ON EXCEPTIONAL POINTS ON CUBIC CURVES

G. Billing *and* K. Mahler†.

[*Extracted from the Journal of the London Mathematical Society, Vol.* 15, 1940.]

Introduction.

1. Let C be a cubic curve of genus one and let P_0 be any point on it. The tangent at P_0 cuts C in a point P_1, the tangent at P_1 cuts C in a point P_2, and so on. If this construction leads to only a finite number of different points, then P_0 is called an exceptional point. Otherwise P_0 is called an ordinary point.

Suppose that all the coefficients of the equation of C in some coordinate-system lie in a field Ω. If the coordinates of P_0 also belong to Ω, it may be called an exceptional (or ordinary) point in Ω; and it is clear that the derived points P_n ($n = 1, 2, \ldots$) are then exceptional (or ordinary) points in Ω. The third point of intersection of C with a straight line joining two exceptional points in Ω is also an exceptional point in Ω. All the points obtained in this way from a given exceptional point form a finite group (G. Billing [**2**]). We may suppose, without loss of generality, that one of the exceptional points in Ω is a point of inflexion, since otherwise we can apply a suitable birational transformation with coefficients in Ω. We express the coordinates as elliptic functions of some parameter u chosen in such a way that the point of inflexion in Ω has an argument $u \equiv 0$ (mod ω, ω_1), where ω, ω_1 is a primitive pair of periods of the elliptic functions. The argument of any exceptional point in Ω is then $(m\omega+m_1\omega_1)/n$, where $(m, m_1, n) = 1$ and n is a divisor of the number of elements of the group. The group of exceptional points derived from the point $(m\omega+m_1\omega_1)/n$ consists of the n points $k(m\omega+m_1\omega_1)/n$ ($k = 0, 1, \ldots, n-1$). This group is cyclic, but there are also non-cyclic groups of exceptional points. In this paper we consider only the cyclic cases.

The problem arises of determining the possible values of n when Ω is the rational field. The chief known results are due to B. Levi [**4**], A. Hurwitz [**3**], and T. Nagell [**6**, **7**], who have proved that the following values of n are possible:

$$n = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 12.$$

Levi also proved that n cannot be 14, 16, or 20.

---

† Received 13 July, 1939; read 15 December, 1939.

Another problem is to determine whether there exist curves whose rational points form an exceptional point-group of given structure. In the cyclic cases, this problem has been solved by Levi, Hurwitz, and Nagell for $n = 1, 2, 3, 4$, and 6. Recently C. E. Lind [5] gave examples of curves whose rational points form cyclic groups of 8, 10, and 12 elements.

In this paper we suppose that we are given five points, say 0, 1, 2, 3, 4, for brevity. We describe a construction by which we can in general determine a unique cubic which passes through these points and through certain other points determined by them. If this cubic is of genus one, then 0 is a point of inflexion and the elliptic arguments of the points 0, 1, ... can be taken as ku ($k = 0, 1, \dots, 4$). We show that, if the positions of the points 0, 1, 2, 3, 4 satisfy certain conditions, these points are elements of cyclic groups of exceptional points ($n \geqslant 5$). If these conditions can be satisfied by five points with rational coordinates, then the cubic has n rational exceptional points. For small values of n, the conditions are simple. For $n \geqslant 8$ we choose a homogeneous coordinate-system such that the points 0, 1, 2, 3 are at (1, 1, 1), (1, 0, 0), (0, 1, 0), and (0, 0, 1), and the point 4 at (x_1, x_2, x_3).

If the five points belong to an exceptional group of order n, then 4 lies on a certain curve, namely

a straight line,	if $n = 8$ or 9;
a conic,	if $n = 10$ or 12;
a cubic of genus one,	if $n = 11$;
a hyperelliptic quartic,	if $n = 13$, 14, or 15.

The coordinates of 4 are rational if x_1, x_2, x_3 satisfy a diophantine equation.

