$J(r,s,t) = 0$$

identically in z whenever

(2.8) $$r+s > t.$$

This is one relation between the $R_j(z)$ but we shall deduce a simpler one. Keep t fixed and let r, s vary subject only to the condition (2.8). Then on writing

$$\binom{r}{j} = \frac{r(r-1)\ldots(r-j+1)}{j!}$$

etc. in (2.6) we see that

$$J(r,s,t)\prod_{j=1}^{t}(r+s-j)$$

is a *polynomial* in r, s whose coefficients are meromorphic functions of z (and depend also on t). Since this polynomial vanishes whenever $r+s > t$, it must vanish identically in r, s. In particular, on picking out the terms of highest degree in r and s we obtain

(2.9) $$0 = \sum_{j+k=t} r^j s^k \frac{R_j(z)}{j!}\,\frac{R_k(z)}{k!} + rs(r+s)^{t-2}\frac{R'_{t-1}(z)}{(t-1)!} -$$
$$- \sum_{\substack{j+k=t\\ j\geq 0}} (sr^j + rs^j)(r+s)^{k-1}\frac{b_j}{j!}\,\frac{R_k(z)}{k!}.$$

Here $t \geq 0$ is an integer, z is a complex variable and now r, s may take all complex values. We recall the definition

(2.10) $$F(r,z) = \sum_{j=0}^{\infty} r^{j-1}R_j(z)/j!$$

in the enunciation of Theorem 1 and put

(2.11) $$G_1(r) = \sum_{j\geq 0} r^{j-1}b_j/j!.$$

The identities (2.9) for $t = 0, 1, 2, \ldots$ together give

(2.12) $$0 = F(r,z)F(s,z) + F_z(r+s,z) - \{G_1(r)+G_1(s)\}F(r+s,z),$$

where the suffix z denotes $\partial/\partial z$. Indeed one readily verifies that the right-hand side of (2.9) is just the portion of the right hand side of (2.12) of weight t in r, s multiplied by rs. (Note that $b_0 = 1$, $b_1 = 0$.)

3. We now obtain relations between the formal series $G_j(r)$ where

(3.1) $$F(r,z) = \sum_j z^{j-1}G_j(r)/j!$$

(which is compatible with the earlier definition of G_1). On equating the coefficients of z^{t-2} in (2.12) for any given t, we obtain

(3.2) $$0 = \sum_{j+k=t} \frac{G_j(r)}{j!}\,\frac{G_k(s)}{k!} + (t-1)\frac{G_t(r+s)}{t!} -$$
$$- \{G_1(r)+G_1(s)\}\frac{G_{t-1}(r+s)}{(t-1)!}$$

identically in r, s. Since $G_0(r) = 1$, this is a trivial identity for $t = 0$ and $t = 1$. For $t = 2$ we obtain

(3.3) $$0 = \tfrac{1}{2}\{G_2(r)+G_2(s)+G_2(r+s)\} +$$
$$+ G_1(r)G_1(s) - \{G_1(r)+G_1(s)\}G_1(r+s).$$

Since $G_1(r)$ is an odd function of r and $G_2(r)$ is even, we get a more elegant identity on putting

$$r = r_1, \quad s = r_2, \quad -r-s = r_3.$$

Then

(3.4) $$\Big\{\sum_{j=1}^{3} G_1(r_j)\Big\}^2 + \sum_{j=1}^{3}\{G_2(r_j) - G_1^2(r_j)\} = 0$$

for all values of the variables r_1, r_2, r_3 satisfying

(3.5) $$r_1 + r_2 + r_3 = 0.$$

This immediately recalls the following identity of Frobenius and Stickelberger [2]:

(3.6) $$\Big\{\sum_{j=1}^{3}\zeta(z_j)\Big\}^2 = \sum_{j=1}^{3}\wp(z_j)$$

whenever

(3.7) $$z_1 + z_2 + z_3 = 0.$$

Following up this clue, a simple calculation shows that

(i) the coefficients of $G_1(r)$ and $G_1^2(r)-G_2(r)$ coincide with those of $\zeta(r)$, $x(r)$ in degree $\leqslant 6$.

