DIOPHANTINE PROPERTIES OF THE PERIODS OF THE FERMAT CURVE

Michel Waldschmidt†

Most of this lecture will be devoted to the investigation of the arithmetic nature of the numbers $\beta(a,b)$ for rational numbers a and b. We consider the transcendence, algebraic independence and linear independence of numbers related to the gamma and beta functions, as well as some associated quantitative results.

1. Transcendence of the Values of the Beta Function

After the early result obtained by Siegel [Si] in 1931, Schneider [Sc] proved in 1940 the following theorem.

Theorem 1.1. *Let* a *and* b *be rational numbers. We assume that* a,b *and* $a+b$ *are nonintegral. Then the number* $\beta(a,b)$ *is transcendental.*

Of course, for rational, nonintegral a,b, the number $\beta(a,b)$ vanishes if $a+b$ is either zero or a negative integer, but is transcendental if $a+b$ is a positive integer, because of the transcendence of the number π.

Let us give some ideas of the tools which are involved in the proof of Theorem 1.1. We may assume $a=r/d$, $b=s/d$, where r,s,d are positive integers with

$$d>2,\quad 0<r<d,\quad 0<s<d,\quad r+s\neq d,\quad \gcd(r,s,d)=1\ .$$

Then the number

$$\beta(r/d,s/d) = \int_0^1 t^{(r/d)-1}(1-t)^{(s/d)-1}\,dt$$

appears in the periods of the differential form

$$\eta_{rs} = x^{r-1}y^{s-d}\,dx$$

on the Fermat curve $x^d + y^d = 1$. The η_{rs}, with $r+s<d$, give a basis for the differentials of the first kind, which are defined over $\mathbf{Q}$. We consider the Jacobian $J(d)$ of the Fermat curve. Its period lattice L relative to the chosen basis of holomorphic differentials can be written in $\mathbf{C}^g$, with $g = (d-1)(d-2)/2$,

$$L = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_{2g} \quad ,$$

where one coordinate of ω_j, say the first one, is of the form

$$\omega_{1j} = \alpha_j \beta(r/d, s/d) \quad ,$$

and α_j is an algebraic number (in the field $\mathbf{Q}(\zeta)$ of d-th roots of unity). These facts are well-known. Recent references on this subject are [G], [K], [K-R], [L4], [La], [R], [We].

For the proof of Theorem 1.1, let us assume first $r+s<d$. It is clearly sufficient to prove that at least one of the $2g$ numbers ω_{1j}, $(1 \leqslant j \leqslant 2g)$ is transcendental. Indeed, this fact will hold for any abelian variety defined over the field $\bar{\mathbf{Q}}$ of algebraic numbers (see Corollary 1.3 below). We will deduce this statement from the following general result [W2] (théorème 5.2.1).

Main Theorem 1.2. *Let* G *be a commutative connected algebraic group which is defined over* $\bar{\mathbf{Q}}$, $\varphi:\mathbf{C}^n \to G(\mathbf{C})$ *an analytic homomorphism, and* $u_1,\ldots,u_n$ *a basis of* $\mathbf{C}^n$*, such that* $\varphi(u_j) \in G(\bar{\mathbf{Q}})$, $(1 \leqslant j \leqslant n)$. *We assume that the tangent linear map* $\mathrm{Lie}\,\varphi:\mathbf{C}^n \to T_G(\mathbf{C})$ *is defined over* $\bar{\mathbf{Q}}$. *Then* $\varphi(\mathbf{C}^n)$ *is contained in an algebraic subgroup of* G *of dimension at most* n.

This Theorem 1.2 has been proved by S. Lang when G is either an abelian variety, or a linear group variety [L1] Chap. IV §4 Th.2. More generally, Lang's proof applies whenever the exponential map of G can be represented by meromorphic functions of finite order (see [L1] Chap. III §4 Th.4 for the case $n=1$), and it has been proved by Serre (in Appendix 1 of [W2]) that this assumption is always fulfilled.

We now deduce from Theorem 1.2 the following corollary, due to Schneider [Sc].

