ARKIV FÖR MATEMATIK Band 2 nr 14

Communicated 27 February 1952 by F. CARLSON and T. NAGELL

A generalization of a theorem of Nagell

By GÖSTA BERGMAN

1. As is well known, the coordinates of the curve

$$y^2 = x^3 - A x - B \qquad (4 A^3 - 27 B^2 \neq 0) \tag{1}$$

can be represented by Weierstrass's $\wp$-function with the invariants $4A$ and $4B$:

$$\begin{cases} x = \wp(u; \quad 4A, \ 4B) \\ y = \frac{1}{2}\wp'(u; \quad 4A, \ 4B). \end{cases}$$

If u is commensurable with a period, the point (x, y) is called *exceptional.* In this case there is a natural number n, which makes nu a period, while $n'u$ is not a period, if $0 < n' < n$. This number n is called the *order* of the point (x, y). The point of order 1, corresponding to $u = 0$, is the infinite point of inflexion on the curve.

If A and B belong to a field Ω and if (x, y) is a point on (1), whose coordinates belong to Ω, we shall say that (x, y) is a *point in* Ω.

In 1935 T. NAGELL ([3], p. 8–15) proved the following theorem:

Theorem 1. — *If A and B are integers in $k(1)$ and if (x, y) is a finite exceptional point in $k(1)$ on the curve* (1), *then x and y are integers. If $y \neq 0$, then y^2 divides $4A^3 - 27B^2$.*

According to G. BILLING ([1], p. 120) this theorem remains true, if $k(1)$ is replaced by a quadratic or cubic field, but BILLING's proof is incomplete, since his lemmas do not say anything, if the order of the point (x, y) is a prime. BILLING's theorem is, however, contained in a generalization of theorem 1, which will be given in this paper.

2. We begin with a lemma on the function

$$x = \wp(u; \quad 4A, \ 4B).$$

It is known that if n is a natural number >1 and if nu is a period but u is not, then

$$\Psi_n(u) = 0,$$

where

$$\Psi_n(u) = \frac{\sigma(nu)}{[\sigma(u)]^{n^2}}.$$

For the function $\Psi_n(u)$ we have the following expression:

$$\Psi_n(u) = \begin{cases} P_n[\wp(u)] & \text{if } n \text{ is odd,} \\ \wp'(u)\, Q_n[\wp(u)] & \text{if } n \text{ is even.} \end{cases}$$

Here P_n and Q_n denote polynomials, whose coefficients are polynomials in A and B with integral rational coefficients. For $n = 3$ we have

$$P_3(x) = 3x^4 - 6Ax^2 - 12Bx - A^2.$$

If we write

$$P_n(x) = \alpha_{n,0}\, x^{\frac{1}{2}(n^2-1)} + \alpha_{n,1}\, x^{\frac{1}{2}(n^2-1)-1} + \cdots + \alpha_{n,\frac{1}{2}(n^2-1)},$$

it is known that $\alpha_{n,0} = n$ and $\alpha_{n,1} = 0$.

Now we shall prove that the polynomials $\alpha_{n,m}$ have the following property:

Lemma. — *If p is a prime > 5, every coefficient of the polynomial $\alpha_{p,m}$ is divisible by p for $m = 2, 3, \ldots, \frac{1}{2}(p-3)$.*

Proof. — If u is absolutely smaller than the shortest period, the function $\wp(u)$ can be expanded in the following series:

$$\wp(u) = \frac{1}{u^2}(1 + c_2 u^4 + c_3 u^6 + \cdots + c_m u^{2m} + \cdots),$$

where $c_2 = \frac{1}{5}A$, $c_3 = \frac{1}{7}B$ and

$$c_m = \frac{3}{(m-3)(2m+1)}(c_2 c_{m-2} + c_3 c_{m-3} + \cdots + c_{m-2} c_2),$$

if $m > 3$. (See, for example, GRAESER [2], p. 25). Thus c_m is a polynomial in A and B with rational coefficients, and if p is a prime and $m \leqq \frac{1}{2}(p-3)$, the coefficients of c_m do not contain p in their denominators.

