A DECISION METHOD FOR p-ADIC INTEGRAL ZEROS OF DIOPHANTINE EQUATIONS

BY A. NERODE[1]

Communicated by Deane Montgomery, February 18, 1963

1. **Introduction.** The question addressed here arose from a simple observation about Hilbert's 10th problem. The 10th problem is that of giving a uniform effective procedure which, when applied to a diophantine equation $f(x_1, \cdots, x_n)=0$, would decide whether or not f has a rational integral zero. Which equations are easy to decide? If f does indeed have a rational integral zero, this can be found out by testing n-tuples of rational integers. If f has no real zero, this can be determined by the Sturm-Tarski algorithm [5]. If f has no p-adic integral zero, this can be ascertained by testing for zeros mod p, mod $p^2, \cdots$ until a modulus is found for which there are no zeros. A fortiori, there is no rational integral zero if there is no real zero or if for some p there is no p-adic integral zero. Consequently, the "difficult" equations certainly lie amongst those having no rational integral zero, but having real zeros and p-adic integral zeros for all p. It is thus natural to look for effective properties of solvability in these domains. Of course, the Sturm-Tarski algorithm actually gives a decision procedure which answers whether or not f has a real zero.

MAIN RESULT. Let p be a rational integral prime. Then there is a uniform effective method for deciding, given a diophantine equation $f(x_1, \cdots, x_n)=0$, whether or not it has a p-adic integral zero.

Actually, the procedure works for a wider class of polynomials f. Let Z be the rational integers, let $Z(p)$ be the p-adic integers, and let $ZA(p)$ be the p-adic algebraic integers—i.e., $ZA(p)$ consists of those $\alpha \in Z(p)$ such that α satisfies an equation with rational integral coefficients. The procedure works for f with coefficients in $ZA(p)$.

THEOREM 1. *If $f \in ZA(p)[x_1, \cdots, x_n]$ has a zero in $\mathbf{X}^n Z(p)$, then f has a zero in $\mathbf{X}^n ZA(p)$.*

THEOREM 2. *$ZA(p)$ can be construed naturally as a computable domain—i.e., the operations of addition and multiplication can be effectively performed in $ZA(p)$. (The exact meaning of Theorem 2 will become clear in* §3.)

In outline, the decision method is this. *Part* 1. Test $f=0$ for solvability mod p, mod $p^2, \cdots$. *Part* 2. Simultaneously with Part 1,

[1] Research supported in part under National Science Foundation grant GP-124.

enumerate all n-tuples $(\alpha_1, \cdots, \alpha_n)$ of elements of $ZA(p)$ and test (via Theorem 2) whether or not $f(\alpha_1, \cdots, \alpha_n)=0$ for each such n-tuple. If f has no zero in $\mathbf{X}^n Z(p)$, compactness implies f has no zero mod p^u for some u. This will be detected in Part 1. If f has a zero in $\mathbf{X}^n Z(p)$, Theorem 1 assures that f has a zero in $\mathbf{X}^n ZA(p)$. This will be detected in Part 2.

Theorem 1 can obviously be restated as a specialization theorem; namely, over $ZA(p)$, a p-adic integral point $(\alpha_1, \cdots, \alpha_n)$ can be specialized in $ZA(p)$. Among other consequences of Theorem 1, the following seems worth noting. Suppose $f \in ZA(p)[x_1, \cdots, x_n]$ maps $\mathbf{X}^n Z(p)$ onto $Z(p)$. Then Theorem 1 implies that f maps $\mathbf{X}^n ZA(p)$ onto $ZA(p)$. Thus for example the fact that every p-adic integer is a sum of four squares implies that every p-adic algebraic integer is a sum of four squares of p-adic algebraic integers.

2. **p-adic elimination.** In the present context it is appropriate to give a fairly constructive proof of Theorem 1. This is embodied in the proof of Theorem 1′ below, via elimination and without geometry or ideal theory. There exist, however, nice geometric proofs of Theorem 1. The following argument for plane curves is easily generalized. Suppose that $f(x, y)=0$ has a zero in $\mathbf{X}^2 Z(p)$. Let $g(x, y)=0$ be obtained from $f=0$ by eliminating multiple factors. Of course f and g have the same zeros. If g has a nonsingular zero in $\mathbf{X}^2 Z(p)$, Hensel's lemma implies that g has a nonsingular zero in $\mathbf{X}^2 ZA(p)$. Otherwise, g has a singular zero in $\mathbf{X}^2 Z(p)$. But all singular zeros of g are algebraic, hence g again has a zero in $\mathbf{X}^2 ZA(p)$.

