Abraham Robinson's Notes

*On a relatively effective procedure getting all
quasi-integer solutions of diophantine
equations with positive genus*

Abraham ROBINSON

These notes were written by Abraham Robinson in preparation for his paper with Peter Roquette [4]. They were written shortly before his death in 1974, but were omitted from the published paper. The published material was in much more polished, and use different terminology. Nevertheless these notes are easily understood with a knowledge of [4]. What Robinson aimed at in those notes was done by number-theoretical methods in [6]. See also [5] for the logical side of the subject.

In those notes, Robinson used the elementary and familiar idea that consequence relative to nonstandard models is recursively enumerable in the set of axioms defining the class. The idea is intriguing because nonstandard models are usually associated with very nonconstructive ideas especially, because the models needed cannot be recursive. These notes should be a useful reminder for applications of the idea in nonstandard mathematics. (G.T.)

Effectiveness. Consider to begin with, Siegel's theorem for a curve of genus 1 over the rational numbers. This is a special case of the theorem of section 6 and states that the number of points with rational integer coordinates on a curve of genus 1 is finite. We are going to discuss the problem of finding an effective bound for this case.

Let K be a set of sentences in the lower predicate calculus which satisfies the following conditions. (i) There is a predicate $Z(x)$ in the vocabulary of K which may or may be not atomic such that (together with appropriate functions or relations for addition, multiplication and order) $Z(x)$ determines, in any model M of K , an ordered integral domain, in which 1 is the smallest positive element. In other words the elements of M which satisfy $Z(x)$ constitute a domain $*Z$ of the kind just described. Thus, the ring of integers, Z , can be injected into $*Z$ in one and only one way. (ii) There exists a model M_0 of K in which $*Z$ coincides with Z .

Let $*M$ be any model of K . A point (ξ, η) in $*M \times *M$ is *integer* if $(\xi, \eta) \in *Z \times *Z$; and it is *infinite* if at least one of ξ, η does not belong to (the image of Z). Thus, a point is infinite if and only if $\xi^2 + \eta^2 > n$ for all $n \in Z$. Now let $f(x, y) \in Z[x, y]$. Let $X_n, n = 1, 2, 3, \dots$, be the assertion, formalized in the vocabulary of

K , that there *do not exist* ξ, η , $\xi^2 + \eta^2 > n$, which satisfy $f(x, y), f(\xi, \eta) = 0$. Suppose that, for any model $*M$ of K , we can prove that for any infinite (ξ, η) , $f(\xi, \eta) \neq 0$. Then we claim that *there exists a positive integer m such that $K \vdash X_m$ (X_m is a consequence of K)*. Indeed, this assertion is an immediate consequence of the familiar compactness theorem of the lower predicate calculus. Suppose that there is no n as asserted. Evidently $K \vdash X_n \supset X_{n+1}$ (where $\supset$ is the symbol of implication). Suppose that the set $H = K \cup \{\neg X_1, \neg X_2, \dots\}$ is consistent and let $*M$ be a model of H . Then, within $*M$, (ξ, η) denotes an infinite point which satisfies $f(x, y) = 0$. And this is impossible, by assumption. Accordingly H is inconsistent and so, by the compactness theorem, a finite subset of H , $K \cup \{\neg X_1, \neg X_2, \dots, \neg X_m\}$ is inconsistent. But then $K \vdash \neg[\neg X_1 \wedge \dots \wedge \neg X_m]$ and, hence, $K \vdash X_1 \vee \dots \vee X_m$. Since $K \vdash X_n \supset X_{n+1}$, for $n = 1, 2, \dots, m-1$, we conclude that $K \vdash X_m$. This proves the assertion.