In the usual way we get

$$\zeta(u) = \frac{1}{u} - \left(\frac{1}{3} c_2 u^3 + \frac{1}{5} c_3 u^5 + \cdots + \frac{1}{2m-1} c_m u^{2m-1} + \cdots\right)$$

and

$$\sigma(u) = u e^{-\left(\frac{1}{3.4} c_2 u^4 + \frac{1}{5.6} c_3 u^6 + \cdots + \frac{1}{2m(2m-1)} c_m u^{2m} + \cdots\right)} =$$

$$= u\left(1 - \frac{1}{60} A u^4 + d_3 u^6 + \cdots + d_m u^{2m} + \cdots\right). \qquad (2)$$

Here d_m is a polynomial in A and B with rational coefficients, which do not contain p in their denominators, if $m \leqq \frac{1}{2}(p-3)$.

We put $x = \wp(u)$ in the polynomial

$$P_p(x) = p x^N + \alpha_{p,2} x^{N-2} + \cdots + \alpha_{p,N},$$

where $N = \frac{1}{2}(p^2 - 1)$, and find

$$u^{2N} P_p[\wp(u)] = p(1 + c_2 u^4 + c_3 u^6 + \cdots)^N + \alpha_{p,2} u^4 (1 + c_2 u^4 + \cdots)^{N-2} + \cdots +$$

$$+ \alpha_{p,m} u^{2m} (1 + c_2 u^4 + \cdots)^{N-m} + \cdots + \alpha_{p,N} u^{2N} = p + \left(\alpha_{p,2} + \frac{1}{5} A p N\right) u^4 + \cdots \quad (3)$$

If we remember the identity

$$P_p[\wp(u)] [\sigma(u)]^{p^2} = \sigma(p u),$$

we get by (2) and (3)

$$\left[p + \left(\alpha_{p,2} + \frac{1}{5} A p N\right) u^4 + \cdots\right] \left[1 - \frac{1}{60} A p^2 u^4 + \cdots\right] = p - \frac{1}{60} A p^5 u^4 + \cdots \quad (4)$$

By this identity we get

$$\alpha_{p,2} = -\frac{1}{60} A p (p^2 - 1)(p^2 + 6),$$

and thus the lemma holds for $m = 2$.

Now suppose that the lemma is true for $\alpha_{p,2}, \alpha_{p,3}, \ldots, \alpha_{p,m-1}$, where $m \leqq \frac{1}{2}(p - 3)$. Then the coefficient of u^{2m} in the left member of (4) may be written

$$\alpha_{p,m} + p \varphi.$$

Here φ is a polynomial in A and B, where p does not appear in the denominator of any coefficient. If we compare the coefficients of u^{2m} in the two members of (4), we get

$$\alpha_{p,m} = p(p^{2m} d_m - \varphi) = p \varphi_1,$$

where the coefficients of φ_1 do not contain p in their denominators. It follows that they are integral, since $\alpha_{p,m}$ has integral coefficients, and the lemma is proved.

3. Now we suppose that A and B are integers in əqʇ algebraic number field Ω. If $n u$ is not a period, it is known that

$$\wp(n u) = \wp(u) - \frac{\Psi_{n+1}(u) \Psi_{n-1}(u)}{[\Psi_n(u)]^2} = \frac{x^{n^2} + \cdots}{n^2 x^{n^2-1} + \cdots}, \quad (5)$$

where both the numerator and the denominator of the last member have integral coefficients. Thus if $\wp(n u)$ is an integer in some algebraic field, x is also an integer.

First let the order of the point (x, y) be even and equal to $2n$. Then the number $\wp(nu)$ satisfies the equation

$$[\wp(nu)]^3 - A\wp(nu) - B = 0.$$

Thus $\wp(nu)$ is integral, and consequently x is integral.

Next let the order of (x, y) be divisible by the odd prime p and equal to pn. Then the number $\wp(nu)$ satisfies the equation

$$P_p[\wp(nu)] = 0.$$

Thus $p\wp(nu)$ is integral, and by (5) we see that the same is true of px.

If the order of (x, y) is divisible by the two odd primes p and q, px and qx are integral, and consequently x is integral.