THEOREM 1′. *Suppose $f \in ZA(p)[x_1, \cdots, x_n]$, suppose that the system $f(x_1, \cdots, x_n)=0$, $x_1 \equiv a_1$ mod p^u, $\cdots$, $x_n \equiv a_n$ mod p^u has a zero in $\mathbf{X}^n Z(p)$. Then this system has a zero in $\mathbf{X}^n ZA(p)$.*

PROOF. This is obvious for $n=1$. Assume it known for n, and prove for $n+1$. Let $(\sigma_1, \cdots, \sigma_{n+1}) \in \mathbf{X}^{n+1} Z(p)$ be a zero of $f(x_1, \cdots, x_{n+1})=0$, $x_1 \equiv a_1$ mod p^u, $\cdots$, $x_{n+1} \equiv a_{n+1}$ mod p^u. Let $h(x_1, \cdots, x_n, y)=f(x_1, \cdots, x_n, a_{n+1}+p^u y)$. We produce a system $g(x_1, \cdots, x_n)=0$, $x_1 \equiv c_1$ mod p^w, $\cdots$, $x_n \equiv c_n$ mod p^w such that: (i) $w \geqq u$ and $(\sigma_1, \cdots, \sigma_n)$ satisfies the system; (ii) if $(\alpha_1, \cdots, \alpha_n) \in \mathbf{X}^n Z(p)$ satisfies the system, then there exists a p-adic integer y algebraic over $Z(p)[\alpha_1, \cdots, \alpha_n]$ such that $h(\alpha_1, \cdots, \alpha_n, y)=0$. An application of the inductive hypothesis will then conclude the proof.

To produce the system write

$$h(x_1, \cdots, x_n, y) = \sum_{i=0}^{k} h_i(x_1, \cdots, x_n) y^i$$

and proceed as follows. *Case* 1. $(\sigma_1, \cdots, \sigma_n)$ satisfies the system $h_0(x_1, \cdots, x_n)=0, \cdots, h_k(x_1, \cdots, x_n)=0$. Let

$$g \in ZA(p)[x_1, \cdots, x_n]$$

be a single polynomial with the same zeros in $Z(p)$ as this system. (The existence of g follows easily from the observation that $x^2+py^2=0$ if and only if $x=y=0$.) Then $g(x_1, \cdots, x_n)=0$, $x_1\equiv a_1 \bmod p^u$, $\cdots$, $x_n\equiv a_n \bmod p^u$ is the desired system. *Case* 2. $h(\sigma_1, \cdots, \sigma_n, y) \in ZA(p)[\sigma_1, \cdots, \sigma_n][y]$ is of positive degree in y. The euclidean algorithm yields an $\bar{h}(\sigma_1, \cdots, \sigma_n, y) \in ZA(p)[\sigma_1, \cdots, \sigma_n][y]$ with the same irreducible factors as h, but such that $\bar{h}$ has simple factors. ($\bar{h}$ is $h/\gcd(h, h_y)$ multiplied by an element of $ZA(p)[\sigma_1, \cdots, \sigma_n]$.) The way in which $\bar{h}$ is obtained with $\sigma_1, \cdots, \sigma_n$ as parameters by the euclidean algorithm depends on which coefficient in each divisor is the first nonvanishing coefficient; that is, on the vanishing or nonvanishing of a finite number of polynomials in $\sigma_1, \cdots, \sigma_n$. Thus $\bar{h}(x_1, \cdots, x_n, y) \in ZA(p)[x_1, \cdots, x_n][y]$ and $g_1, \cdots, g_p, g_1', \cdots, g_q' \in ZA(p)[x_1, \cdots, x_n]$ can be selected to satisfy (i), (ii) below. (i) $(\sigma_1, \cdots, \sigma_n)$ satisfies $g_1= \cdots =g_p=0$, $g_1' \neq 0, \cdots, g_q' \neq 0$. (ii) Whenever $(\alpha_1, \cdots, \alpha_n) \in \mathbf{X}^n Z(p)$ satisfies this system, then (as polynomials in y with coefficients in $ZA(p)[\alpha_1, \cdots, \alpha_n]$) h and $\bar{h}$ have the same irreducible factors, $\bar{h}$ has simple factors, and $\bar{h}$ has nonzero formal leading coefficient.

