ON THE EXCEPTIONAL GROUP OF A WEIERSTRASS CURVE IN AN ALGEBRAIC FIELD

BY

GÖSTA BERGMAN

1. Let A and B be two numbers satisfying

$$4A^3 - 27B^2 \neq 0. \tag{1}$$

Then

$$y^2 = x^3 - Ax - B \tag{2}$$

is a curve of genus 1, and its coordinates can be represented by

$$\begin{cases} x = \wp(u;\, 4A,\, 4B); \\ y = \tfrac{1}{2}\wp'(u;\, 4A,\, 4B). \end{cases} \tag{3}$$

If ω, ω' is a primitive pair of periods of the $\wp$-function, the number u is determined mod ω, ω' by the point (x, y), which will be called *the point* u. If ν is a rational integer, and if

$$\nu u \not\equiv 0 \pmod{\omega, \omega'},$$

the coordinates of the point νu will generally be denoted by (x_ν, y_ν). Three points u_1, u_2, u_3 lie on a straight line, if

$$u_1 + u_2 + u_3 \equiv 0 \pmod{\omega, \omega'},$$

and conversely. If the number u is commensurable with a period, and if q is the smallest natural number that makes qu a period, then u is called an *exceptional point of order* q (see Nagell [7]). Since there are two independent periods, there exist q^2 exceptional points, whose orders divide q. The point of order 1 is the infinite point of inflexion, and the points of order 2 are given by $y = 0$.

If A and B belong to a field $\mathbf{\Omega}$, a point on (2) is said to be a *point in* $\mathbf{\Omega}$, if its coordinates belong to this field. If u_1 and u_2 are exceptional points in $\mathbf{\Omega}$, the same is true of $u_1 + u_2$, and in this way the exceptional points in $\mathbf{\Omega}$ form an abelian group, the *exceptional group in* $\mathbf{\Omega}$ on the curve (2) (see Châtelet [5]). If $\mathbf{\Omega}$ is an algebraic field, the following result is known (see Cassels [4] and Bergman [1]):

Theorem 1. *Let* $\mathbf{\Omega}$ *be an algebraic field, let* A *and* B *be integers in* $\mathbf{\Omega}$ *which satisfy* (1), *and let* u *be an exceptional point of order* $q > 1$ *in* $\mathbf{\Omega}$ *on the curve* (2). *Then the coordinates* (x, y) *of this point are integers in* $\mathbf{\Omega}$, *if* q *is not a power of an odd prime, and if* q *is a power of the odd prime* p, *then* px *is an integer in* $\mathbf{\Omega}$.

It follows from a theorem due to Weil [9] that the exceptional group in an algebraic field is finite, but Weil's proof does not make it possible to find the points of the group, if $\mathbf{\Omega}$, A and B are given. In the case $\mathbf{\Omega} = \boldsymbol{K}(1)$ this problem has been solved by Nagell ([7], p. 8–15), who has proved the following theorem:

Theorem 2. *Let* A *and* B *be integers in* $\boldsymbol{K}(1)$, *which satisfy* (1), *and let* (x, y) *be an exceptional point in* $\boldsymbol{K}(1)$ *on the curve* (2), *whose order is* > 2. *Then* x *and* y *are integers, and* y^2 *divides* $4A^3 - 27B^2$.

By a similar theorem the exceptional points can be found, if $\mathbf{\Omega}$ is an imaginary quadratic field (see Billing [3], p. 120, Nagell [8], p. 12, Cassels [4], and Bergman [1]). Châtelet has tried to solve the general problem (see [5], [6]), but he has not published his results.

In this paper we shall find a limit of the order of an exceptional point in $\mathbf{\Omega}$ on a given curve (2), if $\mathbf{\Omega}$ is a given algebraic field, and at the same time we shall give an independent proof of this special case of Weil's theorem. If the order of an exceptional point cannot exceed an assigned limit M, there cannot be more than M^2 exceptional points in $\mathbf{\Omega}$, and hence they can be determined (see Nagell [8], p. 9–11). A limit of the order of a point is given by theorem 6 and theorem 12.

2. If ν is a rational integer, we define

$$\psi_\nu(u) = \frac{\sigma(\nu u)}{[\sigma(u)]^{\nu^2}} \qquad (\psi_0(u) = 0);$$

then $\psi_{-\nu}(u) = -\psi_\nu(u)$, and it is known that

$$x_\varkappa - x_\lambda = \wp(\varkappa u) - \wp(\lambda u) = -\frac{\psi_{\varkappa+\lambda}(u)\,\psi_{\varkappa-\lambda}(u)}{\psi_\varkappa^2(u)\,\psi_\lambda^2(u)}, \tag{4}$$

if $\varkappa$ and λ are rational integers $\neq 0$. If $\varkappa$, λ and μ are rational integers $\neq 0$, we have

$$[\wp(\varkappa u) - \wp(\lambda u)] + [\wp(\lambda u) - \wp(\mu u)] + [\wp(\mu u) - \wp(\varkappa u)] = 0,$$

and consequently

$$(5) \qquad \psi_{\varkappa+\lambda}(u)\,\psi_{\varkappa-\lambda}(u)\,\psi_{\mu}^{2}(u)+\psi_{\lambda+\mu}(u)\,\psi_{\lambda-\mu}(u)\,\psi_{\varkappa}^{2}(u)+\psi_{\mu+\varkappa}(u)\,\psi_{\mu-\varkappa}(u)\,\psi_{\lambda}^{2}(u)=0;$$

here $\varkappa$, λ, μ may be supposed to be any rational integers. If we choose

$$\begin{cases}\varkappa=\nu+1;\\ \lambda=\nu-1;\\ \mu=1\end{cases} \quad\text{or}\quad \begin{cases}\varkappa=\nu+1;\\ \lambda=\nu;\\ \mu=1,\end{cases}$$

we find (the letter u is omitted):

$$(6) \qquad \begin{cases}\psi_{2\nu}\,\psi_2=\psi_\nu\,[\psi_{\nu+2}\,\psi_{\nu-1}^{2}-\psi_{\nu-2}\,\psi_{\nu+1}^{2}];\\ \psi_{2\nu+1}\;=\psi_{\nu+2}\,\psi_{\nu}^{3}-\psi_{\nu-1}\,\psi_{\nu+1}^{3}.\end{cases}$$

We may also take

$$\begin{cases}\varkappa=\nu-1;\\ \lambda=\nu+1\end{cases} \quad\text{or}\quad \begin{cases}\varkappa=\nu;\\ \lambda=\nu+1\end{cases}$$

in (4) and find

$$(7) \qquad \begin{cases}\psi_{2\nu}\,\psi_2=\psi_{\nu-1}^{2}\,\psi_{\nu+1}^{2}\,(x_{\nu-1}-x_{\nu+1});\\ \psi_{2\nu+1}\;=\psi_{\nu}^{2}\,\psi_{\nu+1}^{2}\,(x_{\nu}-x_{\nu+1}).\end{cases}$$

Now it is known that

$$\psi_1=1;\ \psi_2=-2\,y;$$
$$\psi_3=3\,x^4-6\,A\,x^2-12\,B\,x-A^2;$$
$$\psi_4=-2\,y\,(2\,x^6-10\,A\,x^4-40\,B\,x^3-10\,A^2\,x^2-8\,A\,B\,x+2\,A^3-16\,B^2),$$

and it follows from the formulas (6) that $\psi_{2\nu+1}$ and $\frac{1}{\psi_2}\psi_{2\nu}$ are polynomials in x, A and B with rational integral coefficients. It is also known (see for instance Bergman [2], p. 493–494) that

$$(8) \qquad \frac{y_\nu}{y_1}=\frac{\wp'(\nu u)}{\wp'(u)}=-\frac{\psi_{2\nu}}{\psi_2\,\psi_\nu^{4}}.$$

A line

$$y=\delta\,x+\varepsilon$$

cuts the curve (2) in three points u_1, u_2, u_3, and it is seen that

$$\delta^2=\wp(u_1)+\wp(u_2)+\wp(u_3).$$

If ν is a natural number $\geqq 2$, and if neither $(\nu \pm 1)u$ nor νu is a period, the three finite points u, $(\nu-1)u$, $-\nu u$ lie on a straight line, and we have

$$x_\nu \neq x_1, \quad -\delta = \frac{y_\nu + y_1}{x_\nu - x_1}$$

and consequently

$$\left(\frac{y_\nu + y_1}{x_\nu - x_1}\right)^2 = x_1 + x_{\nu-1} + x_\nu . \tag{9}$$

If $\nu = 2$, and if $2u$ is not a period, we also have

$$\delta = \frac{3x_1^2 - A}{2y_1} \tag{10}$$

and hence

$$\left(\frac{3x_1^2 - A}{2y_1}\right)^2 = 2x_1 + x_2 . \tag{11}$$

By (10) we may write

$$\begin{cases} A = 3x_1^2 - 2\delta y_1; \\ B = x_1^3 - Ax_1 - y_1^2 = -2x_1^3 + 2\delta x_1 y_1 - y_1^2, \end{cases}$$

and it follows that

$$4A^3 - 27B^2 = y_1^2[36x_1^2(x_2 - x_1) + 108\delta x_1 y_1 - 32\delta^3 y_1 - 27y_1^2], \tag{12}$$

if $y_1 \neq 0$ and if δ is defined by (10).

If $\mathfrak{p}$ is a prime ideal in an algebraic field $\mathbf{\Omega}$, and if α is a number $\neq 0$ in $\mathbf{\Omega}$, it will be convenient to write

$$\mathfrak{p}^\nu // \alpha, \tag{13}$$

f

$$\alpha = \frac{\mathfrak{p}^\nu \mathfrak{a}}{\mathfrak{b}},$$

where $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals in $\mathbf{\Omega}$ and $\mathfrak{p} \nmid \mathfrak{a}\mathfrak{b}$. Here ν may be any rational integer, but if $\nu \geqq 0$, α is said to be an *integer mod* $\mathfrak{p}$.

If $\mathfrak{p}$ is a divisor of 2, and if A and B are integers mod $\mathfrak{p}$, it follows from theorem 1 that the coordinates of a finite exceptional point in $\mathbf{\Omega}$ on the curve (2) are integers mod $\mathfrak{p}$.

