ON THE DIVISION-VALUES OF WEIERSTRASS'S $\wp$-FUNCTION

By KURT MAHLER (*Groningen*)

[Received 3 October 1934]

SUPPOSE that g_2 and g_3 are two rational numbers with

$$\Delta = g_2^3 - 27g_3^2 \neq 0,$$

and that ω, ω' are the fundamental periods of Weierstrass's function

$$\wp(u) = \wp(u \mid g_2, g_3) = \wp(u; \omega, \omega').$$

It is well known that all division-values

$$\wp\left(\frac{h\omega + h'\omega'}{n}\right),$$

where $n \neq 0$ and h, h' denote integers, are algebraic numbers. I intend to give a simple method for finding all division-values which are rational numbers, and shall show that their number is finite.

1. By the duplication theorem for Weierstrass's $\wp$-function

$$\wp(2u) = \frac{\wp(u)^4 + \frac{1}{2}g_2\,\wp(u)^2 + 2g_3\,\wp(u) + \frac{1}{16}g_2^2}{4\wp(u)^3 - g_2\,\wp(u) - g_3}. \tag{1}$$

Here the two polynomials

$$P_0(t) = t^4 + \tfrac{1}{2}g_2\,t^2 + 2g_3\,t + \tfrac{1}{16}g_2^2,$$

$$Q_0(t) = 4t^3 - g_2\,t - g_3$$

have no common factor; for to every given value of $\wp(2u)$ there must be exactly four (different or equal) values of $\wp(u)$ which satisfy (1), since both functions $\wp(2u)$ and $\wp(u)$ are even and the first one is of order eight and the second one of order two. By hypothesis g_2 and g_3 are rational; therefore we can determine an integer $N \neq 0$, such that both polynomials

$$P(t) = N(t^4 + \tfrac{1}{2}g_2\,t^2 + 2g_3\,t + \tfrac{1}{16}g_2^2),$$

$$Q(t) = N(4t^3 - g_2\,t - g_3)$$

have integer coefficients. We write

$$P(x, y) = N(x^4 + \tfrac{1}{2}g_2\,x^2y^2 + 2g_3\,xy^3 + \tfrac{1}{16}g_2^2\,y^4),$$

$$Q(x, y) = N(4x^3y - g_2\,xy^3 - g_3\,y^4)$$

for their corresponding binary forms of degree four. The resultant, say R, of these forms is not zero; hence there exist cubic forms

$$P_1(x,y), \quad Q_1(x,y) \qquad \text{and} \qquad P_2(x,y), \quad Q_2(x,y)$$

with integer coefficients such that identically

$$P(x,y)P_1(x,y)+Q(x,y)Q_1(x,y) = Rx^7,$$
$$P(x,y)P_2(x,y)+Q(x,y)Q_2(x,y) = Ry^7.$$

These identities show that for coprime integers p and q the greatest common divisor

$$\delta = (P(p,q),\ Q(p,q))$$

must be a factor of R and therefore is not greater than $|R|$.

2. When, for a certain argument u, the value $\wp(u)$ is a rational number, then $\wp(2u)$ is also rational. Suppose

$$\wp(u) = \frac{p}{q}, \qquad \wp(2u) = \frac{r}{s},$$

where p and q as well as r and s are coprime integers,

i.e. $$(p,q) = 1, \qquad (r,s) = 1.$$

By the duplication theorem

$$r = \frac{1}{\delta}P(p,q), \qquad s = \frac{1}{\delta}Q(p,q),$$

where $$\delta = (P(p,q),\ Q(p,q)) \leqslant |R|,$$

since $$\wp(2u) = \frac{r}{s} = \frac{P_0(\wp(u))}{Q_0(\wp(u))} = \frac{P(p,q)}{Q(p,q)}.$$

Hence

$$r^2+s^2 = \frac{1}{\delta^2}\{P(p,q)^2+Q(p,q)^2\} \geqslant \frac{1}{R^2}\{P(p,q)^2+Q(p,q)^2\}.$$

