ON THE LATTICE POINTS ON CURVES OF GENUS 1

By KURT MAHLER†.

[Received and read 26 April, 1934.]

Suppose that

$$F(x, y) = a_0 x^3 + a_1 x^2 y + a_2 xy^2 + a_3 y^3$$

is a cubic binary form with integer coefficients, which is irreducible in the field of all rational numbers, and that $k \neq 0$ is an integer. A special case of Thue's famous theorem states that the equation

$$F(x, y) = k$$

has only a finite number $A(k)$ of solutions in integers x, y; more recent researches of the author have proved that this number $A(k)$ can be large only if the integer k is the product of a great number of equal or different prime factors. A result due to C. L. Siegel includes the inequality

$$\sum_{h=1}^{k} A(h) = O(k^{\frac{2}{3}}),$$

and therefore $A(k)$ must be zero for nearly all integers k.

Until recently, there did not seem to exist theorems in the other direction, *i.e.* whether the number $A(k)$ can, in fact, be very large for suitably chosen integers k, or whether $A(k)$ is absolutely bounded. I shall prove in this paper that $A(k)$ is greater than any given number t for certain integers k, and that there is even an infinity of integers k for which

$$A(k) \geqslant \sqrt[4]{\log k}.$$

I cannot prove similar results for the "primitive" solutions of $F(x, y) = k$, *i.e.* those solutions x, y for which x and y are coprime integers;

† This paper is an extension of one previously contributed to a Festschrift for Prof. Hellinger.

whether their number is bounded is still an open question, and I doubt whether it can be solved by a method similar to that of this paper.

The cubic equation $F(x, y) = k$ defines a cubic curve of genus 1 in the (x, y)-plane, and so such curves exist on which more than t lattice points lie, where t is an arbitrary integer. Now these cubic curves $F(x, y) = k$ are not the most general ones, since their invariant g_2 is zero. A special case of a theorem of Siegel shows that on every cubic curve of genus 1 which is defined by an equation with rational coefficients, there are only a finite number of lattice points. Two cubic curves which have the same absolute invariant J can be transformed into one another by a birational transformation, and this transformation has rational coefficients when there are points with rational coordinates on both curves; also the systems of these rational points are changed into each other by the transformation and therefore are invariants. It is interesting to observe that a corresponding result for lattice points on these curves does not exist, for I shall prove in this paper that, for any given integer t and for any given rational value of the invariant J, there exists a cubic curve defined by an equation with rational coefficients on which lie more than t lattice points.

The method of the text is useful for the study of all curves of genus 1 in two or more dimensions; I give a number of results obtained by it, which perhaps are not all new. It may be remarked that curves of genus 0 with only a finite number of lattice points may be treated also in this way; the reader will not find it difficult to establish, for example, the existence of rational numbers a such that there are at least t lattice points on the lemniscate

$$(x^2+y^2)^2+a(x^2-y^2) = 0,$$

where t is an arbitrarily large integer.

I.

1. Suppose that

$$F(x, y) = a_0 x^3+a_1 x^2 y+a_2 xy^2+a_3 y^3$$

is a cubic binary form with integer coefficients and with only simple linear factors. The equation

$$F(x, y) = 1$$

defines a cubic curve C without double points and therefore of genus 1 in the (x, y)-plane. Its three asymptotes may be denoted by $\Gamma', \Gamma'', \Gamma'''$.

If (x_0, y_0) is any point with integer coordinates not lying on Γ', Γ'', Γ''', and

$$F(x_0, y_0) = k,$$

then k is an integer and $k \neq 0$; there is one and only one curve

$$F(x, y) = k,$$

say $C(k)$, which goes through (x_0, y_0) and is similar and similarly situated to the curve C relative to the origin.

2. Since C is of genus 1, a uniformisation of C,

$$x = \phi(u), \quad y = \psi(u),$$

exists; here $\phi(u)$ and $\psi(u)$ are two elliptic functions of u of order 2 or 3 and with periods ω_1 and ω_2, say. Instead of the point (x, y) on C, we shall speak also of the point u, where u is the elliptic argument of (x, y). Then u and u' are the same point if and only if

$$u \equiv u' \pmod{\omega_1, \omega_2},$$

i.e. if

$$u = u' + h_1 \omega_1 + h_2 \omega_2$$

with two integers h_1 and h_2.

Now let us take any straight line Γ; it cuts C in three points u_1, u_2, u_3 which satisfy the congruence

$$u_1 + u_2 + u_3 \equiv C_0 \pmod{\omega_1, \omega_2}.$$

Here C_0 is a constant, not depending on Γ, which may be assumed, without loss of generality, to be zero; then the congruence takes the simpler form

$$u_1 + u_2 + u_3 \equiv 0 \pmod{\omega_1, \omega_2}.$$

If, in particular, Γ is a tangent with u_1 its point of contact and u_2 its other point of intersection with C, *i.e.* if u_2 is the tangential of u_1, then

$$2u_1 + u_2 \equiv 0 \pmod{\omega_1, \omega_2}.$$

3. Beginning with any point u on C we construct an infinite set U of points

$$u_1 = u, \ u_{-2}, \ u_4, \ u_{-5}, \ u_7, \ u_{-8}, \ \ldots, \ u_{3m+1}, \ u_{-3m-2}, \ \ldots$$

on C, given by their elliptic arguments

$$u_1 = u, \quad u_{-2} = -2u, \quad u_4 = 4u, \quad \ldots,$$

$$u_{3m+1} = (3m+1)u, \quad u_{-3m-2} = -(3m+2)u, \quad \ldots.$$

Since

$$2u_1 + u_{-2} \equiv 0 \pmod{\omega_1, \omega_2} \quad \text{and} \quad 2u_{-2} + u_4 \equiv 0 \pmod{\omega_1, \omega_2},$$

u_{-2} is the point of intersection of C with the tangent to C at u, and u_4 is the point of intersection of C with the tangent to C at u_{-2}. Further, since

$$u_{-2} + u_{-3(m-1)-2} + u_{3m+1} \equiv 0 \pmod{\omega_1, \omega_2} \quad (m = 2, 3, \ldots)$$

and

$$u_1 + u_{3m+1} + u_{-(3m+2)} \equiv 0 \pmod{\omega_1, \omega_2} \quad (m = 1, 2, \ldots),$$

the point

$$u_{3m+1} \quad (m = 2, 3, \ldots)$$

is the point of intersection with C of the straight line through u_{-2} and u_{-3m+1}; and the point

$$u_{-(3m+2)} \quad (m = 1, 2, \ldots)$$

is the point of intersection with C of the line through u_1 and u_{3m+1}.

This construction makes use only of such properties of C as remain unaltered by collineations, and is therefore invariant when we apply a transformation of this kind. Now the transformation

$$x \to k^{\frac{1}{3}} x, \quad y \to k^{\frac{1}{3}} y$$

changes C into $C(k)$, and so changes the set U of points

$$u_{3m+1}, \; u_{-3m-2} \quad (m = 0, 1, 2, \ldots)$$

on C into a set V of points

$$v_{3m+1}, \; v_{-3m-2} \quad (m = 0, 1, 2, \ldots)$$

on $C(k)$, which has the same properties with regard to $C(k)$ as U has with regard to C. It is obvious that the line joining the point u_λ and the corresponding point v_λ passes through the origin.

4. It is possible that some of the points of U coincide. Let us consider the $2n$ points

$$u_{3m+1}, \; u_{-3m-2} \quad (m = 0, 1, 2, \ldots, n-1)$$

of this set. If they are not all different, then one of the congruences

$$(3m_1+1)u \equiv (3m_2+1)u \quad (\text{mod } \omega_1, \omega_2),$$

$$(3m_1+1)u \equiv -(3m_2+2)u \quad (\text{mod } \omega_1, \omega_2),$$

$$-(3m_1+2)u \equiv -(3m_2+2)u \quad (\text{mod } \omega_1, \omega_2)$$

$$(m_1, m_2 = 0, 1, \ldots, n-1; \; m_1 \neq m_2)$$

must be satisfied, and therefore u is of the form

$$u \equiv \frac{h_1 \omega_1 + h_2 \omega_2}{3N} \quad (\text{mod } \omega_1, \omega_2),$$

where the denominator $3N$ is one of the numbers

$$3N = 3, 6, 9, \ldots, 3(2n-1),$$

and h_1 and h_2 are any two integers. For every N, this gives only $9N^2$ different points u, and so there are at most

$$\sum_{N=1}^{2n-1} 9N^2 \leqslant (2n-1) . 9(2n-1)^2 < 72n^3$$

different positions of u on C, say

$$u_1', u_1'', \ldots, u_1^{(\mu)} \quad (\mu \leqslant 72n^3),$$

such that the $2n$ first points

$$u_{3m+1}, u_{-3m-2} \quad (m = 0, 1, \ldots, n-1)$$

are not all different from one another.

5. Since C is a cubic curve, it has three points u', u'', u''' at infinity. It is possible that one of the first $2n$ points

$$u_{3m+1}, u_{-3m-2} \quad (m = 0, 1, \ldots, n-1)$$

of the set U coincides with u' or u'' or u'''. Then one of the congruences

$$(3m+1)u \equiv u^{(i)} \; (\text{mod } \omega_1, \omega_2) \quad (i = 1, 2, 3; \; m = 0, 1, \ldots, n-1),$$

or one of the congruences

$$-(3m+2)u \equiv u^{(i)} \; (\text{mod } \omega_1, \omega_2) \quad (i = 1, 2, 3; \; m = 0, 1, \ldots, n-1),$$

must be satisfied, and therefore u has one of the values

$$u \equiv \frac{u^{(i)}+h_1\omega_1+h_2\omega_2}{3m+1} \pmod{\omega_1, \omega_2} \quad (i=1, 2, 3)$$

or

$$u \equiv \frac{-u^{(i)}+h_1\omega_1+h_2\omega_2}{3m+2} \pmod{\omega_1, \omega_2} \quad (i=1, 2, 3),$$

where h_1 and h_2 are two integers. For every m this gives only

$$3\,.\,(3m+1)^2+3\,.\,(3m+2)^2 \leqslant 6\,.\,9\,.\,(m+1)^2$$

different points u. Hence there are at most

$$\sum_{m=0}^{n-1} 6\,.\,9\,.\,(m+1)^2 \leqslant n\,.\,54n^2 = 54n^3$$

different positions of u on C, say

$$u_2', u_2'', \ldots, u_2^{(\nu)} \quad (\nu \leqslant 54n^3),$$

such that one of the $2n$ points

$$u_{3m+1}, u_{-3m-2} \quad (m=0, 1, \ldots, n-1)$$

of the set U lies at infinity.