For $n = 11$, we show that the cubic for 4 has only five rational points (a result which is of interest in itself as the first example of a cubic of this kind), and we deduce that a cubic cannot have a group of 11 rational points.

The construction.

2. Let 0, 1, 2, 3, 4 denote five different points in the plane, no four of which are collinear. Let $(L;\ L')$ denote the point of intersection of the two straight lines L and L', and $\{k_1, k_2\}$ the straight line through the points k_1. and k_2. We define five more points $-1, \dots, -5$ in the following way:

$$-3 = (\{0, 3\};\ \{1, 2\}), \qquad -4 = (\{0, 4\};\ \{1, 3\}),$$

$$-5 = (\{1, 4\};\ \{2, 3\}), \qquad -1 = (\{0, 1\};\ \{-3, 4\}),$$

$$-2 = (\{0, 2\};\ \{-1, 3\}).$$

3. We consider two cases.

I. *The general case.* No three of the points 0, 1, 2, 3, 4 lie on a straight line.

We prove that the nine points $0, \pm 1, 2, \pm 3, \pm 4, -5$ are all different, and that there is only one cubic C passing through them.

For if, *e.g.*, -5 and -1 coincide, 0, 1, 4 lie on a straight line. Similarly, no other two of the nine points can coincide.

Through the eight points $0, \pm 1, 2, \pm 3, \pm 4$ there pass an infinity of cubics, all of which pass through the same ninth point. This ninth point must be the point -2 (which may possibly coincide with 2, but not with any other of the nine points, as is easily seen by an argument of the above type). For consider the two degenerate cubics consisting of three straight lines: $\{4, 0, -4\}, \{1, 2, -3\}, \{-1, 3\}$ and $\{4, -1, -3\} \{-4, 1, 3\}, \{0, 2\}$. Both pass through the eight given points and also through the ninth point -2. Hence they do not both pass through -5, and so there is only one cubic C which contains the nine points $0, \pm 1, 2, \pm 3, \pm 4, -5$.

4. The point 0 is either a point of inflexion or a point on a straight line forming part of C, if C degenerates into a straight line and a conic, or into three straight lines.

For consider the two degenerate cubics $\{4, 0, -4\}, \{3, 0, -3\}, \{1, 0, -1\}$ and $\{4, -3, -1\}, \{-4, 3, 1\}, \{0, 0\}$. They evidently meet C in the six points $\pm 4, \pm 3, \pm 1$ and in three points at 0. If C does not degenerate, then 0 is not a double point. For if it were, by considering the line $\{4, 0, -4\}$ we see that -4 would coincide with 0, which is impossible from § 2.

5. The cubic cannot degenerate into a proper conic Q and a straight line L.

For, from § 4, 0 would lie on L. If any one of the points 1, 2, 3, 4 also lies on L, then none of the other three can do so. Hence either both 1 and 4 or both 2 and 3 lie on Q, and so -5 lies on L. But then -5, 0 and one of the point-pairs 1, 4, or 2, 3 lies on L, *i.e.* on the same straight line, contrary to hypothesis. Hence none of the points 1, 2, 3, 4, lies on L and so also none of the points $-1, -2, -3, -4$. This is impossible, since it implies that the three collinear points $-1, -2, 3$ lie on Q.

6. The cubic may, however, degenerate into three straight lines L_0, L_1, L_{-1}. We prove that two and only two configurations are

possible:

(i) The points congruent to k (mod 3) lie on L_k ($k = 0, 1, -1$).

(ii) The points congruent to k (mod 4) lie on L_k, if $k = 0$, 1, or -1, and the points congruent to 2 (mod 4) coincide with the point (L_1; L_{-1}).

Since no three of the points 0, 1, 2, 3, 4 lie on a straight line, at least one of them and at most two of them lie on each of the three lines L_0, L_1, L_{-1}. Hence, by § 2, no two of the points -3, -4, -5 lie on one and the same line L_k. Suppose then that -3 lies on L_α, -4 on L_β, -5 on L_γ, α, β, γ denoting the values 0, $+1$, and -1 taken in some order.