Corollary 1.3. *Let* A *be an abelian variety, of dimension* g, *defined over* $\bar{\mathbf{Q}}$. *We choose a basis, defined over* $\bar{\mathbf{Q}}$, *of the tangent space at the origin* $T_A(\mathbf{C})$ *of* A. *Let* $\omega_1,\ldots,\omega_g$ *be* **C**-*linearly independent periods of the exponential map* $\exp_A\colon T_A(\mathbf{C})\to A(\mathbf{C})$ *of* A, *and let* ω_{ij}, $(1\leq i\leq g)$ *be the coordinates of* ω_j, $(1\leq j\leq g)$, *with respect to the chosen basis. Then in the* $g\times g$ *matrix*

$$(\omega_1,\ldots,\omega_g) = \begin{pmatrix} \omega_{11} & \cdots & \omega_{1g} \\ \cdots & \cdots & \cdots \\ \omega_{g1} & \cdots & \omega_{gg} \end{pmatrix} ,$$

on each row there is at least one transcendental number.

For the proof of Corollary 1.3, we identify $\mathbf{C}^g$ with $T_A(\mathbf{C})$, thanks to our basis, and if we are interested with the first row, say, then we consider the analytic homomorphism $\mathbf{C}^g\to\mathbf{C}\times A(\mathbf{C})$ given by $z\mapsto(z_1,\exp_A z)$.

Hence the Main Theorem 1.2 implies Corollary 1.3, and therefore yields the transcendence of $\beta(r/d,s/d)$ for $r+s<d$.

Next consider the case $r+s>d$. Now η_{rs} is of the second kind, and to complete the proof of Theorem 1.1, Schneider [Sc] argues as follows. Consider again an abelian variety as in 1.3, with g periods $\omega_1,\ldots,\omega_g$ which are **C**-linearly independent. Let η be a differential form of the second kind on A, which is defined over $\bar{\mathbf{Q}}$, and is not the sum of a differential of the first kind and an exact differential. We view η as a **R**-linear map from $T_A(\mathbf{C})$ into **C**. Then one at least of the g numbers

$$\eta(\omega_j)\ ,\qquad (1\leq j\leq g)$$

is transcendental.

We deduce this result from Theorem 1.2 by considering the algebraic group G, extension of A by the additive group $\mathbf{G}_a$, which is associated with η. We write $T_G(\mathbf{C})=T_A(\mathbf{C})\oplus\mathbf{C}$, and we consider the analytic homomorphism $\varphi\colon T_A(\mathbf{C})\to G(\mathbf{C})$ given by $\varphi(z)=\exp_G(z,0)$. From Theorem 1.2 we deduce that the image by φ of $\mathbf{Z}\omega_1+\cdots+\mathbf{Z}\omega_g$ is not contained in $G(\bar{\mathbf{Q}})$. In a projective embedding of G into some $\mathbf{P}_N$, the coordinates of φ are given by theta functions (corresponding to A) and by a quasi-periodic function K:

$$K(z+\omega) = K(z)+\eta(\omega) .$$

The fact that one of $\varphi(\omega_j)$ is not in $G(\bar{\mathbf{Q}})$ means that one of $\eta(\omega_j)$ is not in $\bar{\mathbf{Q}}$. This completes the proof of Theorem 1.1 as a consequence of the Main Theorem 1.2.

As pointed out in [B-M2] (see also [B3]), a further consequence of Schneider's results [Sc] is the linear independence over $\bar{\mathbf{Q}}$ of the three numbers

$$1, \quad \beta(a,b), \quad \pi/\beta(a,b) \qquad ,$$

algebraic
for any positive real numbers a, b with a, b and $a+b$ not in $\mathbf{Z}$.

Let us come back to the matrix $(\omega_1,\ldots,\omega_g)$ in Corollary 1.3. The following result is due to Lang [L1] Chap. III §4 Cor. of Th.3.