6. Now we draw in the (x, y)-plane the three asymptotes

$$\Gamma', \Gamma'', \Gamma'''$$

of C, all the straight lines

$$\Gamma_1', \Gamma_1'', \ldots, \Gamma_1^{(\mu)}$$

which go through the origin (0, 0) and one of the points

$$u_1', u_1'', \ldots, u_1^{(\mu)},$$

and all the straight lines

$$\Gamma_2', \Gamma_2'', \ldots, \Gamma_2^{(\nu)}$$

which go through the origin and one of the points

$$u_2', u_2'', \ldots, u_2^{(\nu)}.$$

The total number of these straight lines is not greater than

$$3+72n^3+54n^3 \leqslant 130n^3.$$

But on every one of these lines Γ, Γ_1, Γ_2 there are at most

$$130n^3+1$$

lattice points which lie in the square Q defined by

$$\max(|x|, |y|) \leqslant 65n^3.$$

Hence the number of lattice points in Q, which lie on any one of the straight lines Γ, Γ_1, Γ_2, does not exceed

$$130n^3(130n^3+1),$$

and so is less than the number

$$(130n^3+1)^2$$

of all lattice points in Q. It follows that there must be a point

$$(x_1, y_1)$$

with integer coordinates satisfying the inequality

$$\max(|x_1|, |y_1|) \leqslant 65n^3,$$

which does *not* lie on any one of the straight lines

$$\Gamma', \Gamma'', \Gamma'''; \; \Gamma_1', \Gamma_1'', \ldots, \Gamma_1^{(\mu)}; \; \Gamma_2', \Gamma_2'', \ldots, \Gamma_2^{(\nu)}.$$

7. The number

$$F(x_1, y_1) = k_1$$

is an integer different from zero, since (x_1, y_1) does not lie on the asymptotes Γ_1, Γ_2, Γ_3. Hence the equation

$$F(x, y) = k_1$$

defines a cubic curve $C(k_1)$ which goes through (x_1, y_1). Denote by $k_1^{\frac{1}{3}}$ the real cube root of k_1. Then the transformation

$$x \rightarrow \frac{x}{k_1^{\frac{1}{3}}}, \quad y \rightarrow \frac{y}{k_1^{\frac{1}{3}}},$$

changes $C(k_1)$ into C and the point (x_1, y_1) on $C(k_1)$ into the point

$$u_1 = \left(\frac{x_1}{k_1^{\frac{1}{3}}}, \quad \frac{y_1}{k_1^{\frac{1}{3}}}\right)$$

on C. The three points

$$(0, 0),\ (x_1, y_1),\ u_1$$

lie on the same straight line, and so u_1 must be different from all the points

$$u_1', u_1'', \ldots, u_1^{(\mu)}, u_2', u_2'', \ldots, u_2^{(\nu)},$$

since (x_1, y_1) does not lie on any one of the lines

$$\Gamma_1', \Gamma_1'', \ldots, \Gamma_1^{(\mu)}, \Gamma_2', \Gamma_2'', \ldots, \Gamma_2^{(\nu)}.$$

Now construct the $2n$ points

$$u_{3m+1} = \left(\frac{x_{3m+1}}{k_1^{\frac{1}{3}}}, \frac{y_{3m+1}}{k_1^{\frac{1}{3}}}\right), \quad u_{-3m-2} = \left(\frac{x_{-3m-2}}{k_1^{\frac{1}{3}}}, \frac{y_{-3m-2}}{k_1^{\frac{1}{3}}}\right) \quad (m = 0, 1, \ldots, n-1)$$

of the set U belonging to u_1 on the curve C. Then we know that they are all different from one another and that none of them lies at infinity. The $2n$ corresponding points

$$(x_{3m+1}, y_{3m+1}),\ (x_{-3m-2}, y_{-3m-2}) \quad (m = 0, 1, \ldots, n-1)$$

on $C(k_1)$ must therefore also be different from one another, and none of them can lie at infinity. Furthermore, when m_1, m_2, m_3 are three different members of the set of $2n$ indices $3m+1$, $-3m-2$ $(m = 0, 1, \ldots, n-1)$ with

$$m_1+m_2+m_3 = 0,$$

then the three points

$$(x_{m_1}, y_{m_1}),\ (x_{m_2}, y_{m_2}),\ (x_{m_3}, y_{m_3})$$

on $C(k_1)$ lie on the same straight line, and when m_1 and m_2 are two different members of this set of indices with

$$2m_1+m_2 = 0,$$

then the straight line through the two points

$$(x_{m_1}, y_{m_1}),\ (x_{m_2}, y_{m_2})$$

is a tangent to $C(k_1)$ at (x_{m_1}, y_{m_1}).

8. We make use of the abbreviations

$$F_1(x, y) = \frac{\partial}{\partial x} F(x, y), \quad F_2(x, y) = \frac{\partial}{\partial y} F(x, y).$$

$F_1(x, y)$ and $F_2(x, y)$ vanish simultaneously only at the point $x = y = 0$; for the binary form $F(x, y)$ has simple linear factors only, and its discriminant, *i.e.* the resultant of $F_1(x, y)$ and $F_2(x, y)$, cannot be zero.

Let (x''', y''') be the third point of intersection of the straight line through two points (x', y') and (x'', y'') on $C(k_1)$ with this curve. Then

$$F(x''', y''') = k_1,$$

and

$$\begin{vmatrix} x' & y' & 1 \\ x'' & y'' & 1 \\ x''' & y''' & 1 \end{vmatrix} = x'''(y'-y'')+y'''(x''-x')+(x'y''-x''y') = 0,$$

and therefore x''' and y''' must satisfy the cubic equations

$$F\{x'''(x'-x''),\ x'''(y'-y'')+(x'y''-x''y')\} = k_1(x'-x'')^3,$$

$$F\{y'''(x'-x'')-(x'y''-x''y'),\ y'''(y'-y'')\} = k_1(y'-y'')^3.$$

If we expand the left-hand sides in powers of x''' or y''', we get

$$F(x'-x'', y'-y'')x'''^3+F_2(x'-x'', y'-y'')(x'y''-x''y')x'''^2+{}^*x''' +{}^*1 = 0,$$

$$F(x'-x'', y'-y'')y'''^3-F_1(x'-x'', y'-y'')(x'y''-x''y')y'''^2+{}^*y''' +{}^*1 = 0,$$

where the asterisks denote the coefficients of x''' and 1, or of y''' and 1, which are of no importance.

Now we know two roots x' and x'', or y' and y'', of these cubic equations; their third roots therefore have the values

$$(\mathrm{A}_1)\quad \begin{cases} x''' = -x'-x''-\dfrac{(x'y''-x''y')\,F_2(x'-x'', y'-y'')}{F(x'-x'', y'-y'')}, \\[2ex] y''' = -y'-y''+\dfrac{(x'y''-x''y')\,F_1(x'-x'', y'-y'')}{F(x'-x'', y'-y'')}. \end{cases}$$

When we introduce homogeneous coordinates

$$x' : y' : 1 = x^{(1)} : y^{(1)} : z^{(1)}, \quad x'' : y'' : 1 = x^{(2)} : y^{(2)} : z^{(2)}, \quad x''' : y''' : 1 = x^{(3)} : y^{(3)} : z^{(3)},$$

and use the abbreviations

$$(xy) = x^{(1)}y^{(2)}-x^{(2)}y^{(1)}, \quad (xz) = x^{(1)}z^{(2)}-x^{(2)}z^{(1)}, \quad (yz) = y^{(1)}z^{(2)}-y^{(2)}z^{(1)}$$

and

$$G_1(x^{(1)}y^{(1)}z^{(1)},\ x^{(2)}y^{(2)}z^{(2)})$$
$$= -(x^{(1)}z^{(2)}+x^{(2)}z^{(1)})\,F\{(xz),\ (yz)\}-z^{(1)}z^{(2)}(xy)\,F_2\{(xz),\ (yz)\},$$
$$G_2(x^{(1)}y^{(1)}z^{(1)},\ x^{(2)}y^{(2)}z^{(2)})$$
$$= -(y^{(1)}z^{(2)}+y^{(2)}z^{(1)})\,F\{(xz),\ (yz)\}-z^{(1)}z^{(2)}\,(xy)\,F_1\{(xz),\ (yz)\},$$
$$G_3(x^{(1)}y^{(1)}z^{(1)},\ x^{(2)}y^{(2)}z^{(2)}) = z^{(1)}z^{(2)}\,F\{(xz),\ (yz)\},$$

these formulae take the simple form

$$(\mathrm{A}_2)\qquad \begin{cases} x^{(3)}= G_1(x^{(1)}y^{(1)}z^{(1)},\ x^{(2)}y^{(2)}z^{(2)}), \\ y^{(3)} = G_2(x^{(1)}y^{(1)}z^{(1)},\ x^{(2)}y^{(2)}z^{(2)}), \\ z^{(3)} = G_3(x^{(1)}y^{(1)}z^{(1)},\ x^{(2)}y^{(2)}z^{(2)}). \end{cases}$$

The expressions G_1, G_2, G_3 on the right-hand side are forms in the six arguments $x^{(1)}$, $y^{(1)}$, $z^{(1)}$, $x^{(2)}$, $y^{(2)}$, $z^{(2)}$ with integer coefficients; they are of degree four in the coordinates $x^{(1)}$, $y^{(1)}$, $z^{(1)}$, and also in the coordinates $x^{(2)}$, $y^{(2)}$, $z^{(2)}$. It is obvious that, when $x^{(1)}$, $y^{(1)}$, $z^{(1)}$, $x^{(2)}$, $y^{(2)}$, $z^{(2)}$ have integral values, so also have $x^{(3)}$, $y^{(3)}$, $z^{(3)}$. If we write

$$w^{(i)} = \max(|x^{(i)}|,\ |y^{(i)}|,\ |z^{(i)}|) \quad (i = 1,\ 2,\ 3),$$

the formulae give the inequality

$$(\mathrm{A}_3)\qquad w^{(3)} \leqslant c_1(w^{(1)}w^{(2)})^4,$$

where c_1 is a positive constant depending only on the coefficients of the cubic form $F(x, y)$.

