<table>
<thead>
<tr>
<th>Title</th>
<th>Applications of Baker's theory of linear forms in logarithms to exponential diophantine equations (Analytic Number Theory)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Shorey, T.N.</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (1994), 886: 48-60</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1994-09</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/84315">http://hdl.handle.net/2433/84315</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
Applications of Baker's theory of linear forms in logarithms to exponential diophantine equations

T.N. Shorey (Tata Institute, India)

Let \( p_1, \ldots, p_n \) be distinct primes that are not necessarily the first \( n \) primes. We write \( b_1, \ldots, b_n \) for integers which are not all zero. Further we put

\[
\Omega = p_1^{b_1} \cdots p_n^{b_n} - 1.
\]

The fundamental theorem of arithmetic states that \( \Omega \neq 0 \). In fact \( \Omega \) is a non-zero rational number such that

\[
p_1^{\lfloor b_1 \rfloor} \cdots p_n^{\lfloor b_n \rfloor} \Omega
\]

is an integer. Therefore

\[
|\Omega| \geq p_1^{-\lfloor b_1 \rfloor} \cdots p_n^{-\lfloor b_n \rfloor}.
\]

We put

\[
P = \max_{1 \leq i \leq n} p_i, \quad B' = \max_{1 \leq i \leq n} |b_i|, \quad B = \max(B', 2).
\]

Then

\[
|\Omega| \geq P^{-nB}.
\]

This estimate has been improved to

\[
(1) \quad |\Omega| \geq B^{-C_1}
\]

where \( C_1 \) is an effectively computable number depending only on \( n \) and \( P \). This means that \( C_1 \) can be determined explicitly in terms of \( n \) and \( P \). All the constants that will appear in this talk are effectively computable; they can be determined explicitly in terms of the various parameters involved. In particular, the subsequent constants \( C_2, C_3, \ldots, C_{16} \) are effectively computable. For an integer \( \nu \) with \(|\nu| > 1\), we write \( P(\nu) \) and \( \omega(\nu) \) for the greatest prime
factor and the number of distinct prime divisors of \( \nu \), respectively. Further we put \( P(\pm 1) = 1 \) and \( \omega(\pm 1) = 0 \).

The estimate (1) has several applications. For giving an idea how to apply (1), we derive an old result of Størmer [26] that

\[
P(x(x + 1)) \to \infty \text{ effectively, as } x \to \infty.
\]

Let \( P(x(x + 1)) = P \) and we write

\[
x = p_1^{\mu_1} \cdots p_n^{\mu_n}, \quad x + 1 = p_1^{\nu_1} \cdots p_n^{\nu_n}
\]

where \( \mu_1, \ldots, \mu_n, \nu_1, \ldots, \nu_n \) are non-negative integers. Then

\[
1 = x\left(\frac{x + 1}{x} - 1\right) = x(p_1^{\nu_1 - \mu_1} \cdots p_n^{\nu_n - \mu_n} - 1).
\]

We apply (1) for estimating the second factor on the right hand side. For this, we observe that \( n \leq \pi(P) \) where \( \pi(P) \) denotes the number of primes not exceeding \( P \) and for \( 1 \leq i \leq n \),

\[
|\nu_i - \mu_i| \leq \max(\nu_i, \mu_i) \leq \log (x + 1)/\log 2.
\]

Then the estimate (1) implies that

\[
p_1^{\nu_1 - \mu_1} \cdots p_n^{\nu_n - \mu_n} - 1 \geq (\log x)^{-C_2}
\]

where \( C_2 = C_2(P) \) is a number depending only on \( P \). Thus

\[
1 \geq x(\log x)^{-C_2}
\]

which implies that \( x \) is bounded by a number depending only on \( P \). This completes the proof of (2).