(ii) the identity (3.4) determines the coefficients of $G_1(r)$ and $G_1^2(r)-G_2(r)$ of degree >6 recursively in terms of the earlier ones.

Hence,

$$G_1(r) = \zeta(r) = R_1(r), \tag{3.8}$$

$$G_2(r) = \zeta^2(r)-x(r) = R_2(r) \tag{3.9}$$

and, of course,

$$G_0(r) = 1 = R_0(r). \tag{3.10}$$

In particular, on comparing (2.10), (3.1) and (3.6) we have

$$G_j(r) = b_j+O(r) \qquad (j\neq 1,\ r\to 0) \tag{3.11}$$

and

$$G_1(r) = \zeta(r) = r^{-1}+O(r). \tag{3.12}$$

We now revert to the identity (3.2) which we write in the shape

$$0 = \sum_{\substack{j\neq 1\\ j+k=t}} \frac{G_j(r)}{j!}\,\frac{G_k(s)}{k!} + G_1(r)\,\frac{G_{t-1}(s)-G_{t-1}(r+s)}{(t-1)!} + $$
$$+(t-1)\frac{G_t(r+s)}{t!} - \frac{G_1(s)G_{t-1}(r+s)}{(t-1)!}.$$

On letting $r\to 0$ and using (3.11), (3.12) we deduce that

$$0 = \sum_{j+k=t} \frac{b_j}{j!}\,\frac{G_k(s)}{k!} - \frac{G'_{t-1}(s)}{(t-1)!} + (t-1)\frac{G_t(s)}{t!} - \frac{G_1(s)G_{t-1}(s)}{(t-1)!} \tag{3.13}$$

or, on multiplying by $-(t-1)!$ and recollecting that $b_0 = 1$:

$$0 = G_1(s)G_{t-1}(s)+G'_{t-1}(s)-G_t(s)-\sum_{\substack{j>0\\ j+k=t}}\binom{t-1}{j} b_j \frac{G_k(s)}{k}. \tag{3.14}$$

This is a recurrence relation which determines $G_t(s)$ recursively for $t = 3, 4, \ldots$ We shall deduce that

$$G_t(s) = R_t(s)$$

for all t by showing that $R_t(s)$ satisfies the same relation.

Indeed, by (2.4) we have

$$R_1(z)R_{t-1}(z)+R'_{t-1}(z)-R_t(z)-\sum_{\substack{j>0\\ j+k=t}}\binom{t-1}{j} b_j \frac{R_k(z)}{k} \tag{3.15}$$
$$= I(1, t-1)(z) = \text{constant}$$

by (2.4′).

Suppose we know already the identities

$$G_v(s) = R_v(s) \qquad (\text{all } v<t).$$

Then (3.14), (3.15) imply that

$$G_t(s) = R_t(s)+\text{constant}.$$

But

$$G_t(0) = b_t = R_t(0)$$

by (3.11). Hence identically

$$G_t(s) = R_t(s).$$

This is just the enunciation of Theorem 1 by (0.20) and (3.1).

4. Some further complex identities. For later reference we note and transform slightly the identities that arise from differentiating (0.12) with respect to z. We have

$$-\frac{d}{dz}R_r(z) = \sum_{j=0}^{r}\binom{r}{j}\left\{-\frac{d}{dz}L_j(x, y)+jxL_{j-1}(x, y)\right\}\zeta^{r-j}. \tag{4.1}$$

Put

$$-\frac{d}{dz}R_r(z) = rS_{r-1}(z) \tag{4.2}$$

and

$$-\frac{d}{dz}L_j(x, y)+jxL_{j-1}(x, y) = jM_j(x, y), \tag{4.3}$$

so

$$M_j(x, y)\in C[x, y]. \tag{4.4}$$

Then (4.1) becomes

$$S_r(z) = \sum_{j=0}^{r}\binom{r}{j} M_j(x, y)\,\zeta^{r-j} \tag{4.5}$$

on writing r, j for $r-1, j-1$. By (4.2) and (0.18) we have

$$S_r(\omega+z) = \{\eta(\omega)\}^r z^{-2}+O(1). \tag{4.6}$$

The sequence M_r is easily seen to be defined by the properties

(4.7) $$M_0 = x, \quad M_1 = -y$$

and

(4.8) $$\sum_{j=0}^{r} \binom{r}{j} M_j(x, y) x^{(r-j)/2} = O(1) \quad (r \geqslant 2)$$