Now choose w so large that $g_1'(\sigma_1, \cdots, \sigma_n) \not\equiv 0 \bmod p^w, \cdots, g_q'(\sigma_1, \cdots, \sigma_n) \not\equiv 0 \bmod p^w$, $w \geqq u$; and if δ is the order of the discriminant of $\bar{h}(\sigma_1, \cdots, \sigma_n, y)$ as a polynomial in y, also require that $w \geqq 2\delta+1$. Let c_i be a rational integer with $\sigma_i \equiv c_i \bmod p^w$, $i=1, \cdots, n$. Let g be a single polynomial whose zeros in $Z(p)$ are exactly the common zeros of $g_1, \cdots, g_p$. Then $g = 0$, $x_i \equiv c_i \bmod p^w$, $i=1, \cdots, n$, is the required system. To see this, suppose $(\alpha_1, \cdots, \alpha_n)$ satisfies this system. By construction δ is the order of the discriminant of $\bar{h}(\alpha_1, \cdots, \alpha_n, y)$ and $\bar{h}(\alpha_1, \cdots, \alpha_n, (\sigma_{n+1}-a_{n+1})/p^u) \equiv \bar{h}(\sigma_1, \cdots, \sigma_n, (\sigma_{n+1}-a_{n+1})/p^u) \equiv 0 \bmod p^{2\delta+1}$. Since $\bar{h}(\alpha_1, \cdots, \alpha_n, y) \equiv 0 \bmod p^{2\delta+1}$ is solvable in $Z/(p^{2\delta+1})$, it follows (see the first paragraph of §3) that $\bar{h}(\alpha_1, \cdots, \alpha_n, y)=0$ is solvable for a $y \in Z(p)$. Since $\bar{h}(\alpha_1, \cdots, \alpha_n, y)$ has degree $\geqq 1$ in y, the latter is certainly algebraic over $ZA(p)[\alpha_1, \cdots, \alpha_n]$.

3. $ZA(p)$ **as a computable domain.** Let $f(x) \in Z(p)[x]$ have simple factors and nonvanishing leading coefficient. Let D be the discriminant of f. Then $D \neq 0$ has some order δ—i.e., $D \equiv 0 \bmod p^\delta$, $D \not\equiv 0 \bmod p^{\delta+1}$. The Hensel-Rychlik theorem [**2**, p. 68; **4**, p. 100] shows how to determine the zeros of f in $Z(p)$. Find all solutions to

$f(x)\equiv 0 \bmod p^{2\delta+1}$ and reduce each of these mod $p^{\delta+1}$ to obtain distinct residues $x_1, \cdots, x_k$ mod $p^{\delta+1}$ (possibly none). Then $x_1, \cdots, x_k$ constitute a complete system of residues mod $p^{\delta+1}$ for the zeros of f in $Z(p)$. This means that each x_i arises by reduction mod $p^{\delta+1}$ from exactly one zero of f in $Z(p)$. Now suppose further that the coefficients of f are effectively given; that is, for each coefficient $c=\sum a_ip^i$, $0\leqq a_i <p$, a procedure is given for computing a_i from i. Then $\delta, x_1, \cdots, x_k$ can be effectively determined, and the corresponding zeros of f in $Z(p)$ can be effectively given. To see this, note that by computing the coefficients of f mod p, mod $p^2, \cdots$, one can compute D mod p, D mod $p^2, \cdots$ and can effectively determine the first δ with $D\equiv 0 \bmod p^\delta$, $D\not\equiv 0 \bmod p^{\delta+1}$. Then by computing the coefficients of f mod $p^{2\delta+1}$ and solving $f(x)\equiv 0 \bmod p^{2\delta+1}$, the $x_1, \cdots, x_k$ mod $p^{\delta+1}$ can be effectively determined. Finally, the Newton approximation technique used to prove the Hensel-Rychlik theorem allows the corresponding zeros to be effectively given.