Assume, in particular, that none of the three points

$$\left(\frac{x^{(1)}}{z^{(1)}},\ \frac{y^{(1)}}{z^{(1)}}\right),\quad \left(\frac{x^{(2)}}{z^{(2)}},\ \frac{y^{(2)}}{z^{(2)}}\right),\quad \left(\frac{x^{(3)}}{z^{(3)}},\ \frac{y^{(3)}}{z^{(3)}}\right)$$

lies at infinity, that $(x^{(1)}/z^{(1)}, y^{(1)}/z^{(1)})$ and $(x^{(2)}/z^{(2)}, y^{(2)}/z^{(2)})$ do not coincide, and that $z^{(1)} \neq 0$ and $z^{(2)} \neq 0$. Then it is obvious that the straight line through these three points is not parallel to one of the asymptotes Γ', Γ'', Γ'''; hence the point

$$\left(\frac{x^{(1)}}{z^{(1)}}-\frac{x^{(2)}}{z^{(2)}},\ \frac{y^{(1)}}{z^{(1)}}-\frac{y^{(2)}}{z^{(2)}}\right)$$

does not lie on Γ' or Γ'' or Γ''', and so the number

$$F\Big((xz),\ (yz)\Big) = (z^{(1)}z^{(2)})^3\,F\left(\frac{x^{(1)}}{z^{(1)}}-\frac{x^{(2)}}{z^{(2)}},\ \frac{y^{(1)}}{z^{(1)}}-\frac{y^{(2)}}{z^{(2)}}\right)$$

does not vanish, and we also have

$$(\mathrm{A}_4) \qquad z_3 = z^{(1)} z^{(2)} F\Big((xz),\ (yz)\Big) \neq 0.$$

9. By the method of § 8 we can calculate the coordinates (x''', y''') of the point of intersection of $C(k)$ with its tangent at the point (x', y'). The result is

$$(\mathrm{B}_1) \qquad \begin{cases} x''' = -2x' - \dfrac{F_2(Y', -X')(x'X' + y'Y')}{F(Y', -X')}, \\ y''' = -2y' + \dfrac{F_1(Y', -X')(x'X' + y'Y')}{F(Y', -X')}, \\ \qquad\qquad [X' = F_1(x', y'),\ Y' = F_2(x', y')]. \end{cases}$$

We also arrive at these formulae by making (x'', y'') tend to (x', y') in the formulae (A_1), for then

$$(x' - x'') : (y' - y'') \rightarrow Y' : (-X').$$

It is useful to remark that the binary form of degree 6,

$$F(Y', -X'),$$

is divisible by the cubic form

$$x'X' + y'Y' = 3F(x', y').$$

To establish this result, we show that the first form vanishes when the second vanishes. This is trivial for $x' = y' = 0$. Therefore, let x' (or y') be different from zero; then

$$X' = -\frac{y'}{x'} Y' \quad \left(\text{or } Y' = -\frac{x'}{y'} X'\right),$$

and so

$$F(Y', -X') = F\left(Y', +\frac{y'}{x'} Y'\right) = \left(\frac{Y'}{x'}\right)^3 F(x', y') = 0$$

$$\left[\text{or } = F\left(-\frac{x'}{y'} X', -X'\right) = -\left(\frac{X'}{y'}\right)^3 F(x', y') = 0\right].$$

Hence $$F(Y', -X') = \frac{z}{a} F(x', y') F^*(x', y'),$$

where $F^*(x', y')$ is a certain cubic form with integer coefficients and a is a constant integer depending only on the coefficients of $F(x, y)$.

If we introduce homogeneous coordinates

$$x' : y' : 1 = x^{(1)} : y^{(1)} : z^{(1)}, \quad x''' : y''' : 1 = x^{(3)} : y^{(3)} : z^{(3)}$$

and use the abbreviations

$$H_1(x^{(1)}y^{(1)}z^{(1)}) = -2x^{(1)}z^{(1)3} - a\,F_2\,\{F_2(x^{(1)}, y^{(1)}),\ -F_1(x^{(1)}, y^{(1)})\},$$
$$H_2(x^{(1)}y^{(1)}z^{(1)}) = -2y^{(1)}z^{(1)3} + a\,F_1\,\{F_2(x^{(1)}, y^{(1)}),\ -F_1(x^{(1)}, y^{(1)})\},$$
$$H_3(x^{(1)}y^{(1)}z^{(1)}) = z^{(1)}\,F^*(x^{(1)}, y^{(1)}),$$

the formulae (B_1) now take the form

$$(B_2) \qquad \begin{cases} x^{(3)} = H_1(x^{(1)}y^{(1)}z^{(1)}), \\ y^{(3)} = H_2(x^{(1)}y^{(1)}z^{(1)}), \\ z^{(3)} = H_3(x^{(1)}y^{(1)}z^{(1)}). \end{cases}$$

The expressions H_1, H_2, H_3 on the right-hand side are forms in the three arguments $x^{(1)}$, $y^{(1)}$, $z^{(1)}$ with integer coefficients; they are of degree four in these variables. Hence the two maxima

$$w^{(i)} = \max\,(|x^{(i)}|,\ |y^{(i)}|,\ |z^{(i)}|) \qquad (i = 1,\ 3)$$

are connected by the inequality

$$(B_3) \qquad w^{(3)} \leqslant c_2 (w^{(1)})^4,$$

where c_2 is a positive constant depending only on the coefficients of the cubic form $F(x, y)$.

If neither of the points

$$\left(\frac{x^{(1)}}{z^{(1)}},\ \frac{y^{(1)}}{z^{(1)}}\right),\quad \left(\frac{x^{(3)}}{z^{(3)}},\ \frac{y^{(3)}}{z^{(3)}}\right)$$

is at infinity and if $z^{(1)}$ is not zero, then the tangent to $C(k_1)$ at the first point cannot be parallel to one of the asymptotes Γ', Γ'', Γ'''; hence

$$F(Y',\ -X') \neq 0 \quad \text{and also} \quad F^*(x^{(1)}, y^{(1)}) \neq 0,$$

and so we have also

$$(B_4) \qquad z^{(3)} = z^{(1)}\,F^*(x^{(1)}, y^{(1)}) \neq 0.$$

We add the obvious remark that, if $x^{(1)}$, $y^{(1)}$, $z^{(1)}$ are integers, so also are $x^{(3)}$, $y^{\prime 3)}$, $z^{(3)}$.

10. Now we proceed to the application of the results (A) and (B) to the study of the $2n$ points

$$P_{3m+1} = (x_{3m+1},\ y_{3m+1}),\quad P_{-3m-2} = (x_{-3m-2},\ y_{-3m-2}) \quad (m = 0,\ 1,\ \ldots,\ n-1)$$

on the curve $C(k_1)$. We know that P_{-2} is the tangential of P_1, and P_4 the tangential of P_{-2}; that for $m = 2, 3, \ldots, n-1$ the three points

$$P_{3m+1},\ P_{-3m+1},\ P_{-2}$$

are collinear; and for $m = 1, 2, \ldots, n-1$ the three points

$$P_{-3m-2},\ P_{3m+1},\ P_1$$

are collinear. We know also that the coordinates of P_1 are integers and that none of the $2n$ points P_{3m+1}, P_{-3m-2} lies at infinity. Hence, from the formulae (A_1) and (B_1), it is obvious that the coordinates of all these points are rational numbers, say

$$x_{3m+1} = \frac{x^{(3m+1)}}{z^{(3m+1)}},\ y_{3m+1} = \frac{y^{(3m+1)}}{z^{(3m+1)}};\quad x_{-3m-2} = \frac{x^{(-3m-2)}}{z^{(-3m-2)}},\ y_{-3m-2} = \frac{y^{(-3m-2)}}{z^{(-3m-2)}},$$

where the new x's, y's, and z's are integers; in particular,

$$x^{(1)} = x_1,\ y^{(1)} = y_1,\ z^{(1)} = 1.$$

Since $z^{(1)} \neq 0$, all denominators

$$z^{(3m+1)},\ z^{(-3m-2)} \quad (m = 0, 1, \ldots, n-1)$$

are different from zero. If we write

$$w^{(3m+1)} = \max\left(|x^{(3m+1)}|,\ |y^{(3m+1)}|,\ |z^{(3m+1)}|\right),$$
$$w^{(-3m-2)} = \max\left(|x^{(-3m-2)}|,\ |y^{(-3m-2)}|,\ |z^{(-3m-2)}|\right),$$

then
$$w^{(1)} = \max(|x_1|,\ |y_1|,\ 1) \leqslant 65n^3,$$

and, using (A_3) and (B_3), we get the system of inequalities

$$w^{(-2)} \leqslant c_2(w^{(1)})^4,\quad w^{(4)} \leqslant c_2(w^{(-2)})^4,$$
$$w^{(3m+1)} \leqslant c_1(w^{(-3m+1)} w^{(-2)})^4 \quad (m = 2, 3, \ldots, n-1),$$
$$w^{(-3m-2)} \leqslant c_1(w^{(3m+1)} w^{(1)})^4 \quad (m = 1, 2, \ldots, n-1),$$

