On Certain Plane Curves with Many Integral Points

Fernando Rodriguez Villegas and José Felipe Voloch

CONTENTS

We define a sequence of polynomials $P_d \in \mathbb{Z}[x, y]$, such that P_d is absolutely irreducible, of degree d, has low height, and has at least $d^2 + 2d + 3$ integral solutions to $P_d(x, y) = 0$. We know of no other nontrivial family of polynomials of increasing degree with as many integral solutions in terms of their degree.

1. INTRODUCTION

In the course of another investigation (briefly described in the last section of this paper) we came across a sequence of polynomials $P_d \in \mathbb{Z}[x, y]$ such that P_d is absolutely irreducible, of degree d, has low height, and has at least d^2+2d+3 integral solutions to $P_d(x, y) = 0$. We know of no other family of polynomials of increasing degree with as many integral solutions in terms of their degree, except of course those with infinitely many rational points.

Siegel's theorem [Siegel 1929] implies that these polynomials have finitely many integral zeros, since their homogeneous part of highest degree has distinct roots. Siegel [1929, § 7] speculated whether there is a bound for the number of integral zeros of a polynomial as a function of the number of nonzero coefficients, provided it has only finitely many zeros. This is still very much of an open problem, but Caporaso, Harris, and Mazur [Caporaso et al. 1997] have shown that a similar statement for rational points on curves (with the genus replacing the number of coefficients) would follow from a conjecture of Lang. Abramovich [1997] proved an analogue of the result of [Caporaso et al. 1997] for integral points on elliptic curves. See also [Abramovich and Voloch 1996].

A polynomial in two variables and degree d has $N = \binom{d+2}{2}$ coefficients, so, given points (x_1, y_1), …, (x_{N-1}, y_{N-1}), one can find a nonzero polynomial that vanishes on these points. If these points have integer coordinates of absolute value at most H, then such a polynomial can be chosen with integer coefficients of absolute value at most $(NH^d)^N$,

1058-6458/1999 $0.50 per page

by a straightforward application of Siegel's lemma. We can choose $H = N/2$, for instance, and it will turn out that our polynomials P_d have slightly lower height and twice as many points as this construction gives. If we are unlucky, the polynomial obtained is not absolutely irreducible. A slightly better construction, suggested by Ed Schaffer, is to take a polynomial of the shape $(x-x_1)\cdots(x-x_d)+\alpha(y-y_1)\cdots(y-y_d)$; such a polynomial vanishes on the d^2 points (x_i, y_j) for $i, j = 1, \dots, d$, is irreducible for most choices of α and has height at most $|\alpha| H^d$. Our polynomials P_d have larger height but more points.

We have checked that $P_d = 0$ defines a smooth projective curve for $d = 1, 2, \dots, 25$. We do not know whether this is true in general, though it is very likely. Also, we can prove the existence of certain points on the curve, but numerical experimentation shows that they may contain a few more. We present the data in Section 4.

2. DEFINITION OF THE POLYNOMIALS AND MAIN RESULT

Let $T_k \in \mathbb{Z}[x, y]$ be defined recursively by

$$\begin{aligned} &T_0 = 1, \quad T_1 = y, \\ &T_{k+1} = yT_k + k(x+k-1)T_{k-1}, \quad k \in \mathbb{N}. \end{aligned} \tag{2–1}$$

The first few polynomials are

$$T_2 = x + y^2,$$

$$T_3 = 3yx + y^3 + 2y,$$

$$T_4 = 3x^2 + 6y^2x + 6x + y^4 + 8y^2,$$

$$T_5 = 15yx^2 + 10y^3x + 50yx + y^5 + 20y^3 + 24y,$$

$$T_6 = 15x^3 + 45y^2x^2 + 90x^2 + 15y^4x + 210y^2x + 120x + y^6 + 40y^4 + 184y^2.$$

From the recursion it follows easily that

$$T_k(x, -y) = (-1)^k T_k(x, y), \quad k \in \mathbb{N}.$$

Hence, for $k = 2d$ with $d \in \mathbb{N}$, we have $T_k(x, y) = P_d(-x, y^2)$ with $P_d \in \mathbb{Z}[x, y]$.

We will use the following notation: given a polynomial

$$H = \sum_{m,n} a_{m,n} x^m y^n \quad \in \mathbb{C}[x, y],$$

we set

$$\|H\|_1 = \sum_{m,n} |a_{m,n}|.$$

We will prove the following.