3. Let $\mathbf{\Omega}$ be an algebraic field, let $\mathfrak{p}$ be a prime ideal in $\mathbf{\Omega}$, let A and B be integers mod $\mathfrak{p}$ in $\mathbf{\Omega}$ which satisfy (1), and let u be a finite point in $\mathbf{\Omega}$ on (2), whose coordinates are integers mod $\mathfrak{p}$. Then the numbers $\psi_\nu(u)$ $(\nu = 0, \pm 1, \pm 2, \ldots)$ are integers mod $\mathfrak{p}$, and we suppose

$$\psi_2 \psi_3 \psi_4 \neq 0, \quad \mathfrak{p}^{3r} // \psi_2, \quad \mathfrak{p}^{8r} // \psi_3, \quad \mathfrak{p}^{15r} // \psi_4, \tag{14}$$

where r is a rational integer $\geqq 0$. Then it follows from the formulas (6) that

$$\mathfrak{p}^{(\nu^2-1)r} / \psi_\nu, \quad \text{if } \nu \neq 0, \tag{15}$$

and we shall examine the conditions for

$$\mathfrak{p}^{(\nu^2-1)r+1} / \psi_\nu .$$

The result will be found in theorem 3, but the following lemmas are needed:

Lemma 1. *If ν and t are natural numbers, and if $\psi_t \neq 0$, then*

$$\mathfrak{p}^{(\nu^2-1)t^2 r} \Big/ \frac{\psi_{\nu t}}{\psi_t} .$$

Proof. By (6)

$$\frac{\psi_{2t}}{\psi_t} = \frac{1}{\psi_2} [\psi_{t+2} \psi_{t-1}^2 - \psi_{t-2} \psi_{t+1}^2],$$

and then it follows from (15) that the lemma is true for $\nu = 2$. Now let γ be a natural number and choose

$$\begin{cases} \varkappa = \gamma t + 1; \\ \lambda = \gamma t - 1; \\ \mu = 1 \end{cases} \quad \text{or} \quad \begin{cases} \varkappa = (\gamma + 1) t; \\ \lambda = \gamma t; \\ \mu = 1 \end{cases}$$

in (5). We find

$$\frac{\psi_{2\gamma t}}{\psi_t} = \frac{1}{\psi_2} \frac{\psi_{\gamma t}}{\psi_t} [\psi_{\gamma t+2} \psi_{\gamma t-1}^2 - \psi_{\gamma t-2} \psi_{\gamma t+1}^2];$$

$$\frac{\psi_{(2\gamma+1)t}}{\psi_t} = \psi_{(\gamma+1)t+1} \psi_{(\gamma+1)t-1} \left(\frac{\psi_{\gamma t}}{\psi_t}\right)^2 - \psi_{\gamma t+1} \psi_{\gamma t-1} \left(\frac{\psi_{(\gamma+1)t}}{\psi_t}\right)^2 .$$

Here we take $\gamma = 1, 2, 3, \ldots,$ and the lemma follows by induction.

Lemma 2. *If*

$$\mathfrak{p}^{(s^2-1)r+1} / \psi_s \quad \textit{and} \quad \mathfrak{p}^{(t^2-1)r+1} / \psi_t,$$

where $0 < s < t$, we have $t - s \geqq 3$.

Proof. First suppose $t = s + 1$. Then we choose

$$\begin{cases} \varkappa = s - 1; \\ \lambda = 2; \\ \mu = 1 \end{cases}$$

in (5) and find

$$\psi_{s+1}\,\psi_{s-3} + \psi_3\,\psi_{s-1}^2 - \psi_s\,\psi_{s-2}\,\psi_2^2 = 0\,.$$

It follows that

$$\mathfrak{p}^{(s^2-2s)r+1}/\psi_{s-1},$$

but then s may be replaced by $s-1$ and so on, and this is impossible, since $\mathfrak{p}^{15r+1} \nmid \psi_4$.

Next suppose $t = s + 2$. Then we take

$$\begin{cases} \varkappa = s; \\ \lambda = 2; \\ \mu = 1 \end{cases}$$

in (5) and find

$$\psi_{s+2}\,\psi_{s-2} + \psi_3\,\psi_s^2 - \psi_{s+1}\,\psi_{s-1}\,\psi_2^2 = 0.$$

It follows that

$$\mathfrak{p}^{(s^2 \pm 2s)r+1}/\psi_{s\pm 1},$$

but this is impossible, according to the first part of the proof.

Consequently $t - s \geqq 3$, and the lemma is proved.

Lemma 3. *Suppose*

$$\mathfrak{p}^{(\nu^2-1)r}//\psi_\nu,\ \ \nu = 1, 2, 3, \ldots, s-1;\ \ \mathfrak{p}^{(s^2-1)r+1}/\psi_s,$$

where s is a natural number $\geqq 5$. Then

$$\mathfrak{p}^{(t^2-1)r+1}/\psi_t,$$

if and only if t is divisible by s.

Proof. If $\psi_s = 0$, we have $\psi_{\nu s} = 0$ $(\nu = 1, 2, 3, \ldots)$, and if $\psi_s \neq 0$, $\dfrac{\psi_{\nu s}}{\psi_s}$ is divisible by $\mathfrak{p}^{(\nu^2-1)s^2 r}$ by lemma 1. This proves the first part of the lemma.

To prove the second part we suppose

$$\mathfrak{p}^{(t^2-1)r+1}/\psi_t,\ \text{where}\ \nu s < t = \nu s + \gamma < (\nu+1)\,s.$$

By lemma 2 $\gamma \geqq 3$, and we may suppose

$$\mathfrak{p}^{(h^2-1)r} // \psi_h, \quad h = \nu s + 1, \ \nu s + 2, \ \ldots, \ \nu s + \gamma - 1.$$

If γ is even ($\gamma = 2\beta$), we take

$$\begin{cases} \varkappa = \nu s + \beta - 1; \\ \lambda = \beta + 1; \\ \mu = \beta - 1 \end{cases}$$

in (5) and find

$$\psi_t \, \psi_{\nu s-2} \, \psi_{\beta-1}^2 + \psi_\gamma \, \psi_2 \, \psi_{\nu s+\beta-1}^2 - \psi_{t-2} \, \psi_{\nu s} \, \psi_{\beta+1}^2 = 0,$$

but this is impossible, since $0 < \gamma < s$ and $\nu s < \nu s + \beta - 1 < t$.

If γ is odd ($\gamma = 2\beta + 1$), we take

$$\begin{cases} \varkappa = \nu s + \beta; \\ \lambda = \beta + 1; \\ \mu = \beta \end{cases}$$

in (5) and find

$$\psi_t \, \psi_{\nu s-1} \, \psi_\beta^2 + \psi_\gamma \, \psi_{\nu s+\beta}^2 - \psi_{t-1} \, \psi_{\nu s} \, \psi_{\beta+1}^2 = 0,$$

and this is impossible, since $0 < \gamma < s$ and $\nu s < \nu s + \beta < t$.

Consequently t must be divisible by s, and the lemma is proved.

Lemma 4. *There exists a number $s \geqq 5$ satisfying*

$$\mathfrak{p}^{(\nu^2-1)r} // \psi_\nu, \quad \nu = 1, 2, \ldots, s-1; \quad \mathfrak{p}^{(s^2-1)r+1} / \psi_s,$$

and if N is the norm of $\mathfrak{p}$, we have

$$s \leqq 2N + 1.$$

Proof. Let t be a number $\geqq 5$, and suppose

$$\mathfrak{p}^{(\nu^2-1)r} // \psi_\nu, \quad \nu = 1, 2, \ldots, t-1.$$

Then it follows from (4) that

$$\mathfrak{p}^{2r} // x_\varkappa - x_\lambda,$$

if $0 < \lambda < \varkappa$ and $\varkappa + \lambda < t$. Hence the numbers

$$0, \ x_2 - x_1, \ x_3 - x_1, \ \ldots, \ x_{\frac{1}{2}(t-1)} - x_1 \quad (t \text{ odd})$$

or

$$0, \ x_2 - x_1, \ x_3 - x_1, \ \ldots, \ x_{\frac{1}{2}t} - x_1 \quad (t \text{ even})$$

are divisible by $\mathfrak{p}^{2r}$ but incongruent mod $\mathfrak{p}^{2r+1}$, and consequently

$$t \leqq 2N+1.$$

If t is taken as large as possible, we have

$$\mathfrak{p}^{(t^2-1)r+1}/\psi_t,$$

and the lemma is proved.

If the lemmas 3 and 4 are combined, we get the following theorem:

Theorem 3. *Let $\mathbf{\Omega}$ be an algebraic field, let $\mathfrak{p}$ be a prime ideal in $\mathbf{\Omega}$ with the norm N, let A and B be integers mod $\mathfrak{p}$ in $\mathbf{\Omega}$ which satisfy* (1), *and let u be a finite point in $\mathbf{\Omega}$ on* (2), *whose coordinates are integers mod $\mathfrak{p}$. Finally let r be a rational integer and suppose*

$$\psi_2\,\psi_3\,\psi_4 \neq 0;\ \mathfrak{p}^{3r}//\psi_2;\ \mathfrak{p}^{8r}//\psi_3;\ \mathfrak{p}^{15r}//\psi_4.$$

Then

$$\mathfrak{p}^{(\nu^2-1)r}/\psi_\nu,\ \textit{if}\ \nu \neq 0,$$

and there exists a number $s \geqq 5$ satisfying

$$\mathfrak{p}^{(\nu^2-1)r}//\psi_\nu,\ \textit{if ν is not divisible by s};$$
$$\mathfrak{p}^{(\nu^2-1)r+1}/\psi_\nu,\ \textit{if ν is divisible by s};$$
$$s \leqq 2N+1.$$

4. In the following sections $\mathfrak{p}$ is supposed to be a divisor of 2, and a natural number m is defined by

$$\mathfrak{p}^m//2. \tag{16}$$

Since the curves (2) and

$$y^2 = x^3 - A\,\alpha^4\,x - B\,\alpha^6$$

are equivalent, if α is a number $\neq 0$ in $\mathbf{\Omega}$, we shall also suppose that A and B are integers mod $\mathfrak{p}$ and that A^3 and B^2 are not both divisible by $\mathfrak{p}^{12}$.

The following theorem will often be used:

Theorem 4. *Let u be an exceptional point in $\mathbf{\Omega}$ of order $q > 4$, and suppose*

$$\mathfrak{p}^c//y_1,\ \mathfrak{p}^c//y_2,$$

where c is a rational integer $\geqq 0$. Define a number n by

$$n = m + c,$$

where m is defined by (16). *Then* $\mathfrak{p}^{n}//\psi_2$ *and* $\mathfrak{p}^{5n}//\psi_4$, *and we have one of the following cases:*

1. $\mathfrak{p}^{8n}//\psi_3^3$. *Then theorem* 3 *may be applied.*

2. $\mathfrak{p}^{8n}\nmid\psi_3^3$. *Then* $4/q$, *and if the numbers k and d are defined by*

$$\mathfrak{p}^{k}//\psi_3;\ 8n=3k+d,$$

we have

$$\left\{\begin{array}{ll} \mathfrak{p}^{\frac{1}{8}(\nu^2-1)k}//\psi_\nu, & \textit{if}\ \nu\equiv\pm1 \pmod 4; \\ \mathfrak{p}^{\frac{1}{8}[(\nu^2-1)k+d]}//\psi_\nu, & \textit{if}\ \nu\equiv2 \pmod 4; \\ \mathfrak{p}^{\frac{1}{8}[(\nu^2-1)k+5d]}/\psi_\nu, & \textit{if}\ \nu\equiv0 \pmod 4). \end{array}\right. \tag{17}$$

3. $\mathfrak{p}^{8n+1}/\psi_3^3$. *Then* $3/q$, *and if the numbers k and d are defined by*

$$\mathfrak{p}^{k}//\psi_3;\ 3k=8n+d,$$

we have

$$\left\{\begin{array}{l} \mathfrak{p}^{\frac{1}{3}(\nu^2-1)n}//\psi_\nu,\ \textit{if}\ 3\nmid\nu; \\ \mathfrak{p}^{\frac{1}{3}[(\nu^2-1)n+d]}/\psi_\nu,\ \textit{if}\ 3/\nu. \end{array}\right. \tag{18}$$

Proof. Since $\psi_2=-2y_1$, we have $\mathfrak{p}^{n}//\psi_2$, and if we take $\nu=2$ in (8), it follows that $\mathfrak{p}^{5n}//\psi_4$. The formulas (17) and (18) may be proved by induction, if (6) is used. In the second case it follows from (17) that q is divisible by 4, and in the third case it follows from (18) that q is divisible by 3.

