WHEN DOES AN AFFINE CURVE HAVE AN ALGEBRAIC INTEGER POINT?

by B. J. BIRCH

To Robert Rankin on the occasion of his 70th birthday

1. The purpose of this note is to draw attention to the question in the title. If $C \subseteq K^n$ is an (absolutely) irreducible affine curve, defined by equations over a number field K, an *algebraic integer point* of C is a point $P = (x_1, \ldots, x_n)$ with all of $x_1, \ldots, x_n$ integers of some finite extension L of K. For such an algebraic integer point P to exist, there are obviously necessary local conditions: for every prime $\mathfrak{p}$ of K there must exist a prime $\mathfrak{P}$ above $\mathfrak{p}$ and a corresponding finite extension $L_{\mathfrak{P}}$ of the completion $K_{\mathfrak{p}}$ such that C has a $\mathfrak{P}$-adic integer point. We would like to know whether these obviously necessary local conditions are also sufficient.

The problem arose during the boat trip of the 1984 Bonn Arbeitstagung. Franz Oort wished to construct curves of arbitrarily high genus, over suitable number fields, with everywhere good reduction, and it was clear that a theorem that an affine curve defined over a number field always has an algebraic integer point in some finite extension "unless it obviously hasn't" would answer his question very naturally. Shortly afterwards, Oort answered his original question by direct construction of appropriate hyperelliptic curves, but the problem of finding algebraic integer points on affine curves seems to be harder, and is as yet unanswered, despite assistance from Mike Artin. Artin pointed out that a Hasse principle is not to be expected for loci that are not irreducible: the equation $2x^2 + x + 1 = 0$ has a $\mathfrak{p}$-adic integer zero for every prime $\mathfrak{p}$ of $\mathbb{Q}(\sqrt{-7})$, but has no algebraic integer zero, of course.

In the next section, I will provide a small piece of evidence in favour of such a Hasse principle: it is valid for Thue curves, that is to say curves C of the shape $f(X, Y) = k$ with f homogeneous and k a non-zero constant. Precisely, I will prove the following.

THEOREM 2. *Let K be a number field with integers $\mathfrak{o}_K$, let $f(X, Y) = \sum_{i=0}^{d} h_i X^{d-i} Y^i$ be a homogeneous form of degree d with coefficients in $\mathfrak{o}_K$, and let $k \in \mathfrak{o}_K$. Suppose that k is in the ideal $(h_0, \ldots, h_d)$ of $\mathfrak{o}_K$. Then there is an algebraic extension L of K and integers $x, y \in \mathfrak{o}_L$ such that $f(x, y) = k$.*

I will actually prove a little more, that if $h_0, h_1, \ldots, h_d$ are coprime then we may solve $f(x, y) = 1$ with x, y algebraic *units*. This stronger result (Theorem 1) is simply deduced from lemmas about linear equations; it could be known to those interested in sets of exceptional units (cf. [**1**], [**2**]), since an immediate corollary is that any set of exceptional units may be extended; but I have not seen it anywhere. One can give an explicit estimate for the degree and height of x, y, in terms of the height of the coefficients of f; if our problem were solved, it would be nice to have such an estimate.

Glasgow Math. J. **27** (1985) 1–4.

https://doi.org/10.1017/S0017089500006017 Published online by Cambridge University Press

The author is grateful to the organisers of the Arbeitstagung, and to friends to whom he has talked about this question.

2. If K is any number field, $\mathfrak{o}_K$ denotes its ring of integers, and, if $\mathfrak{p}$ is a prime of K, $\mathfrak{o}_\mathfrak{p}$ denotes the integers of the $\mathfrak{p}$-adic completion $K_\mathfrak{p}$ of K.

Our object is to prove Theorem 1 below. We will deduce it from a pair of lemmas on linear equations: a local Lemma 1, and Lemma 2 (almost equivalent to the theorem) which follows from Lemma 1 by a local-to-global argument.