Theorem 2.1. *Let $d \in \mathbb{N}$ and P_d be the polynomial defined above. Then*:

(a) *P_d has degree d.*
(b) *P_d is absolutely irreducible.*
(c) *The coefficients of $P_d(-x, y)$ are relatively prime nonnegative integers.*
(d) $\|P_d\|_1 = (2d)!$.
(e) *P_d vanishes at the $d^2 + 2d + 3$ integral points*
  I. $(n, 0)$, $(n, 2^2)$, $(n, 4^2)$, $\dots$, (n, n^2), *for* $0 \le n \le 2d-1$, *n even;*
  II. $(n, 1^2)$, $(n, 3^2)$, $(n, 5^2)$, $\dots$, (n, n^2), *for* $0 \le n \le 2d-1$, *n odd;*
  III. $(4d, 2^2)$, $(4d, 6^2)$, $(4d, 10^2)$, $\dots$, $(4d, 4(2d-1)^2)$;
  IV. $(8d+1, 3^2)$, $(2d-4, -6d+4)$, $(2d-3, -2d+1)$.

Note that P_d and P_{d+1} intersect in exactly $d(d+1)$ of these points.

3. THE PROOF

Fix x, y and consider the generating function

$$F(\lambda) = \sum_{k=0}^{\infty} \frac{T_k}{(x)_k} \frac{\lambda^k}{k!},$$

where $(z)_0 = 1$ and

$$(z)_k = z(z+1)\cdots(z+k-1), \quad k \in \mathbb{N}.$$

It is not hard to see that the recursion defining T_k implies that F satisfies the differential equation

$$\lambda \frac{d^2F}{d\lambda^2} + x\frac{dF}{d\lambda} - (\lambda + y)F = 0.$$

To get a formula for T_k, consider $G(\lambda) = e^{\lambda}F(\lambda)$. A calculation shows that G satisfies the differential equation

$$\lambda \frac{d^2G}{d\lambda^2} + (x - 2\lambda)\frac{dG}{d\lambda} - (x + y)G = 0.$$

It follows that

$$G(\lambda) = \Phi\bigl(\tfrac{1}{2}(x+y),\, x,\, 2\lambda\bigr),$$

where Φ is the confluent hypergeometric function; see, for example, [Lebedev 1965, § 9.9].

If we write

$$G(\lambda) = \sum_{k=0}^{\infty} \frac{S_k}{(x)_k} \frac{\lambda^k}{k!},$$

the differential equation implies that

$$S_{k+1} = (y + x + 2k)S_k, \quad k \in \mathbb{N}.$$

Therefore,

$$S_k = (y+x)(y+x+2)\cdots(y+x+2k-2),$$

from which we obtain

$$T_k = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} \times (x+y)(x+y+2)\cdots(x+y+2j-2) \times (x+j)(x+j+1)\cdots(x+k-1). \quad (3\text{–}1)$$

We now may see why P_d vanishes at the points I and II of the theorem. The principle is based on the following self-proving lemma; we leave the details to the reader.

Lemma 3.1. *Let $x_1, \dots, x_n$ and $y_1, \dots, y_n$ be two sets of n elements of a field K. Let $\varphi_0 = \psi_0 = 1$ and define*

$$\varphi_\nu(x) = (x - x_1)(x - x_2)\cdots(x - x_\nu) \in K[x],$$
$$\psi_\nu(y) = (y - y_1)(y - y_2)\cdots(y - y_\nu) \in K[y],$$

where $1 \le \nu \le n$ and x, y are indeterminates. Then any linear combination

$$\sum_{\nu=0}^{n} \alpha_\nu\, \varphi_\nu(x)\, \psi_{n-\nu}(y) \in K[x, y],$$

with $\alpha_\nu \in K$ for all ν, has degree at most n and vanishes at (x_μ, y_ν) for all $1 \le \mu \le \nu \le n$.

Remark 3.2. Don Zagier suggested to us a simpler way to study the properties of the polynomials T_k. One may *define* the polynomials by means of the generating series

$$H(\lambda) = (1-\lambda)^x (1+\lambda)^y = \sum_{k=0}^{\infty} T_k(-x-y, -x+y)\frac{\lambda^k}{k!},$$

which satisfies the differential equation

$$\frac{dH/d\lambda}{H} = -\frac{x}{(1-t)} + \frac{y}{(1+t)},$$

giving the recursion (2–1). As an example of this approach, P_d clearly vanishes at the points I and II of the theorem, since H is a polynomial of degree $x + y$, for $x, y \in \mathbb{N}$.