5. In this section we shall suppose

$$\mathfrak{p}/A,\ \text{if}\ \mathfrak{p}^{m}//B, \tag{19}$$

where m is defined by (16). In this case a limit of the order of an exceptional point in $\mathbf{\Omega}$ is found in the following way:

Theorem 5. *Let A and B satisfy* (19), *let u be an exceptional point in $\mathbf{\Omega}$ of order $q>2$, and define a rational integer $c\geqq0$ by*

$$\mathfrak{p}^{c}//y_1.$$

Then c depends on $\mathbf{\Omega}$, $\mathfrak{p}$, A and B only. The number c also satisfies the inequality

$$2c\leqq m+3,$$

except if $\mathfrak{p}^{2}//A$ *and* $\mathfrak{p}^{m+3}//B$, *but in this case the only possible value of q is* 4.

Proof. We have the following cases:

1. $\mathfrak{p}\nmid A$; $\mathfrak{p}^{b}//B$, $b<m$. Since the coordinates of an exceptional point are integers mod $\mathfrak{p}$, (11) gives $\mathfrak{p}^{m}/3x_1^2-A$, but then $\mathfrak{p}^{m}/x_1^3-Ax_1$ and $\mathfrak{p}^{b}//x_1^3-Ax_1-B$. Hence $2c=b$, and b depends on $\mathbf{\Omega}$, $\mathfrak{p}$ and B only.

2. $\mathfrak{p}\nmid A$; $\mathfrak{p}^{m+1}/B$. As in case 1, $\mathfrak{p}^{m}/3x_1^2-A$, but then $\mathfrak{p}/y_1$, and now (11) shows that $\mathfrak{p}^{m+1}/3x_1^2-A$. It follows that $\mathfrak{p}\nmid x_1$ and $\mathfrak{p}^{m}//x_1^2-A$, and hence $\mathfrak{p}^{m}//x_1^3-Ax_1-B$ and $2c=m$.

3. $\mathfrak{p}//A$. Since $\mathfrak{p}^{m}/3x_1^2-A$, we have $\mathfrak{p}/x_1$. But then $\mathfrak{p}//3x_1^2-A$, and since $2x_1+x_2$ is an integer mod $\mathfrak{p}$, (11) shows that $c=0$.

4. $\mathfrak{p}^2//A$; $\mathfrak{p}\nmid B$. As in case 3, $\mathfrak{p}^{m}/3x_1^2-A$ and $\mathfrak{p}/x_1$. Consequently $\mathfrak{p}\nmid x_1^3-Ax_1-B$ and $c=0$.

5. $\mathfrak{p}^2//A$; $\mathfrak{p}/B$. Since $\mathfrak{p}/x_1$, we have $c>0$. If $q\neq 4$, we replace u by $2u$ in (11) and find $\mathfrak{p}/x_2$. But $2x_1+x_2$ is a square, and consequently $\mathfrak{p}^2/2x_1+x_2$ and $\mathfrak{p}^2/x_2$. Then $\mathfrak{p}^2//3x_2^2-A$, and since $\mathfrak{p}/y_2$, we have $m=1$ and $\mathfrak{p}\nmid 2x_2+x_4$. But this is impossible, since if $q\neq 8$, we may replace u by $4u$ in (11) and find $\mathfrak{p}/x_4$, and if $q=8$, we have

$$x_4^3-Ax_4-B=0$$

and consequently $\mathfrak{p}/x_4$. It follows that $q=4$ and

$$x_2^3-Ax_2-B=0. \tag{20}$$

Consequently $\mathfrak{p}/x_2$, and since $2x_1+x_2$ is a square, we have $\mathfrak{p}^2/x_2$. Then it follows from (11) that $\mathfrak{p}^3/3x_1^2-A$, and hence $\mathfrak{p}//x_1$. Now (20) shows that $\mathfrak{p}^4/B$, and if $B\neq 0$, we define b by $\mathfrak{p}^{b}//B$. Then $\mathfrak{p}^{b-2}//x_2$ by (20).

5.1. $b<m+3$. Then $\mathfrak{p}^{b-2}//2x_1+x_2$, and (9) gives ($\nu=2$)

$$\left(\frac{y_1}{x_2-x_1}\right)^2=2x_1+x_2. \tag{21}$$

Consequently $2c=b$.

5.2. $b=m+3$. Define d by $\mathfrak{p}^{d}//4A^3-27B^2$. If $2c<2m+3$, (12) shows that $4c=d$, and if $2c>2m+3$, (12) gives $2c+2m+3=d$. Hence $4c=d$, if $d<4m+6$, and $2c=d-2m-3$, if $d>4m+6$ ($d=4m+6$ is impossible).

5.3. $b>m+3$. Then $\mathfrak{p}^{m+1}//2x_1+x_2$, and (21) gives $2c=m+3$.

5.4. $B=0$. Since $\mathfrak{p}^2/x_2$, we cannot have

$$x_2^2-A=0;$$

consequently $x_2=0$, and (21) gives $2c=m+3$.

6. $\mathfrak{p}^3/A$; $\mathfrak{p}\nmid B$. Since $\mathfrak{p}/x_1$, we have $c=0$.

7. $\mathfrak{p}^3/A$; $\mathfrak{p}^{b}//B$, where $1\leqq b\leqq 4$. As in case 5, $\mathfrak{p}/x_2$. But since $\mathfrak{p}/x_1$ and $\mathfrak{p}/B$, we have $c>0$, and then (11) shows that $\mathfrak{p}^2/x_1$. Consequently $\mathfrak{p}^{b}//x_1^3-Ax_1-B$ and $2c=b$.

8. $\mathfrak{p}^3//A$; $\mathfrak{p}^5/B$. As in case 7, $\mathfrak{p}/x_2$ and $\mathfrak{p}^2/x_1$. But then $\mathfrak{p}^2/y_1$, and since $\mathfrak{p}^3//3x_1^2-A$, we find $\mathfrak{p}\not/\,2x_1+x_2$, and this is impossible.

9. $\mathfrak{p}^4/A$; $\mathfrak{p}^5//B$. As in case 7, $\mathfrak{p}^2/x_1$, but then $\mathfrak{p}^5//y_1^2$, and this is impossible.

It follows from theorem 5 that if A and B satisfy (19), and if u is an exceptional point of order $q>4$, one of the three cases of theorem 4 can be applied to the point u. We shall prove three lemmas which correspond to these cases:

Lemma 5. *Let A and B satisfy* (19), *let N be the norm of $\mathfrak{p}$, let u be an exceptional point in $\boldsymbol{\Omega}$ of order $q>4$, and suppose that the first case of theorem* 4 *applies to the point u. Then*

$$q=2^\lambda t\leqq(2N+1)\sqrt{2(m+1)},$$

where t is an odd number $\leqq 2N+1$ *and*

$$2^\lambda\leqq\max\left(2N,\ \sqrt{2(m+1)}\right).$$

Proof. We may use theorem 3. Since $\psi_q=0$, the number s defined in this theorem is a divisor of q, and we have

$$5\leqq s\leqq 2N+1.$$

Now suppose $s<q$ and define c by $\mathfrak{p}^c//y_1$. Then s is an odd number, since otherwise $\mathfrak{p}^{c+1}/y_{\frac{1}{2}s}$ by (8), and this is impossible according to theorem 5.

Suppose $\mathfrak{p}^{(s^2-1)r+d}//\psi_s$, where $d>0$. If $y_s\neq 0$, it follows from theorem 5 that $\mathfrak{p}^c//y_s$, and hence, by (8), $\mathfrak{p}^{(4s^2-1)r+4d}//\psi_{2s}$. If $y_{2s}\neq 0$, we have $\mathfrak{p}^c//y_{2s}$, and (8) gives $\mathfrak{p}^{(16s^2-1)r+16d}//\psi_{4s}$. If $y_{2^\nu s}\neq 0$ $(\nu\geqq 0)$, it is shown by induction that

$$\mathfrak{p}^{(4^{\nu+1}s^2-1)r+4^{\nu+1}d}//\psi_{2^{\nu+1}s},$$

but according to theorem 3 we have

$$\mathfrak{p}^{(4^{\nu+1}s^2\pm 2^{\nu+2}s)r}//\psi_{2^{\nu+1}s\pm 1},$$

and hence

$$\mathfrak{p}^{2(r-4^{\nu+1}d)}//x_{2^{\nu+1}s}-x_1. \tag{22}$$

Now $x_{2^{\nu+1}s}-x_1$ is an integer mod $\mathfrak{p}$, and since $q>4$, we have

$$2c\leqq m+3$$

by theorem 5 and consequently

$$2r\leqq m+1.$$

But then (22) shows that

$$4^{\nu+2} \leqq 2\,(m+1). \tag{23}$$

It follows from (23) that $\frac{q}{s}$ cannot contain an odd prime factor, and we may write

$$q = 2^{\lambda}\, s.$$

If $\lambda \geqq 2$, we may take $\nu = \lambda - 2$ in (23) and find

$$2^{\lambda} \leq \sqrt{2\,(m+1)},$$

and the lemma is proved.