where

(4.9) $$x = x(z), \quad y = y(z), \quad z \to 0.$$

Similarly, the functions

(4.10) $$T_r(z) = -\frac{1}{2}\frac{d}{dz} S_r(z)$$

satisfy

(4.11) $$T_r(\omega+z) = \{\eta(\omega)\}^r z^{-3} + O(1)$$

and are of the form

(4.12) $$T_r(z) = \sum_{j=0}^{r} \binom{r}{j} N_j(x, y) \zeta^{r-j},$$

where

(4.13) $$N_j(x, y) \in C[x, y]$$

are defined by

(4.14) $$N_0 = y, \quad N_1 = -x^2$$

and

(4.15) $$\sum_{j=0}^{r} \binom{r}{j} N_j(x, y) x^{(r-j)/2} = O(1).$$

Theorem 1 allows us to make the estimates (4.6) and (4.11) more precise. Define B_j, C_j, D_j $(j \geqslant 0)$ by the expansions

(4.16) $$\begin{aligned} \frac{1}{1!} R_1(z) &= \zeta(z) = z^{-1} + \sum_{j=0}^{\infty} B_j z^j, \\ \frac{1}{2!} R_2(z) &= \frac{1}{2}(\zeta^2 - x) = \sum_{j=0}^{\infty} C_j z^j, \\ \frac{1}{3!} R_3(z) &= \frac{1}{6}(\zeta^3 - 3x\zeta + 2y) = \sum_{j=0}^{\infty} D_j z^j. \end{aligned}$$

Then Theorem 1 gives us the first few coefficients in the expansion of $R_j(z)$ as

(4.17) $$\begin{aligned} R_j(z) &= j!\{B_{j-1} + C_{j-1}z + D_{j-1}z^2 + \ldots\} \quad (j > 1), \\ R_1(z) &= z^{-1} + B_0 + C_0 z + D_0 z^2 + \ldots \end{aligned}$$

Hence in the neighbourhood of $z = 0$ we have:

(4.18) $$S_r(z) = -\frac{1}{(r+1)}\frac{d}{dz} R_{r+1}(z) = \begin{cases} z^{-2} + O(z) & (r = 0), \\ -r!\,C_r + O(z) & (r > 0) \end{cases}$$

and similarly

(4.19) $$T_r(z) = \begin{cases} z^{-3} + O(z) & (r = 0), \\ -r!\,D_r + O(z) & (r > 0). \end{cases}$$

5. The finite field case. As in § 1, let

(5.1) $$\mathscr{C}:\ y^2 = x^3 + Ax + B$$

be defined over the field F of p elements and let

(5.2) $$\phi:\ \mathscr{C} \to \mathscr{C}$$

be a separable isogeny of degree p. We use $\mathfrak{X} = (X, Y)$ and $\mathfrak{x} = (x, y)$ for a pair of generic points related by

(5.3) $$\mathfrak{x} = \phi\mathfrak{X}$$

and suppose that the function $g(\mathfrak{X})$ in (1.5) is so normalised that

(5.4) $$g(\mathfrak{X}) - y/x$$

vanishes when $\mathfrak{X}$ is the point at infinity on $\mathscr{C}$. Then

(5.5) $$g(-\mathfrak{X}) = -g(\mathfrak{X}).$$

We no longer have the Weierstrass variable z and choose $x^{-1/2}$ as a local uniformizer in the neighbourhood of the point at infinity $\mathfrak{o}$. Then

(5.6) $$g(\mathfrak{X}) = x^{+1/2} + O(x^{-1/2})$$

(note the majuscule on the left-hand side and the minuscule on the right-hand side). Further

(5.7) $$g(\mathfrak{X} + j\mathfrak{d}) = g(\mathfrak{X}) + j\mathfrak{H},$$

where $\mathfrak{d}$ is the point in the kernel of ϕ belonging to $\mathfrak{H}$ as explained in § 1.