Suppose first that -1 lies on L_α. Then 4 also lies on L_α. Hence no one of the points 0, 1, 2, 3 lies on L_α, for then three of the points 0, 1, 2, 3, 4 would lie on L_α. Also 4 cannot be one of the points (L_α; L_β) or (L_α; L_γ); *e.g.* if 4 were (L_α; L_β) then 1 lying on the line $\{4, -5\}$ would coincide with 4. Hence 0 lies on L_γ, since 4, -4 and 0 lie on a straight line. But now none of 1, 2, or 3 can lie on L_γ since -5 lies there, and so they would lie on L_β. Hence -1 cannot lie on L_α.

If -1 lies on L_β, then 2 is the only one of 0, 1, 2, 3, 4 which can also lie on L_β. As before, 2 cannot be one of the points (L_β; L_α) or (L_β; L_γ). Therefore the points 1, 4, -2 lie on L_γ, the points 3, 0 on L_α. This case is, in fact, possible, *e.g.*:

$$0 = (1, 1, 1),\ 1 = (1, 0, 0),\ 2 = (0, 0, 1),\ 3 = (0, 1, 0),\ 4 = (3, 2, 1).$$

If finally -1 lies on L_γ, then none of 0, 1, or 4 can lie there. Hence 2 and 3 lie on L_γ. As before, 3 cannot be one of the points (L_γ; L_α) or (L_γ; L_β). Hence 0 and 4 lie on L_β and then 1 and so also 2 lie on L_α. Therefore 2 must be the point (L_γ; L_α), and -2 must coincide with 2. This cases arises, for example, if the points 0, 1, 2, 3, 4 form the consecutive vertices of a regular pentagon.

7. We now construct further points 5, -6, 6, -7, ... on C by the following recursion method. The point k ($k \geqslant 5$) is taken as the common point of intersection of the lines

$$\{k_1 - k, -k_1\} \qquad (0 \leqslant k_1 < \tfrac{1}{2}k);$$

the point $-k'$ ($k' \geqslant 6$) as the common point of intersection of the lines

$$\{k' - k_1', k_1'\} \qquad (1 \leqslant k_1' < \tfrac{1}{2}k').$$

We show that the new points are uniquely determined and that they lie on C.

We prove that there is a unique point k on C such that the points k, $k_1 - k$, $-k_1$ ($0 \leqslant k_1 < \frac{1}{2}k$) are collinear for any k_1, and a point $-k'$ on C

such that the points $-k'$, $k'-k_1'$, k_1' $(1 \leqslant k_1' < \frac{1}{2}k')$ are collinear for any k_1'. Suppose that this assertion holds for all $k < k_*$ and $k' \leqslant k_*$. Then it also holds for $k = k_*$.

Let k_{11}, k_{12} be two values of k_1 satisfying $0 \leqslant k_{11}, k_{12} < \frac{1}{2}k_*$ and such that the lines $\{k_{11}-k_*, -k_{11}\}$ and $\{k_{12}-k_*, -k_{12}\}$ are determinate and do not coincide. There exist two such values k_{11}, k_{12}.

For $k_* = 5$ or 6 the values $k_{11} = 1$, $k_{12} = 2$ give two such lines.

For $k_* > 6$, consider the four lines

$$\{-k_*, 0\}, \quad \{1-k_*, -1\}, \quad \{2-k_*, -2\}, \quad \{3-k_*, -3\}.$$

No three of these coincide, since no three of the points 0, -1, -2, and -3 are collinear. Also at most one of them is indeterminate. For suppose that the points $l-k_*$ and $-l$ coincide and also the points $l'-k_*$ and $-l'$, where $0 \leqslant l < l' \leqslant 3$. The line through the points $-l$ and $l'-k_*$ has a third point of intersection $-(-l+l'-k_*) = l-l'+k_*$ with C, and the line through the points $l-k_* = -l$ and $l-l'+k_*$ has a third point of intersection $-(l-k_*+l-l'+k_*) = l'-2l$, which then coincides with $l'-k_* = -l'$. But this is impossible from §3, since the only possible values for $l'-2l$ are 3, 2, 1, 0, and -1. Hence there exist values k_{11} and k_{12} with the required properties.