LEMMA 1. *Let L be a number field with ring of integers $\mathfrak{o}_L$. Let $\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k$ be k pairs of coprime integers of $\mathfrak{o}_L$, write $\Delta = \det_{1\leq i,j\leq k} (\alpha_j^{k+1-i}\beta_j^i)$ and suppose that $\Delta \neq 0$. Then for every prime $\mathfrak{p}$ of L there is a natural number $n(\mathfrak{p})$ such that the equations*

$$\sum_{i=0}^{n} c_i\alpha_j^{n-i}\beta_j^i = 1 \quad \text{for } j = 1, \ldots, k \tag{1}$$

are simultaneously soluble when $n = n(\mathfrak{p})$ with $c_0 = c_n = 1$ and every $c_i \in \mathfrak{o}_\mathfrak{p}$.

Proof. If $\mathfrak{p} \nmid \Delta$, the lemma is obvious—we just take $n = k+1$ and solve for $c_1, \ldots, c_k$.

Suppose now that $\mathfrak{p}^r$ exactly divides Δ. Take a root of unity, ζ say, so that $\alpha_j + \zeta\beta_j$ are all prime to $\mathfrak{p}$; then we can find $m = m(\mathfrak{p})$ so that $\zeta^m = 1$ and $(\alpha_j + \zeta\beta_j)^m \equiv 1(\mathfrak{p}^{2r})$ for $j = 1, \ldots, k$. So whenever n is a multiple of $m(\mathfrak{p})$, there are algebraic integers $e_0, \ldots, e_n$ determined by $(X+\zeta Y)^n = \sum e_i X^{n-i}Y^i$ so that $e_0 = e_n = 1$ and

$$\sum_{i=0}^{n} e_i\alpha_j^{n-i}\beta_j^i \equiv 1 \ (\mathfrak{p}^{2r});$$

say

$$\sum_{i=0}^{n} e_i\alpha_j^{n-i}\beta_j^i = (\alpha_j + \zeta\beta_j)^n = 1 + d_j \quad \text{for } j = 1, \ldots, k \tag{2}$$

with each d_j divisible by $\mathfrak{p}^{2r}$.

Fix $n = n(\mathfrak{p})$ as a multiple of $m(\mathfrak{p})$ exceeding $k+1$, fix an algebraic integer μ so that each $\alpha_j^{n-k-1} + \mu\beta_j^{n-k-1}$ is prime to $\mathfrak{p}$, and solve the linear equations

$$\left(\sum_{i=1}^{k} f_i\alpha_j^{k+1-i}\beta_j^i\right)(\alpha_j^{n-k-1} + \mu\beta_j^{n-k-1}) = d_j \quad \text{for } j = 1, \ldots, k \tag{3}$$

for $f_1, \ldots, f_k$. Then $f_1, \ldots, f_k$ are local integers in the extension $L_\mathfrak{p}(\mu)$ of $L_\mathfrak{p}$. Piecing together (2) and (3) we have a solution of (1) with $c_0 = c_n = 1$ and $c_1, \ldots, c_{n-1}$ integral over $\mathfrak{o}_\mathfrak{p}$; so there is a solution of (1) with $c_1, \ldots, c_{n-1} \in \mathfrak{o}_\mathfrak{p}$.

COROLLARY. *The equations* (1) *are soluble with $c_0 = c_n = 1$ and every $c_i \in \mathfrak{o}_\mathfrak{p}$ whenever n is a multiple of $n(\mathfrak{p})$.*

Proof. $\sum c_i\alpha_j^{n-i}\beta_j^i = 1$ implies $(\sum c_i\alpha_j^{n-i}\beta_j^i)^r = 1$ for every integer r.

https://doi.org/10.1017/S0017089500006017 Published online by Cambridge University Press

LEMMA 2. *Suppose that* $L, \alpha_1, \beta_1, \ldots, \alpha_k, \beta_k, \Delta$ *are as in Lemma* 1. *Then there is a natural number N such that the equations* (1) *are soluble with* $c_0 = c_n = 1$ *and* $c_1, \ldots, c_{n-1} \in \mathfrak{o}_L$, *whenever n is a multiple of N.*