It is clear from the recursion (2–1) that T_k has degree k, that the coefficients of T_k are nonnegative integers and that the coefficient of y^k is 1. This proves parts (a) and (c) of the theorem. To prove part (d), let $c_k = T_k(1, 1)$. Note that $c_k = \|T_k\|_1$ since the coefficients of T_k are nonnegative. From the recursion we have

$$c_0 = 1, \quad c_1 = 1,$$
$$c_{k+1} = c_k + k^2 c_{k-1}, \quad k \in \mathbb{N}.$$

It follows easily that $c_k = k!$, hence

$$\|T_k\|_1 = k!\,, \quad k \in \mathbb{N}.$$

We remark that (3–1) implies that

$$\frac{T_k(m, n)}{k!} \in \mathbb{Z}, \quad \text{for all } m, n \in \mathbb{Z}.$$

Let $\widetilde{T}_k = z^k T_k(x/z^2, y/z)$. Then $\widetilde{T}_k$ is isobaric of weight k, if we assign x, y, and z weights 2, 1, and 1. These polynomials satisfy the recursion

$$\widetilde{T}_0 = 1, \quad \widetilde{T}_1 = y,$$
$$\widetilde{T}_{k+1} = y\widetilde{T}_k + k\big(x + z^2(k-1)\big)\widetilde{T}_{k-1}, \quad k \in \mathbb{N}.$$

Now set $R_k = \widetilde{T}_k(1, t, 0)$, the leading terms of $\widetilde{T}_k$ at infinity. Then

$$R_0 = 1, \quad R_1 = t,$$
$$R_{k+1} = tR_k - kR_{k-1}, \quad k \in \mathbb{N}.$$

It follows that $R_k(t) = 2^{-k/2} H_k(t/\sqrt{2})$, where H_k is the classical Hermite polynomial; see, for example, [Lebedev 1965, § 4.9]. More precisely,

$$R_k(t) = z^k T(1/z^2, t/z)\big|_{z=0} = k! \sum_{j=0}^{[k/2]} \frac{(-1)^j}{j!\,(k-2j)!\,2^j}\, t^{k-2j}.$$

It is interesting that the discriminant can be computed explicitly as

$$\operatorname{disc} R_k = \prod_{j=1}^{k} j^j,$$

but we only need to know that it is nonzero.

Lemma 3.3. *Let K be a perfect field and $\overline{K}$ an algebraic closure of K. Let $P \in K[x, y, z]$ be a homogeneous polynomial of degree d. Suppose that $P(t, 1, 0) \in K[t]$ also has degree d, is irreducible over K and $P(x, y, z) = 0$ has more than $d^2/4$ projective solutions over K. Then P is irreducible over $\overline{K}$.*

Proof. Since $P(t, 1, 0)$ has degree d and is irreducible over K it follows that $P(x, y, z)$ is also irreducible over K. Suppose P is not absolutely irreducible. Then, $P = \prod_\sigma Q^\sigma$, where Q is an irreducible factor of P over $\overline{K}$ of degree $e \le d/2$ and σ runs through the embeddings of the field of definition of Q into $\overline{K}$. Any K-rational point of $P = 0$ is a rational point of $Q^\sigma = 0$ for every σ. Since the Q^σ's are all distinct, Bezout's theorem implies that the number of K-rational points of $P = 0$ is bounded by $e^2 \le d^2/4$, a contradiction. ∎

According to Schur [1931], the polynomials R_k for k even and R_k/t for k odd are irreducible over $\mathbb{Q}$. Hence, the above lemma applies and we deduce part (b) of the theorem.