We may apply this result to the analysis of the preceding sections, for Siegel's theorem, with $g = 1$. There are several methods by which we may reformulate that analysis within the lower predicate calculus. One is to introduce all the necessary notions as well as their required properties *ad hoc* as we go along, including in particular, predicates for valuations, ideals, the field of real numbers, the logarithmic function, etc. For example, for the field of real numbers, R , we may introduce the axioms of an ordered field and the assumption that it carries a logarithmic function with the appropriate properties. For any model $*M$ of the set of sentences thus obtained, we still have the notion of infinitesimals and infinitely large numbers since the model of R within $*M$ is, at any rate, an ordered field. However, there are two distinct problems which arise in this procedure and which require separate consideration.

The first problem concerns the handling of the standard part of a function. In our original approach, the nonstandard field of real numbers, $*R$, was a proper extension of the standard field of real numbers. Accordingly, we were able to assume that every finite real number has a standard part within the nonstandard model under consideration. In the present circumstances, $*M$ is an arbitrary model of the set of axioms K , in which the field which represents the real numbers, to be called again $*R$, is not necessarily an extension of R .

A survey of sections 2-6 shows that the standard part was involved in the following contexts. In section 2, equations 2.2 and 2.3 led to the conclusion that $w_p(\alpha) = {}^0(v_p(\alpha)/v_p(\alpha_0))$ for finite primes and $w_p(\alpha) = {}^0(\ln |\alpha|_p / \ln |\alpha_0|_p)$ for nonarchimedean primes. In this case the standard parts in question are actually standard integers and are therefore included in $*Z$ and $*R$, as required. In section 6, we had to consider the standard part ${}^0\pi$ of a place π . But here again, the place turned out to be at least absolutely algebraic and so the number ξ_0 will be included in $*R$ provided we include in K the assumption that the field in question is real closed.

The second problem concerns the statement of Roth's theorem. It may be formulated in the following way :

7.1 Let α and β be arbitrary algebraic numbers and let $k \geq 2$. The number of solutions $\zeta \in Q(\beta)$ of the inequality

$$7.2 \quad |\alpha - \zeta| \leq (H(\zeta))^{-k}$$

is finite.

From this we drew the conclusion that (see 6.3 in a different notation) for a nonstandard number in ${}^*Q(\beta)$

$$7.3 \quad |\alpha - \zeta| > (H(\zeta))^{-k}.$$

Fixing $k=3$, for the sake of simplicity, we have to show how to formalize 7.1 so that this conclusion is still valid in *M in the present context. Since, for the case of Siegel's theorem, we have $Q(\beta)=Q$, $H(\zeta)=\max(|\zeta_1|, |\zeta_2|)$ where $\zeta=\zeta_1/\zeta_2$, and ζ_1 and ζ_2 are relatively prime. It then follows from 7.1 that there is an integer valued function of α , $F(\alpha)$, such that for any solution of 7.2, $H(\zeta) < F(\alpha)$. Instead of considering $F(\alpha)$, we may also define $F(a_0, a_1, \dots, a_n)$ as the joint bound for the $H(\zeta)$ which may occur in 7.2 as α ranges of the roots of $a_0 + a_1x + a_2x^2 + \dots + a_nx^n = 0$, where $a_0, a_1, \dots, a_n$ are integers. Moreover, every finite sequence of integers can be coded into a single natural number by familiar methods, and so, finally, we can write out first order sentences Y_n , involving the *instances* of a number theoretic function $G(n)$, $n=0, 1, 2, \dots$, which together assume that 7.1 is satisfied, with the *absolute* interpretation of "finite". Once this is done, and all the resulting sentences are included in K , we may then deduce 7.3 (for $Q(\beta)=Q$, $k=3$).