Denote by k_* the point of intersection of the two lines $\{k_{11}-k_*, -k_{11}\}$ and $\{k_{12}-k_*, -k_{12}\}$. Consider the two degenerate cubics

$$\{k_*, k_{11}-k_*, -k_{11}\}, \{k_{12}-k_*, k_*-k_{12}-1, 1\}, \{-k_{12}, k_{12}-k_{11}+1, k_{11}-1\}$$

and

$$\{k_*, k_{12}-k_*, -k_{12}\}, \; \{k_{11}-k_*, k_*-k_{12}-1, k_{12}-k_{11}+1\}, \; \{-k_{11}, 1, k_{11}-1\}.$$

Since eight of their nine common points lie on C, the ninth, k_*, also lies on C.

By considering the two degenerate cubics

$$\{k_*, k_{11}-k_*, -k_{11}\}, \quad \{k_1-k_*, k_*-k_1-1, 1\}, \quad \{-k_1, k_1-k_{11}+1, k_{11}-1\}$$

and

$$\{k_1-k_*, -k_1\}, \quad \{k_{11}-k_*, k_*-k_1-1, k_1-k_{11}+1\}, \quad \{-k_{11}, 1, k_{11}-1\},$$

where $0 \leqslant k_1 < \frac{1}{2}k$, we find that the points k_*, k_1-k_*, $-k_1$ are collinear for all the values of k_1.

Similarly, if the assertion holds for $k < k_*$ and $k' < k_*$, then it holds for $k' = k_*$.

From the above it follows that any points k_1, k_2, k_3 with $k_1+k_2+k_3 = 0$ are collinear. This also holds if two of these k's are equal, *i.e.* if the tangent to C at the point k passes through $-2k$.

8. Suppose now that C is of genus 1, and that its coordinates are expressed by means of elliptic functions, with the primitive pair of periods ω, ω_1. We may assume that the argument of the point 0 is congruent to $0 (\text{mod } \omega, \omega_1)$. Denote by u_k the argument of the point k. Since 0 is a point of inflexion, $u_{k_1}+u_{k_2}+u_{k_3}\equiv 0$ if k_1, k_2, k_3 lie on a straight line, *i.e.* if $k_1+k_2+k_3=0$. Hence, since $u_k+u_{-k}+u_0\equiv 0$ and $u_0\equiv 0$, we have

$$u_1+u_2\equiv u_3,$$

$$u_1+u_3\equiv 2u_1+u_2\equiv u_4,$$

$$u_1+u_4\equiv 3u_1+u_2\equiv u_2+u_3\equiv u_1+2u_2\equiv u_5,$$

and
$$u_2\equiv 2u_1\equiv 2u$$

say, and generally
$$u_k\equiv ku.$$

9. We consider now the *special cases* in which three of the points 0, 1, 2, 3, 4 lie on a straight line.

The points $\pm k$ are constructed as above. In most of these cases, it can be proved that the cubic degenerates into three straight lines. It may, however, happen in some cases that more than one and so an infinity of cubics pass through the points $\pm k$, or that some of these points become indeterminate. We give some illustrations without detailed proof.

(α) 0, 1, 2 lie on a straight line. If the line $\{3, 4\}$ does not pass through any of the points 0, 1, or 2, then it can be shown that C degenerates into three straight lines L_α, L_β, L_γ. On one of them, say L_α, lie all points congruent to 1 (mod 8), on another, L_β say, all points congruent to 3 (mod 8), and on the third L_γ all points congruent to 4 (mod 8). All points congruent to 2 (mod 8) coincide in (L_α, L_β) and all points congruent to 0, 5, 6, 7 (mod 8) in (L_α, L_γ).