Next, for $p > 2$ a prime number, we consider the recursion defining T_k modulo p. It turns out to have a very simple structure. First, from (3–1) and

$$\prod_{j=0}^{p-1}(x-j) \equiv x^p - x \bmod p$$

it follows that

$$T_p \equiv y^p - y \bmod p, \quad p > 2, \quad p \text{ prime}.$$

Also, from (2–1) it follows easily that

$$T_{p+k+1} \equiv yT_{p+k} + k(x+k-1)T_{p+k-1} \bmod p,$$

and hence by induction in k

$$T_{p+k} \equiv (y^p - y)T_k \bmod p.$$

We conclude that

$$T_k \equiv T_{a_0}(y^p-y)^{a_1}(y^{p^2}-y^p)^{a_2}\cdots \bmod p, \qquad \text{for } k = a_0 + a_1p + a_2p^2 + \cdots \in \mathbb{N}.$$

We now prove that P_d vanishes on the points III of the theorem. First we need the following. For each $k \in \mathbb{N}$ consider the polynomials

$$U_k(z,w) = T_k(x,y),$$

where $z = \frac{1}{2}(x-y)$ and $w = x-k+1$. Let λ be an indeterminate and z, w two fixed integers. Then using (3–1) we obtain

$$\sum_{k=0}^{\infty} U_k(z,w)\frac{\lambda^k}{k!} = \frac{(1+2\lambda)^z}{(1+\lambda)^w}, \quad z,w \in \mathbb{Z}.$$

From this identity it is not hard to see that

$$\frac{U_k(z,w)}{k!} = \sum_{j=0}^{w-1}(-2)^j\binom{z}{j}\binom{k+w-j-1}{w-j-1}, \tag{3–2}$$

for $0 \le z \le w$.

It follows that P_d vanishes at the points III if

$$\sum_{j=0}^{m}(-2)^j\binom{m}{k}\binom{2k-j}{k} = 0, \quad 0 \le m \le k, \ m \text{ odd}, \tag{3–3}$$

where $k = 2d$.

To prove this identity we start with

$$\binom{a+b}{k} = \sum_{r=0}^{a}\binom{a}{r}\binom{b}{k-r}, \quad a,b \in \mathbb{Z}_{\ge 0},$$

which one derives from the binomial theorem by comparing the k-th coefficients on both sides of

$$(1+\lambda)^{a+b} = (1+\lambda)^a(1+\lambda)^b.$$

Applying this to $a = m-j$, $b = 2k-m$ we obtain

$$\binom{2k-j}{k} = \sum_{r=0}^{m-j}\binom{m-j}{r}\binom{2k-m}{k-r},$$

and hence (3–3) is equivalent to

$$\sum_{j=0}^{m}\sum_{r=0}^{m-j}(-2)^j\binom{m}{j}\binom{m-j}{r}\binom{2k-m}{k-r} = 0.$$

This in turn follows from the stronger fact

$$\sum_{j=0}^{m-r}(-2)^j\binom{m}{j}\binom{m-j}{r} = (-1)^m\sum_{j=0}^{r}(-2)^j\binom{m}{j}\binom{m-j}{m-r},$$

since $\binom{2k-m}{k-r} = \binom{2k-m}{k-m+r}$, obtained by expanding

$$(\lambda-1)^m = (\lambda+1-2)^m$$

and comparing the coefficients of λ^r and λ^{m-r} respectively.

The fact that the points listed in IV are in $P_d = 0$ will be left to the reader. (One may use, for example, the fact that they sit on lines that intersect the curve on $d-1$ other explicitly known points.)

4. FURTHER ZEROS

We now present the experimental data. We first discuss the cases $d = 3$ and $d = 4$, where the equations $P_d(x,y) = 0$ determine smooth projective curves of genus 1 and 3, respectively. For $d = 3$ we have

$$P_3 = -15x^3 + 45yx^2 + 90x^2 - 15y^2x - 210yx - 120x + y^3 + 40y^2 + 184y.$$

The equation $P_3 = 0$ defines an elliptic curve with minimal Weierstrass equation (courtesy of F. Hajir)

$$y^2 + xy + y = x^3 - x^2 - 62705x + 5793697$$

and conductor $N = 29734650 = 2 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 6007$.

An exhaustive computer search for points with $|x| \le 1000$ yielded a total of 25 integral solutions (x,y) to $P_3(x,y) = 0$. The seven that were not predicted by Theorem 2.1 are shown in Table 1.