Having thus formulated a suitable set of axioms K , we show, as before, that the curve ${}^*\Gamma$ which is given by some specific numerical equation $f(x, y)=0$ cannot contain an infinite point (ξ, η) . According to the principle proved at the beginning of the section, we then have, for some standard positive integer m , that X_m is deducible from K . It follows that if K were recursively enumerable, i.e. if we could formulate the sentences of K effectively one by one, then the set of sentences in the vocabulary of K and deducible from K would also be recursively enumerable, by the successive systematic deduction of these sentences from K . However, in actual fact, K contains, in addition to the sentences which are required to lead up to the proof of 6.2, also the sentences Y_n which are needed in connection with Roth's theorem, as explained above, and these involve the number theoretic function $G(n)$ *which is not known effectively*. It follows that the set of sentences in the vocabulary of K which are deducible from K is known to be recursively enumerable only *relative to* $G(n)$ or, to put it informally, only relative to Roth's theorem. If now we confine our attention to equations $f(x, y)=0$ with rational integer coefficients, which are absolutely irreducible and of genus $g=1$ — and this is a matter which can

be checked effectively by means of standard formulae for the genus — then our systematic procedure for deducing consequences of K will, sooner or later, yield an X_m , i.e. a bound for the integer solutions of $f(x, y) = 0$. Accordingly, our argument shows that the integer points on an elliptic curve possess *a bound which can be calculated effectively relative to Roth's theorem for the special case that the approximating numbers are rational*.

As mentioned in the introduction, A. Baker has obtained a stronger result by giving an explicit bound for the number of integer points on an elliptic curve. This is superior to our result not only because the bound is explicit but also because its effectiveness is absolute. In order to deduce the latter conclusion within our present framework, we should have to show that there is an effective bound on the height in Roth's theorem (for rational approximations), i.e. that $G(n)$ can be chosen so as to be recursive. However, while it is known that there is an effective bound for the *number of solutions* of Roth's inequality [2], (compare [3] where the matter is discussed from a proof theoretic point of view), the question of the existence of an effective bound for the height of the approximating numbers is still open.

Our method applies equally well to Siegel's theorem, for $g=1$ and for an arbitrary algebraic number field k . The standard parts $w_p(\alpha) = {}^0(v_p(\alpha)/v_p(\alpha_0))$ and $w_p(\alpha) = {}^0(\ln |\alpha|_p / \ln |\alpha_0|_p)$ are, as before standard rational numbers. As for the standard part ${}^0\pi$ of a place π , we now have to consider also complex and P-adic completions. Correspondingly, we have to lay down that K include sentences which state that the corresponding fields are algebraically closed or henselized. Finally, taking $k=3$ in 7.1, we again define $G(n)$ as a number theoretic function from N into N .

There is nothing essentially new in the application of this procedure to the case $g > 1$. Thus we obtain the result that *the k -integer points* on a curve of genus $g > 1$ possess a bound which can be calculated effectively relative to Roth's theorem.

As far as we know, this result is established here for the first time. It is interesting in principle and of decisive practical convenience that our method bypasses the need for proving the effectiveness of the many intermediate steps that are involved in the proof of Siegel's theorem.

References

- [1] A. Baker, Effective Methods in the theory of numbers; Proc. Int. Congr. Math. Nice 1970; Paris (1971), Vol. 1, 19-26.
- [2] H. Davenport-K.F. Roth, Rational approximations to algebraic numbers; *Mathematica* 2 (1955), 160-167.
- [3] G. Kreisel, Five notes on the application of proof theory to computer science, Institute for Mathematical Studies in the Social Sciences, Stanford University Technical Report No. 182. Psychology and Education Series, 1971, (mimeographed).

- [4] A. Robinson-P. Roquette, On the finiteness theorem of Siegel and Mahler concerning diophantine equations, *Journal of Number Theory*, Vol. 7 (1975), 121-176.
- [5] G. Kreisel and A. Macintyre, Constructive logic versus algebraization I, pp. 217-260, *The L.E.J. Brouwer Centenary Symposium*, ed. D. van Dalen and A.S. Troelstra, North-Holland 1982.
- [6] J.P. Serre and M. Waldschmidt, *Autour du Theoreme de Mordell-Weil*, *Publications Mathematiques de l' Universite Pierre et Marie Curie* No. 62, 1983.