If the line $\{3, 4\}$ passes through 0, then the points $\pm k$ are distributed on three lines L_α, L_β, L_γ according to the residue of $\pm k$ (mod 15). All the points congruent to 1 (mod 15) lie on one line L_α and their positions are arbitrary except for the point 1. All the points congruent to 4 (mod 15) lie on another line L_β, but, except for the point 4, these are also indeterminate. On the third L_γ are all points congruent to -5 (mod 15), all indeterminate except the point -5. The points congruent to 2, -6 (mod 15) coincide in (L_α, L_γ), the points congruent to 3, -4 (mod 15) in (L_β, L_γ), and all points belonging to the remaining residue classes in (L_α, L_β).

Configurations of a similar kind arise if the line $\{3, 4\}$ passes through the point 2; the position of the point $\pm k$ is, however, determined by the residue of $\pm k$ (mod 10).

In the case in which $\{3, 4\}$ passes through the point 1, every point $\pm k$ coincides with one of the five original points, the points congruent to 0, 5, 6, 7 (mod 8) with 0, the points congruent to k' (mod 8) ($k' = 1, 2, 3, 4$) with k'. The cubic C degenerates into three straight lines $\{0, 1, 2\}$, $\{4, 0\}$, $\{3, 2\}$.

10. (β) In the following five cases, the points $\pm k$ form groups of 5, 6, 7, 8, or 9 exceptional points respectively.

(i) 0, 1, 4 are collinear and 0, 2, 3 are also collinear. All points congruent to k' (mod 5) ($k' = 0, 1, 2, 3, 4$) coincide in k' and the tangent to any one of them passes through the point congruent to $-2k'$ (mod 5). There is a simple infinity of cubic curves satisfying these conditions, since

$$0+2.1+2.2+2.3+2.4 \equiv 0 \pmod 5,$$

and an infinity of these curves are of genus 1 and have a group of five exceptional points in 0, 1, 2, 3, 4.

(ii) 0, 2, 4, are collinear and 1, 2, 3 are collinear. All points congruent (mod 6) coincide, and both 2 and 4 are points of inflexion, if the curve does not degenerate, since $3.2 \equiv 3.4 \equiv 0$ (mod 6). In this case, we get an infinity of cubics of genus 1 with a group of six exceptional points in 0, 1, 2, 3, 4, and -1.

Note. If 0, 2, 4 are collinear, but the line $\{1, 3\}$ does not pass through any of the points 0, 2, or 4, the general case of a cubic degenerating into a line and a conic arises. All points congruent to 0 (mod 2) lie on the straight line and all the others on the conic.

(iii) 0, 3, 4 and 1, 2, 4 lie on straight lines. In this case we can construct a simple infinity of cubics with a group of seven exceptional points in 0, 1, 2, 3, 4, -1, and -2. The points of intersection of a line through 3, arbitrary but different from the lines $\{3, 2\}$, $\{3, 0, 4\}$ and $\{3, 1\}$, with the lines $\{1, 0\}$ and $\{2, 0\}$, give two new points, -1 and -2 respectively. Every point congruent to k' (mod 7) ($k' = 0, 1, 2, 3, 4, -1, -2$) coincides with k'. By these points and two of the known tangents the cubic is uniquely determined in this case. But since there is a simple infinity of lines through 3 we also get an infinity of curves, viz. one corresponding to each of these lines.

(iv) If the points 1, 3, 4, but no other three of the points 0, 1, 2, 3, 4, are collinear, we get only eight points 0, ± 1, ± 2, ± 3, 4 which together with one of the known tangents determine a unique cubic. In general, this curve is of genus 1, *i.e.* the points form a group of eight exceptional points.

(v) If finally the points 2, 3, 4, but no other three of the points 0, 1, 2, 3, 4, are collinear we get nine different points only, which together with one of the known tangents determine a unique cubic which is generally of genus 1. The nine points then form a group of nine exceptional points on this curve.