There remains the case where the order of the point (x, y) is a power of an odd prime.

First let (x, y) be a point in Ω of order 3. We may suppose $x \neq 0$. Then $3x$ and, by (1), $9y$ are integral, and if we put

$$3x = \xi, \quad 9y = \eta,$$

the equation (1) takes the form

$$\eta^2 = 3(\xi^3 - 9A\xi - 27B). \tag{6}$$

The number ξ also satisfies the equation

$$27P_3\left(\frac{\xi}{3}\right) = \xi^4 - 18A\xi^2 - 108B\xi - 27A^2 = 0. \tag{7}$$

Let $\mathfrak{p}$ be a prime ideal which divides 3, and suppose that 3 is divisible by $\mathfrak{p}^h$ but not by $\mathfrak{p}^{h+1}$ and that ξ is divisible by $\mathfrak{p}^k$ but not by $\mathfrak{p}^{k+1}$.

Suppose $k < h < 8$. Then (6) shows that

$$k \equiv h \pmod 2,$$

and consequently $h \geqq 2$ and $k \leqq h - 2$. In (7) the first term is not divisible by $\mathfrak{p}^{4k+1}$, while the other terms are divisible by

$$\mathfrak{p}^{2h+2k}, \quad \mathfrak{p}^{3h+k} \text{ and } \mathfrak{p}^{3h},$$

respectively. But

$$2h + 2k > 4k, \quad 3h + k > 4k \text{ and } 3h > 4k,$$

because we have supposed $k \leqq h - 2 \leqq 5$. Since this is impossible, we have $k \geqq h$, if $h < 8$. It follows that if 3 is not divisible by the eighth power of any prime ideal in Ω, then x and y are integral, if (x, y) is a point in Ω of order 3. If (x, y) has the order 3^ν, $\nu > 1$, we put $n = 3^{\nu-1}$ in (5) and conclude that x is integral in this case too, since $\wp(3^{\nu-1}u)$ is integral.

Next let (x, y) be a point in Ω of order p, where p is a prime > 3, and suppose $x \neq 0$. If we put $px = \xi$ and $p^2y = \eta$, the equation (1) takes the form

$$\eta^2 = p(\xi^3 - A p^2 \xi - B p^3). \tag{8}$$

The number ξ also satisfies the equation

$$p^{N-1} P_p\left(\frac{\xi}{p}\right) = \xi^N + \alpha_{p,2} p\, \xi^{N-2} + \cdots + \alpha_{p,m} p^{m-1} \xi^{N-m} + \cdots + \alpha_{p,N} p^{N-1} = 0, \tag{9}$$

where $N = \frac{1}{2}(p^2 - 1)$. Let $\mathfrak{p}$ be a prime ideal which divides p, and let p and ξ be divisible by $\mathfrak{p}^h$ and $\mathfrak{p}^k$ respectively, but not by $\mathfrak{p}^{h+1}$ and $\mathfrak{p}^{k+1}$.

Suppose $k < h < p - 1$. By (8) we conclude

$$k \equiv h \pmod 2,$$

and consequently $h \geqq 2$ and $k \leqq h - 2$. The number

$$\alpha_{p,m} p^{m-1} \xi^{N-m} \tag{10}$$

is divisible by

$$\mathfrak{p}^{kN + (h-k)m - h}$$

and a fortiori by

$$\mathfrak{p}^{kN + 2m - h}.$$

If $m > \frac{1}{2}(p-3)$, the last exponent is $> kN$. But if $m \leqq \frac{1}{2}(p-3)$, our lemma shows that $\alpha_{p,m}$ is divisible by $\mathfrak{p}^h$, and thus (10) is divisible by

$$\mathfrak{p}^{kN+2m}$$

and a fortiori by

$$\mathfrak{p}^{kN+4}.$$

Since the first term of (9) is not divisible by

$$\mathfrak{p}^{kN+1},$$

we have reached a contradiction. Thus $k \geqq h$, if $h < p - 1$. As in the case $p = 3$ we find that a point (x, y) in Ω of order p^ν, $\nu \geqq 1$, has integral coordinates, if p is not divisible by the $(p-1)$:th power of any prime ideal in Ω.

