ELSEVIER Journal of Pure and Applied Algebra 117 & 118 (1997) 97–103

JOURNAL OF
PURE AND
APPLIED ALGEBRA

On a sequence of polynomials

Frits Beukers*

Instituut of Mathematics, Universiteit Utrecht, Budapestlaan 6, Utrecht, Netherlands

Abstract

In connection with studies of hierarchies of solutions to the Korteweg–de Vries equation, J. Sanders asked if $\gcd(p_k, p_l)$ is trivial for all k, l, where $p_k = (x+1)^k - x^k - 1$. In this paper we propose a positive reply to this question. © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: Primary 11B37; Secondary 35Q53

1. Introduction

Consider for any $k \in \mathbf{Z}_{\geq 2}$ the polynomial $p_k(X) = (X+1)^k - X^k - 1$. Factorisation of p_k in $\mathbf{Q}[X]$ for the first few values of k very soon suggests that we have obvious divisors when k is in a given residue class modulo 6,

k even: X,

$k \equiv 3 \pmod 6$: $X(X+1)$,

$k \equiv 5 \pmod 6$: $X(X+1)(X^2+X+1)$,

$k \equiv 1 \pmod 6$: $X(X+1)(X^2+X+1)^2$.

The proof is a very easy exercise. The following problem was raised by Sanders from CWI, Amsterdam, in connection with hierarchies of solutions of the Korteweg–de Vries equation.

Question 1.1. *Show that for any* $k, l \in \mathbf{Z}$ *with* $l > k > 1$ *we have that* $\gcd(p_k, p_l)$ *contains only the trivial divisors mentioned above.*

This question was posed as a challenge problem during the MEGA conference. The prize, a large cake, was to be divided among the submitters towards a solution of the

* E-mail: beukers@math.ruu.nl.

PII S0022-4049(97)00006-6

problem. It turned out that it is not very easy for computers to say something nontrivial about this problem, so the number of submissions to the problem was very small indeed, one. The prize winner subsequently made himself very popular among his local neighbourhood by organising a cake party. Let us now turn to the problem.

A quick computer test for $1 < k < 100$ leads one to believe the following conjecture.

Conjecture 1.2. *Write $p_k = t_k q_k$, where t_k is one of the trivial divisors mentioned above. Then q_k is irreducible in $\mathbf{Q}[X]$.*

If we would be able to prove this conjecture the solution to the original question would be very simple. Unfortunately, no such proof could be found until now and I have no idea whether the solution of this conjecture can be considered easy or not. Lacking such a proof we shall solve the question by a very heavy handed method based on techniques from Diophantine approximation.

2. The zeros

Before going over to the solution of the problem we like to make a few remarks on the position of the zeros of the polynomials p_k since this seems to have some interest by itself. First a lemma:

Lemma 2.1. *The number of distinct zeros z of p_k on the unit circle such that $z^2 + z + 1 \neq 0$ is at least $[2k/3] - [k/3] - 1$. In particular, if $k \neq 2,3,5,7$ there exists a zero z on the unit circle such that $|z+1| < 0.5$.*

Proof. Substitute $X = \mathrm{e}^{\mathrm{i}t}$ in p_k. After some rewriting we obtain

$$\left(2\cos\frac{t}{2}\right)^k = 2\cos k\frac{t}{2}.$$

Note that the left-hand side is ≤ 1 in absolute value if $\pi/3 \leq t/2 \leq 2\pi/3$. We now count the number N of values of t in this interval for which $\cos k(t/2)$ has value ± 1. Since the values $1, -1$ occur in alternating fashion the number of zeros in this interval should then be at least $N-1$. Note that $\cos k(t/2) = \pm 1$ if and only if $t/2 = \pi m/k$ for some $m \in \mathbf{Z}$. Together with the condition $\pi/3 \leq t/2 \leq 2\pi/3$ this implies $k/3 \leq m \leq 2k/3$. Hence $N \geq [2k/3] - [k/3]$.