and so we are able to give an upper bound for all numbers

$$w^{(3m+1)},\ w^{(-3m-2)} \quad (m = 0, 1, \ldots, n-1).$$

11. We obtain, however, a much better result in a different way. The equations

$$(6m+1)+(-3m-2)+(-3m+1) = 0,\ (-6m-5)+(3m+1)+(3m+4) = 0,$$
$$(-6m-2)+2(3m+1) = 0,\quad (6m+4)+2(-3m-2) = 0$$

show that, for every m, the three points

$$P^{(6m+1)},\ P^{(-3m-2)},\ P^{(-3m+1)} \quad (m \geqslant 1)$$

are collinear; also the three points

$$P^{(-6m-5)},\ P^{(3m+1)},\ P^{(3m+4)}$$

are collinear; and that, of the two points

$$P^{(-6m-2)},\ P^{(3m+1)},$$

or of the two points

$$P^{(6m+4)},\ P^{(-3m-2)},$$

the first is the tangential of the second. Hence we obtain the recurrence inequalities

$$w^{(6m+1)} \leqslant c_1 (w^{(-3m-2)} w^{(-3m+1)})^4, \quad w^{(6m+4)} \leqslant c_2 (w^{(-3m-2)})^4,$$

$$w^{(-6m-2)} \leqslant c_2 (w^{(3m+1)})^4, \quad w^{(-6m-5)} \leqslant c_1 (w^{(3m+1)} w^{(3m+4)})^4.$$

They assume a simpler form when the new numbers

$$c_3 = \max (c_1^{\frac{1}{7}},\ c_2^{\frac{1}{3}},\ 1),\ \ c_3 w^{(3m+1)} = w_{3m+1},\ \ c_3 w^{(-3m-2)} = w_{-3m-2}$$

$$(m = 0,\ 1,\ \ldots,\ n-1)$$

are introduced; they become

$$w_{6m+1} \leqslant w_{-3m-2}^4 w_{-3m+1}^4, \quad w_{6m+4} \leqslant w_{-3m-2}^4,$$

$$w_{-6m-2} \leqslant w_{3m+1}^4, \quad w_{-6m-5} \leqslant w_{3m+1}^4 w_{3m+4}^4.$$

Hence

$$w_{3m+1} \leqslant w_1^{f(3m+1)},\ \ w_{-3m-2} \leqslant w_1^{f(-3m-2)} \quad (m = 0,\ 1,\ \ldots,\ n-1),$$

where the arithmetical function $f(h)$ is defined for all $h \equiv 1 \pmod 3$ by the equations

$$(\mathrm{C}) \begin{cases} f(6m+1) = 4f(-3m-2) + 4f(-3m+1), & f(6m+4) = 4f(-3m-2), \\ f(-6m-2) = 4f(3m+1), & f(-6m-5) = 4f(3m+1) + 4f(3m+4), \end{cases}$$

and the initial value $f(1) = 1$.

12. Although $f(h)$ is a complicated function, it is not difficult to find a simple upper bound for its values when h is large.

By applying the formulae C twice to this function, we obtain the system of equations

$$f(12m+1) = 32f(3m+1)+16f(3m-2),$$

$$f(-12m-2) = 16f(-3m-2)+16f(-3m+1),$$

$$f(12m+4) = 16f(3m+1),$$

$$f(-12m-5) = 32f(-3m-2)+16f(-3m+1),$$

$$f(12m+7) = 16f(3m+4)+32f(3m+1),$$

$$f(-12m-8) = 16f(-3m-2),$$

$$f(12m+10) = 16f(3m+4)+16f(3m+1),$$

$$f(-12m-11) = 16f(-3m-5)+32f(-3m-2).$$

Now let α be a number such that

$$4^{\alpha} > 48,$$

and introduce the new function

$$g(h) = f(h)\,|h|^{-\alpha}.$$

It is obvious then that, for every $\epsilon > 0$ and $m \geqslant m_0(\epsilon)$, we have the system of inequalities

$$g(12m+1) \leqslant (1+\epsilon)\left(\frac{32}{4^{\alpha}}\,g(3m+1)+\frac{16}{4^{\alpha}}\,g(3m-2)\right),$$

$$g(-12m-2) = (1+\epsilon)\left(\frac{16}{4^{\alpha}}\,g(-3m-2)+\frac{16}{4^{\alpha}}\,g(-3m+1)\right),$$

$$g(12m+4) \leqslant (1+\epsilon)\left(\frac{16}{4^{\alpha}}\,g(3m+1)\right),$$

$$g(-12m-5) = (1+\epsilon)\left(\frac{32}{4^{\alpha}}\,g(-3m-2)+\frac{16}{4^{\alpha}}\,g(-3m+1)\right),$$

$$g(12m+7) \leqslant (1+\epsilon)\left(\frac{16}{4^{\alpha}}\,g(3m+4)+\frac{32}{4^{\alpha}}\,g(3m+1)\right),$$

$$g(-12m-8) = (1+\epsilon)\left(\frac{16}{4^{\alpha}}\,g(-3m-2)\right),$$

$$g(12m+10) \leqslant (1+\epsilon)\left(\frac{16}{4^{\alpha}}\,g(3m+4)+\frac{16}{4^{\alpha}}\,g(3m+1)\right),$$

$$g(-12m-11) = (1+\epsilon)\left(\frac{16}{4^{\alpha}}\,g(-3m-5)+\frac{32}{4^{\alpha}}\,g(-3m-2)\right).$$

Assume that, in particular,

$$4^{\alpha} = 48(1+\epsilon),$$

and write

$$\max_{\substack{|h| \leqslant 12m_0(\epsilon) \\ h \equiv 1 \bmod 3}} g(h) = c_4.$$

Then it can be deduced at once from the last two inequalities that, for all integers $h \equiv 1 \pmod 3$,

$$g(h) \leqslant c_4.$$

Hence

$$f(h) \leqslant c_4 |h|^{\alpha}$$

for all such values of h.

13. The results in §§ 11 and 12 show that there are on $C(k_1)$ at least $2n$ rational points

$$P_{3m+1},\ P_{-3m-2} \quad (m = 0, 1, \ldots, n-1),$$

and that the coordinates of these points are of the form

$$x_{3m+1} = \frac{x^{(3m+1)}}{z^{(3m+1)}},\ y_{3m+1} = \frac{y^{(3m+1)}}{z^{(3m+1)}};\ x_{-3m-2} = \frac{x^{(-3m-2)}}{z^{(-3m-2)}},\ y_{-3m-2} = \frac{y^{(-3m-2)}}{z^{(-3m-2)}}$$

$$(m = 0, 1, \ldots, n-1),$$

where the x's, y's, z's are integers which satisfy the inequalities

$$\max(|x^{(h)}|, |y^{(h)}|, |z^{(h)}|) \leqslant \frac{1}{c_3} w_1^{f(h)} \leqslant \frac{1}{c_3} (65 c_3 n^3)^{c_4 |h|^{\alpha}},\ z^{(h)} \neq 0$$

$$\begin{pmatrix} h = 3m+1, & -3m-2 \\ m = 0, 1, \ldots, n-1 & \end{pmatrix},$$

α being a number such that

$$4^{\alpha} > 48,$$

and c_4 being a positive constant depending only on α and the coefficients of the form $F(x, y)$.

Therefore, in particular,

$$|z^{(3m+1)}| \leqslant \frac{1}{c_3} (65 c_3 n^3)^{c_4 (3m+1)^{\alpha}},\quad |z^{(-3m-2)}| \leqslant \frac{1}{c_3} (65 c_3 n^3)^{c_4 (3m+2)^{\alpha}}$$

$$(m = 0, 1, \ldots, n-1),$$

and the least common multiple Z of all denominators

$$z^{(3m+1)},\ z^{(-3m-2)} \quad (m = 0, 1, \ldots, n-1)$$

has a value

$$Z \leqslant \left(\frac{1}{c_3}\right)^{2n} (65c_3 n^3)^{\sum\limits_{m=0}^{n-1}\{c_4(3m+1)^a + c_4(3m+2)^a\}} \leqslant \left(\frac{1}{c_3}\right)^{2n} (65c_3 n^3)^{2c_4(3n)^a n}.$$

14. Let us now write

$$k = Z^3 k_1$$

and

$$Zx_{3m+1} = p_{3m+1},\ Zy_{3m+1} = q_{3m+1};\ Zx_{-3m-2} = p_{-3m-2},\ Zy_{-3m-2} = q_{-3m-2}$$
$$(m = 0, 1, \ldots, n-1).$$

Then all the $2n$ points

$$(p_{3m+1}, q_{3m+1}),\ (p_{-3m-2}, q_{-3m-2}) \quad (m = 0, 1, \ldots, n-1)$$

have integer coordinates; they are different from one another and they lie on the same cubic curve $C(k)$. Now, evidently,

$$0 < |k_1| \leqslant c_5\,(65n^3)^3,$$

with a positive constant c_5 depending only on the coefficients of the form $F(x, y)$, and so

$$0 < |k| \leqslant c_5(65n^3)^3 \left\{ \left(\frac{1}{c_3}\right)^{2n} (65c_3 n^3)^{2c_4(3n)^a n} \right\}^3.$$

Since a is restricted only by the condition

$$4^a > 48,$$

it may be assumed less than 3. Hence, if γ is any positive constant, we have, for $n \geqslant n_0(\gamma)$,

$$0 < |k| \leqslant e^{16\gamma n^4},$$

and, when we replace $2n$ by t, the following theorem is proved.

THEOREM 1. *If γ is any positive number, then there is a positive number $t_0(\gamma)$ such that, corresponding to every integer $t \geqslant t_0(\gamma)$, there exists an integer k with*

$$0 < |k| \leqslant e^{\gamma t^4},$$

which can be represented by the binary form $F(x, y)$ in at least t different ways,

$$k = F(p_h, q_h) \quad (h = 1, 2, \ldots, t)$$

with integers p_h, q_h.