Corollary 1.4. *With the same notations as in Corollary 1.3, on each column of the matrix there is at least one transcendental number.*

Consider, say, the first column, whose components are the coordinates of ω_1, and apply Theorem 1.2 to the analytic homomorphism $\varphi:\mathbf{C}\to\mathbf{C}\times A(\mathbf{C})$ given by $\varphi(t)=(t,\exp_A(t\omega_1))$, with $n=1$, $u_1=1$. We deduce $\omega_1\notin\bar{\mathbf{Q}}^g$.

For an abelian variety with sufficiently many endomorphisms, it is possible to get sharper results, as shown by Lang [L2] and Masser [M1] (cf. [W2] Chap. 6).

Corollary 1.5. *With the notations of Corollary 1.3, assume* A *is simple of* C.M. *type, i.e., that* $(\mathrm{End}\,A)\otimes_{\mathbf{Z}}\mathbf{Q}$ *is a field* F *of degree* 2g *over* $\mathbf{Q}$. *Choose a basis of* $T_A(\mathbf{C})$ *consisting of eigenvectors for the action of* F. *Then each entry* ω_{ij} *of our matrix is a transcendental number.*

In connection with Theorem 1.1, it should be mentioned that the Jacobian $J(d)$ of the Fermat curve $x^d+y^d=1$ splits into a product of abelian varieties, each of dimension $\Phi(d)/2$ (where Φ is the Euler characteristic), defined over $\mathbf{Q}(\zeta)$, and with complex multiplication by $\mathbf{Z}[\zeta]$ (see [K], [K-R], [R] and [La]).

We deduce Corollary 1.5 from Theorem 1.2 in two steps. Assume first $\omega_{11}\in\bar{\mathbf{Q}}$, and $\omega_{i1}\neq 0$ for $1\leqslant i\leqslant g$. Then apply Theorem 1.2 to the analytic homomorphism $z\mapsto(z_1,\exp_A z)$ from $\mathbf{C}^g$ into $\mathbf{C}\times A(\mathbf{C})$; since the action of F on the point ω_1 gives rise to g elements $\mathbf{C}$-linearly independent (in fact to a lattice in $T_A(\mathbf{C})$), we get a contradiction. Therefore it remains to prove that no coordinate of ω_1, say, can vanish. Assume $\omega_{11} = \ldots = \omega_{i1} = 0$, while $\omega_{i+1,1}, \ldots, \omega_{g1}$ do not vanish. Then apply Theorem 1.2 to the map $\mathbf{C}^g \to \mathbf{C} \times A(\mathbf{C})$ which sends z to $(z_1, \exp_A(0,\ldots,0,z_{i+1},\ldots,z_g))$, and consider the images of the point $(1,\ldots,1,\omega_{i+1,1},\ldots,\omega_{g1})$ through the action of F. Alternative arguments for this second step are given in a lecture by D. Bertrand (Queen's papers in *Pure and Applied Math.* 54 (1980), 316).

Further consequences of the Main Theorem 1.2 are described in [W2] Chap. 3 and Chap. 5.

Later, Bertrand and Masser obtained the unexpected result that Baker's theorem on the nonvanishing of linear forms in logarithms of algebraic numbers can also be deduced from Theorem 1.2. They take for G a linear algebraic group, and therefore this special case of the Main Theorem was already known by Lang before Baker's proof in 1966! An important consequence of this alternative approach is that it enabled Bertrand and Masser [B-M1] to prove the elliptic analog of Baker's theorem (only the case of complex multiplication was previously known, due to Masser). They extended their method to certain abelian varieties [B-M2], [B2], [B3].

By means of the method of Bertrand and Masser, M. Laurent derived some further transcendence results on the beta function; for instance he proved the transcendence of the number

$$\beta(1/10,3/20)/\beta(1/10,13/20).$$

It seems very likely that this method is not exhausted.

2. Diophantine Approximation

The problem of the diophantine approximation of the number $\beta(a,b)$ was investigated for the first time only in 1979, by M. Laurent [La], who proved the following rather sharp estimate.