Representation of the points k in homogeneous coordinates.

11. In this paragraph we suppose that no three of the points 0, 1, 2, 3 are collinear. We use homogeneous coordinates x_1, x_2, x_3. The lines $\{2, 3\}$, $\{3, 1\}$, $\{1, 2\}$ are taken as $x_1=0$, $x_2=0$, $x_3=0$ and the coordinates of the points 1, 2, 3 as (1, 0, 0), (0, 1, 0), (0, 0, 1). There is no loss of generality in taking 0 to be the point (1, 1, 1). Let the coordinates of the point 4 be (x_1, x_2, x_3). Then the coordinates of all points $\pm k$ become functions of x_1, x_2, x_3, thus

$$0=(1,\ 1,\ 1)$$

$$1=(1,\ 0,\ 0), \qquad -1=(x_1-x_2+x_3,\ x_3,\ x_3),$$

$$2=(0,\ 1,\ 0), \qquad -2=(x_1-x_2+x_3,\ x_3,\ x_1-x_2+x_3),$$

$$3=(0,\ 0,\ 1), \qquad -3=(1,\ 1,\ 0),$$

$$4=(x_1,\ x_2,\ x_3), \qquad -4=(x_1-x_2,\ 0,\ x_3-x_2),$$

$$5=\big(x_1x_2+x_1x_3-x_2^2,\ x_1x_3,\ x_2(x_1-x_2+x_3)\big), \qquad -5=(0,\ x_2,\ x_3),$$

$$6=\big((x_1-x_2+x_3)(x_1^2x_2-x_1x_2^2-x_1x_3^2+x_2^2x_3),$$
$$x_3(x_2-x_3)(x_1x_2+x_1x_3-x_2^2),\ x_1x_3(x_2-x_3)(x_1-x_2+x_3)\big),$$

$$-6=\big(x_1x_2(x_1-x_2+x_3),\ x_1x_3^2,\ x_2x_3(x_1-x_2+x_3)\big),$$

$$7=\big((x_1-x_2+x_3)(x_2^2-x_1x_3),\ x_1^2x_2-x_1x_2^2-x_1x_3^2+x_2^2x_3,$$
$$(x_2-x_3)(x_1x_2+x_1x_3-x_2^2)\big),$$

$$-7=\big(x_1(x_1x_2+x_1x_3-x_2^2),\ x_2(x_1x_2+x_1x_3-x_2^2),\ x_1x_2(x_1-x_2+x_3)\big),$$

$$8=\big(-x_1^2x_2^2+x_1x_2^3+x_1x_2x_3^2-x_1x_3^3-x_2^3x_3+x_2^2x_3^2,\ x_3^2(x_2^2-x_1x_3),$$
$$x_3(x_1^2x_2-x_1x_2^2-x_1x_3^2-x_2^2x_3)\big),$$

$$-8=\big((x_1x_2+x_1x_3-x_2^2)(x_1^2x_2-x_1x_2^2-x_1x_3^2+x_2^2x_3),$$
$$x_1x_3(x_1^2x_2-x_1x_2^2-x_1x_3^2+x_2^2x_3),\ x_1x_3(x_2-x_3)(x_1x_2+x_1x_3-x_2^2)\big).$$

... ...

Exceptional points.

12. LEMMA 1. *A necessary condition for the points* $\pm k$ $(k=0, 1, \ldots)$ *to form a group of* n $(n \geqslant 5)$ *exceptional points is that any set of three points* k_1, k_2, k_3, *satisfying*

$$k_1+k_2+k_3=0 \pmod{n}$$

lie on a straight line.

If a particular set k_1, k_2, k_3, *where* $|k_1+k_2+k_3|=n \geqslant 5$, *lie on a straight line, then the points* $\pm k$ $(k=0, 1, \ldots)$ *form a group of* n *exceptional points provided that*

(1) *the cubic considered is of genus* 1,

(2) *no points* k_1', k_2', k_3' *with*

$$0<|k_1'+k_2'+k_3'|<n$$

lie on a straight line.