15. We apply Theorem 1 to the special form

$$F(x,\ y) = x(y^2 - ax^2),$$

where $a \neq 0$ is an arbitrary integer. Then we know that, for large t, there exist integers k with

$$0 < |k| \leqslant e^{t^4},$$

such that the equation

$$p_h(q_h^2 - ap_h^2) = k$$

has at least $2t$ different integer solutions

$$(p_h,\ q_h) \quad (h = 1,\ 2,\ \ldots,\ 2t).$$

Solving with respect to q_h, we get

$$(p_h\ q_h)^2 = ap_h^4 + kp_h,$$

and hence it is obvious that to every p_h there belong at most two different q_h. Therefore the numbers

$$p_1,\ p_2,\ \ldots,\ p_{2t}$$

assume at least t different values, and we have proved

THEOREM 2. *If $a \neq 0$ is any integer and t is a sufficiently large positive integer, then there is an integer k with*

$$0 < |k| \leqslant e^{t^4},$$

such that the polynomial

$$f(x) = ax^4 + kx$$

is a perfect square for at least t different integer values of the argument x, and these values of x may be assumed to divide the number k.

By a similar method we can also prove

THEOREM 3. *If $a \neq 0$ is any integer and t is a sufficiently large positive integer, then there is an integer k with*

$$0 < |k| \leqslant e^{t^4},$$

such that the polynomial

$$g(x) = ax^3 + k$$

is a perfect square for at least t different integer values of the argument x, and these values of x may be assumed to divide the number k.

THEOREM 4. *If $a \neq 0$ is any integer and t is a sufficiently large positive integer, then there is an integer k with*

$$0 < |k| \leqslant e^{t^4},$$

such that the polynomial

$$g(x) = ax^3 + k$$

is a perfect cube for at least t different integers x.

II.

16. The result of Theorem 1 can be generalized by a simple change in the method of the first chapter.

We have constructed a set of $2n$ rational points

$$P_{3m+1} = (x_{3m+1}, y_{3m+1}), \quad P_{-3m-2} = (x_{-3m-2}, y_{-3m-2}) \qquad (m = 0, 1, \ldots, n-1)$$

on the curve $C(k_1)$ with the following properties:

(*a*) The corresponding points

$$u_{3m+1} = \left(\frac{x_{3m+1}}{k_1^{\frac{1}{3}}}, \frac{y_{3m+1}}{k_1^{\frac{1}{3}}}\right), \quad u_{-3m-2} = \left(\frac{x_{-3m-2}}{k_1^{\frac{1}{3}}}, \frac{y_{-3m-2}}{k_1^{\frac{1}{3}}}\right) \quad (m = 0, 1, \ldots, n-1)$$

on the curve C have arguments of the form

$$u_{3m+1} = (3m+1)u_1, \quad u_{-3m-2} = -(3m+2)u_1 \quad (m = 0, 1, \ldots, n-1).$$

(*b*) If h_1, h_2, h_3 are three different indices of the set

$$3m+1, \quad -3m-2 \quad (m = 0, 1, \ldots, n-1)$$

with

$$h_1 + h_2 + h_3 = 0,$$

then P_{h_1}, P_{h_2}, P_{h_3} are collinear, and when h_1 and h_2 are two different indices with

$$h_1 + 2h_2 = 0$$

then P_{h_1} is the tangential of P_{h_2}.

(*c*) The $2n$ points

$$P_{3m+1}, \quad P_{-3m-2} \quad (m = 0, 1, \ldots, n-1)$$

are all different.

(*d*) None of these $2n$ points lies at infinity.

17. Now let us consider, also, the additional points

$$u_{3m+1} = \left(\frac{x_{3m+1}}{k_1^{\frac{1}{3}}}, \frac{y_{3m+1}}{k_1^{\frac{1}{3}}}\right), \quad u_{-3m-2} = \left(\frac{x_{-3m-2}}{k_1^{\frac{1}{3}}}, \frac{y_{-3m-2}}{k_1^{\frac{1}{3}}}\right)$$

$$(m = n,\ n+1,\ n+2,\ \ldots)$$

on C with elliptic arguments

$$u_{3m+1} = (3m+1)u_1, \quad u_{-3m-2} = (-3m-2)u_1 \quad (m = n,\ n+1,\ n+2,\ \ldots)$$

and their corresponding points

$$P_{3m+1} = (x_{3m+1}, y_{3m+1}), \quad P_{-3m-2} = (x_{-3m-2}, y_{-3m-2})$$

$$(m = n,\ n+1,\ n+2,\ \ldots)$$

on $C(k_1)$; we arrange them with their indices in the order

$$1,\ -2,\ 4,\ -5,\ 7,\ -8,\ \ldots,\ -3m+1,\ 3m+1,\ -3m-2,\ \ldots.$$

It is obvious that the enlarged system of points

$$P_1,\ P_{-2},\ P_4,\ P_{-5},\ P_7,\ P_{-8},\ \ldots$$

still has the property (*b*); but in general the two other properties (*c*) and (*d*) no longer hold.

It can easily be proved that all arguments

$$u_{3m+1}, \quad u_{-3m-2} \quad (m = 0,\ 1,\ 2,\ \ldots)$$

are congruent (mod ω_1, ω_2) to real numbers. For the curve C has at least one real asymptote; hence there is a real linear transformation

$$x = \alpha X + \beta Y, \quad y = \gamma X + \delta Y \quad (\alpha\delta - \beta\gamma \neq 0),$$

such that C takes the form

$$X(Y^2 - aX^2) = 1 \quad (a \neq 0)$$

with a real constant a; then, if we write

$$X = \frac{1}{\xi}, \quad Y = \frac{\eta}{\xi},$$

it becomes

$$\eta^2 = \xi^3 + a.$$

But the curve in the (ξ, η)-plane corresponding to this equation has only one real branch; hence, as is well known, all real points of the curve and, therefore, also all real points of C are obtained, if, and only if, u assumes all values congruent to a real number (mod ω_1, ω_2).

Denote by ω the real fundamental period of the two functions $\phi(u)$ and $\psi(u)$. We may assume that u_1, and so all arguments

$$u_{3m+1},\ u_{-3m-2} \quad (m = 0,\ 1,\ 2,\ \ldots),$$

are real numbers. Two real arguments u' and u'' will give the same point on C, if, and only if,

$$u' \equiv u'' \quad (\text{mod } \omega),$$

i.e. if there is an integer h with

$$u' = u'' + h\omega.$$

18. It is possible that no two points of the system of points

$$P_{3m+1},\ P_{-3m-2} \quad (m = 0,\ 1,\ 2,\ \ldots)$$

on $C(k_1)$ coincide. Then, also, all points

$$u_{3m+1},\ u_{-3m-2} \quad (m = 0,\ 1,\ 2,\ \ldots)$$

on C must be different; there is no integer $h \neq 0$ with

$$3hu_1 \equiv 0 \quad (\text{mod } \omega)$$

and therefore the quotient

$$\frac{u_1}{\omega}$$

is an irrational number. Hence, by a well-known theorem, the system of real numbers

$$u_1,\ u_{-2},\ u_4,\ u_{-5},\ u_7,\ u_8,\ \ldots$$

is "gleichverteilt" mod ω, and the corresponding points on C will be everywhere dense on every arc Γ of this curve. To every arc Γ there belongs a positive constant γ, such that, for sufficiently large N, at least

$$\gamma N$$

of the points

$$u_{3m+1},\ u_{-3m-2} \quad (m = 0,\ 1,\ \ldots,\ N-1)$$

on C lie on Γ. Hence, also, at least γN of the points

$$P_{3m+1},\ P_{-3m-2} \quad (m = 0,\ 1,\ \ldots,\ N-1)$$

lie on the arc $\Gamma(k_1)$ on $C(k_1)$ corresponding to Γ on C.

Since both curves C and $C(k_1)$ are cut in only one real point by any straight line through the origin, we may define the arcs Γ and $\Gamma(k_1)$ by conditions of the form

$$A \leqslant \frac{y}{x} \leqslant B,$$

or the form

$$A \leqslant \left(\frac{y}{x}\right)^{-1} \leqslant B,$$

where A and B are any two real numbers with $A < B$.

19. If at least two points of the set

$$P_{3m+1},\ P_{-3m-2} \quad (m = 0, 1, 2, \ldots)$$

coincide, then there is an index $N \geqslant n$ such that all points

$$P_{3m+1},\ P_{-3m-2} \quad (m = 0, 1, \ldots, N-1)$$

are different, while at least two of the points

$$P_{3m+1},\ P_{-3m-2} \quad (m = 0, 1, \ldots, N)$$

coincide. This means that all the numbers

$$u_{3m+1} = (3m+1)u_1,\ u_{-3m-2} = (-3m-2)u_1 \quad (m = 0, 1, \ldots, N-1),$$

but not all the numbers

$$u_{3m+1} = (3m+1)u_1,\ u_{-3m-2} = (-3m-2)u_1 \quad (m = 0, 1, \ldots, N),$$

are incongruent (mod ω). Therefore, either

$$u_{3N+1} \equiv u_{-3N+1} \pmod{\omega}, \quad i.e. \quad 6Nu_1 \equiv 0 \pmod{\omega},$$

with $\quad 3hu_1 \not\equiv 0 \pmod{\omega}$ for $h = 1, 2, \ldots, 2N-1$;

or $\quad u_{-3N-2} \equiv u_{3N+1} \pmod{\omega}$, *i.e.* $3(2N+1)u_1 \equiv 0 \pmod{\omega}$,

with $\quad 3hu_1 \not\equiv 0 \pmod{\omega}$ for $h = 1, 2, \ldots, 2N$.