For $d = 4$ we have

$$P_4 = 105x^4 - 420x^3y - 1260x^3 + 210x^2y^2 + 4200x^2y + 4620x^2 - 28xy^3 - 1540xy^2 - 11872xy - 5040x + y^4 + 112y^3 + 2464y^2 + 8448y.$$

d	new points	total points found
3	$(-14,-56)$, $(-4,-20)$, $(-1,-9)$, $(1,1)$, $(16,144)$, $(67,25)$, $(345,1225)$	25
4	$(0,-24)$, $(3,-3)$, $(3,-35)$, $(-11,-35)$	31
5	$(16,144)$, $(17,81)$, $(25,441)$, $(99,589)$	42
6	$(1,-11)$, $(17,121)$, $(34,784)$	54
7	$(16,16)$, $(17,49)$, $(25,169)$, $(36,676)$, $(98,16)$	71
8	none	85
9	$(9,-35)$, $(33,289)$	104
10	none	123
11	$(34,784)$, $(36,676)$, $(41,441)$, $(57,2601)$, $(67,3249)$	160
12	none	171

TABLE 1. Extra points found experimentally on the curves P_d, for $3 \leq d \leq 12$. Together with the points predicted by Theorem 2.1, these are all the integer points satisfying $|x| < 1000$.

Again we searched the range $|x| \leq 1000$ by computer and found 31 integral solutions (x, y) to $P_4 = 0$; the new ones are shown in Table 1.

The remaining rows of Table 1 show the points not given by the theorem found by an exhaustive search in the same range ($|x| \leq 1000$) for $5 \leq d \leq 12$. We haven't found any patterns in the extra points; perhaps a more attentive reader will.

To verify that $P_d = 0$ defines a smooth curve is enough to check that it has no affine singularities, since the Hermite polynomial is separable. For this we verified, by computing modulo p for various primes p using the recursion, that the quantity

$$\operatorname{Res}_y\left(\operatorname{Res}_x\left(P_d, \frac{\partial P_d}{\partial x}\right), \operatorname{Res}_x\left(P_d, \frac{\partial P_d}{\partial y}\right)\right) \bmod p,$$

where Res_t stands for resultant in the variable t, is not zero for $d = 2, 3, \ldots, 25$.

5. ORIGIN OF THE POLYNOMIALS

These polynomials arose when we were studying the Picard–Fuchs equation for a period of a holomorphic differential on the family of varieties given by

$$(x_1 + \cdots + x_N)(x_1^{-1} + \cdots + x_N^{-1}) = \lambda,$$

with $\lambda \in \mathbb{C}$ a parameter. The Picard–Fuchs equation may easily be related to the equation satisfied by J_0^N, where J_0 is the standard J-Bessel function, and this equation can be computed recursively. The polynomials T_k appear as the coefficients of highest order in this recursion. The vanishing of T_k at some of the integral points of the theorem is then connected to the location of the bad fibers of the family.

ACKNOWLEDGEMENTS AND ELECTRONIC AVAILABILITY

We thank R. Coleman, A. Granville, F. Hajir, B. Poonen, and D. Zagier for suggestions, and the NSF (Rodriguez Villegas) and NSA (Voloch) for financial support. We also acknowledge the use of the software PARI for the numerical calculations. The routines we used are available at the URL http://www.ma.utexas.edu/users/voloch/polynomial.html.

REFERENCES

[Abramovich 1997] D. Abramovich, "Uniformity of stably integral points on elliptic curves", *Invent. Math.* **127**:2 (1997), 307–317.

[Abramovich and Voloch 1996] D. Abramovich and J. F. Voloch, "Lang's conjectures, fibered powers, and uniformity", *New York J. Math.* **2** (1996), 20–34.

[Caporaso et al. 1997] L. Caporaso, J. Harris, and B. Mazur, "Uniformity of rational points", *J. Amer. Math. Soc.* **10**:1 (1997), 1–35.

[Lebedev 1965] N. N. Lebedev, *Special functions and their applications*, Revised ed., Prentice-Hall, Englewood Cliffs, N.J., 1965. Reprinted by Dover, New York, 1972.

[Schur 1931] I. Schur, "Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome", *J. Reine Angew. Math.* **165** (1931), 52–58.

[Siegel 1929] C. L. Siegel, "Über einige Anwendungen Diophantischer Approximationen", *Abh. Preuss. Akad. Wiss. Phys. Math. Kl.* (1929), 41–69. Reprinted as pp. 209–266 of his *Gesammelte Abhandlungen I*, Springer, Berlin, 1966.

Fernando Rodriguez Villegas, Department of Mathematics, University of Texas at Austin, Austin, TX 78712 USA (villegas@math.utexas.edu)

José Felipe Voloch, Department of Mathematics, University of Texas at Austin, Austin, TX 78712 USA (voloch@math.utexas.edu)

Received December 12, 1997; accepted in revised form May 21, 1998