To prove the second part, we take m to be the smallest integer larger than or equal to $k/2$. For the moment assume $k > 20$. Clearly, there is a zero $\mathrm{e}^{\mathrm{i}t}$ with $\pi m/k < t/2 < \pi(m+1)/k$. Hence, $\pi(m/k - \frac{1}{2}) < (t-\pi)/2 < \pi((m+1)/k - \frac{1}{2})$. Because of our choice of m we find that there exists a t with $0 < t - \pi < 3\pi/k$. When $k > 20$ this implies $|\mathrm{e}^{\mathrm{i}t} + 1| < 3\pi/k < 0.5$. The remaining cases can be checked by hand. □

For odd k the location of the zeros is now more or less clear. In this case we see that if z is a zero, the same holds for $-1-z$ and $1/z$. Under the group generated by these transformations the images of the unit circle $|z|=1$ are $|z+1|=1$ and $\Re z=-\frac{1}{2}$. From the above lemma we saw that about one-third of the zeros are on the unit circle. The other zeros are on the circle $|z+1|=1$ and the line $\Re z=-\frac{1}{2}$.

For even k the situation is slightly more complicated. In this case we can prove that there are no zeros on $|z+1|=1$ except $z=0$. To see this let $z=\mathrm{e}^{it}-1$ and substitute in $p_k(z)=0$. We obtain, $2\mathrm{i}\sin k(t/2)=(2\mathrm{i}\sin(t/2))^k$. Since k is even the right-hand side of the equation is real and the left-hand side imaginary. Hence, $\sin(t/2)=0$ and we find $t=0$, which implies $z=0$. However, starting with w_0 a kth root of unity such that $|w_0-1|<1$, we see that the recurrence $w_{r+1}=w_0(\sqrt[k]{1+(w_r-1)^k})$ very quickly converges to a solution of $w^k-(w-1)^k-1=0$. In fact, the difference of this solution with w_0 is of the order $|w_0-1|^k$. When k is large, this tends to be a very small number. Plotting the zeros of p_k for even k with a computer one indeed observes that, with a few exceptions, about one-third of the zeros is indistinguishably close to $|z+1|=1$. Since we still have the symmetry $z\longrightarrow 1/z$ the same remark holds for the line $\Re z=-\frac{1}{2}$.

3. Diophantine approximation

In the following statements we will use the concept of height of an algebraic point in projective space. Let K be an algebraic number field, i.e. a finite field extension of the rational numbers. A valuation on K is a multiplicative norm on the elements of K. As is well known there exist infinite or archimedean valuations (finitely many) and finite, or non-archimedean ones (infinitely many). We normalise the valuations as follows. For any finite valuation we take $|p|_v=p^{-d_v/d}$. Here p is the rational prime corresponding to the valuation, d is the degree of the extension K and d_v the degree of K_v over the p-adic numbers. Here K_v the completion of K with respect to the valuation. For infinite valuations we use the normalisation $|x|_v=|x|^{d_v/d}$, where $|.|$ denotes the ordinary absolute value. For any $a\in K^*$ we have the so-called product formula

$$\prod_v |a|_v=1.$$

The height of an n-tuple $(a_1,\dots,a_n)\in K^n$ is defined by

$$H(a_1,\dots,a_n)=\prod_v \max(|a_1|_v,\dots,|a_n|_v).$$

Due to the product formula we have the property that $H(a_1,\dots,a_n)=H(\lambda a_1,\dots,\lambda a_n)$ for any $\lambda\in K^*$. Hence, the height is a measure on projective space.

For future use we record the following properties which are easy to prove from the definition. For any $k\in\mathbf{Z}_{\geq 1}$ we have $H(a_1^k,\dots,a_n^k)=H(a_1,\dots,a_n)^k$. Secondly, $H(a_1^{-1},\dots,a_n^{-1})\leq H(a_1,\dots,a_n)^{n-1}$.

Let us now turn to the results from Diophantine approximation.

Lemma 3.1. *Let $a,b,A,B \in \overline{\mathbf{Q}}^*$ such that $a \neq b$, $A+B=1$ and $aA+bB=1$. Then $H(A,B,1) \leq 2H(a,b,1)$.*

This is a lemma with a very elementary proof and can be found in [1, Corollary 2.2]. The following lemma is [1, Lemma 2.3] and its proof uses hypergeometric polynomials. This is a method which derives from famous work of Thue (1909) on rational approximation of algebraic numbers.

Lemma 3.2. *Let $a,b,A,B \in \overline{\mathbf{Q}}^*$ and $r \in \mathbf{N}$ such that $A+B=1$ and $aA^{2r}+bB^{2r}=1$. Then $H(A,B,1) \leq 2^{1/r}cH(a,b,1)^{1/r}$ where $c=6\sqrt{3}$.*

The following lemma can be found in [4] or [2]. At first it was found as a consequence of Arakelov intersection theory on $\mathbf{P}^1$ by Zhang in 1992. Very soon Zagier gave a very elementary but ingenious proof.