It follows that, in the first case,

$$u_1 = \frac{M\omega}{6N},$$

and that, in the second case,

$$u_1 = \frac{M\omega}{3(2N+1)},$$

with an integer $N \geqslant n$ and a second integer M prime to $2N$ or $2N+1$ respectively. Hence in the first case the points

$$u_1, u_{-2}, u_4, u_{-5}, \ldots, u_{3N-2}, u_{-3N+1}$$

are the same as the points

$$\frac{M(3g+1)\omega}{6N} \quad (g = 0, 1, \ldots, 2N-1),$$

and in the second case the points

$$u_1, u_{-2}, u_4, u_{-5}, \ldots, u_{-3N+1}, u_{3N+1}$$

are the same as the points

$$\frac{M(3g+1)\omega}{3(2N+1)} \quad (g = 0, 1, ., \ldots, 2N),$$

when we disregard the order of the terms.

Therefore, for sufficiently large N, *i.e.* for sufficiently large n, those of the points

$$u_{3m+1}, u_{-3m-2} \quad (m = 0, 1, 2, \ldots),$$

on C which are different, will be everywhere dense on every arc of the curve, and similarly for the corresponding points

$$P_{3m+1}, P_{-3m-2} \quad (m = 0, 1, 2, \ldots)$$

on $C(k_1)$. To every such arc there belongs again a positive constant γ, such that for sufficiently large n and N at least

$$\gamma N$$

of the different points of the set

$$u_{3m+1}, u_{-3m-2} \quad (m = 0, 1, 2, \ldots)$$

on C, or of the points

$$P_{3m+1}, P_{-3m-2} \quad (m = 0, 1, 2, \ldots)$$

on $C(k_1)$, lie on that arc. As in § 18 the arc can be defined by inequalities of the form

$$A \leqslant \frac{y}{x} \leqslant B,$$

or the form

$$A \leqslant \left(\frac{y}{x}\right)^{-1} \leqslant B,$$

where the real numbers A and B satisfy the condition $A < B$.

20. The results of the last two paragraphs lead to the following lemma.

Assume G to be an angle about the origin $(0, 0)$, *i.e. the part of the* (x, y)*-plane with*

$$A \leqslant \frac{y}{x} \leqslant B \quad \textit{or} \quad A \leqslant \left(\frac{y}{x}\right)^{-1} \leqslant B,$$

where A and B are two real numbers with $A < B$. Then there is a positive constant c_6 depending only on G, such that corresponding to every integer $t > 0$, there are three integers n, N, k_1, and $2N$ points

$$P_{3m+1} = (x_{3m+1}, y_{3m+1}), \quad P_{-3m-2} = (x_{-3m-2}, y_{-3m-2}) \quad (m = 0, 1, \ldots, N-1)$$

on the curve $C(k_1)$ with the following properties:

(1) *All points P_{3m+1}, P_{-3m-2} have rational coordinates; P_1 has integer coordinates with* $\max(|x_1|, |y_1|) \leqslant 65n^3$.

(2) *All points P_{3m+1}, P_{-3m-2} are different from one another; at least $t+3$ of them lie in the angle G.*

(3) *When h_1, h_2, h_3 are three different indices of the set*

$$3m+1, \quad -3m-2 \quad (m = 0, 1, \ldots, N-1)$$

with $h_1+h_2+h_3 = 0$, then P_{h_1}, P_{h_2}, P_{h_3} are collinear; when h_1 and h_2 are two of them with $h_1+2h_2 = 0$, then P_{h_1} is the tangential of P_{h_2}.

(4) *The integers n, N, and t satisfy the inequality*

$$n \leqslant N \leqslant c_6 t.$$

It is now possible that some, say j, of the $2N$ points P_{3m+1}, P_{-3m-2} lie at infinity; but $C(k_1)$ being of degree 3, there are at most three such points, and so $j = 0, 1, 2$, or 3. Call these points $P_{\kappa_1}, \ldots, P_{\kappa_j}$.

21. The coordinates of the points P_{3m+1}, P_{-3m-2} are rational numbers and can be written in the form

$$x_{3m+1} = \frac{x^{(3m+1)}}{z^{(3m+1)}}, \quad y_{3m+1} = \frac{y^{(3m+1)}}{z^{(3m+1)}}; \quad x_{-3m-2} = \frac{x^{(-3m-2)}}{z^{(-3m-2)}}, \quad y_{-3m-2} = \frac{y^{(-3m-2)}}{z^{(-3m-2)}}$$

$$(m = 0, 1, \ldots, N-1),$$

as in § 10, with integer x's, y's, and z's, which are finite and not all three zero. The denominators z_{3m+1} and z_{-3m-2} are different from zero, with the exception of the j denominators $z_{\kappa_1}, \ldots, z_{\kappa_j}$. We write

$$w^{(3m+1)} = \max(|x^{(3m+1)}|, |y^{(3m+1)}|, |z^{(3m+1)}|)$$

$$w^{(-3m-2)} = \max(|x^{(-3m-2)}|, |y^{(-3m-2)}|, |z^{(-3m-2)}|)$$

$$(m = 0, 1, \ldots, N-1),$$

and have again

$$w^{(1)} \leqslant 65n^3.$$

Furthermore, it is obvious that

$$w^{(\kappa_i)} \leqslant c_6 \quad (i = 1, 2, \ldots, j),$$

where c_6 is a positive constant depending only on the coefficients of the form $F(x, y)$, but not on t, n, or N; and similarly

$$w^{(-2\kappa_i)} \leqslant c_7 \quad (i = 1, 2, \ldots, j),$$

where the positive constant c_7 also depends only on the coefficients of the form $F(x, y)$. We remark that, if $j \geqslant 2$, then $j = 3$, for then P_{κ_1}, P_{κ_2}, and P_{κ_3} lie on the line at infinity.

If one of these points P_{κ_i} is collinear with two different finite points P_{h_1} and P_{h_2}, three equations of the following form will be satisfied by the coordinates of these finite points:

$$x^{(h_2)} = K_1^{(i)}(x^{(h_1)}, y^{(h_1)}, z^{(h_1)}), \quad y^{(h_2)} = K_2^{(i)}(x^{(h_1)}, y^{(h_1)}, z^{(h_1)}),$$

$$z^{(h_2)} = K_3^{(i)}(x^{(h_1)}, y^{(h_1)}, z^{(h_1)});$$

here $K_1^{(i)}, K_2^{(i)}, K_3^{(i)} (i = 1, \ldots, j)$ denote ternary forms with integer coefficients, of degree e say, which depend only on the coefficients of the form $F(x, y)$. Their actual calculation by the method in §§ 8 and 9 shows that $z^{(h_2)}$ is not zero, when P_{h_1} and P_{h_2} are different and finite. Obviously these equations lead to the inequality

$$w^{(h_2)} \leqslant c_8 (w^{(h_1)})^e$$

with another constant $c_8 > 0$ depending only on the coefficients of $F(x, y)$.

22. It is possible now to obtain an upper bound for all maxima

$$w^{(3m+1)}, \; w^{(-3m-2)} \quad (m = 0, 1, \ldots, N-1)$$

by using the method of § 11. As far as these maxima correspond to finite points, they are connected by the recurrence formulae

$$w^{(6m+1)} \leqslant c_1 (w^{(-3m-2)} w^{(-3m+1)})^4, \quad w^{(6m+4)} \leqslant c_2 w^{(-3m-2)4},$$

$$w^{(-6m-2)} \leqslant c_2 w^{(3m+1)4}, \quad w^{(-6m-5)} \leqslant c_1 (w^{(3m+1)} w^{(3m+4)})^4.$$

But these formulae must be replaced by others when at least one of the points in them lies at infinity. Hence at most three of them change into

$$w^{(\kappa_i)} \leqslant c_6,$$

at most three into

$$w^{(-2\kappa_i)} \leqslant c_7,$$

and at most six into

$$w^{(h_2)} \leqslant c_8 (w^{(h_1)})^e.$$

Therefore the results in § 12 lead to a system of inequalities

$$c_9 w^{(3m+1)} \leqslant (c_9 w^{(1)})^{e^6 f(3m+1)}, \quad c_9 w^{(-3m-2)} \leqslant (c_9 w^{(1)})^{e^6 f(-3m-2)}$$
$$(m = 0, 1, \ldots, N-1),$$

where c_9 is a constant depending only on the coefficients of $F(x, y)$ and where the arithmetical function $f(h)$ satisfies the inequality

$$f(h) \leqslant c_4 |h|^a.$$

So we have, in particular,

$$|z^{(3m+1)}| \leqslant \frac{1}{c_9} (65 c_9 n^3)^{c_4 e^6 (3m+1)^a}, \quad |z^{(-3m-2)}| \leqslant \frac{1}{c_9} (65 c_9 n^3)^{c_4 e^6 (3m+2)^a}$$
$$(m = 0, 1, \ldots, N-1).$$

Now, by § 20, at least $t+3$ of the points

$$P_{3m+1}, P_{-3m-2} \quad (m = 0, 1, \ldots, N-1)$$

lie in the angle G, and so there must be at least t of these points, say

$$P_{h_1}, P_{h_2}, \ldots, P_{h_t},$$

which lie in G and are all finite. Therefore their denominators are different from zero and satisfy the inequalities

$$|z^{(h_i)}| \leqslant \frac{1}{c_9} (65 c_9 n^3)^{c_4 e^6 (3N)^a} \quad (i = 1, 2, \ldots, t),$$

so that their least common multiple is not greater than

$$\left\{\frac{1}{c_9}(65c_9 n^3)^{c_4 e^{6(3N)^\alpha}}\right\}^t.$$

If Z is this least common multiple, we write

$$Zx_{h_i} = \frac{Zx^{(h_i)}}{z^{(h_i)}} = p_i, \quad Zy_{h_i} = \frac{Zy^{(h_i)}}{z^{(h_i)}} = q_i \quad (i = 1, 2, \ldots, t)$$

and $$k = Z^3 k_1.$$

Then the coordinates of all points

$$(p_i, q_i) \quad (i = 1, 2, \ldots, t)$$

are integers; these points are finite and different and all lie in the angle G and on the curve $C(k)$. For the number k we have

$$0 < |k| \leqslant c_5(65n^3)^3 \left\{\frac{1}{c_9}(65n^3)^{c_4 e^{6(3N)^\alpha}}\right\}^{3t} \quad (N \leqslant c_6 t),$$

and so for any positive constant γ and sufficiently large t, that is, sufficiently large n and N, we have

$$0 < |k| \leqslant e^{\gamma t^4},$$

since the exponent α may be assumed less than 3.