Lemma 6. *Let A and B satisfy* (19), *let u be an exceptional point in $\mathbf{\Omega}$ of order $q > 4$, and suppose that the second case of theorem 4 applies to the point u. Then*

$$q = 2^{\lambda} \leq 4\sqrt{3\,(m+1)}.$$

Proof. The formulas (17) may be used, and if $4/\nu$, we define

$$S_{\nu} = \tfrac{1}{8}\,[(\nu^2 - 1)\,k + 5\,d]; \tag{24}$$

then

$$S_{2\nu} - 4\,S_{\nu} - \tfrac{1}{8}\,(3\,k + d) = -2\,d,$$

and we have $\mathfrak{p}^{S_4}//\psi_4$. We define c by $\mathfrak{p}^{c}//y_1$. If $y_4 \neq 0$, it follows from theorem 5 that $\mathfrak{p}^{c}//y_4$, and then (8) shows that $\mathfrak{p}^{S_8+2d}//\psi_8$. If $y_8 \neq 0$, we have $\mathfrak{p}^{c}//y_8$ and $\mathfrak{p}^{S_{16}+10d}//\psi_{16}$. If $y_{2^{\nu}} \neq 0$, it is shown by induction that

$$\mathfrak{p}^{S_{2^{\nu+1}} + \frac{2}{3}(4^{\nu-1}-1)d} // \psi_{2^{\nu+1}},$$

but then it follows from (17) that

$$\mathfrak{p}^{\frac{1}{12}(3\,k + d - 4^{\nu+1}\,d)} // x_{2^{\nu+1}} - x_1,$$

and since $x_{2^{\nu+1}} - x_1$ is an integer mod $\mathfrak{p}$, we must have

$$4^{\nu+1}\,d \leq 3\,k + d.$$

But

$$3\,k + d = 8\,n = 8\,m + 8\,c \leq 8\,m + 4\,(m+3) = 12\,(m+1),$$

and consequently

$$4^{\nu} \leq 3\,(m+1). \tag{25}$$

It follows that q is a power of 2, and if $q = 2^\lambda$, we may take $\nu = \lambda - 2$ in (25) and find

$$2^\lambda \leqq 4\sqrt{3\,(m+1)}.$$

Lemma 7. *Let A and B satisfy* (19), *let u be an exceptional point in Ω of order $q > 4$, and suppose that the third case of theorem* 4 *applies to the point u. Then*

$$q = 3.2^\lambda \leqq 3\sqrt{6\,(m+1)}.$$

Proof. The formulas (18) may be used, and if $3/\nu$, we define

$$T_\nu = \tfrac{1}{3}\,[(\nu^2 - 1)\,n + d]; \tag{26}$$

then

$$T_{2\nu} - 4\,T_\nu - n = -d,$$

and we have $\mathfrak{p}^{T_3}//\psi_3$. Define c by $\mathfrak{p}^c//y_1$. If $y_3 \neq 0$, it follows from theorem 5 that $\mathfrak{p}^c//y_3$, and then (8) shows that $\mathfrak{p}^{T_6+d}//\psi_6$. If $y_6 \neq 0$, we have $\mathfrak{p}^c//y_6$ and hence $\mathfrak{p}^{T_{12}+5d}//\psi_{12}$. If $y_{3.2^\nu} \neq 0$ $(\nu \geqq 0)$, it is shown by induction that

$$\mathfrak{p}^{T_{3.2^{\nu+1}} + \frac{1}{3}(4^{\nu+1}-1)d}//\psi_{3.2^{\nu+1}},$$

but then it follows from (18) that

$$\mathfrak{p}^{\frac{1}{3}(n - 4^{\nu+1}d)}//x_{3.2^{\nu+1}} - x_1,$$

and since $x_{3.2^{\nu+1}} - x_1$ is an integer mod $\mathfrak{p}$, we must have

$$4^{\nu+1}\,d \leqq n.$$

But

$$2\,n = 2\,m + 2\,c \leqq 3\,(m+1),$$

and consequently

$$4^{\nu+2} \leqq 6\,(m+1). \tag{27}$$

According to theorem 4, q is divisible by 3, but it follows from (27) that $\frac{1}{3}\,q$ is a power of 2, and if $q = 3.2^\lambda$, where $\lambda \geqq 2$, we may take $\nu = \lambda - 2$ in (27) and find

$$2^\lambda \leqq \sqrt{6\,(m+1)}.$$

If the lemmas 5, 6 and 7 are combined, we get the following result:

Theorem 6. *Let Ω be an algebraic field, and let $\mathfrak{p}$ be a prime ideal in Ω, which divides* 2. *Let A and B be integers mod $\mathfrak{p}$ in Ω which satisfy* (1), *and suppose*

$$\mathfrak{p}^m//2;$$
$$\textit{if } \mathfrak{p}^4/A, \textit{ then } \mathfrak{p}^6\nmid B;$$
$$\textit{if } \mathfrak{p}^m//B, \textit{ then } \mathfrak{p}/A.$$

Finally let N be the norm of $\mathfrak{p}$, and suppose that there is an exceptional point of order q in $\mathbf{\Omega}$ on the curve (2). *Put*

$$q=2^\lambda t,$$

where $\lambda \geqq 0$ and t is an odd number $\geqq 1$. Then

$$t \leqq 2N+1;$$
$$2^\lambda \leqq \max\,(2N,\ 4\sqrt{3\,(m+1)});$$
$$q \leqq \max\,(2N+1,\ 3\sqrt{6\,(m+1)}),\ \textit{if } t=3;$$
$$q \leqq (2N+1)\sqrt{2\,(m+1)},\ \textit{if } t \geqq 5.$$

The limit of q given by this theorem depends on $\mathbf{\Omega}$ only. If $\mathbf{\Omega}=\boldsymbol{K}(1)$, we have $q=2^\lambda \leqq 8$, or $q=3.2^\lambda \leqq 6$, or $q=5.2^\lambda \leqq 10$.

6. In the following sections we shall suppose

$$\mathfrak{p}\nmid A;\ \mathfrak{p}^m//B. \tag{28}$$

Theorem 5 cannot be extended to this case, but in the sections **6**–**8** (except in lemma 8) we shall suppose

$$\mathfrak{p}^c//y_2, \text{ if } c \text{ is defined by } \mathfrak{p}^c//y_1, \tag{29}$$

and then theorem 4 can be applied. In the first case a limit of q is found in the following way:

Lemma 8. *Let A and B satisfy* (28), *and let u be an exceptional point in $\mathbf{\Omega}$ of order $q>4$. Then*

$$\mathfrak{p}^m/y_\nu^2, \textit{ and } \mathfrak{p}\nmid x_\nu, \textit{ if } y_\nu \neq 0.$$

If $y_\nu \neq 0$ and $x_\nu \neq x_1$, the numbers

$$\frac{y_\nu \pm y_1}{x_\nu - x_1}$$

are integers mod $\mathfrak{p}$, and at least one of them is not divisible by $\mathfrak{p}$.

Proof. If $y_\nu \neq 0$, we replace u by νu in (11), and since $2x_\nu + x_{2\nu}$ is an integer mod $\mathfrak{p}$, it is seen that $\mathfrak{p}^m/3x_\nu^2 - A$. But then $\mathfrak{p}\nmid x_\nu$, $\mathfrak{p}^m/x_\nu^3 - Ax_\nu$ and $\mathfrak{p}^m/y_\nu^2$.

Now we put $\nu=2$ in (9), and since $\mathfrak{p}\nmid x_2$, the number

$$\frac{y_2+y_1}{x_2-x_1}$$

is an integer mod $\mathfrak{p}$, which is not divisible by $\mathfrak{p}$. Since $\mathfrak{p}/y_2$ and $\mathfrak{p}/y_1$, it follows that $\mathfrak{p}/x_2-x_1$.

But (9) may be written in the following way:

$$\left(\frac{y_\nu+y_1}{x_\nu-x_1}\right)^2=2\,x_1+(x_{\nu-1}-x_1)+x_\nu, \tag{30}$$

and if $y_\nu\neq 0$ and $\mathfrak{p}/x_{\nu-1}-x_1$, the right member is not divisible by $\mathfrak{p}$, and hence $\mathfrak{p}/x_\nu-x_1$. Here we may take $\nu=2, 3, \ldots, q-2$, if q is odd, and $\nu=2, 3, \ldots, \frac{1}{2}q-1$, if q is even.

If q is odd, it follows from (30) that

$$\frac{y_\nu+y_1}{x_\nu-x_1} \tag{31}$$

is not divisible by $\mathfrak{p}$ for $\nu=2, 3, \ldots, q-2$. If q is even, the number (31) is not divisible by $\mathfrak{p}$ for $\nu=2, 3, \ldots, \frac{1}{2}q-1$, and since

$$x_{q-\nu}=x_\nu \text{ and } y_{q-\nu}=-y_\nu,$$

the number

$$\frac{y_\nu-y_1}{x_\nu-x_1} \tag{32}$$

is not divisible by $\mathfrak{p}$ for $\nu=\frac{1}{2}q+1, \frac{1}{2}q+2, \ldots, q-2$. It follows that at least one of the numbers (31) and (32) is not divisible by $\mathfrak{p}$, if $y_\nu\neq 0$ and $x_\nu\neq x_1$, and the lemma is proved.

Theorem 7. *Let A and B satisfy* (28), *let N be the norm of $\mathfrak{p}$, let u be an exceptional point in Ω of order $q>4$, let y_2 satisfy* (29), *and suppose that the first case of theorem 4 applies to the point u. Then*

$$c\leqq 2m, \text{ and } q=2^\lambda t\leqq 2m\,(2N+1),$$

where $\lambda\geqq 0$ and t is an odd number $\leqq 2N+1$.

Proof. Theorem 3 may be used, and since $\psi_q=0$, the number s defined in this theorem is a divisor of q.

Now suppose $s<q$. If $\psi_{2^\nu s}\neq 0$, we define a natural number d_ν by

$$\mathfrak{p}^{(4^\nu s^2-1)\,r+d_\nu}//\psi_{2^\nu s}. \tag{33}$$

9 – 533807 *Acta Mathematica*. 91. Imprimé le 10 juin 1954.

Since

$$x_2 - x_1 = -\frac{\psi_3}{\psi_2^2},$$

we have $\mathfrak{p}^{2r}//x_2 - x_1$, and then it follows from lemma 8 that

$$(34) \qquad c \leqq 2r,$$

and hence $c \leqq 2m$ and $r \leqq m$.