Proof. Since exceptional points are defined only on curves of genus 1, the first part follows immediately from the parametrical representation in § 8.

If the curve is of genus 1 and u is the argument of the point 1 and $|k_1+k_2+k_3|=n$, then

$$u \equiv w/n \pmod{\omega, \omega_1},$$

where w is a period. Hence all the points k form a group of n' exceptional points, where $n' | n$. But if $n'<n$, there would be points k_1', k_2', k_3' on a straight line with

$$0<|k_1'+k_2'+k_3'|=n'<n,$$

contrary to hypothesis.

From this lemma and § 11 we obtain the following necessary conditions for the coordinates of the point 4, in order that all the points $\pm k$ should form a group of n exceptional points:

$n=7$: $$x_1-x_2=0, \ x_3=0.$$

This determines 4 as the point $(1, 1, 0)$, but then the point -1 has coordinates $(x_1', 1, 1)$ with x_1' indeterminate. In this case the value of x_1' specifies the cubic.

$n=8:\ \ x_2=0$

$n=9:\ \ x_1=0$

$n=10:\ \ x_1x_2+x_1x_3-x_2^2=0$

$n=11:\ \ x_1^2x_2-x_1x_2^2-x_1x_3^2+x_2^2x_3=0$

$n=12:\ \ x_2^2-x_1x_3=0$

$n=13:\ \ x_1^2x_2^2-x_1x_2^3-x_1x_2x_3^2+x_1x_3^3+x_2^3x_3-x_2^2x_3^2=0$

$n=14:\ \ x_1^3x_2-x_1^2x_2^2-x_1^2x_2x_3-x_1^2x_3^2-x_1x_2^3+x_1x_2x_3^2+x_2^4-x_2^3x_3=0$

$n=15:\ \ x_1^2x_2^2+x_1^2x_2x_3+x_1^2x_3^2-x_1x_2^3-x_1x_2^2x_3-x_1x_2x_3^2+x_2^3x_3=0,$

... ...

The case $n=11$.

13. Lemma 2. *The curve*

(1) $$x_1^2x_2-x_1x_2^2-x_1x_3^2+x_2^2x_3=0$$

has five and only five rational points $(x_1,\ x_2,\ x_3)$, *namely*

(X) $(1,\ 0,\ 0),\ (0,\ 1,\ 0),\ (0,\ 0,\ 1),\ (1,\ 1,\ 0)$, *and* $(1,\ 1,\ 1)$.

Proof. By the birational transformation

$$\frac{x_1}{x_3}=\frac{(12+\xi)^2}{6(108-\eta)},\qquad \xi=36\,\frac{x_1}{x_2}-12,$$

$$\frac{x_2}{x_3}=\frac{6(12+\xi)}{108-\eta},\qquad \eta=108-\frac{216\,x_1x_3}{x_2^2},$$

the curve (1) is transformed into

(2) $$\eta^2=\xi^3-16\,.\,27\xi+19\,.\,16\,.\,27=f(\xi),$$

say. The five rational points (X) on (1) correspond to the five points $(\xi,\ \eta)$

(Y) $(\infty,\ \infty),\ (-12,\ \pm108),\ (24,\ \pm108)$

on (2). It is sufficient to prove that these five points are the only rational points on (2). We do this by the method given by G. Billing [1, 41-46].

Let θ be the real root of the equation $f(\theta)=0$ and ϑ the real root of

$$t^3-4t-4=0.$$

The two numbers θ and ϑ generate the same algebraic field K. We have, in fact,

$$\theta=24-9\vartheta^2=-12(1+3/\vartheta).$$

The field K has the basis 1, ϑ, $\frac{1}{2}\vartheta^2$ and the discriminant $D=-44$; the discriminant of θ is $\Delta(\theta)=-11.16^2.27^4$.