Proof. Indeed, we take N as the least common multiple of $k+1$ and of the $n(\mathfrak{p})$ as $\mathfrak{p}$ runs through the prime divisors of Δ. Then by Lemma 1 we can solve (1) in $\mathfrak{p}$-adic integers for every $\mathfrak{p}$, so by the Chinese remainder theorem we can find $c'_0 = c'_n = 1$ and $c'_1, \ldots, c'_{n-1} \in \mathfrak{o}_L$ so that

$$\sum_{i=0}^{n} c'_i \alpha_j^{n-i} \beta_j^i = 1 \text{ modulo } \Delta \prod_j \alpha_j^n \beta_j^n.$$

Fix $c_i = c'_i$ for $i = 0$ and $i \geq k+1$, and determine $c_1, \ldots, c_k$ to satisfy (1); then $c_1, \ldots, c_k$ are in $\mathfrak{o}_L$ too.

THEOREM 1. *Let K be a number field with ring of integers* $\mathfrak{o}_K$ *and let* $f(X, Y) = \sum_{i=0}^{d} h_i X^{d-i} Y^i$ *be a homogeneous polynomial of degree d, with* $h_0, \ldots, h_d$ *coprime integers of* $\mathfrak{o}_K$. *Then we can find a finite extension M of K and a unit x of* $\mathfrak{o}_M$ *such that* $f(x, 1)$ *is a unit of* $\mathfrak{o}_M$.

Proof. Let K_1 be the splitting field of f over K, and let L be the class field of K_1, so that every ideal of the ring of integers of K_1 becomes principal in $\mathfrak{o}_L$. We may factor

$$f(X, Y) = h_b X^a Y^b \prod_{j=1}^{k} (X - \theta_j Y)^{c(j)}$$

where $\theta_1, \ldots, \theta_k$ are the distinct non-zero roots of $f(X, 1) = 0$ in K_1, and then

$$f(X, Y) = \varepsilon X^a Y^b \prod_{j=1}^{k} (\beta_j X - \alpha_j Y)^{c(j)}$$

where ε is a unit of $\mathfrak{o}_L$ and $\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k$ are pairs of coprime integers of $\mathfrak{o}_L$, with $\alpha_j/\beta_j = \theta_j$ distinct and non-zero for $j = 1, \ldots, k$.

Accordingly, it will be enough to show that we can find a unit x of the ring of integers of an extension M of L so that $\beta_j x - \alpha_j$ $(j = 1, \ldots, k)$ are all units—for then $f(x, 1)$ will be a unit. Since the α_j/β_j are distinct and no α_j or β_j vanishes, the relevant Δ is non-zero, so Lemma 2 is applicable. Choose N and $c_0, \ldots, c_N$ as in Lemma 2, and let x be a root of $\sum c_i X^{N-i} = 0$; then x is a unit of an extension M of L, and each $\beta_j x - \alpha_j$ divides $\sum c_i \alpha_j^{N-i} \beta_j^i = 1$, so each $\beta_j x - \alpha_j$ is a unit too. The proof is complete.

Finally, we prove Theorem 2. In the notation of the theorem, we are trying to solve $f(x, y) = k$, where k is in the ideal $(h_0, \ldots, h_d)$ generated by the coefficients of f. Let K_1 be the class field of K, so that the ideal $(h_0, \ldots, h_d)$ becomes principal, generated by h, say. By Theorem 1, we can find an extension L and a unit z of $\mathfrak{o}_L$ so that $h^{-1} f(z, 1) = \varepsilon$ is a unit of $\mathfrak{o}_L$, and then we have an integral solution $(x, y) = (k/\varepsilon h)^{1/d}(z, 1)$ of $f(x, y) = k$.

https://doi.org/10.1017/S0017089500006017 Published online by Cambridge University Press

REFERENCES

1. H. W. Lenstra Jr., Euclidean fields of large degree, *Invent. Math.* **38** (1977), 237–254.

2. A Leutbecher and J. Martinet, Lenstra's constant and Euclidean number fields, *Astérisque* **94** (1982), 87–131.

Mathematical Institute
24–29 St. Giles'
Oxford
OX1 3LB

https://doi.org/10.1017/S0017089500006017 Published online by Cambridge University Press