If $2^{\nu+1} s$ is not divisible by q, we have $y_{2^\nu s} \neq 0$, and (8) gives

$$(35) \qquad \mathfrak{p}^{c+d_{\nu+1}-4d_\nu}//y_{2^\nu s}.$$

If $d_{\nu+1} < 4 d_\nu$, it follows from (35) that

$$\mathfrak{p}^{c+d_{\nu+1}-4d_\nu}//y_{2^\nu s} \pm y_1,$$

and hence, by lemma 8,

$$(36) \qquad \mathfrak{p}^{c+d_{\nu+1}-4d_\nu}//x_{2^\nu s} - x_1.$$

But according to (33) and theorem 3 we also have

$$(37) \qquad \mathfrak{p}^{2(r-d_\nu)}//x_{2^\nu s} - x_1,$$

and from (34), (36) and (37) it is seen that

$$d_{\nu+1} = 2d_\nu + 2r - c \geqq 2d_\nu.$$

Now $d_0 \geqq 1$, and consequently $d_{\nu+1} \geqq 2^{\nu+1}$. If ν is replaced by $\nu+1$ in (37), we find

$$(38) \qquad 2^{\nu+1} \leqq d_{\nu+1} \leqq r \leqq m.$$

It follows that $\frac{q}{s}$ is a power of 2, and if

$$q = 2^\lambda s,$$

where $\lambda \geqq 2$, we may put $\nu = \lambda - 2$ in (38) and find

$$2^\lambda \leqq 2m.$$

7. If (29) is satisfied, and if the second case of theorem 4 applies to the point u, a limit of q is found in the following way:

Theorem 8. *Let A and B satisfy* (28), *let u be an exceptional point in $\mathbf{\Omega}$ of order $q > 4$, let y_2 satisfy* (29), *and suppose that the second case of theorem* 4 *applies to the point u. Then*

$$q = 2^\lambda \leqq 8m.$$

Proof. Suppose $\mathfrak{p}^c//y_{2^\nu}$ $(\nu=0, 1, \ldots, \varkappa; \varkappa \geqq 1)$. The formulas (17) may be used, S_ν is defined by (24), and $\mathfrak{p}^{S_4}//\psi_4$. If $\varkappa \geqq 2$, (8) gives $\mathfrak{p}^{S_8+2d}//\psi_8$; if $\varkappa \geqq 3$, we must have $\mathfrak{p}^{S_{16}+10d}//\psi_{16}$ and so on. Generally we find

$$\mathfrak{p}^{S_{2^\nu+1}+\frac{2}{3}(4^{\nu-1}-1)d}//\psi_{2^\nu+1} \qquad (\nu \leqq \varkappa+1),$$

and hence

$$\mathfrak{p}^{\frac{1}{12}[3k-(4^\nu-1)d]}//x_{2^\nu}-x_1 \qquad (\nu \leqq \varkappa+1). \tag{39}$$

Now $\mathfrak{p}^c/y_{2^\varkappa} \pm y_1$, and since $y_{2^\varkappa} \neq 0$, it follows from (39) and lemma 8 that

$$12\,c \leqq 3\,k-(4^\varkappa-1)\,d = 8\,n-4^\varkappa d = 8\,m+8\,c-4^\varkappa\,d,$$

and hence

$$c \leqq 2\,m-4^{\varkappa-1}\,d. \tag{40}$$

But $x_{2^\varkappa+1}-x_1$ is an integer mod $\mathfrak{p}$, and consequently, by (39),

$$4^{\varkappa+1}\,d \leqq 3\,k+d = 8\,n \leqq 8\,(3\,m-4^{\varkappa-1}\,d)$$

or

$$4^{\varkappa-1} \leqq m. \tag{41}$$

Since (41) gives a limit of $\varkappa$, we may suppose $\mathfrak{p}^{c+1}/y_{2^\varkappa+1}$ or $\mathfrak{p}^c \nmid y_{2^\varkappa+1}$.

First suppose $\mathfrak{p}^{c+h}//y_{2^\varkappa+1}$, where $h>0$. Then $\mathfrak{p}^c//y_{2^\varkappa+1} \pm y_1$, and since $y_{2^\varkappa+1} \neq 0$, (39) and lemma 8 give

$$12\,c = 3\,k-(4^{\varkappa+1}-1)\,d = 8\,n-4^{\varkappa+1}\,d$$

or

$$c = 2\,m-4^\varkappa\,d. \tag{42}$$

Now (8) gives

$$\mathfrak{p}^{S_{2^\varkappa+2}+\frac{1}{3}(4^\varkappa-1)d+h}//\psi_{2^\varkappa+2},$$

and then, by (42),

$$\mathfrak{p}^{c-4^\varkappa d-2h}//x_{2^\varkappa+2}-x_1.$$

If $y_{2^\varkappa+2} \neq 0$, we find

$$\mathfrak{p}^{c-4^\varkappa d-2h}//y_{2^\varkappa+2},\ \mathfrak{p}^{S_{2^\varkappa+3}+\frac{1}{3}(5.4^\varkappa-2)d+2h}//\psi_{2^\varkappa+3}$$

and

$$\mathfrak{p}^{c-3.4^\varkappa d-4h}//x_{2^\varkappa+3}-x_1.$$

If $y_{2^\varkappa+\nu} \neq 0$ $(\nu \geqq 1)$, it is shown by induction that

$$\mathfrak{p}^{S_{2^\varkappa+\nu+1}+[2^{2\varkappa+\nu-1}-\frac{1}{3}(4^\varkappa+2)]\,d+2^{\nu-1}h}//\psi_{2^\varkappa+\nu+1}$$

and

$$\mathfrak{p}^{c-4^\varkappa(2^\nu-1)\,d-2^\nu h}//x_{2^\varkappa+\nu+1}-x_1. \tag{43}$$

Since $x_{2^\varkappa+\nu+1}-x_1$ is an integer mod $\mathfrak{p}$, it follows from (43) and (42) that

$$2^\nu(h+4^\varkappa d) \leqq c+4^\varkappa d = 2\,m,$$

and hence

$$2^\nu(1+4^\varkappa) \leqq 2\,m. \tag{44}$$

(44) gives a limit of $\varkappa+\nu$, and since $\varkappa \geqq 1$, it is seen that

$$2^{\varkappa+\nu} \leqq \frac{2^{\varkappa+1}}{1+4^\varkappa}\,m \leqq \frac{4}{5}\,m. \tag{45}$$

Consequently q is a power of 2, and if $q=2^\lambda$ $(\lambda \geqq 3)$, we may take $\nu=\lambda-\varkappa-2$ in (45) and find

$$q=2^\lambda \leqq \frac{16}{5}\,m.$$

Next suppose $\mathfrak{p}^{c-h}//y_{2^\varkappa+1}$, where $h>0$. Then $\mathfrak{p}^{c-h}//y_{2^\varkappa+1} \pm y_1$, and since $y_{2^\varkappa+1} \neq 0$, lemma 8 gives (compare (39))

$$12\,(c-h) = 3\,k-(4^{\varkappa+1}-1)\,d = 8\,n-4^{\varkappa+1}\,d$$

or

$$c-3\,h = 2\,m-4^\varkappa d, \tag{46}$$

and (40) shows that

$$h \leqq 4^{\varkappa-1}\,d. \tag{47}$$

Now (8) gives

$$\mathfrak{p}^{S_{2^\varkappa+2}+\frac{1}{3}(4^\varkappa-1)d-h}//\psi_{2^\varkappa+2},$$

and then, by (46),

$$\mathfrak{p}^{c-4^\varkappa d+h}//x_{2^\varkappa+2}-x_1.$$

Now $h<4^\varkappa d$ by (47), and if $y_{2^\varkappa+2} \neq 0$, it follows that

$$\mathfrak{p}^{c-4^\varkappa d+h}//y_{2^\varkappa+2},\quad \mathfrak{p}^{S_{2^\varkappa+3}+\frac{1}{3}(5.4^\varkappa-2)\,d-3\,h}//\psi_{2^\varkappa+3}$$

and

$$\mathfrak{p}^{c-3.4^{\varkappa}d+5d}//x_{2^{\varkappa}+3}-x_1.$$

If $y_{2^{\varkappa}+\nu}\neq 0$, it is shown by induction that

$$\mathfrak{p}^{s_{2^{\varkappa}+\nu+1}+[2^{2\varkappa+\nu-1}-\frac{1}{3}(4^{\varkappa}+2)]d-(2^{\nu}-1)h}//\psi_{2^{\varkappa}+\nu+1}$$

and

$$\mathfrak{p}^{c-4^{\varkappa}(2^{\nu}-1)d+(2^{\nu+1}-3)h}//x_{2^{\varkappa}+\nu+1}-x_1.$$

Hence

$$2^{\nu+1}(2^{2\varkappa-1}d-h)\leqq c-3h+4^{\varkappa}d=2m,$$

or, if (47) is used,

$$2^{2\varkappa+\nu-1}\leqq 2m.$$

Consequently q is a power of 2, and since $\varkappa\geqq 1$, it is seen that

(48) $$2^{\varkappa+\nu}\leqq 2m.$$

If $q=2^{\lambda}$ $(\lambda\geqq 3)$, we may take $\nu=\lambda-\varkappa-2$ in (48) and find

$$q=2^{\lambda}\leqq 8m.$$

Finally suppose $y_{2^{\varkappa}+1}=0$. Then $q=2^{\varkappa+2}$, and (41) gives

$$q=2^{\varkappa+2}\leqq 8\sqrt{m}.$$

8. If (29) is satisfied, and if the third case of theorem 4 applies to the point u, a limit of q is found in the following way:

Lemma 9. *Let A and B satisfy* (28), *let u be an exceptional point in $\mathbf{\Omega}$ of order $q>6$, let y_2 satisfy* (29), *and suppose that the third case of theorem* 4 *applies to the point u. If*

$$\mathfrak{p}^{c+1}/y_3,$$

we have

$$m\geqq 3 \text{ and } q=3.2^{\lambda}\leqq 4m.$$

Proof. It follows from theorem 4 that q is divisible by 3, and a natural number h may be defined by $\mathfrak{p}^{c+h}//y_3$. Now $\mathfrak{p}^{c}//y_3\pm y_1$, and since (18) gives

$$\mathfrak{p}^{\frac{1}{3}(n-d)}//x_3-x_1,$$

it follows from lemma 8 that

$$3c=2(n-d)$$

or

$$c = 2\,(m - d). \tag{49}$$

If T_ν is defined by (26), we have $\mathfrak{p}^{T_3}//\psi_3$ and $\mathfrak{p}^{T_6+d+h}//\psi_6$. But then $\mathfrak{p}^{c-2(d+h)}//x_6 - x_1$, and if $y_6 \neq 0$, it follows that $\mathfrak{p}^{c-2(d+h)}//y_6$, $\mathfrak{p}^{T_{12}+3d+2h}//\psi_{12}$ and $\mathfrak{p}^{c-2(3d+2h)}//x_{12} - x_1$. If $y_{3.2^\nu} \neq 0$, it may be shown by induction that

$$\mathfrak{p}^{T_{3.2^{\nu+1}} + (2^{\nu+1}-1)\,d + 2^\nu h}//\psi_{3.2^{\nu+1}}$$

and

$$\mathfrak{p}^{c-2\,(2^{\nu+1}-1)\,d - 2^{\nu+1}h}//x_{3.2^{\nu+1}} - x_1.$$

Hence

$$2^{\nu+1}\,(2\,d + h) \leqq c + 2\,d,$$

or, by (49),

$$3.2^{\nu+1} \leqq 2\,m. \tag{50}$$

It follows that $\frac{1}{3}\,q$ is a power of 2, and if $q = 3.2^\lambda$ $(\lambda \geqq 2)$, we may take $\nu = \lambda - 2$ in (50) and find

$$q = 3.2^\lambda \leqq 4\,m.$$

Lemma 10. *Let A and B satisfy* (28), *let N be the norm of $\mathfrak{p}$, let u be an exceptional point in $\boldsymbol{\Omega}$ of order $q > 6$, let y_2 satisfy* (29), *and suppose that the third case of theorem* 4 *applies to the point u. If*

$$\mathfrak{p}^c \nmid y_3,$$

we have

$$q = 2^\lambda \cdot 3\,t \leqq 6\,m\,(2\,N + 1),$$

where t is an odd number $\leqq 2\,N + 1$.