We can now mimic the argument of § 4. The conditions (4.7), (4.8) determine the M_j $(j < p-1)$ uniquely and M_{p-1} up to an additive constant which for the moment we suppose chosen arbitrarily. Consider

(5.8) $$\mathfrak{S}_{p-1}(\mathfrak{X}) = \sum_{j=0}^{p-1} \binom{p-1}{j} M_j(x, y)\{g(\mathfrak{X})\}^{p-1-j};$$

so the arbitrary additive constant in M_{p-1} implies the same arbitrary constant in $\mathfrak{S}_{p-1}$. Then

$$g(\mathfrak{X}+j\mathfrak{d}) = x^{1/2}+j\mathfrak{H}+O(x^{-1/2}) \tag{5.9}$$

and so

$$\mathfrak{S}_{p-1}(\mathfrak{X}+j\mathfrak{d}) = (j\mathfrak{H})^{p-1}x+O(1) \tag{5.10}$$

by the analogue of (4.6). But, in characteristic p,

$$(j\mathfrak{H})^{p-1} = 0 \quad (j = 0); \qquad (j\mathfrak{H})^{p-1} = H \quad (1 \leqslant j \leqslant p-1). \tag{5.11}$$

Further X, considered as a function of $\mathfrak{X} = (X, Y)$ is regular except at $\mathfrak{X} = \mathfrak{o}$ and there

$$X = J^2x+O(x^{-1}) \tag{5.12}$$

where the constant J is defined by

$$\frac{dx}{y} = J\frac{dX}{Y}. \tag{5.13}$$

Hence

$$\mathfrak{S}_{p-1}(\mathfrak{X})-\mathfrak{S}_{p-1}(\mathfrak{o})+HJ^{-2}X-Hx = 0 \tag{5.14}$$

since it has no singularities and vanishes at $\mathfrak{X} = \mathfrak{o}$. This gives us a fairly explicit expression for X as an element of $C[x, y, g]$ and so a fairly explicit expression for $X(\mathfrak{d})$ as a polynomial in $\mathfrak{H}$.

One may similarly use T_{p-1} defined in (4.10) to find an expression for Y as an element of $C[x, y, g]$ and to determine $Y(\mathfrak{d})$.

6. From the foregoing it appears that g is to some extent a substitute in characteristic p for the function ζ which is defined only in characteristic 0. Let us investigate the analogy further. On applying the operator

$$(') = -2y\,d/dx \quad (= d/dz \text{ in characteristic } 0) \tag{6.1}$$

to (1.5) and noting that

$$\frac{d}{dx}g^p = 0,$$

$$\frac{d}{dx}\left\{y\sum_{j=0}^{\infty}\lambda_j x^{(p-3)/2-j}\right\} = \frac{d}{dx}\left(\frac{y}{x}\right)^p = 0,$$

one readily obtains

$$-Hg' = \lambda_{(p-1)/2}x-\lambda_{(p+1)/2}. \tag{6.2}$$

Hence

$$g' = -x+H^{-1}\lambda_{(p+1)/2}, \tag{6.3}$$

since

$$H = \lambda_{(p-1)/2}. \tag{6.4}$$

On comparison with (0.10) we see that the analogy between g (in characteristic p) and ζ (in characteristic 0) will be particularly close when

$$g' = -x \tag{6.5}$$

or, what is the same thing (²),

$$\lambda_{(p+1)/2} = 0. \tag{6.5'}$$

As Mr. A. D. McGettrick pointed out to me, this is certainly the case when the isogeny ϕ is the reduction of an isogeny $\tilde{\phi}$ on an elliptic curve $\tilde{\mathscr{C}}$ defined over a complex quadratic field K. Then p is the norm of an integer π of K which can be chosen in such a way that

(i) the reduction is induced by the specialization

$$K \to K(\operatorname{mod}\pi); \tag{6.6}$$

(ii) $\tilde{\phi}$ is complex multiplication by the conjugate π' of π.

We now want to show that the function $g(\mathfrak{X})$ of § 5 is the reduction of some function $\tilde{g}(\mathfrak{X})\in K(\mathfrak{X})$ on $\tilde{\mathscr{C}}$.

We define $\tilde{g}(\mathfrak{X})$ by the following properties:

(i) the only singularities of $\tilde{g}(\mathfrak{X})$ are simple poles at $\mathfrak{o}$ and at the π'-division points $\mathfrak{d} \neq \mathfrak{o}$ with residues $(1-p)/\pi'$ and $1/\pi'$ respectively.