We have thus proved the following generalisation of Theorem 1.

THEOREM 5. *Let A and B be two real numbers with $A < B$ and G be the angle*

$$A \leqslant \frac{y}{x} \leqslant B \quad or \quad A \leqslant \left(\frac{y}{x}\right)^{-1} \leqslant B$$

about the origin, and let γ be any positive number. Then there is a positive number $t_0(A, B, \gamma)$, such that to every integer $t \geqslant t_0(A, B, \gamma)$ exists an integer k with

$$0 < |k| \leqslant e^{\gamma t^4},$$

for which the conditions

$$F(x, y) = k, \quad (x, y) \text{ in } G,$$

have at least t different solutions in points

$$x = p_i, \quad y = q_i \quad (i = 1, 2, \ldots, t)$$

with finite integer coordinates.

We specialize the binary form $F(x, y)$ and the angle G in this theorem and obtain the two following results.

THEOREM 6. *There is an infinite set of positive integers* $k_1, k_2, k_3, \ldots$ *with*

$$1 \leqslant k_1 < k_2 < k_3 < \ldots,$$

such that the number of representations of k_ν *as a sum of two cubes of positive integers is greater than* $\sqrt[4]{\log k_\nu}$.

THEOERM 7. *There is an infinite set of positive integers* $k_1, k_2, k_3, \ldots$ *with*

$$1 \leqslant k_1 < k_2 < k_3 < \ldots,$$

such that the number of representations of k_ν *in the form*

$$k_\nu = pq(p+q)$$

with positive integers p, q *is greater than* $\sqrt[4]{\log k_\nu}$.

III.

23. So far we have treated only cubic curves of the special kind

$$F(x, y) = k.$$

But our method suffices for the study of much more general cubic curves. Suppose

$$f(x, y) = 0$$

to be the equation of a cubic curve of genus 1, and

$$g(x, y) = 0,$$

the equation of another curve, of degree less than or equal to 3, both $f(x, y)$ and $g(x, y)$ being polynomials with rational coefficients. Then to every point (x', y') in the (x, y)-plane with rational coordinates, which is not a point of intersection of the two curves, there belongs a rational number λ, such that the cubic curve $C(\lambda)$,

$$f(x, y) + \lambda g(x, y) = 0,$$

goes through (x', y'), and if this point lies sufficiently near to $f = 0$, but not to a point of intersection of $f = 0$, $g = 0$, then $|\lambda|$ will be very small. Now there is a uniformisation of the curve $C(\lambda)$,

$$x = \phi_\lambda(u), \quad y = \psi_\lambda(u),$$

by means of two elliptic functions

$$\phi_\lambda(u), \ \psi_\lambda(u)$$

with the same periods $\omega_\lambda^{(1)}, \omega_\lambda^{(2)}$ and of order 2 or 3; as functions of the parameter λ the expressions

$$\phi_\lambda(u),\ \psi_\lambda(u),\ \omega_\lambda^{(1)},\ \omega_\lambda^{(2)}$$

are analytic and even regular for sufficiently small $|\lambda|$.

If the point (x', y') on $C(\lambda)$ has the elliptic argument u, we can construct on this curve the set of points with arguments

$$(3m+1)u,\ (-3m-2)u \quad (m = 0, 1, \ldots, n-1)$$

by the same process as in § 3, for any given integer $n \geqslant 1$. All these $2n$ points will be different from one another and none lie at infinity if a certain finite number of incongruences of the type

$$u \not\equiv v_\lambda^{(i)} \pmod{\omega_\lambda^{(1)}, \omega_\lambda^{(2)}} \quad (i = 1, 2, \ldots, j)$$

are satisfied; here

$$v_\lambda^{(1)},\ v_\lambda^{(2)},\ \ldots,\ v_\lambda^{(j)}$$

denote analytical functions of λ, which are regular for sufficiently small $|\lambda|$. Now for variable and sufficiently small λ, every congruence

$$u \equiv v_\lambda^{(i)} \pmod{\omega_\lambda^{(1)}, \omega_\lambda^{(2)}} \quad (i = 1, 2, \ldots, j)$$

represents an arc of a certain analytic curve. Hence, in order that all $2n$ points on $C(\lambda)$ with elliptic arguments

$$(3m+1)u,\ (-3m-2)u \quad (m = 0, 1, \ldots, n-1)$$

are different and finite, we must choose the special point (x', y') of argument u in such a way that it lies sufficiently near to the curve $f = 0$ and not on a finite number of arcs of certain analytical curves. But here it is obvious, that in any neighbourhood of any arc of the curve $f = 0$, there is a point (x', y') with these properties and with rational coordinates. Therefore we arrive at the following result.

THEOREM 8. *Suppose that*

$$f(x, y) = 0 \quad \textit{and} \quad g(x, y) = 0$$

are the equations of two different cubic curves, of which the first has the genus one, and that these equations have rational coefficients. Let ϵ be any positive number, $t \geqslant 1$ any integer. Then there is a rational number λ with

$$0 < |\lambda| \leqslant \epsilon,$$

such that at least t different finite points with rational coordinates lie on the cubic curve

$$f(x, y) + \lambda g(x, y) = 0.$$

The method of the second chapter may be applied to prove that all these t points can also be assumed to lie in any neighbourhood of any finite arc of the curve $f=0$.

It is also possible to obtain an upper bound

$$e^{t^{\alpha}}$$

for the general denominator of the coordinates of these t points, when t is large enough; here α denotes an absolute positive constant.

24. We now mention some applications of Theorem 8. Take

$$f(x,\, y) = x^3+y^3+1-3Axy$$

with any rational number $A \neq 1$, so that this curve has genus 1, and

$$g(x,\, y) = 3\lambda xy.$$

Then we get the result:

THEOREM 9. *For any given rational number $A \neq 1$, any given positive number ϵ, and any integer $t \geqslant 1$, there is a rational number A' with*

$$0 < |A'-A| < \epsilon,$$

such that the equation

$$x^3+y^3+z^3-3A'xyz = 0$$

has at least t different solutions in co-prime integers x, y, z.

It is trivial that this theorem remains true also for $A = 1$. For then take a rational number A'' with

$$A+\tfrac{1}{2}\epsilon \leqslant A'' \leqslant A+\tfrac{3}{4}\epsilon,$$

and apply the theorem with A'' instead of A and $\frac{1}{4}\epsilon$ instead of ϵ; then

$$|A'-A''| \leqslant \tfrac{1}{4}\epsilon \quad \text{and therefore} \quad 0 < |A'-A| \leqslant \epsilon.$$

As a second example take

$$f(x,\, y) = y^2-(4x^3-g_2x-g_3),$$

where g_2 and g_3 are two rational numbers with

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

so that the curve $f=0$ is of genus 1, and

$$g(x,\, y) = -(4x^3-g_2x-g_3).$$

We have

$$f(x,\, y)+\lambda g(x,\, y) = y^2-(1+\lambda)(4x^3-g_2 x-g_3),$$

and so obtain the result:

THEOREM 10. *For any two given rational numbers g_2 and g_3 with*

$$g_2{}^3-27g_3{}^2 \neq 0,$$

any given positive number ϵ and any integer $t \geqslant 1$ there exists a rational number λ with

$$0 < |\lambda| \leqslant \epsilon,$$

such that the cubic curve

$$y^2-(1+\lambda)(4x^3-g_2 x-g_3) = 0$$

has at least t different points with rational coordinates.

25. The last theorem has a remarkable consequence. Evidently the curve

$$C_\lambda(1): \qquad y^2-(1+\lambda)(4x^3-g_2 x-g_3) = 0$$

has the same absolute invariant

$$J = \frac{g_2{}^3}{g_2{}^3-27g_3{}^2}$$

as the curve

$$C: \qquad y^2-(4x^3-g_2 x-g_3) = 0,$$

and the same is true for all curves

$$C_\lambda(Z): \qquad \left(\frac{y}{Z}\right)^2-(1+\lambda)\left\{4\left(\frac{x}{Z}\right)^3-g_2\,\frac{x}{Z}-g_2\right\} = 0,$$

where $Z \neq 0$ is any number. Now we may choose this number Z as an integer in such a way that the t rational points on $C_\lambda(1)$ change into points on $C_\lambda(Z)$ with integer coordinates. It is obvious also that, corresponding to every rational value of the absolute invariant J, two rational numbers g_2 and g_3 can be found with

$$J = \frac{g_2{}^3}{g_2{}^3-27g_3{}^2}.$$

Hence we have:

THEOREM 11. *Corresponding to every integer $t \geqslant 1$ and to every rational number J, there exists a cubic curve with absolute invariant J, on which lie at least* *t different points with integer coordinates, and which is defined by an equation of the special form*

$$Ay^2+Bx^3+Cx+D=0$$

with integer coefficients.