Theorem 2.1. *Let* a *and* b *be rational numbers, with* a, b, $a+b$ *not in* $\mathbf{Z}$. *Let* d *be a common denominator of* a *and* b. *Define* $n = \max(1, \Phi(d)/2)$. *Then there exists an effectively computable number* $C > 0$ *such that, if* ξ *is any algebraic number of degree* $\leqslant D$ *and height* $\leqslant H$ *(with* $H \geqslant e^e$*),*

$$|\beta(a,b) - \xi| \geqslant \exp\{-CD^n T(\log T)^n\},$$

where $T = \log H + D \log D$.

Here, the height of ξ is the maximum of the absolute values of the coefficients of the minimal polynomial of ξ over $\mathbf{Z}$.

According to a claim of Chudnovsky [Ch2], it is possible to remove the factor $(\log T)^n$ in the special case where H is sufficiently large with respect to D. In particular, for $D=1$, this means

$$\left|\beta(a,b) - \frac{p}{q}\right| > q^{-C'}$$

for $p/q \in \mathbf{Q}$, $q>0$, where $C'>0$ depends only on a and b. Similar results are announced in [Ch2] for the numbers $\Gamma(1/4)$ and $\Gamma(1/3)$.

3. Algebraic Independence

The following result has been proved by G.V. Chudnovsky [Ch1].

Theorem 3.1. *Let* $\wp$ *be a Weierstrass elliptic function with algebraic invariants* g_2, g_3, *let* ζ *be the corresponding Weierstrass zeta function,* ω *be a non-zero period of* $\wp$, *and* $\eta = \zeta(z+\omega) - \zeta(z)$. *Then the two numbers*

$$\pi/\omega, \quad \eta/\omega$$

are algebraically independent.

In the case of complex multiplication, one deduces the algebraic independence of the two numbers π and ω.

For $d=3$, 4 or 6, we have $\Phi(d)=2$, and therefore the abelian variety $J(d)$ splits into a product of elliptic curves of C.M. type. These elliptic curves are $y^2 = 4x^3 - 4x$ (for $d=4$) and $y^2 = 4x^3 - 4$ (for $d=3$ or $d=6$). For the first one, a pair (ω_1, ω_2) of fundamental periods is given by (see [Co2], [B1], [M2], [W1], [W2]):

$$\omega_1 = i\omega_2, \quad \omega_2 = 2\int_1^\infty \frac{dx}{\sqrt{4x^3-4x}} = \frac{1}{2}\,\beta\left(\frac{1}{4},\frac{1}{2}\right) = \Gamma(1/4)^2/(8\pi)^{1/2} \quad .$$

For the second one, a pair of fundamental periods is (do *not* see [Co2] p. 79, [B1] p. 02, [M2] p. 231, *neither* [W2] p. 75)

$$\omega_1 = j\omega_2, \quad \omega_2 = 2\int_1^\infty \frac{dx}{\sqrt{4x^3-4}} = \frac{1}{3}\,\beta\left(\frac{1}{6},\frac{1}{2}\right) = \Gamma(1/3)^3/(2^{4/3}\pi) \quad .$$

Therefore the two numbers $\Gamma(1/4)$ and π are algebraically independent, and also the two numbers $\Gamma(1/3)$ and π are algebraically independent.

In the higher dimensional case, for an abelian variety of dimension g defined over $\mathbf{Q}$, if $(\omega_1,\ldots,\omega_{2g})$ is a basis of the lattice of periods, and $(\omega_{ij})_{1\leqslant i\leqslant g}$ are the coordinates of ω_j, $(1\leqslant j\leqslant 2g)$ with respect to a basis of the tangent space defined over $\bar{\mathbf{Q}}$, and finally if η_{ij} are the corresponding quasi-periods, then two at least of the $4g^2$ numbers

$$\omega_{ij},\quad \eta_{ij}, \qquad\qquad (1\leqslant i\leqslant g,\quad 1\leqslant j\leqslant 2g)$$

are algebraically independent (cf. [Ch1]; in fact D.W. Masser--private communication--proved that it is enough to take the η_{ij} only for $g+1$ values of j). For instance two at least of the three numbers $\Gamma(1/5)$, $\Gamma(2/5)$, π are algebraically independent.