For \( P \geq 2 \), we denote by \( S \) the set of all positive integers composed of primes not exceeding \( P \). In fact we have proved above that for all \( x \in S \) and \( y \in S \) with \( x > y \),

\[
x - y \geq x(\log x)^{-C_3}, \quad C_3 = C_3(P).
\]

In particular, for \( k > 0 \), the equation

\[
x - y = k \quad \text{in integers } x \in S, y \in S \text{ with } \gcd(x, y) = 1
\]
implies that \( x < C_4 = C_4(k, p) \). In fact we derive below that

(5) \[ x < C_5 = C_5(P(k), P). \]

Let \( q \) be a prime number dividing \( k \). We observe that either \( x \) or \( y \) is not divisible by \( q \). We prove (5) when \( y \) is not divisible by \( q \) and the proof for the other case \( q \nmid x \) is similar. Then we observe from (4) that

\[ \text{ord}_q(k) = \text{ord}_q \left( \frac{x}{y} - 1 \right). \]

We write

\[ x = p_1^{k_1} \cdots p_n^{k_n}, \quad y = p_1^{\ell_1} \cdots p_n^{\ell_n} \]

where \( k_1, \ldots, k_n, \ell_1, \ldots, \ell_n \) are non-negative integers. Then

(6) \[ \text{ord}_q(k) = \text{ord}_q(p_1^{k_1-\ell_1} \cdots p_n^{k_n-\ell_n} - 1) \leq C_6 \log x \]

where \( C_6 = C_6(q, P) \). The trivial estimate (6) has been sharpened to

(7) \[ \text{ord}_q(k) \leq C_7 \log \log x \]

where \( C_7 = C_7(q, P) \). The inequalities (7) for all prime divisors \( q \) of \( k \) yield

\[ \log k \leq C_8 \log \log x \]

where \( C_8 = C_8(P(k), P) \). On the other hand, we combine (4) and (3) for deriving that

\[ \log k \geq \log x - C_3 \log \log x. \]

Finally we derive (5) from the upper and lower estimate for \( \log k \). The above argument depends on the fact that the contributions from fixed primes in \( k \) is small. This idea on combining the archimedian and non-archimedian valuation is due to Mahler.

We observe that \( \Omega \) is close to 1 if and only if \( \log (p_1^{b_1} \cdots p_n^{b_n}) \) is close to zero. But

\[ \log (p_1^{b_1} \cdots p_n^{b_n}) = b_1 \log p_1 + \cdots + b_n \log p_n \]

is a linear form in logarithms. The estimate (1) is a lower bound for the absolute value of a linear form in logarithms. The estimate (7) can be considered as a \( q \)-adic analogue of (1). These estimates constitute the theory of linear forms in logarithms and \( p \)-adic theory of linear forms in logarithms.
Thus we were giving applications of this theory. The estimate (1) is proved in a more general set up and this is useful for applications. The estimate (1) is contained in the following theorem of Baker which is still enough for most of the applications.

By an algebraic number we mean a complex number that is a root of a non-zero polynomial with rational numbers as coefficients. The height of an algebraic number is defined as the maximum of the absolute values of the coefficients of its minimal polynomial with relatively prime integral coefficients. Let $\alpha_1, \cdots, \alpha_n$ be non-zero algebraic numbers of heights not exceeding $A_1, \cdots, A_n$, respectively, where we assume that $A_j \geq 3$ for $1 \leq j \leq n$. We write $K$ for the field generated over rationals by $\alpha_1, \cdots, \alpha_n$ and $d$ for the degree of $K$ over rationals. We put

$$\Omega = \prod_{j=1}^{n} \log A_j, \quad \Omega' = \Omega / \log A_n.$$  

Then we have

**Theorem (Baker [3]).** There exist absolute constants $C_9$ and $C_{10}$ such that the inequalities

$$0 < |\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| < \exp(-C_9nd)C_{10}^{n} \log \Omega' \log B)$$

have no solution in rational integers $b_1, \cdots, b_n$ of absolute values not exceeding $B(\geq 2)$.