If $c \leqq 2\,m$, we have

$$q = 3.2^\lambda \leqq 6\,m.$$

Proof. By theorem 4, q is divisible by 3. A natural number h is defined by $\mathfrak{p}^{c-h}//y_3$, and the numbers T_ν are defined by (26). Now $\mathfrak{p}^{c-h}//y_3 \pm y_1$, and hence, by (18) and lemma 8:

$$c - h = \tfrac{2}{3}\,(n - d),$$

or

$$c - 3\,h = 2\,(m - d). \tag{51}$$

Since $\mathfrak{p}^c/y_2 \pm y_1$, (18) and lemma 8 also give

$$c \leqq \tfrac{1}{3}\,(2\,n + d),$$

or

$$c \leqq 2\,m + d,$$

and hence, by (51),

$$h \leqq d. \tag{52}$$

Now (8) gives $\mathfrak{p}^{T_6+d-h}//\psi_6$, and then $\mathfrak{p}^{c-2d+h}//x_6-x_1$. Here the exponent is $<c$ by (52), and if $y_6 \neq 0$, it follows that $\mathfrak{p}^{c-2d+h}//y_6$, $\mathfrak{p}^{T_{12}+3(d-h)}//\psi_{12}$ and $\mathfrak{p}^{c-6d+5h}//x_{12}-x_1$. If $y_{3.2^\nu} \neq 0$ $(\nu \geqq 0)$, it is shown by induction that

$$\mathfrak{p}^{T_{3.2^{\nu+1}}+(2^{\nu+1}-1)(d-h)}//\psi_{3.2^{\nu+1}}$$

and

$$\mathfrak{p}^{c-2(2^{\nu+1}-1)d+(2^{\nu+2}-3)h}//x_{3.2^{\nu+1}}-x_1.$$

If $h<d$, it follows that

$$2^{\nu+2} \leqq 2^{\nu+2}(d-h) \leqq c+2d-3h=2m,$$

and it is seen that $q=3.2^\lambda$ $(\lambda \geqq 2)$, where

$$2^\lambda \leqq 2m. \tag{53}$$

If $h=d$, (51) gives $c=2m+d$, and if $y_{3.2^\nu} \neq 0$ $(\nu \geqq 0)$, we have $\mathfrak{p}^{2m}//y_{3.2^\nu}$. If $q>12$, it follows that one of the three cases of theorem 4 can be applied to the point $3u$, since we have $\mathfrak{p}^{2m}//y_3$ and $\mathfrak{p}^{2m}//y_6$. Now $\mathfrak{p}^{2m}/x_3-x_1$ and $\mathfrak{p}^{2m}/x_6-x_1$ and consequently $\mathfrak{p}^{2m}/x_6-x_3$, but if u is replaced by $3u$ in (4), it is seen that

$$x_6-x_3=-\frac{\psi_3(3u)}{\psi_2^2(3u)}, \tag{54}$$

and since $\psi_2(3u)=-2y_3$, it follows that $\mathfrak{p}^{8m}/\psi_3(3u)$. Thus the second case of theorem 4 does not apply to the point $3u$.

If the first case applies, theorem 7 gives

$$q=2^\lambda \cdot 3t \leqq 6m(2N+1),$$

where t is an odd number $\leqq 2N+1$.

If the third case applies, (54) shows that $\mathfrak{p}^{2m+1}/x_6-x_3$, but (4) also gives

$$x_6-x_3=-\frac{\psi_9}{\psi_6^2\,\psi_3},$$

and hence $\mathfrak{p}^{T_9+1}/\psi_9$. Consequently $\mathfrak{p}^{2m} \nmid x_9-x_1$, and if $q \neq 18$, it follows from lemma 8 that $\mathfrak{p}^{2m} \nmid y_9$. Hence we may replace u by $3u$ in the proof of lemma 10, and there will be two numbers h' and d', which correspond to h and d. But since $\mathfrak{p}^{2m+1} \nmid y_3$, it is seen that $h'<d'$, and then $q=9.2^\lambda$, where, by (53),

$$2^\lambda \leqq 2m.$$

Lemma 11. *Let A and B satisfy* (28), *let u be an exceptional point in $\boldsymbol{\Omega}$ of order $q>6$, let y_2 satisfy* (29), *and suppose that the third case of theorem* 4 *applies to the point u. If*

$$\mathfrak{p}^c//y_3,$$

we have

$$m \geqq 2 \ \textit{and} \ q = 3.2^\lambda \leqq 6\,m.$$

Proof. Suppose $\mathfrak{p}^c//y_{3.2^\nu}$ $(\nu=0,\,1,\,\ldots,\,\varkappa;\ \varkappa\geqq 0)$. Then (8) gives $\mathfrak{p}^{T_6+d}//\psi_6$, $\mathfrak{p}^{T_{12}+5d}//\psi_{12}$ and finally

$$\mathfrak{p}^{T_{3.2^{\varkappa+1}}+\frac{1}{3}(4^{\varkappa+1}-1)\,d}//\psi_{3.2^{\varkappa+1}}.$$

Hence $\mathfrak{p}^{\frac{2}{3}(n-4^\nu d)}//x_{3.2^\nu}-x_1$ $(\nu=0,\,1,\,\ldots,\,\varkappa+1)$. But $\mathfrak{p}^c/y_{3.2^\varkappa}\pm y_1$, and since $y_{3.2^\varkappa}\neq 0$, lemma 8 gives

$$c \leqq \tfrac{2}{3}\,(n-4^\varkappa d)$$

and hence

$$c \leqq 2\,(m-4^\varkappa d). \tag{55}$$

Now $x_{3.2^\varkappa+1}-x_1$ is an integer mod $\mathfrak{p}$, and consequently (by (55))

$$4^{\varkappa+1}\,d \leqq n \leqq 3\,m-2.4^\varkappa\,d$$

or

$$m \geqq 2 \ \text{ and } \ 4^{\varkappa+1} \leqq 2\,m. \tag{56}$$

Since (56) gives a limit of $\varkappa$, we may suppose $\mathfrak{p}^{c+1}/y_{3.2^\varkappa+1}$ or $\mathfrak{p}^c/y_{3.2^\varkappa+1}$.

First suppose $\mathfrak{p}^{c+h}//y_{3.2^\varkappa+1}$, where $h>0$. Then $\mathfrak{p}^c//y_{3.2^\varkappa+1}\pm y_1$, and since $y_{3.2^\varkappa+1}\neq 0$, lemma 8 gives

$$c = \tfrac{2}{3}\,(n-4^{\varkappa+1}\,d)$$

or

$$c = 2\,(m-4^{\varkappa+1}\,d). \tag{57}$$

Now (8) gives

$$\mathfrak{p}^{T_{3.2^{\varkappa+2}}+\frac{1}{3}(4^{\varkappa+2}-1)\,d+h}//\psi_{3.2^{\varkappa+2}},$$

and then, by (57),

$$\mathfrak{p}^{c-2.4^{\varkappa+1}d-2h}//x_{3.2^\varkappa+2}-x_1.$$

If $y_{3.2^\varkappa+2}\neq 0$, it follows that

$$\mathfrak{p}^{c-2.4^{\varkappa+1}d-2h}//y_{3.2^\varkappa+2},$$

$$\mathfrak{p}^{T_{3.2^{\varkappa}+3}+\frac{1}{3}(10.4^{\varkappa+1}-1)d+2h}//\psi_{3.2^{\varkappa}+3}$$

and

$$\mathfrak{p}^{c-6.4^{\varkappa+1}d-4h}//x_{3.2^{\varkappa}+3}-x_1.$$

If $y_{3.2^{\varkappa}+\nu} \neq 0$ $(\nu \geqq 1)$, it is shown by induction that

$$\mathfrak{p}^{T_{3.2^{\varkappa}+\nu+1}+[2^{2\varkappa+\nu+2}-\frac{1}{3}(2^{2\varkappa+3}+1)]d+2^{\nu-1}h}//\psi_{3.2^{\varkappa}+\nu+1}$$

and

$$\mathfrak{p}^{c-2^{2\varkappa+3}(2^{\nu}-1)d-2^{\nu}h}//x_{3.2^{\varkappa}+\nu+1}-x_1.$$

Hence

$$2^{\nu}(2^{2\varkappa+3}d+h) \leqq c+2^{2\varkappa+3}d = 2m,$$

and since h and d are natural numbers, it follows that

$$2^{\nu}(2^{2\varkappa+3}+1) \leqq 2m.$$

Consequently

$$2^{\varkappa+\nu} \leqq \frac{2^{\varkappa+1}}{2^{2\varkappa+3}+1}m \leqq \frac{2}{9}m, \tag{58}$$

and $\frac{1}{3}q$ must be a power of 2. If $q=3.2^{\lambda}$ $(\lambda \geqq 2)$, we may take $\nu=\lambda-\varkappa-2$ in (58) and find

$$2^{\lambda} \leqq \frac{8}{9}m.$$

Next suppose $\mathfrak{p}^{c-h}//y_{3.2^{\varkappa}+1}$, where $h>0$. Then $\mathfrak{p}^{c-h}//y_{3.2^{\varkappa}+1} \pm y_1$, and since $y_{3.2^{\varkappa}+1} \neq 0$, lemma 8 gives

$$c-h = \frac{2}{3}(n-4^{\varkappa+1}d)$$

or

$$c-3h = 2(m-4^{\varkappa+1}d), \tag{59}$$

and (55) shows that

$$h \leqq 2.4^{\varkappa}d. \tag{60}$$

Now (8) gives

$$\mathfrak{p}^{T_{3.2^{\varkappa}+2}+\frac{1}{3}(4^{\varkappa+2}-1)d-h}//\psi_{3.2^{\varkappa}+2},$$

and then, by (59),

$$\mathfrak{p}^{c-2.4^{\varkappa+1}d+h}//x_{3.2^{\varkappa}+2}-x_1.$$

But $h<2.4^{\varkappa+1}d$ by (60), and if $y_{3.2^{\varkappa}+2} \neq 0$, it follows that

$$\mathfrak{p}^{c-2.4^{\varkappa+1}d+h}//y_{3.2^{\varkappa}+2},$$

$$\mathfrak{p}^{T_{3.2^{\varkappa}+3}+\frac{1}{3}(10.4^{\varkappa+1}-1)d-3h}//\psi_{3.2^{\varkappa}+3}$$

and

$$\mathfrak{p}^{c-6.4^{\varkappa+1}d+5h}//x_{3.2^{\varkappa}+3}-x_1.$$

If $y_{3.2^{\varkappa}+\nu} \neq 0$ $(\nu \geqq 1)$, it is shown by induction that

$$\mathfrak{p}^{T_{3.2^{\varkappa}+\nu+1}+[2^{2\varkappa+\nu+2}-\frac{1}{3}(2^{2\varkappa+3}+1)]d-(2^{\nu}-1)h}//\psi_{3.2^{\varkappa}+\nu+1}$$

and

$$\mathfrak{p}^{c-2^{2\varkappa+3}(2^{\nu}-1)d+(2^{\nu+1}-3)h}//x_{3.2^{\varkappa}+\nu+1}-x_1.$$

Hence

$$2^{\nu+1}(4^{\varkappa+1}d-h) \leqq c+2^{2\varkappa+3}d-3h=2m,$$

or, if (60) is used,

$$2^{2\varkappa+\nu+2} \leqq 2m.$$

It follows that

$$2^{\varkappa+\nu} \leqq \tfrac{1}{2}m, \tag{61}$$

and $\frac{1}{3}q$ must be a power of 2. If $q=3.2^{\lambda}$ $(\lambda \geqq 2)$, we may take $\nu=\lambda-\varkappa-2$ in (61) and find

$$2^{\lambda} \leqq 2m.$$

Finally suppose $y_{3.2^{\varkappa}+1}=0$. Then $q=3.2^{\varkappa+2}$, and (56) gives

$$2^{\varkappa+2} \leqq 2\sqrt{2m} \leqq 2m,$$

since $m \geqq 2$.