For further comments on this topic, we refer to [Ch1], [M3], [B-W], and also [L3] for the conjecture of Rohrlich.

4. Linear Independence

We discussed already several problems of linear independence at the end of the first section, arising from the work of Bertrand and Masser. Here is a further statement, due to Masser [M3] (see his article in [B-W]), who applied a general result of his (using Baker's method) on quasi-periods of abelian varieties of dimension 2 to the Jacobian of the curve $y^2+x^6-x=0$ which is a simple factor of $J(5)$.

Theorem 4.1. *As* r,s *run over all positive integers, the numbers* $\beta(r/5,s/5)$ *span a vector space of dimension* 6 *over the field of algebraic numbers.*

5. Conclusion

A very recent development of the subject is "a version of Theorem 1.2 in which the map φ is not necessarily normalized with respect to the derivative, but which allows a subgroup with sufficiently many independent points over the rationals" [L1] p. 39. It turns out that the condition of equidistribution of the linear combinations of the log vectors of algebraic points with integer coefficients, mentioned in [L1] p. 44, involves merely the "generalized Dirichlet exponent" introduced in [W2]. Therefore it is easy to check that such combinations satisfy the equidistribution property.

This approach involves a generalization of Schneider's method to several variables. It gives a third way (after Baker and Bertrand-Masser) of proving Baker's theorem, and also Masser's elliptic analog for the C.M. case. Moreover it yields new lower bounds for linear forms (the elliptic case has been worked out by Yu Kunrui).

The main tool for Schneider's method in several variables is a "zero estimate" due to Masser and Wüstholz, which replaces the conjectural Schwarz lemma of [W2]. In other circumstances, this zero estimate plays the role of the algebraic arguments which were introduced in the theory of transcendental numbers by J. Coates [Co1] in 1970, and subsequently used in most papers dealing with Baker's method.

In connection with FLT, let us quote the following sentence from [M1] III, p. 564: "An immediate corollary, more curious than useful, is that positive integers x,y,z satisfying Fermat's equation $x^p + y^p = z^p$ are approximately equal in the sense that if λ,μ are any two of $\log x$, $\log y$, or $\log z$ we have

$$\mu = \lambda + O(\lambda^{\varepsilon})$$

for any $\varepsilon > 0$." Masser has pointed out to me that one can now take

$$\mu = \lambda + O(\log\lambda(\log\log\lambda)^{C})$$

for $C = C(g)$ (cf. Masser's paper in *Invent. Math.* 45 (1978), pp. 61-82).

For a p-adic analog of this result, see D. Bertrand and Y. Flicker, *Acta Arith.* 38 (1980), pp. 47-61.

Finally, we notice that FLT is equivalent to a statement from the theory of irrational numbers: for rational x, $0 < x < 1$, and integer d, $d \geqslant 3$, the number $(1 - x^d)^{1/d}$ is irrational.

Transcendence methods have already been applied to this kind of problem. For the last ten years, there has been some works by Schneider, Bundschuh, Sprindzuk and Bombieri on the rational values of algebraic functions, and these can be viewed as initiated by the fundamental paper of Siegel in 1929 on integer points on curves and G-functions.

References

[B1] D. Bertrand. "Transcendance de valeurs de la fonction gamma," Sém. Delange-Pisot-Poitou (Groupe d'Etude de Théorie des Nombres), 17è année, 1975/76, n°G8, 5 p.

[B2] D. Bertrand. "Variétés abéliennes et formes linéaires d'intégrales elliptiques," Sém. Théorie des Nombres Paris 1979-80 (Sém. Delange-Pisot-Poitou), Birkhäuser, Ser. *Progress in Math.* vol. 12 (1981), pp. 15-27.

[B3] D. Bertrand. "Abelian Functions and Transcendence," Journées arithmétiques, Exeter, Avril 1980, Cambridge Univ. Press.

[B-M1] D. Bertrand and D.W. Masser. "Linear Forms in Elliptic Integrals," *Invent. Math.* 58 (1980), 283-288.