Finally we shall use the identity

$$4A^3 - 27B^2 = (6Ax^2 - 9Bx - 4A^2)(3x^2 - A) - 9(2Ax - 3B)(x^3 - Ax - B). \tag{11}$$

Suppose $y \neq 0$. In the right member of (11) A and B can be eliminated, if we put

$$\frac{3x^2 - A}{2y} = t$$

and use the equation (1). Then (11) is transformed into

$$4A^3 - 27B^2 = y^2[36x^2(t^2 - 3x) + 108xyt - 32yt^3 - 27y^2]. \tag{12}$$

Since

$$2x + \wp(2u) = \left(\frac{3x^2 - A}{2y}\right)^2,$$

the number t is integral, if x and $\wp(2u)$ are integral. But then (12) shows that y^2 divides $4A^3 - 27B^2$.

We have proved the following theorem:

Theorem 2. — *Let A and B be integers in the algebraic number field Ω, and let (x, y) be an exceptional point in Ω of order $n > 1$ on the curve*

$$y^2 = x^3 - Ax - B. \qquad (4A^3 - 27B^2 \neq 0)$$

Then x and y are integers in the following cases:

1. *If n is not a power of an odd prime.*
2. *If n is a power of 3 and the number 3 is not divisible by the eighth power of any prime ideal in Ω.*
3. *If n is a power of a prime $p > 3$ and p is not divisible by the $(p-1)$:th power of any prime ideal in Ω.*

If n is a power of the odd prime p, the number px is always integral.

If $n > 2$ and the two numbers $\wp(u) = x$ and $\wp(2u)$ are integral, then y is an integer $\neq 0$, and y^2 divides $4A^3 - 27B^2$.

It is not possible to substitute "p:th" for "$(p-1)$:th" in the case 3. above, as is shown by the following examples:

Example 1. — In $\Omega = k(\sqrt[4]{5})$ the curve

$$y^2 = x^3 - 27 \cdot 269x + 54 \cdot 9481\sqrt{5}$$

has the following points of order 5:

$$\left[\frac{3 \cdot 97}{\sqrt[4]{5}}, \pm\frac{2^6 \cdot 3^4}{(\sqrt[4]{5})^3}\right], \quad \left[-\frac{3 \cdot 47}{\sqrt[4]{5}}, \pm\frac{2^4 \cdot 3^5}{(\sqrt[4]{5})^3}\right].$$

Example 2. — In $\Omega = k(\sqrt[6]{7})$ the curve

$$y^2 = x^3 - 27 \cdot 967\sqrt[3]{7}\,x + 27 \cdot 165086$$

has the following points of order 7:

$$\left[-\frac{3 \cdot 71}{\sqrt[3]{7}}, \pm\frac{2^5 \cdot 3^5}{\sqrt{7}}\right], \quad \left[\frac{3 \cdot 73}{\sqrt[3]{7}}, \pm\frac{2^4 \cdot 3^4}{\sqrt{7}}\right], \quad \left[\frac{3 \cdot 145}{\sqrt[3]{7}}, \pm\frac{2^3 \cdot 3^6}{\sqrt{7}}\right].$$

In the case $p = 3$ NAGELL gives an example ([4], p. 12), where Ω has the degree 8.

BIBLIOGRAPHY. [1]. **Billing, G.** Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht Eins, Nova Acta Reg. Soc. Sci. Ups., ser. IV, t. 11, n:o 1, Uppsala 1938. — [2]. **Graeser, E.** Einführung in die Theorie der elliptischen Funktionen und deren Anwendungen, München 1950. — [3]. **Nagell, T.** Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre, Skrifter utg. av det Norske Videnskaps-Akademi i Oslo, 1935, Mat.-Naturv. Kl., No. 1. — [4]. ——. Les points exceptionnels sur les cubiques planes du premier genre, I, Nova Acta Reg. Soc. Sci. Ups., ser. IV, t. 14, n:o 1, Uppsala 1946.

Tryckt den 18 september 1952

Uppsala 1952. Almqvist & Wiksells Boktryckeri AB