On the Arithmetic on Algebraic Curves

K. Mahler

Let $P_1, P_2, \ldots, P_t$ be a finite set of prime numbers, and let $\sum$ be the set of all rational numbers of the form

$$\mp P_1^{a_1} P_2^{a_2} \ldots P_t^{a_t}$$

where the a's run over all integers, positive, negative, or zero. Let further

$$f(x,y) = \sum_{h=0}^{m} \sum_{k=0}^{n} a_{h,k} x^h y^k,$$

$$\text{where } F = \sum_{h=0}^{m} \sum_{k=0}^{n} |a_{h,k}| > 0,$$

be a non-constant polynomial with integral coefficients, irreducible over the rational field. The algebraic curve C defined by $f(x,y) = 0$ may be reducible, however.

Theorem: If there exists an infinite set S of points (x,y) on C for which both x and y belong to $\sum$, then $f(x,y)$ is the sum of exactly two terms.

Proof: For every rational number $x = a/b$, where the integers a,b are relatively prime, write $*x = \max(|a|, |b|)$. It is easily proved that

(1): $\quad *y \leq F(*x)^m, \quad *x \leq F(*y)^n$

for every element (x,y) of S.

If $\min(*x, *y)$ is bounded in S, then $f(x,y)$ is of the form $ax + b$ or $ay + b$, where a and b are integers different from zero. We exclude this case; then both $*x$ and $*y$ tend to infinity when (x,y) runs over S[1]).

---

7) Here and later, it may be necessary to replace S by a suitable infinite subsequence; but, for shortness, we shall not mention this each time.

On, if necessary, replacing x by 1/x, or interchanging x and y, or doing both, we may assume that

(2): $1/|x|$ is bounded for the elements (x,y) of S.

CASE A: $*x \leq |x|^2$ for the elements of S; hence $|x|$ tends to infinity.

The points (x,y) of S lie therefore on an infinite branch of C defined by a convergent series

(3): $y = ax^{p/q} + a_1 x^{(p-1)/q} + a_2 x^{(p-2)/q} + \ldots;$

here x and q are integers satisfying

(4): $q \geq 1, \quad (p,q) = 1,$

and $a \neq 0$, a_1, a_2,.... are real algebraic numbers.

If $a_1 = a_2 = \ldots = 0$, then C is the curve $g(x,y) \equiv y^q - a^q x^p = 0$, a^q is a rational number, and $f(x,y)$ has the asserted form since $g(x,y)$ is irreducible. Let this case be excluded.

Denote by a_r, where $r \geq 1$, the first of the numbers a_1, a_2,.... which does not vanish; further put

(5): $z = x^{-p} y^q, \; A = a^q,$

so that

$$\lim z = A \neq 0$$

when (x,y) runs over S. Also z belongs to Σ, and by (1) and (5)

(6): $$*z \leq (*x)^p\,(*y)^q \leq c_1\,(*x)^{p+mq};$$

here c_1, and similarly c_2, $c_3, \ldots,$ denote positive numbers independent of (x,y).

By (3) and the definition of r, z may be written as a convergent series

(7): $$z = A + A_\nu x^{-\nu/q} + A_{\nu+1}\,x^{-(\nu+1)/q} + \ldots,$$

where, in particular, $A \neq 0$ and $A_r \neq 0$. Hence, for (x,y) in S,

$$0<|z-A| < c_2|x|^{-\nu/q} \longrightarrow 0.$$

Therefore, by the hypothesis $*x \leq |x|^2$ and by (6),

(8): $$0<|z-A| < c_2(*x)^{-\nu/2q} < c_3(*z)^{-\gamma},$$

where $\gamma = \dfrac{\nu}{2q(p+mq)}$,

contrary to a well-known consequence of the Thue-Siegel theorem[2].

---

[2]) If $A \neq 0$ is an algebraic and ε a positive number, then $0<|z-A| < (*z)^{-\varepsilon}$ for at most a finite number of elements z of Σ. See my paper, Proc. Kon. Akad. Amsterdam, 39 (1936), 633-640, 729-737, Satz 3.

CASE B: $*x>|x|^2$, so that $|x|$ is possibly bounded.

Write $x = a/b$ where $(a,b) = 1$, $ab \neq 0$. We have, either $*x = |b|$, or $*x = |a| > a^2/b^2$, whence $b^2>|a|$, $|b|>|a|^{1/2} = (*x)^{1/2}$. Hence in either case,

$$|b| \geq (*x)^{1/2}.$$

On factoring b, let P^s by the greatest power of a prime dividing b; therefore

$$P^s \geq |b|^{1/t}$$

from the definition of $\sum$. We may assume P is the same prime for all elements of S.

Denote by $|u|_P$ the P-adic value of the arbitrary P-adic number u, where the P-adic value is normed by the condition that $P\ |P|_P = 1$. Then

(9): $$|x|_P = P^s \geq |b|^{1/t} \geq (*x)^{1/2t}$$

for the elements (x,y) of S. Hence x, considered as a P-adic number, tends to infinity as (x,y) runs over S. This enables us to proceed just as in Case A, except that we are now dealing with P-adic numbers and values.

Again the points (x,y) of S lie on an infinite branch of C defined by a series (3), except that this series converges now in the P-adic sense and that its coefficients $a \neq 0$, a_1, $a_2, \ldots$ are P-adic algebraic numbers; let (4) still be satisfied.

We exclude once more the case that $a_1 = a_2 = \ldots = 0$, when the assertion is certainly true, and denote again by a_r, where $r \geq 1$, the first non-vanishing coefficient a_1, a_2 .... Define z and A by (5) so that now

$$\lim z = A \neq 0$$

in the P-adic sense as (x,y) runs over S. The inequality (6) remains true, and z may be written in the form (7) where $A \neq 0$ and $A_r \neq 0$,
and where the convergence is in the P-adic sense.

Therefore now, for (x,y) in S,

$$0 < |z-A|_P < c\ |x|_P^{-\nu/q} \longrightarrow 0.$$

By (6) and (9), this implies that

$$0<|z-A|_P< c_4(*x)^{-r/2qt} \leq c_5(*z)^{-S}, \text{ where}$$

$$S = \frac{\nu}{2qt(\rho + mq)}.$$

This inequality, however, contradicts the P-adic analogue to the theorem quoted in the footnote [2]) [3]).

---

[3]) The proof in [2]) can be extended to the P-adic case by using the result of my paper, Math. Annalen, 107 (193[illegible]), 691-730, Satz 1.

By way of example, take $f(x,y) = x + y - 1$. Then the theorem implies that if u,v are integers different from zero which are relatively prime and for which $x^2 + y^2$ tends to infinity, then the greatest prime factor of $uv(u + v)$ also tends to infinity.

In a later paper, I hope to extend the result of this note to arbitrary finite algebraic fields.