[B-M2] D. Bertrand et D.W. Masser. "Formes linéaires d'intégrales abéliennes," *C.R. Acad. Sc. Paris*, Sér. A, 290 (1980), 725-227.

[B-W] D. Bertrand et M. Waldschmidt (éditeurs). "Fonctions abéliennes et nombres transcendants," Mémoire Soc. Math. France, Nouvelle Série N°2, 1980.

[Ch1] G.V. Chudnovsky. "Algebraic Independence of Values of Exponential and Elliptic Functions," *Proc. Intern. Cong. Math.*, Helsinki, 1978, 339-350.

[Ch2] G.V. Chudnovsky. "Sur la nature de la transcendance de nombres dépendant d'équations différentielles de type Fuchsien," *C.R. Acad. Sc. Paris*, Sér. A., 291 (1980), 485-487.

[Co1] J. Coates. "An Application of the Division Theory of Elliptic Functions to Diophantine Approximation," *Invent. Math.* 11 (1970), 167-182.

[Co2] J. Coates. "Linear Relations between $2\pi i$ and the Periods of Two Elliptic Curves," in *Diophantine Approximation and its Applications*, ed. Ch. Osgood, Academic Press, 1973, 77-99.

[G] B. Gross. "On the Periods of Abelian Integrals and a Formula of Chowla and Selberg," *Invent. Math.* 45 (1978), 193-208.

[K] N. Koblitz. "Gamma Function Identities and Elliptic Differentials on Fermat Curves," *Duke Math. J.* 45 (1978), 87-99.

[K-R] N. Koblitz and D. Rohrlich. "Simple Factors in the Jacobian of a Fermat Curve," *Can. J. Math.* 30 (1978), 1183-1205.

[L1] S. Lang. *Introduction to Transcendental Numbers*. Addison Wesley, 1966.

[L2] S. Lang. "Diophantine Approximation on Abelian Varieties with Complex Multiplication," *Advances in Math.* 17 (1975), 281-336.

[L3] S. Lang. "Relations de distributions et exemples classiques," Sém. Delange-Pisot-Poitou (Théorie des Nombres), 19è année, 1977/78, n°40, 6p.

[L4] S. Lang. "Complex Multiplication,"

[La] M. Laurent. "Approximation diophantienne de valeurs de la fonction Beta aux points rationnels," Ann. Fac. Sc. Toulouse, vol. 11 (1980), 53-65.

[M1] D.W. Masser. "Linear Forms in Algebraic Points of Abelian Functions," I, *MPCPS* 77 (1975), 499-513; II, *id.* 79 (1976), 55-70; III, *Proc. London Math. Soc.* 33 (1976), 549-564.

[M2] D.W. Masser. "The Transcendence of Definite Integrals of Algebraic Functions," Soc. Math. France, *Astérisque* 41-42 (1977), 231-238.

[M3] D.W. Masser. "Some Recent Results in Transcendence Theory," Soc. Math. France, *Astérisque* 61 (1979), 145-154.

[R] D. Rohrlich. "The Periods of the Fermat Curve (Appendix to [GJ)," *Invent. Math.* 45 (1978), 208-211.

[Sc] Th. Schneider. "Zur Theorie der abelschen Funktionen und Integrale," *J. reine angew. Math.* 183 (1941), 110-128.

[Si] C.L. Siegel. "Über die Perioden elliptischer Funktionen," *J. reine angew. Math.* 167 (1932), 62-69.

[W1] M. Waldschmidt. "Les travaux de G.V. Chudnovsky sur les nombres transcendants," Sém. Bourbaki, 28è année, 1975/76, n°488, Springer Verlag, *Lecture Notes in Math.* 567 (1977), 274-292.

[W2] M. Waldschmidt. "Nombres transcendants et groupes algébriques," Soc. Math. France, *Astérisque* 69-70, 1979.

[We] A. Weil. "Sur les periodes des intégrales abéliennes," *Comm. Pure Appl. Math.* 29 (1976), 813-819.

Institut Henri Poincaré
11, rue P. et M. Curie
75231 Paris CEDEX 05
France