Now the binary form of degree eight

$$P(x,y)^2+Q(x,y)^2$$

is positive definite; therefore there exists an absolute positive constant C, such that, for all real x and y,

$$P(x,y)^2+Q(x,y)^2 \geqslant C(x^2+y^2)^4,$$

and, in particular,

$$A(2u) \geqslant \frac{C}{R^2}\{A(u)\}^4,$$

where $A(u)$ and $A(2u)$ denote the arithmetical functions

$$A(u) = p^2+q^2, \qquad A(2u) = r^2+s^2.$$

3. Suppose that
$$A(u) > \left(\frac{C}{R^2}\right)^{-\frac{1}{3}}.$$
Then
$$A(2u) > A(u) > \left(\frac{C}{R^2}\right)^{-\frac{1}{3}},$$
and therefore
$$A(u) < A(2u) < A(4u) < A(8u) < \dots.$$
Thus no two of the rational numbers
$$\wp(u), \quad \wp(2u), \quad \wp(2^2u), \quad \wp(2^3u),\dots$$
are equal.

Now let
$$\wp\left(\frac{h\omega+h'\omega'}{n}\right) = \frac{p}{q}$$
be a division-value which is a rational number. Then all expressions
$$\wp\left(2^f\frac{h\omega+h'\omega'}{n}\right) \qquad (f = 0, 1, 2, 3,\dots)$$
are also division-values with the same denominator n, and they too are rational numbers. But there exist at most n^2 division-values of denominator n; hence the numbers
$$\wp\left(2^f\frac{h\omega+h'\omega'}{n}\right) \qquad (f = 0, 1, 2, 3,\dots)$$
cannot all be different. Therefore we cannot have
$$A\left(\frac{h\omega+h'\omega'}{n}\right) > \left(\frac{C}{R^2}\right)^{-\frac{1}{3}},$$
but must have
$$A\left(\frac{h\omega+h'\omega'}{n}\right) \leqslant \left(\frac{C}{R^2}\right)^{-\frac{1}{3}}.$$
There is only a finite number of solutions of the inequality
$$A(u) \leqslant \left(\frac{C}{R^2}\right)^{-\frac{1}{3}},$$
and they include all division-values which are rational, and so the number of these also must be finite.

4. Our proof gives a method of determining all division-values which are rational numbers.

It is possible, in any special case, to find a constant C and the resultant R. Then we write down all the N fractions p/q, where p and q are coprime integers with
$$p^2+q^2 \leqslant \left(\frac{C}{R^2}\right)^{-\frac{1}{3}}.$$

When p/q is one of these fractions, then we calculate the first $N+1$ members of the sequence

$$\frac{p}{q}, \qquad \frac{p_1}{q_1} = \frac{P(p,q)}{Q(p,q)}, \qquad \frac{p_2}{q_2} = \frac{P(p_1,q_1)}{Q(p_1,q_1)}, \qquad \frac{p_3}{q_3} = \frac{P(p_2,q_2)}{Q(p_2,q_2)}, \ldots.$$

If any one of these fractions, say p_i/q_i, does not satisfy the condition

$$p_i^2+q_i^2 = \left(\frac{C}{R^2}\right)^{-\frac{1}{3}},$$

then p/q is not a division-value. When, however, all members of the set satisfy this inequality, then two members of the set, say p_i/q_i and p_j/q_j, must coincide.

If $p/q = \wp(u)$, then

$$\frac{p_i}{q_i} = \wp(2^i u), \quad \frac{p_j}{q_j} = \wp(2^j u), \quad \wp(2^i u) = \wp(2^j u);$$

hence $$2^i u \equiv \pm 2^j u \pmod{\omega, \omega'}.$$

Therefore $$u = \frac{h\omega + h'\omega'}{n},$$

where n is a divisor of $(2^i - 2^j)(2^i + 2^j)$, i.e. of $2^{2i} - 2^{2j}$, and h and h' are integers, and thus

$$\frac{p}{q} = \wp\left(\frac{h\omega + h'\omega'}{n}\right)$$

is a division-value in this case.

It is not difficult to show, by way of example, that, when $g_2 = 4$, $g_3 = 0$, there are no rational division-values of the $\wp$-function other than $\wp(\frac{1}{2}\omega)$, $\wp(\frac{1}{2}\omega')$, $\wp(\frac{1}{2}\omega + \frac{1}{2}\omega')$.