If the lemmas 9, 10 and 11 are combined, we get the following result:

Theorem 9. *Let A and B satisfy* (28), *let N be the norm of $\mathfrak{p}$, let u be an exceptional point in $\boldsymbol{\Omega}$ of order $q>4$, let y_2 satisfy* (29), *and suppose that the third case of theorem* 4 *applies to the point u. Then*

$$q=2^{\lambda}\cdot 3t \leqq 6m(2N+1),$$

where t is an odd number $\leqq 2N+1$.

9. Now we combine the theorems 7, 8 and 9 in the following way:

Theorem 10. *Let A and B satisfy* (28), *let N be the norm of $\mathfrak{p}$, let u be an exceptional point in $\boldsymbol{\Omega}$ of order $q>4$, and let y_2 satisfy* (29). *Then*

$$q = 2^{\lambda} t \leqq 6\,m\,(2\,N + 1),$$

where t is an odd number $\leqq 3\,(2\,N+1)$.

10. In this section (29) will be replaced by the following condition:

$$\mathfrak{p}^{c}//y_1;\ \mathfrak{p}^{c+1}/y_2;\ y_4 \neq 0;\ \mathfrak{p}^{c}/y_4. \tag{62}$$

Then we may prove the following lemma:

Lemma 12. *Let A and B satisfy* (28), *let u be an exceptional point in* $\mathbf{\Omega}$ *of order $q > 4$, let y_2 and y_4 satisfy* (62), *and define the numbers h and U_ν by*

$$\mathfrak{p}^{c+h}//y_2; \tag{63}$$

$$U_\nu = \tfrac{1}{2}\,\nu\,(\nu-1)\,h + (\nu^2 - 1)\,m \quad (\nu \geqq 1). \tag{64}$$

Then $c = h + 2\,m$, and we have

$$\mathfrak{p}^{U_\nu}//\psi_\nu$$

for $\nu = 1, 2, 3, 4$.

Proof. Since $\mathfrak{p}^{c}//y_2 \pm y_1$ and $y_2 \neq 0$, lemma 8 gives $\mathfrak{p}^{c}//x_2 - x_1$. But $\mathfrak{p}^{c+m}//\psi_2$, and hence, by (4), $\mathfrak{p}^{3c+2m}//\psi_3$. By (8) and the definition of h, we have $\mathfrak{p}^{h+5(c+m)}//\psi_4$, and consequently $\mathfrak{p}^{h+2m}//x_3 - x_1$.

Now $\mathfrak{p}^{c}/y_4 \pm y_1$ and $y_4 \neq 0$, and hence $\mathfrak{p}^{c}/x_4 - x_1$. But then we must have (by (4)) $\mathfrak{p}^{2h+8(c+m)}/\psi_5$, and (4) gives $\mathfrak{p}^{2h+2m}/x_2 - x_3$. Hence $c = h + 2m$, since $x_2 - x_3 = (x_2 - x_1) - (x_3 - x_1)$, and the lemma is proved.

It is easy to verify that the numbers U_ν defined by (64) satisfy the following relations:

$$\begin{cases} U_{\nu-1} + U_{\nu+1} - 2\,U_\nu = h + 2\,m; \\ U_{2\nu} + U_2 = 2\,(U_{\nu-1} + U_{\nu+1}) + (\nu - 1)\,h + 2\,m; \\ U_{2\nu+1} = 2\,(U_\nu + U_{\nu+1}) + \nu\,h + 2\,m; \\ U_{2\nu} - 4\,U_\nu - U_2 = (\nu - 1)\,h, \end{cases} \tag{65}$$

and now a sort of induction is possible:

Lemma 13. *Let A and B satisfy* (28), *let u be an exceptional point in* $\mathbf{\Omega}$ *of order $q > 4$, let y_2 and y_4 satisfy* (62), *let h and U_ν be defined by* (63) *and* (64), *and suppose*

$$\mathfrak{p}^{c}/y_\nu,\ \textit{if}\ (\nu, q) = 1; \tag{66}$$

$$\mathfrak{p}^{U_\nu}//\psi_\nu\ \ (\nu = 1, 2, \ldots, t-1);\ \ \mathfrak{p}^{U_t}/\psi_t, \tag{67}$$

where $4 \leqq t \leqq q$.

Then $\mathfrak{p}^{th+8m}/4A^3-27B^2$, *if* t *is odd, and* $\mathfrak{p}^{(t-1)h+8m}/4A^3-27B^2$, *if* t *is even. If* $\mathfrak{p}^{U_t+1}/\psi_t$, *we have* $(t, q)>1$ *and*

$$\frac{q}{(t, q)}=2^\lambda \leqq 2m,$$

and if $\mathfrak{p}^{U_t}//\psi_t$ *but* $\mathfrak{p}^{U_{t+1}} \nmid \psi_{t+1}$, *we have* $(t, q)>1$ *and*

$$\frac{q}{(t, q)}=2^\lambda t_1 \leqq 2m(2N+1),$$

where t_1 *is an odd number* $\leqq 2N+1$.

Proof. If t is odd, it follows from (4) and (65 a) that $\mathfrak{p}^{h+2m}/x_{\frac{1}{2}(t-1)}-x_1$ and $\mathfrak{p}^{h+2m}/x_{t-1}-x_1$, and hence $\mathfrak{p}^{h+2m}/x_{t-1}-x_{\frac{1}{2}(t-1)}$. But (8) and (65 d) give $\mathfrak{p}^{\frac{1}{2}(t-1)h+2m}/y_{\frac{1}{2}(t-1)}$, and then (12) shows that $\mathfrak{p}^{th+8m}/4A^3-27B^2$, if the point u is replaced by $\frac{1}{2}(t-1)u$. If t is even, we replace t by $t-1$. This proves the first part of the lemma.

To prove the second part we first suppose $(t, q)=1$. Then $\mathfrak{p}^{h+2m}/y_t$ and $y_t \neq 0$, and hence, by lemma 8, $\mathfrak{p}^{h+2m}/x_t-x_1$. If we take $\nu=t$ in (65 a), it follows that $\mathfrak{p}^{U_{t+1}}/\psi_{t+1}$. But we know that $\mathfrak{p}^{h+2m}/x_{t-2}-x_1$ (by (4), (65 a) and (67)), and hence $\mathfrak{p}^{h+2m}/x_t-x_{t-2}$. Now we take $\nu=t-1$ in (7 a) and (65 b) and find $\mathfrak{p}^{U_{2t-2}-(t-3)h}/\psi_{2t-2}$, and then (8) gives $\mathfrak{p}^{2h+2m}/y_{t-1}$. Thus $\mathfrak{p}^{h+2m}//y_{t-1}+y_1$ and $\mathfrak{p}^{h+2m+1} \nmid x_{t-1}-x_1$, and consequently $\mathfrak{p}^{U_t}//\psi_t$.

Next suppose $(t, q)>1$. If $t<q$ but $\mathfrak{p}^{U_t+1}/\psi_t$, we define a natural number d by $\mathfrak{p}^{U_t+d}//\psi_t$. Then $\mathfrak{p}^{h+2m+d}/x_{t-1}-x_1$, but $\mathfrak{p}^{h+2m}//x_2-x_1$, and hence $\mathfrak{p}^{h+2m}//x_{t-1}-x_2$, and (4) gives $\mathfrak{p}^{U_{t+1}-h}//\psi_{t+1}$. Consequently $\mathfrak{p}^{2m-2d}//x_t-x_1$, and if $y_t \neq 0$, it follows that $\mathfrak{p}^{2m-2d}//y_t$. But $\mathfrak{p}^{8m}/4A^3-27B^2$, and if u is replaced by tu in (12), it is seen that $\mathfrak{p}^{2m-4d}//x_{2t}-x_t$, and hence $\mathfrak{p}^{2m-4d}//x_{2t}-x_1$. If $y_{2t} \neq 0$, it follows that $\mathfrak{p}^{2m-4d}//y_{2t}$, but then we replace u by $2tu$ in (12) and find $\mathfrak{p}^{2m-8d}//x_{4t}-x_{2t}$, and hence $\mathfrak{p}^{2m-8d}//x_{4t}-x_1$. If $y_{2^\nu t} \neq 0$, it is shown by induction that

$$\mathfrak{p}^{2m-2^{\nu+2}d}//x_{2^{\nu+1}t}-x_1. \tag{68}$$

It follows that the order of the point tu is a power of 2, and if it is equal to 2^λ, where $\lambda \geqq 2$, we may take $\nu=\lambda-2$ in (68) and find

$$2^\lambda \leqq 2m.$$

Obviously the order of the point tu is $\frac{q}{(t, q)}$.

If $\mathfrak{p}^{U_t}//\psi_t$ but $\mathfrak{p}^{U_{t+1}} \nmid \psi_{t+1}$, we define a natural number e by $\mathfrak{p}^{U_{t+1}-e}//\psi_{t+1}$. Then $\mathfrak{p}^{h+2m-e}//x_t - x_1$, and since $\mathfrak{p}^{h+2m}/x_2 - x_1$, it follows that $\mathfrak{p}^{h+2m-e}//x_t - x_2$. But then (4) gives $\mathfrak{p}^{U_{t+2}-h-e}//\psi_{t+2}$, and consequently $\mathfrak{p}^{2m+e}//x_{t+1} - x_1$. But since $(t+1, q) = 1$, we have $y_{t+1} \neq 0$ and $\mathfrak{p}^c/y_{t+1}$, and then lemma 8 shows that $e \geqq h$.