(ii) $\tilde{g}(\mathfrak{X})$ is an odd function of $\mathfrak{X}$. Clearly $\tilde{g}(\mathfrak{X})$ exists and is unique. The reduction of $\tilde{g}(\mathfrak{X})$ has the same residue $1/(\pi'\operatorname{mod}\pi)$ both at $\mathfrak{o}$ and at the π'-division points $\mathfrak{d} \neq \mathfrak{o}$ and is odd. These properties suffice to identify it with $g(\mathfrak{X})$.

Let Z be the Weierstrass parameter of $\mathfrak{X}$, so $\pi'Z = z$ (say) is that of $\mathfrak{x} = \phi\mathfrak{X}$. Comparison of poles shows that

$$\tilde{g}'(\mathfrak{X}) = \zeta(z)-\pi\zeta(Z), \tag{6.7}$$

the arbitrary additive constant vanishing because $\tilde{g}$ and ζ are odd functions. The application of (6.1) gives

$$\tilde{g}(\mathfrak{X}) = -x+\pi\pi'^{-1}X \equiv -x(\operatorname{mod}\pi); \tag{6.8}$$

and so (6.5) holds on reduction.

The estimates

$$\zeta = x^{1/2}+O(x^{-1/2}); \qquad g = x^{1/2}+O(x^{-1/2}) \tag{6.9}$$

together with (0.10) and (6.5) imply that the expansion of g in terms of a local uniformizer (say $x^{-1/2}$) is the reduction of the corresponding

(²) See Corrigendum, p. 51.

expansion for ζ, at least to $O(x^{-p/2})$. It follows readily from this that the terms of the expansion of

$$\mathfrak{S}_r(\mathfrak{X}) = \sum_{j=0}^{r} \binom{r}{j} M_j(x, y)\{g(\mathfrak{X})\}^{r-j} \tag{6.10}$$

are the reduction of those of the expansion of S_r (defined in (4.5)) at least to $O(x^{-(p-r-1)/2})$. In particular, by (4.18), in the neighbourhood of $\mathfrak{X} = \mathfrak{o}$ we have

$$\mathfrak{S}_0(\mathfrak{X}) = x + O(x^{-1/2}), \tag{6.11}$$

$$\mathfrak{S}_r(\mathfrak{X}) = -r!C_r + O(x^{-1/2}) \tag{6.12}$$

and

$$\mathfrak{S}_{p-1}(\mathfrak{X}) = O(1), \tag{6.13}$$

where we have not distinguished between C_r and its residue class modulo π.

By (5.7) and (6.10) we have

$$\mathfrak{S}_{p-1}(\mathfrak{X}+\mathfrak{d}) = \sum_{j=0}^{p-1} \binom{p-1}{j} \mathfrak{S}_j(\mathfrak{X})\,\mathfrak{H}^{p-1-j}.$$

On substituting (6.14) in (5.14) and letting $\mathfrak{X} \to \mathfrak{o}$ we have

$$HJ^{-2}X(\mathfrak{d}) = \sum_{j=0}^{p-2} \binom{p-1}{j} (j!C_j)\,\mathfrak{H}^{p-1-j}.$$

This expression simplifies. In the first place, by (5.13) and, since we are reducing complex multiplication by π', we have

$$J = \pi' (\operatorname{mod} \pi) = -H$$

by a result of Manin ([3]. The simple example on pp. 154–155, which is only a special case of his general theorem, does all we need).

Secondly

$$\binom{p-1}{j} \equiv (-1)^j (\operatorname{mod} p)$$

and $C_j = 0$ for odd j by (4.16). We deduce that

$$X(\mathfrak{d}) = H^2 \sum_{j=1}^{p-2} j!C_j \mathfrak{H}^{-j}$$

as asserted in Theorem 2.

The formula for $Y(\mathfrak{d})$ in Theorem 2 is proved similarly but using T_r (defined in (4.10)) and its reduction mod π.

7. In conclusion we note that at least when $AB = 0$ the expansion of g is a reduction of that of ζ to a much greater degree of accuracy than the $O(x^{-p/2})$ in the remarks after (6.9). It would be interesting to know whether this is always the case.