In order to find the class-number of K, we have to examine the factorization of the rational prime numbers $p<|\sqrt{D}|<7$ into prime ideals in K; the result is that $(2)=(\frac{1}{2}\vartheta^2)^3$, and that (3) and (5) are prime ideals in K. Hence the class-number $h=1$.

The coordinates of every rational point on the curve (2) can be written as

$$\xi=\frac{x}{z^2},\qquad \eta=\frac{y}{z^3},$$

where x, y, z are integers and $(x, z)=(y, z)=1$. By **1**, Satz 1, 41 the rank of the curve (2) is not greater than 2, and, if the curve has ordinary rational points $(x/z^2, y/z^3)$, there must exist rational integers x, z satisfying

$$x-\theta z^2=\eta\alpha^2,$$

where α is an integer in K, and η is a positive unit which is not the square of another unit. The number $-1+\frac{1}{2}\vartheta^2$ is a unit of this kind and we get

$$(-1+\tfrac{1}{2}\vartheta^2)(x-24z^2+9z^2\vartheta^2)=(\eta\alpha)^2=(a+b\vartheta+\tfrac{1}{2}c\vartheta^2)^2,$$

where a, b, c are rational integers. Hence

$$-x+24z^2=a^2+4bc,$$

$$18z^2=c^2+2ab+4bc,$$

$$\tfrac{1}{2}x-3z^2=b^2+c^2+ac.$$

From the third and first of these equations, x and a are even. Hence z is odd, since $(x, z)=1$, and so the second equation leads to the impossible congruence

$$2\equiv c^2 \pmod 4.$$

The curve (2) has, therefore, no ordinary rational points.

It now remains to determine all exceptional rational points (ξ, η). By a theorem due to T. Nagell [7, p. 14, 15], these points, excluding the point at infinity, have the following properties: (1) ξ and η are integers, (2) η^2 is either 0 or a divisor of $\Delta(\theta) = -11 . 16^2 . 27^4$. There is only a finite number of possibilities for η and ξ, and a discussion which we omit shows that the curve has only the above-mentioned exceptional rational points (Y).

14. THEOREM. *There is no cubic of genus* 1 *with a group of* 11 *rational exceptional points.*

Proof. If such a cubic exists, then from § 12 and Lemma 2, the point 4 must be one of the points

$$(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0), (1, 1, 1),$$

i.e., (§§ 8, 11),

$$4\frac{w}{11} \equiv k\frac{w}{11} \pmod{\omega, \omega_1} \quad (k = 1, 2, 3, -3, \text{ or } 0),$$

which is impossible, since $w/11$ is not a period.

References.

1. Billing, G., " Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht eins ", *Nova Acta Reg. Soc. Sc. Upsaliensis* (4), 11 (1937), No. 1.
2. ———, " Vom Range kubischer Kurven vom Geschlecht eins in algebraischen Rationalitätsbereichen ", *IX Skandin. Matematikerkongressen, Helsingfors* (1938), 146–150.
3. Hurwitz, A., " Über ternäre diophantische Gleichungen dritten Grades ", *Vierteljahrschrift der Naturf. Gesellschaft in Zürich*, 62 (1917), 207–229.
4. Levi, B., " Saggio per una teoria aritmetica delle forme cubiche ternarie ", *Atti della R. Accademia delle Scienze di Torino*, 41 (1906), 739–764; 43 (1908), 99–120, 413–434, 672–681.
5. Lind, C. E., " Kubische Kurven mit gerader Anzahl exzeptioneller Punkte ", *IX Skandin. Matematikerkongressen, Helsingfors* (1938), 201–206.
6. Nagell, T., " Sur les propriétés arithmétiques des cubiques planes du premier genre ", *Acta mathematica*, 52 (1929), 93–126.
7. ——— " Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre ", *Skrifter utg. av. d. Norske Videnskabs-Akademi, Oslo, I. Mat.-Naturv. Klasse* (1935), No. 1.

The University,
Manchester.

Printed by C. F. Hodgson & Son, Ltd., Newton St., London, W.C.2.