We assign a uniquely determined description $(P(x), a)$ to each element α of $ZA(p)$. Call an irreducible polynomial in $Z[x]$ *standard* if its leading coefficient is positive and its coefficients have gcd 1. Let $f(x)$ be the standard irreducible polynomial satisfied by α, let δ be the order of the discriminant of f, and let a, $0\leqq a<p^{\delta+1}$ be the rational integer with $\alpha\equiv a \bmod p^{\delta+1}$. Then $(f(x), a)$ is the description of α.

Observe that if a pair $(f(x), a)$ is given with $f(x)\in Z[x]$ and $a\in Z$, it can be effectively determined whether or not $(f(x), a)$ is a description of an element of $ZA(p)$. Kronecker's factorization algorithm decides whether or not f is standard irreducible. If f is standard irreducible, then δ and $x_1, \cdots, x_k$ can be computed. It can certainly be established whether or not a is among $x_1, \cdots, x_k$. (It is this effective property that permits all n-tuples of descriptions of elements of $ZA(p)$ to be effectively listed for the decision method of §1.)

Finally, we show that from descriptions $(f(x), a)$ of α and $(g(x), b)$ of β, the description $(h(x), c)$ of $\phi(\alpha, \beta)$ $(=\alpha+\beta$ or $\alpha\cdot\beta)$ can be effectively determined. Let Q be the rational field; form $Q[\alpha]$. Since f is given, operations in $Q[\alpha]$ can be effectively performed; and van der Waerden's splitting algorithm for algebraic extensions [6, p. 137] allows the determination of the distinct irreducible factors of $g(x)$ over $Q[\alpha]$. We may assume that $q_1, \cdots, q_k\in Z[\alpha][x]$ are the distinct irreducible factors. Since q_i is irreducible over $Q[\alpha]$, the discriminant $D_i(\alpha)$ of q_i does not vanish. By choice of q_i, $D_i(\alpha)$ is a rational integral polynomial in α. Now α can be effectively given from its description, so the order δ_i of $D_i(\alpha)$ can be determined, and the distinct zeros of $q_i(x)$ in $Z(p)$ can be effectively given. β can also be effectively given from its description; so we may compute mod p^u all zeros in $Z(p)$ of all q_i and also β. For sufficiently large u it will be observed that β differs from all zeros of all q_i except one zero of one q_{i_1}. This can be effectively recognized, and q_{i_1} identified. Since q_{i_1} is the irreducible polynomial over $Q[\alpha]$ satisfied by β, operations in $Q[\alpha, \beta]$ can be carried out effectively. Now enumerate all standard irreducible polynomials h, and for each one test whether or not $h(\phi(\alpha, \beta))=0$; this is a computation in $Q[\alpha, \beta]$. Such an h will eventually be reached since $\phi(\alpha, \beta)$ is algebraic. Compute the order of the discriminant δ_h of h, and use the descriptions of α, β to compute c such that $\phi(\alpha, \beta) \equiv c \bmod p^{\delta_h+1}$. Then (h, c) is the required description.

An exact analysis of computable fields will be found in [1], [3].

References

1. A. Frölich and J. C. Sheperdson, *Effective procedures in field theory*, Philos. Trans. Roy. Soc. London Ser. A **284** (1955), 407–432.

2. K. Hensel, *Theorie der algebraischen Zahlen*, Teubner, Leipzig, 1908.

3. M. Rabin, *Computable algebra*, Trans. Amer. Math. Soc. **95** (1960), 341–360.

4. K. Rychlik, *Zur Bewertungstheorie der algebraischen Körper*, J. Reine Angew. Math. **153** (1924), 95–107.

5. A. Tarski, *A decision method for elementary algebra and geometry*, 2nd ed., Univ. of California Press, Berkeley, Calif., 1951.

6. B. L. van der Waerden, *Modern algebra*, Vol. 1, Ungar, New York, 1949.

Cornell University and
Institute for Advanced Study