The estimate (1) is due to Fel’dman [9] and Yu [30] proved $p$-adic analogue of the Theorem implying $p$-adic analogue (7) of (1). Let $f(X, Y)$ be a binary (homogeneous) form such that $f(X, 1)$ has at least three distinct roots. For a non-zero integer $k$, Thue [27] proved in 1909 a fundamental theorem that equation

$$f(x, y) = k \quad \text{in integers } x, y$$

has only finitely many solutions. The method of Thue is non-effective; it gives no explicit upper bound on the magnitude of the solutions. Baker [1], by way of his fundamental results in the theory of linear forms in logarithms, established an explicit bound for the magnitude of the solutions of the above
equation known as Thue's equation. Furthermore, Baker [2] applied his results on Thue's equation to give effective versions of the results of Siegel that hyper-elliptic equation

$$y^m = P(x)$$

in integers $x, y$

has only finitely many solutions. Here $m \geq 2$ is an integer and $P(X)$ is a polynomial with integer coefficients such that it has at least two simple roots when $m > 2$ and at least three simple roots when $m = 2$. By way of Mahler's idea described above, the $p-$adic theory of linear forms in logarithms led to $p-$adic analogues of the above results of Baker. Thus it has been possible to show effectively that the above equations have only finitely many solutions in rational numbers with denominators composed of fixed primes. Thus

$$P(f(x, y)) \rightarrow \infty$$

effectively

as $\max(|x|, |y|) \rightarrow \infty$ with $\gcd(x, y) = 1$. This is an effective version, due to Coates [6], of a result of Mahler [10] and this initiated studies on Thue-Mahler equation (see [22, chapter 7]).

The role of the theory of linear forms in logarithms is not confined to giving effective versions of earlier known results. It has proved to be a powerful tool for bounding exponents and their bases as variables in certain diophantine equations. For example, the equations (9), (10), (12), (13) and (14) are exponential diophantine equations. For non-zero integers $A, B, x$ and $y$ with $\max(|x|, |y|) > 1$ satisfying

$$Ax^m + By^m = k,$$

we show that

$$(8) \quad m \leq C_{11} = C_{11}(A, B, k).$$

For the proof of (8), we may assume that $|x| \geq |y|$ which implies that $|x| > 1$. We have

$$|k| = |Ax^m ||(-\frac{B}{A})(\frac{y}{x})^m - 1|.$$

We apply the Theorem with $n = 2, \alpha_1 = -B/A, \alpha_2 = y/x$ and $B = m$ for deriving that

$$|(-\frac{B}{A})(\frac{y}{x})^m - 1| \geq |x|^{-C_{12} \log m}.$$
where $C_{12} = C_{12}(A, B)$. Thus
\[ |k| \geq |x|^{m - C_{12} \log m} \]

which implies (8). The estimate of the Theorem is best possible with respect to $A_n$ and this is crucial for the proof of (8). This feature appears for the first time in a paper of Schinzel [12] settling an old problem on primitive divisors of $A^n - B^n$ in algebraic number fields and a paper of Tijdeman [28] for finding an infinite set $S_1$ of prime numbers satisfying $n_{i+1} - n_i \to \infty$ as $i \to \infty$ where $n_1 < n_2 < \cdots$ is the sequence of all positive integers composed solely of primes from the set $S_1$. By (8), we observe that there are only finitely many possibilities for $m$. For each $m \geq 3$, we apply Baker’s effective version of Thue’s result as stated above to conclude that for non-zero integers $A, B$ and $k$, the equation
\[ Ax^m + By^n = k \text{ in integers } m \geq 3, x, y \text{ with } |x| > 1 \]

implies that
\[ \max(|x|, |y|, m) \leq C_{13} = C_{13}(A, B, k). \]

By proving an algebraic analogue of the above result, Schinzel and Tijdeman [13] showed that for a polynomial $P(X)$ with rational numbers as coefficients and with at least two distinct roots, the equation
\[ y^n = P(x) \quad (x, y \text{ integers, } |y| > 1) \]

implies that $m$ is bounded by a number depending only on $P$. Therefore the above hyper-elliptic equation has only finitely many solutions in integers $x, y, m$ with $m \geq 2, |y| > 1$ under necessary conditions. Furthermore, the solutions $x, y, m$ satisfy $\max(|x|, |y|, m) < C_{14} = C_{14}(P)$. It has been possible to replace $C_{14}$ by an absolute constant when
\[ P(X) = X^n \pm 1 \]

and
\[ P(X) = X(X + 1) \cdots (X + k - 1) \text{ with } k > 1. \]