Suppose, for example, that $A = 0$, so that

$$y^2 = x^3 + B. \tag{7.0}$$

In order for there to be complex multiplication we must have

$$p \equiv 1 (\operatorname{mod} 6). \tag{7.1}$$

The equation (1.5) becomes

$$g^p - Hg = y \sum_{f=0}^{(p-7)/6} \binom{\frac{p-1}{2}}{f} (-B)^f x^{(p-3)/2-3f}, \tag{7.2}$$

where

$$H = \binom{\frac{p-1}{2}}{\frac{p-1}{6}} (-B)^{(p-1)/6}. \tag{7.3}$$

Here

$$g = y/x + O(x^{-5/2})$$

and so

$$g^p = (y/x)^p + O(x^{-5p/2}).$$

On substituting $g = (y/x)G$, in (7.2), where G is a power series in x whose coefficients are to be determined, one readily deduces that

$$Hg = y \sum_{f=(p-1)/6}^{(p-1)/2} \binom{\frac{p-1}{2}}{f} (-B)^f x^{(p-3)/2-3f} + O(x^{-5p/2}).$$

On using (7.3) and operating modulo p this gives

$$g = (y/x) F(1, \tfrac{1}{3}, \tfrac{5}{6}; -Bx^3) + O(x^{-5p/2})$$

in the standard hypergeometric function notation. But in characteristic 0,

$$\zeta = (y/x) F(1, \tfrac{1}{3}, \tfrac{6}{5}; -Bx^3).$$

Corrigendum (added in proof, May, 1971). Serre has pointed out to me that (6.5′) on page 49 cannot hold whenever ϕ is the reduction of an isogeny. A counter-example is $y^2 = x^3+x+1$ for $p = 5$ since this curve is the reduction of a curve defined over Q with complex multiplication by the integers of $Q(\sqrt{-11})$. However, (6.5′) is easily seen to be true for $y^2 = x^3+Ax$ and $y^2 = x^3+B$.

References

[1] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Hamburger Abhandlungen 14 (1941), pp. 197–272.

[2] F. G. Frobenius and L. Stickelberger, *Über die Addition und Multiplication der elliptischen Functionen*, Crelle 88 (1880), pp. 146–184 [especially (9) on p. 155].

[3] Ю. И. Манин, *О матрице Хассе–Витта алгебраической кривой*, ИАН, сер. мат., 25 (1961), pp. 153–172.

Received on 4. 10. 1969

ACTA ARITHMETICA
XVIII (1971)

One some general problems in the theory of partitions, I

by

P. Erdös and P. Turán (Budapest)

To the memory of H. Davenport

1. In our fourth paper on statistical group theory (see [2]) we needed and proved that "almost all" sums of *different* prime powers not exceeding x consist essentially of

$$(1.1)\qquad \left(1+o(1)\right)\frac{2\sqrt{6}}{\pi}\log 2\cdot\sqrt{\frac{x}{\log x}}$$

summands. Further needs of this theory make it necessary to find general theorems in this direction, i.e. when the summands are taken from a given sequence

$$(1.2)\qquad A\colon\ 0<\lambda_1<\lambda_2<\ldots$$

of integers. The only result we know in this direction refers to the case when A is the sequence of all positive integers. In this case Erdös and Lehner (see [1]) proved even the stronger result that almost all "unequal" partitions of n (i.e. with exception of at most $o\left(q(n)\right)$ partitions of n into unequal parts) consist of

$$(1.3)\qquad \left(1+o(1)\right)\frac{2\sqrt{3}\log 2}{\pi}\sqrt{n}$$

summands; here $q(n)$ stands for the number of unequal partitions of n for which according to Hardy and Ramanujan (see [3]) the relation

$$(1.4)\qquad q(n)=\frac{1+o(1)}{4\sqrt[4]{3}}\,n^{-\frac{3}{4}}e^{\frac{\pi}{\sqrt{3}}\sqrt{n}}$$

holds. Now we have found that having *only* asymptotical requirement on the counting function

$$(1.5)\qquad \Phi_A(x)=\sum_{\lambda_\nu\leqslant x}1$$

we can prove general theorems. More exactly we assert