Now suppose $e > h$. Since $\mathfrak{p}^{h+2m}//x_{t-1} - x_1$, we have $\mathfrak{p}^{h+2m}//x_{t+1} - x_{t-1}$, and then (7 a) gives

$$\mathfrak{p}^{U_{2t}-(t-2)h-2e}//\psi_{2t}.$$

Consequently $y_t \neq 0$ and $\mathfrak{p}^{2h+2m-2e}//y_t$, and this is impossible by lemma 8, since we know that $\mathfrak{p}^{h+2m-e}/x_t - x_1$.

Consequently $e = h$ and $\mathfrak{p}^{2m}//x_t - x_1$. If $y_t \neq 0$, it follows that $\mathfrak{p}^{2m}//y_t$ and $\mathfrak{p}^{U_{2t}-th}//\psi_{2t}$. Since $\mathfrak{p}^{2m}//x_{t\pm1} - x_t$, (7 b) gives $\mathfrak{p}^{U_{2t-1}-(t-1)h}//\psi_{2t-1}$ and $\mathfrak{p}^{U_{2t+1}-(t+2)h}//\psi_{2t+1}$, and consequently $\mathfrak{p}^{2m}//x_{2t} - x_1$. If $y_{2t} \neq 0$, it follows that $\mathfrak{p}^{2m}//y_{2t}$, and theorem 4 can be applied to the point tu. Now $\mathfrak{p}^{3m}//\psi_2(tu)$, and since $\mathfrak{p}^{2m}/x_{2t} - x_t$, we have $\mathfrak{p}^{8m}/\psi_3(tu)$, and consequently the second case of theorem 4 is impossible. If the first case applies, theorem 7 gives

$$\frac{q}{(t,\, q)} = 2^{\lambda} t_1 \leqq 2m(2N+1),$$

where t_1 is an odd number $\leqq 2N+1$. If the third case applies, we have $\mathfrak{p}^{8m+1}/\psi_3(tu)$, and since $\mathfrak{p}^{15m}//\psi_4(tu)$ and

$$x_{3t} - x_t = -\frac{\psi_2(tu)\,\psi_4(tu)}{\psi_3^2(tu)}, \text{ if } \psi_3(tu) \neq 0,$$

$x_{3t} - x_t$ is not divisible by $\mathfrak{p}^{2m}$. If $y_{3t} \neq 0$, it follows that $\mathfrak{p}^{2m} \nmid y_{3t}$, and then lemma 10 gives

$$\frac{q}{(t,\, q)} = 3.2^{\lambda} \leqq 6m.$$

It follows from lemma 13 that if $(t, q) = 1$, t may be replaced by $t+1$ in (67). Now we take t in (67) as large as possible $(t \leqq q)$. Then it follows from lemma 13 that $(t, q) > 1$ and

$$\frac{q}{(t,\, q)} = 2^{\lambda} t_1 \leqq 2m(2N+1),$$

where t_1 is an odd number $\leqq 2N+1$. Since $\mathfrak{p}^{U_\nu}//\psi_\nu$ for $\nu \leqq 4$, $y_4 \neq 0$ and $\mathfrak{p}^c/y_4$, the proof of lemma 13 shows that $\mathfrak{p}^{U_5}/\psi_5$, and hence $t \geqq 5$. But then lemma 13 gives

$$\mathfrak{p}^{5+8m}/4A^3 - 27B^2,$$

and we have the following result:

Theorem 11. *Let A and B satisfy* (28), *let u be an exceptional point in $\mathbf{\Omega}$ of order $q>4$, let y_2 and y_4 satisfy* (62), *suppose*

$$\mathfrak{p}^c/y_\nu, \text{ if } (\nu,\, q)=1,$$

and define R by

$$\mathfrak{p}^{2m+R}//4A^3-27B^2. \tag{69}$$

Then $R \geqq 6m+5$, and

$$q=2^\lambda t_2 \leqq 2m\,(2N+1)\,(R-6m+1),$$

where t_2 is an odd number $\leqq (2N+1)\,(R-6m)$.

11. Now a limit of the order of an exceptional point in $\mathbf{\Omega}$ may be found in the following way, if A and B satisfy (28). We suppose that there is an exceptional point in $\mathbf{\Omega}$ of order $q>4$, and we choose u in such a way that (66) is satisfied, if c is defined by $\mathfrak{p}^c//y_1$.

Suppose $q \neq 8$. If $\mathfrak{p}^c//y_2$, or if $\mathfrak{p}^{c+1}/y_2$ and $\mathfrak{p}^c/y_4$, a limit of q is given by theorem 10 or theorem 11. Otherwise $\mathfrak{p}^c \nmid y_2$ or $\mathfrak{p}^c \nmid y_4$, and then it follows from (66) that q is even. Consequently the order of the point $2u$ is $\frac{1}{2}q$, and the order of the point $4u$ is $\frac{1}{4}q$ or $\frac{1}{2}q$, according as q is divisible by 4 or not. In any case there is a point of order $\frac{1}{2}q$ or $\frac{1}{4}q$, whose ordinate is not divisible by $\mathfrak{p}^c$, and we can choose among the points $2\nu u$, where $(\nu,\, \frac{1}{2}q)=1$, or among the points $4\nu u$, where $(\nu,\, \frac{1}{4}q)=1$, a point u', whose order q' and ordinate y' satisfy

$$q'=\tfrac{1}{2}q \text{ or } =\tfrac{1}{4}q;\ \mathfrak{p}^{c'}//y', \text{ where } c'<c;\ \mathfrak{p}^{c'}/y'_\nu, \text{ if } (\nu,\, q')=1.$$

Here y'_ν denotes the ordinate of the point $\nu u'$.

If $q'>4$ and $\neq 8$, and if neither theorem 10 nor theorem 11 can be applied to the point u', q' must be even, and we can choose a point u'', whose order is

$$q''=\tfrac{1}{2}q' \text{ or } =\tfrac{1}{4}q',$$

and whose ordinate y'' satisfies

$$\mathfrak{p}^{c''}//y'';\ c''<c';\ \mathfrak{p}^{c''}/y''_\nu, \text{ if } (\nu,\, q'')=1.$$

Since the ordinate of an exceptional point is an integer mod $\mathfrak{p}$, this process will finally come to an end. Thus we find a point $u^{(r)}$, whose order is

$$q^{(r)}=\frac{1}{2^\varkappa}q, \text{ where } r \leqq \varkappa \leqq 2r.$$

If $y^{(r)}$ is the ordinate of $u^{(r)}$, we also have

$$\mathfrak{p}^{c^{(r)}}//y^{(r)}, \text{ where } c^{(r)} \leqq c - r,$$

and if $q^{(r)} > 4$ and $\neq 8$, one of the theorems 10 and 11 can be applied to the point $u^{(r)}$.

Now $2\,c^{(r)} \geqq m$ by lemma 8, and consequently $2\,r \leqq 2\,c - m$. We define R by (69) and then have the following cases:

1. $R < 2\,m$. Then $c < m$ by (12) and hence $2\,r < m$, and since theorem 11 cannot be applied to the point $u^{(r)}$, we have by theorem 10:

$$q^{(r)} = 2^{\lambda}\,t \leqq 6\,m\,(2\,N + 1),$$

where t is an odd number $\leqq 3\,(2\,N + 1)$.

2. $2\,m \leqq R \leqq 6\,m + 4$. Then $2\,c \leqq R$ by (12) and hence $2\,r \leqq R - m$, and theorem 10 gives

$$q^{(r)} = 2^{\lambda}\,t \leqq 6\,m\,(2\,N + 1),$$

where t is an odd number $\leqq 3\,(2\,N + 1)$.

3. $R \geqq 6\,m + 5$. We have $2\,c \leqq R$ by (12) and hence $2\,r \leqq R - m$, and the theorems 10 and 11 give

$$q^{(r)} = 2^{\lambda}\,t \leqq 2\,m\,(2\,N + 1)\,(R - 6\,m + 1),$$

where t is an odd number $\leqq (2\,N + 1)\,(R - 6\,m)$.

Thus we get the following result:

Theorem 12. *Let* $\boldsymbol{\Omega}$ *be an algebraic field, and let* $\mathfrak{p}$ *be a prime ideal in* $\boldsymbol{\Omega}$*, which divides* 2. *Let* A *and* B *be integers mod* $\mathfrak{p}$ *in* $\boldsymbol{\Omega}$ *which satisfy* (1), *and suppose*

$$\mathfrak{p}^{m}//2;$$

$$\mathfrak{p} \nmid A;\ \mathfrak{p}^{m}//B;\ \mathfrak{p}^{2m+R}//4\,A^{3} - 27\,B^{2}.$$

Finally let N *be the norm of* $\mathfrak{p}$, *and suppose that there is an exceptional point of order* q *in* $\boldsymbol{\Omega}$ *on the curve* (2). *Then we have the following cases:*

1. $R < 2\,m$. *Then*

$$q = 2^{\lambda}\,t \leqq 6.4^{[\frac{1}{2}(m-1)]}\,m\,(2\,N + 1),$$

where $\lambda \geqq 0$ *and* t *is an odd number* $\leqq 3\,(2\,N + 1)$.

2. $2m \leqq R \leqq 6m+4$. *Then*

$$q = 2^{\lambda} t \leqq 6.4^{[\frac{1}{2}(R-m)]} m (2N+1),$$

where $\lambda \geqq 0$ *and* t *is an odd number* $\leqq 3(2N+1)$.

3. $R \geqq 6m+5$. *Then*

$$q = 2^{\lambda} t \leqq 2.4^{[\frac{1}{2}(R-m)]} m (2N+1)(R-6m+1),$$

where $\lambda \geqq 0$ *and* t *is an odd number* $\leqq (2N+1)(R-6m)$.

References

[1]. G. Bergman, A generalization of a theorem of Nagell, *Arkiv f. mat.*, bd 2 nr 14 (1952).

[2]. ——, On the exceptional points of cubic curves, *Arkiv f. mat.*, bd 2 nr 27 (1953).

[3]. G. Billing, Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht Eins, *Nova Acta Reg. Soc. Sci. Ups.*, Ser. IV vol. 11 nr 1 (1938).

[4]. J. W. S. Cassels, A note on the division values of $\wp(u)$, *Proc. Cambridge Phil. Soc.*, 45:2 (1949).

[5]. P. Châtelet, Points exceptionnels d'une cubique de Weierstrass, *C. R. Acad. Sci. Paris*, t. 210 (1940), p. 90.

[6]. ——, Groupe exceptionnel d'une classe de cubiques, *C. R. Acad. Sci. Paris*, t. 210 (1940), p. 200.

[7]. T. Nagell, Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre, *Skrifter utg. av det Norske Videnskaps-Akademi i Oslo*, Mat.-naturv. kl., nr 1 (1935).

[8]. ——, Les points exceptionnels sur les cubiques planes du premier genre, *Nova Acta Reg. Soc. Sci. Ups.*, Ser. IV vol. 14 nr 1 (1946).

[9]. A. Weil, L'arithmétique sur les courbes algébriques, *Acta mathematica*, vol. 52 (1929), p. 281.