The first is the case of Catalan equation due to Tijdeman [29]; the equation
\[ x^m - y^n = 1 \text{ in integers } x > 1, y > 1, m > 1, n > 1 \]
has only finitely many solutions and the explicit bounds for the solutions $x,y,m,n$ can be given. The second example is due to Erdős and Selfridge [8]; the product of two or more consecutive positive integers is never a power. In other words, the equation

\[(10) \quad x(x + 1) \cdots (x + k - 1) = y^m \quad \text{in integers} \quad x > 0, y > 0, k > 1, m > 1\]

has no solutions. The proof of Erdős and Selfridge is elementary. The last two examples are equations involving four variables. We give two more. The first is an extension of (9). For integers $A \neq 0, B \neq 0, C$ and $D$, Shorey (see [22, corollary 7.2]) showed that equation

\[(11) \quad Ax^m + By^m = Cx^n + Dy^n\]

has only finitely many solutions in integers $x, y, m, n$ with $|x| \neq |y|, 0 \leq n < m, m > 2, Ax^m \neq Cx^n, Ax^m + By^m \neq 0$ and $(m,n) \neq (4,2)$. It is easy to see that all the above assumptions are necessary. The other example is the equation

\[(12) \quad y^m + 1 = \frac{x^n - 1}{x - 1} \quad \text{in integers} \quad x > 1, y > 1, m > 1, n > 2.\]

Shorey [19], [16] showed that equation (12) has only finitely many solutions. Also, explicit bounds for the magnitudes of the solutions of equations (11) and (12) can be given. Furthermore, Le Maohua has recently shown that equation (12) has no solution. The theory of linear forms in logarithms has been applied to some other equations involving four variables under certain restrictions; for example Fermat’s equation and equations

\[(13) \quad y^m = \frac{x^n - 1}{x - 1} \quad \text{in integers} \quad x > 1, y > 1, m > 1, n > 2,\]

\[(14) \quad \frac{y^m - 1}{y - 1} = \frac{x^n - 1}{x - 1} \quad \text{in integers} \quad x > 1, y > 1, m > 2, n > 2.\]

Shorey and Tijdeman [21] showed that equation (13) has only finitely many solutions whenever $x$ is fixed. Thus, by taking $x = 10$, there are only finitely many powers in integers with all digits equal to one in their decimal expansions. Further Shorey [16] showed that equation (13) has only finitely
many solutions whenever $\omega(n) > m - 2$. Furthermore, Balasubramanian
and Shorey [4] proved that equation (14) has only finitely many solutions
whenever $x$ and $y$ are composed of fixed primes. The equation (14) asks for
positive integers whose all the digits are equal to one with respect to two
distinct bases. Goormaghtigh observed that

$$31 = \frac{2^5 - 1}{2 - 1} = \frac{5^3 - 1}{5 - 1}, \quad 8191 = \frac{2^{13} - 1}{2 - 1} = \frac{90^3 - 1}{90 - 1}.$$  

Shorey [20] showed that these are the only positive integers $N$ with
$\omega(N-1) \leq 5$ such that all the digits of $N$ are equal to one with respect to two
distinct bases. The proof is elementary. Regarding Fermat’s equation, we
refer to Stewart [25] and chapter 11 of [22] which also contains an account of
results on equations (13), (14) and equations of the form $1^k + \cdots + x^k = y^m$.
Algebraic and $p$–adic analogues of the equations considered above have been
worked out (see [22]); in particular an algebraic analogue of (4) leads to
diophantine equations involving terms of linear recurrence sequences (see
[22, chapters 3–4]).

Now we consider an extension of (10). We write $b$ for a positive integer
such that $P(b) \leq k$ and let $d_1, \ldots, d_t$ be distinct integers in $[0, k)$. We consider
the equation

$$(x + d_1) \cdots (x + d_t) = by^m. \tag{15}$$

Since $\{d_1, \ldots, d_t\} = \{0, 1, \ldots, k - 1\}$ if $t = k$, we observe that equation (15)
with $t = k$ and $b = 1$ is equation (10). First we assume that $m > 2$. For
$\varepsilon > 0$, Erdős [7] showed that equation (15) with

$$x > k^m, \quad t \geq k - (1 - \varepsilon)k \frac{\log \log k}{\log k} \tag{16}$$

implies that $k$ is bounded by a number depending only on $\varepsilon$. The assumption
$x > k^m$ is satisfied whenever the left hand side of (15) is divisible by a prime
exceeding $k$. We put

$$\nu_m = \frac{1}{2} \left(1 + \frac{4m^2 - 8m + 7}{2(m - 1)(2m^2 - 5m + 4)} \right).$$

