ON REPRESENTATION OF NUMBERS BY BINARY FORMS

A. I. Vinogradov and V. G. Sprindzhuk

An effective method is given for finding all rational points, the denominators of which are formed from a finite number of fixed primes, on the curve \( f(x, y) = A \), where \( f(x, y) \) is a binary form of degree three at least, irreducible over the field of rational numbers, and \( A \) is a rational number.

Let \( f(x, y) \) be an integral binary form of degree three at least, irreducible over the field \( Q \) of rational numbers, and \( A \) a prime. By virtue of a well known theorem of Thue [6], the equation

\[
f(x, y) = A \tag{1}
\]

has only a finite number of integral solutions \( x, y \). However, Thue's method is not effective in the sense that it does not allow one to obtain an explicit limit for the unknowns \( x, y \) satisfying (1). Such explicit limits can be obtained for forms \( f(x, y) \) of a very special form (i.e., in the case of cubic forms with a negative discriminant [2] or forms \( ax^3 + by^3 \) with appropriate \( a, b \) [3]), but the solution of this problem in the general case was unknown until recently. Baker [4, 5] obtained only a short time ago estimates for the absolute values of linear forms in the logarithms of algebraic numbers, thus providing an effective method for investigation of Eq. (1).

We consider in this note the equation

\[
f(x, y) = A p_1^{a_1} \cdots p_s^{a_s}, (x, y) = 1, z_i > 0 \quad (i = 1, 2, \ldots, s), \tag{2}
\]

where \( p_1, \ldots, p_s \) are fixed primes, which do not belong to a determined finite set of primes. We establish a principal possibility of constructing an explicit limit for the integral unknowns \( x, y, z_1, \ldots, z_s \) satisfying (2). Our arguments use Baker's results mentioned above and its \( p \)-adic analogy.

In what follows, \( c \) denotes a positive quantity (not everywhere the same), depending on parameters which are sometimes explicitly indicated and effectively determine \( c \). I. M. Vinogradov's symbol < covers a quantity \( c \) of the indicated type.

**THEOREM.** Let \( f(x, y) \) be an integral binary form of degree three at least, irreducible over the field \( Q \) of rational numbers, let \( A \) be an integer, and let \( p_1, p_2, \ldots, p_s \) be an arbitrary set of odd primes which do not appear in the discriminant of the form \( f(x, y) \) and in the discriminant of the splitting field of the form \( f(x, y) \). Equation (2) has then only a finite number of solutions in integers \( x, y, z_1, \ldots, z_s \), and they all can be effectively determined.

**COROLLARY.** If the assumptions of the theorem are satisfied, then on the curve \( f(x, y) = A \) lie only a finite number of rational points \( (x, y) \) with denominators containing only the primes \( p_1, p_2, \ldots, p_s \), and all such points can be effectively determined.

**LEMMA 1.** Let \( \alpha_1, \ldots, \alpha_n \) be algebraic numbers \( x_1, \ldots, x_n \) rational integers, and assume \( \varepsilon > 0 \). If \( \lambda = x_1 \ln \alpha_1 + \ldots + x_n \ln \alpha_n = 0 \), then

\[
|\lambda| > c^{-1} (\ln x^n)^{n^{-1-\varepsilon}}, \quad x = \max_{i \in \mathbb{N}} |x_i|, \tag{3}
\]

where \( c = c(\alpha_1, \ldots, \alpha_n, \varepsilon) \).

The proof follows directly from Baker's Theorem 3 [5].

**Lemma 2.** Let \( \alpha_1, \ldots, \alpha_n \) be algebraic, and \( x_1, \ldots, x_n \) rational integers; let \( G \) be the field of algebraic numbers containing \( \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \), let \( p \) be a prime unbranched ideal of \( G \), \( (\mathbb{Z}, p) = 1 \) \((i = 1, 2, \ldots, n), \varepsilon > 0. \) Then, if \( \alpha_1^{x_1} \cdots \alpha_n^{x_n} \neq 1 \), we have

\[
\text{ord}_p (1 - x_1^{\alpha_1} \cdots x_n^{\alpha_n}) < \varepsilon (\ln x)^{n-1}, \quad x = \max_{1 \leq i \leq n} |x_i|, 
\]

where \( c = c(p, \alpha_1, \ldots, \alpha_n, \varepsilon) \), \( \text{ord}_p \alpha \) is the exponent of \( p \) in \( \alpha \).

The proof of this lemma is obtained by translation of Baker's arguments [4] into the language of analytic functions in \( p \)-adic domains [7].

**Lemma 3.** Let \( z_1, z_2 \) be complex numbers, \( |z_1| \leq 1, |z_2| \leq 1, z_1 + z_2 = 1, |\ln |z_2|| \geq \delta, 0 < \delta < 1. \) Then \( |\ln |z_1|| = \ln 2/\delta \).

**Proof.** We find

\[
1 - |z_1|| > 1 - |z_2|| = 1 - \exp(-|\ln |z_2||) > 1 - \exp(-\frac{\delta^2}{2}) = \frac{\delta^2}{2} + \frac{\delta^3}{3!} + \cdots > \frac{\delta^2}{2}. 
\]

Hence \( |z_1| = \exp(-|\ln |z_1||) > \frac{\ln 2}{\delta} \).

**Lemma 4.** Let \( A, B, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \) be nonzero algebraic numbers, and \( x_1, \ldots, x_n \) rational integers,

\[
A x_1^{\alpha_1} \cdots x_n^{\alpha_n} + B \beta_1^{\beta_1} \cdots \beta_n^{\beta_n} = 1, \quad \| Ax_1^{\alpha_1} \cdots x_n^{\alpha_n} \| < 1, \quad \| B \beta_1^{\beta_1} \cdots \beta_n^{\beta_n} \| < 1. 
\]

Then, assuming \( x = \max_{1 \leq i \leq n} |x_i| \), we obtain

\[
|z_1| = \exp(-|\ln |z_1||) > \frac{\ln 2}{\delta}. 
\]

**Lemma 5.** Assume that \( G \) is a field of finite degree over \( \mathbb{Q}, A, B, C, \alpha_i, \beta_i, \gamma_i (i = 1, 2, \ldots, s) \) are nonzero integers of the field \( G \); \( \varepsilon, \xi, \eta, \zeta \) \((j = 1, 2, \ldots, k) \) are units of the field \( G \), every ideal \((\gamma_j)\) has a prime unbranched divisor \( p_j \) in the field \( G \), the numbers \( 2, A, B, \alpha_j, \beta_j \) are relatively prime to \( p_j \) \((i, j = 1, 2, \ldots, s), u_1 > 0, \ldots, u_S > 0, v_1, \ldots, v_k \) are rational integers, \( V = \max_{1 \leq i \leq s, 1 \leq j \leq k} (u_i, |v_j|) \) \((1 \leq i \leq s, 1 \leq j \leq k). \) Then the equation

\[
A x_1^{\alpha_1} \cdots x_n^{\alpha_n} + B \beta_1^{\beta_1} \cdots \beta_n^{\beta_n} + \eta_1^{\varepsilon_1} \cdots \eta_k^{\varepsilon_k} = 0 
\]

implies the inequalities

\[
\max_{1 \leq i \leq s} u_i \leq (\ln V)^{s-1}, 
\]