26. Theorem 10 is a special case of the following more general result.

THEOREM 12. *Suppose that $f(x)$ is a polynomial of exact degree 3 or 4 in x with rational coefficients, and that $t \geqslant 1$ is an integer. Then there is an integer $k \neq 0$ such that, for at least t different rational values of x, the polynomial $kf(x)$ is the square of an integer.*

Proof. If $f(x)=0$ has a multiple root this result is rather trivial; henceforth we assume that the roots of $f(x)=0$ are all simple. Evidently it is sufficient to prove that, for a certain rational number $k_1 \neq 0$, there are at least t different rational points on the curve

$$C(k_1): \qquad y^2-k_1 f(x)=0.$$

The curve $C(1)=C$ has a uniformisation

$$x=\phi(x), \quad y=\psi(x),$$

where $\phi(x)$ and $\psi(x)$ are two elliptic functions with the periods ω_1, ω_2 say. It is cut by every parabola

$$y=Ax^2+Bx+C$$

in exactly four points, and the arguments u_1, u_2, u_3, u_4 of these points satisfy the congruence

$$u_1+u_2+u_3+u_4 \equiv c \pmod{\omega_1, \omega_2},$$

with a certain constant c, which may be assumed equal to zero without loss of generality. Of these four points of intersection, three may be given arbitrarily, and then the last one can be found by a rational construction. In the special case in which the parabola osculates C in the point u_1, we must count this point thrice, and so there is only one other point of intersection u_2, given by the congruence

$$u_2 \equiv -3u_1 \pmod{\omega_1, \omega_2}.$$

When we now construct the set oi t points with arguments

$$u_1, \ -3u_1, \ +9u_1, \ \ldots, \ (-3)^{t-1}u_1$$

on C, there will be only a finite number of initial positions for u_1, for which some of these t points coincide or lie at infinity: this is shown by a method similar to that of the first chapter. Through all these exceptional positions of u_1 and through all points with $f(x) = 0$, $y = 0$ we draw straight lines perpendicular to the x-axis, and then take a rational point (x_1, y_1) not lying on any one of these lines or on the x-axis. Then there is exactly one curve $C(k_1)$ going through this point, with

$$k_1 = \frac{y_1^2}{f(x)}.$$

On this curve we construct the t points

$$(x_1, y_1), \quad (x_2, y_2), \quad \ldots, \quad (x_t, y_t)$$

such that, for $m = 1, 2, \ldots, t-1$, the point (x_{m+1}, y_{m+1}) is the point of intersection with $C(k_1)$ of the parabola

$$y = Ax^2 + Bx + C,$$

which osculates this curve in the point (x_m, y_m). All points

$$(x_1, y_1), \quad (x_2, y_2), \quad \ldots, \quad (x_t, y_t)$$

are different and none lies at infinity, and their coordinates are rational numbers; these facts may be shown by transforming $C(k_1)$ into C by replacing y by $y/\sqrt{|k_1|}$; or by actually giving a recurrence formula for the coordinates of the $(m+1)$-th point, when the m-th is known. This proves our theorem.

27. We mention two trivial consequences of the last theorem.

THEOREM 13. *Let t be an arbitrary positive integer. Then there exists a polynomial $a_0 x^2 + a_1$ $(a_0 a_1 \neq 0)$ of exact degree 2 with integer coefficients, which is a perfect cube for at least t different integer values of the argument.*

THEOREM 14. *Let t be an arbitrary positive integer. Then there exists a polynomial $a_0 x^2 + a_1$ $(a_0 a_1 \neq 0)$ of exact degree 2 with integer coefficients, which is a perfect fourth power for at least t different integer values of the argument.*

To prove these two theorems we need only apply Theorem 12 to the two polynomials

$$f(x) = x^3 - a \quad \text{and} \quad f(x) = x^4 - a,$$

where $a \neq 0$ denotes an arbitrary integer.

28. So far we have considered the lattice points only on plane curves of genus 1. Our method, however, can also be used for the study of these points on curves of genus 1 in spaces of three or more dimensions. It may be sufficient to give one result of this kind.

THEOREM 15. *Suppose that a, b, c, and A, B, C are six integers with*

$$aB-bA \neq 0, \quad aC-cA \neq 0, \quad bC-cB \neq 0,$$

and that t is an arbitrary positive integer. Then there are two integers $k \neq 0$ and $K \neq 0$ such that the system of equations

$$ax^2+by^2+cz^2 = k, \quad Ax^2+By^2+Cz^2 = K$$

has at least t different solutions in integers x, y, z.

Proof. We choose two rational numbers k_0 and K_0 such that the curve

$$C(k_0, K_0): \qquad ax^2+by^2+cz^2 = k_0, \quad Ax^2+By^2+Cz^2 = K_0$$

in three dimensions does not consist of single real points, but has real arcs and is of genus unity. Then the same is true for all curves

$$C(k_1, K_1): \qquad ax^2+by^2+cz^2 = k_1, \quad Ax^2+By^2+Cz^2 = K_1,$$

where k_1 and K_1 are two rational numbers sufficiently near to k_0 and K_0. $C(k_1, K_1)$ is not a plane curve and is of degree 4 and of genus 1. Hence it has a uniformisation

$$x = \phi_{k_1 K_1}(u), \quad y = \psi_{k_1 K_1}(u), \quad z = \chi_{k_1 K_1}(u),$$

by means of three elliptic functions

$$\phi_{k_1 K_1}(u), \quad \psi_{k_1 K_1}(u), \quad \chi_{k_1 K_1}(u),$$

with the same periods $\omega^{(1)}_{k_1 K_1}$, $\omega^{(2)}_{k_1 K_1}$, say. As functions of variable parameters k_1 and K_1, the expressions

$$\phi_{k_1 K_1}(u), \quad \psi_{k_1 K_1}(u), \quad \chi_{k_1 K_1}(u), \quad \omega^{(1)}_{k_1 K_1}, \quad \omega^{(2)}_{k_1 K_1}$$

are analytic and even regular, when

$$|k_1-k_0| \quad \text{and} \quad |K_1-K_0|$$

are sufficiently small.

An arbitrary plane cuts $C(k_1, K_1)$ in four points of elliptic arguments u_1, u_2, u_3, u_4, say; they are connected by the congruence

$$u_1+u_2+u_3+u_4 \equiv c \quad (\text{mod } \omega^{(1)}_{k_1 K_1}, \ \omega^{(2)}_{k_1 K_1})$$

with a certain constant c, which may be assumed equal to zero without loss of generality. Of these four points of intersection, three may be given arbitrarily, and then the last one can be found by a rational construction. In the special case when the plane osculates $C(k_1, K_1)$ in the point u_1, this point must be counted thrice, and so there is only one other point of intersection u_2, given by the congruence

$$u_2 \equiv -3u_1 \pmod{\omega^{(1)}_{k_1 K_1}, \omega^{(2)}_{k_1 K_1}}.$$

When we now construct the t points with the elliptic arguments

$$u_1, \; -3u_1, \; +9u_1, \; \ldots, \; (-3)^{t-1} u_1,$$

they will all be different from one another and none lie at infinity, when a certain finite number of incongruences of the type

$$u \not\equiv v^{(i)}_{k_1 K_1} \pmod{\omega^{(1)}_{k_1 K_1}, \omega^{(2)}_{k_1 K_1}} \quad (i = 1, 2, \ldots, j)$$

is satisfied; here

$$v^{(i)}_{k_1 K_1} \quad (i = 1, 2, \ldots, j)$$

denote analytical functions of k_1, K_1, which are regular for sufficiently small $|k_1 - k_0|$ and $|K_1 - K_0|$. Now for such k_1 and K_1 every congruence

$$u \equiv v^{(i)}_{k_1 K_1} \pmod{\omega^{(1)}_{k_1 K_1}, \omega^{(2)}_{k_1 K_1}}$$

represents a piece of a certain analytical surface. Hence all t points

$$u_1, \; -3u_1, \; +9u_1, \; \ldots, \; (-3)^{t-1} u_1$$

on $C(k_1, K_1)$ will be different and finite, when the first point

$$u_1 = (x', y', z')$$

is chosen in such a way that it lies sufficiently near to the curve $C(k_0, K_0)$ and does not lie on a finite number of pieces of certain analytical surfaces. We can satisfy these conditions by rational numbers x', y', z'. The point (x', y', z') determines uniquely the numbers

$$k_1 = ax'^2 + by'^2 + cz'^2, \quad K_1 = Ax'^2 + By'^2 + Cz'^2,$$

and so also the curve $C(k_1, K_1)$; both k_1 and K_1 are rational, and the former method shows that the t points with elliptic arguments

$$u_1, \; -3u_1, \; +9u_1, \; \ldots, \; (-3)^{t-1} u_1$$

on $C(k_1, K_1)$ are different and finite and have rational coordinates. Assumc Z to be the least common multiple of the denominators of these coordinates; then, on the curve

$$C(k_1 Z^2, K_1 Z^2): \quad ax^2 + by^2 + cz^2 = k_1 Z^2, \quad Ax^2 + By^2 + Cz^2 = K_1 Z^2,$$

there are at least t different and finite lattice points, which proves our theorem.

29. All the considerations of the previous pages were based on the construction of rational points on a curve of genus 1, when one such rational point was known. Evidently the method will lead to still better results when we know more rational points on the curve and when the elliptic arguments, say $u_1, u_2, \ldots, u_s$, of these points do not satisfy any congruence

$$h_1 u_1 + h_2 u_2 + \ldots + h_s u_s \equiv 0 \pmod{\omega_1, \omega_2}$$

with too small integers $h_1, h_2, \ldots, h_s$. Now we have a cubic curve through any nine given points in the plane. We may choose their coordinates as integers in such a way that the curve has no double point and hence is of genus 1, and that the elliptic arguments of the nine points are sufficiently independent in the above-mentioned sense; this will be the case when a certain finite system of inequalities is satisfied. It is very probable that in this way we may be able to prove the result:

"There are an infinity of cubic curves

$$\sum_{i=0}^{3} \sum_{\substack{j=0 \\ i+j \leqslant 3}}^{3} a_{ij} x^i y^j = 0,$$

of genus 1 and with integer coefficients, on which at least

$$(\log a)^2$$

different lattice points lie, where

$$a = \max_{i,\, j} (|a_{ij}|) \text{''}.$$

I hope to attack this question in a later paper.

Krefeld, Ross-str. 243,
Germany.