We observe that

$$\nu_3 = \frac{47}{56}, \quad \nu_4 = \frac{45}{64}, \quad \nu_m < 2/3 \text{ for } m \geq 5.$$
Shorey [17] proved that equation (15) with
\begin{equation}
(17) \quad x > k^m, \ t \geq \nu_m k
\end{equation}
implies that $k$ is bounded by an absolute constant. This is a considerable improvement of the result of Erdős mentioned above. If $m$ is sufficiently large, Shorey [15] showed that the assumption (17) can be relaxed considerably to
\[ x > k^m, \ t \geq k^{1/11} + \pi(k) + 2. \]
Apart from the theory of linear forms in logarithms, the proofs of the above results of Shorey depend on irrationality measures of Baker proved by hypergeometric method and the method of Roth - Halberstam on difference between consecutive $\ell$-free integers. In these applications, linear forms in logarithms with $\alpha's$ very close to one occur and it has been shown by the author in [14] that estimates close to best possible can be obtained for such linear forms in logarithms. Next we consider equation (15) with $m = 2$. Shorey [17] applied the theorem of Baker on integral solutions of hyper-elliptic equations mentioned earlier in this article and sieve theoretic arguments for showing that the assertion of Erdős stated in the beginning of this paragraph continues to be valid in this case. Recently, for $\epsilon > 0$, Balasubramanian and Shorey [5] relaxed (16) with $m = 2$ to
\[ x > e^{1-\theta_0+\epsilon F(k)}, \ t \geq \mu_k \]
where
\[ \mu_k = k(1 - \frac{\log \log k}{\log k} + \frac{\log \log \log k}{\log k} + \frac{\theta_0}{\log k}) \]
for some absolute constant $\theta_0$ and $F(k) = k(\log k)/\log \log k$. Fix $\theta_0$. On the other hand, it has been shown in [5] that for $k$ exceeding a number depending only on $\epsilon$ and
\[ x < e^{-1-\gamma-\theta_0-\epsilon F(k)}, \]
there are distinct integers $d_1, \ldots, d_t$ in $[0, k)$ with $t \geq \mu_k$ such that $(x + d_1) \cdots (x + d_t)$ is a square. Here $\gamma$ denotes Euler's constant.
For a positive integer $d$, we consider an extension of (15):
\begin{equation}
(18) \quad (x + d_1 d) \cdots (x + d_t d) = by^m \quad \text{with} \ \gcd (x, d) = 1.
\end{equation}
There is no loss of generality in assuming that $m$ is a prime number. Equation (18) with $d = 1$ is equation (15) which we have already considered. Therefore we suppose that $d \geq 2$. We also assume that the left hand side of equation (18) is divisible by a prime exceeding $k$. If $t = k$, the left hand side of equation (18) is $x(x + d_1) \cdots (x + (k - 1)d_1)$ and we refer to a result of Shorey and Tijdeman [23] that this product is divisible by a prime exceeding $k$ unless $(x, d, k) = (2, 7, 3)$. Marszalek [11] proved that $k$ is bounded by a number depending only on $d$ whenever equation (18) with $t = k$ and $b = 1$ holds. Further, Shorey [18] applied estimates of Győry on the magnitude of integral solutions of Thue - Mahler equation to show that equation (18) with $t = k$ and $m > 2$ implies that $k$ is bounded by a number depending only on $P(d)$.

For $\varepsilon > 0$ and $m = 2$, Shorey and Tijdeman [24] proved that equation (18) with $t = k$ holds. By taking $t = k$ in the preceding two results, we conclude that $k$ is bounded by a number depending only on $\varepsilon$ and $\omega(d)$.
References


School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Bombay 400 005.
INDIA.