Lemma 3.3. *Let $A,B \in \overline{\mathbf{Q}}^*$ such that $A+B=1$ and $AB \neq 1$. Then $H(A,B,1) \geq 1.21$.*

The final ingredient is a recent improvement by Laurent et al. [3] of a result of Gel'fond in the theory of linear forms in logarithms.

Lemma 3.4. *Let α_1, α_2 be non-zero algebraic numbers and let D be the degree of the field generated by α_1, α_2. Let b_1, b_2 be rational integers. Choose A such that*

$$A \geq \max(\log H(\alpha_i,1), |\log \alpha_i|/D, 1/D)$$

and let $b' = (|b_1|+|b_2|)/DA$. Then,

$$\log|b_1 \log \alpha_1 - b_2 \log \alpha_2| \geq -30.9D^4 \max\left(\log b', \frac{21}{D}, \frac{1}{2}\right)^2 (\log A)^2.$$

Here we can take for $\log \alpha_i$ any determination.

Finally, we need a statement which is not really in the literature.

Lemma 3.5. *Let $a,b,A,B \in \overline{\mathbf{Q}}^*$, $a \neq b$ and $n \in \mathbf{N}$. Suppose $A-B=1$ and $aA^n-bB^n=1$. Then $H(A,B,1) \leq 216H(a,b,1)$.*

Proof. For even n we use Lemma 3.2 with $n=2r$ and $-B$ instead of B to obtain $H(A,B,1) \leq 2^{2/n}6\sqrt{3}H(a,b,1)^{2/n}$. Since $n \geq 2$ we get $H(A,B,1) \leq 12\sqrt{3}H(a,b,1)$.

When n is odd and ≥ 5 we again apply Lemma 3.2 with $n-1=2r$ to find

$$\begin{aligned} H(A,B,1) &\leq 2^{2/n-1}6\sqrt{3}H(aA,bB,1)^{2/n-1}, && (1)\\ &\leq 2^{1/2}6\sqrt{3}H(a,b,1)^{1/2}H(A,B,1)^{1/2}. && (2) \end{aligned}$$

Hence, $H(A,B,1) \leq 2(6\sqrt{3})^2H(a,b,1) = 216H(a,b,1)$.

When, $n=1$ we simply use Lemma 3.1.

The case that remains is $n=3$. We note the following identities:

$$1=(1-3B+6B^2)A^3-(1+3A+6A^2)B^3, \tag{3}$$

$$-A-B=(1-B)A^3+(1+A)B^3. \tag{4}$$

Since

$$\begin{vmatrix} 1-3B+6B^2 & -(1+3A+6A^2) \\ 1-B & 1+A \end{vmatrix} = 12,$$

we have either

$$\begin{vmatrix} 1-3B+6B^2 & -(1+3A+6A^2) \\ a & b \end{vmatrix} \neq 0 \quad \text{or} \quad \begin{vmatrix} 1-B & 1+A \\ a & b \end{vmatrix} \neq 0.$$

Application of [1, Lemma 2.1] implies

$$H(A^3,B^3,1)\leq 2H(a,b,1)M,$$

where

$$M=\max(H(1-B,1+A,A+B),H(1-3B+6B^2,1+3A+6A^2,1)).$$

A straightforward calculation shows that $M\leq 18H(A^2,B^2,1)$. Hence, $H(A^3,B^3,1)\leq 2H(a,b,1)\cdot 18H(A,B,1)^2$. Thus, we find that $H(A,B,1)\leq 36H(a,b,1)$. □

4. Solution of the problem

We shall rephrase the problem into the following shape.

Theorem 4.1. *Let $\theta\in\overline{\mathbf{Q}}$ such that $\theta(\theta+1)(\theta^2+\theta+1)\neq 0$, where $\omega=e^{2\pi i/3}$. Then there is at most one integer $n>1$ such that $(\theta+1)^n-\theta^n-1=0$.*

In the following propositions we give a step by step solution of the problem. We shall adhere to the notations just introduced in our theorem.

Proposition 4.2. *Suppose there exist two integers k,l with $l>k>1$ such that $(\theta+1)^n-\theta^n-1=0$ for $n=l,k$. Then $k<85$.*

Proof. Put $l=mk+d$ with $0\leq d<k$. Now apply Lemma 3.5 with $A=(\theta+1)^k$, $B=\theta^k$, $a=(\theta+1)^d, b=\theta^d$ to find

$$H(\theta+1,\theta,1)^k\leq 216H(\theta+1,\theta,1)^d.$$

Using Lemma 3.3 we get $H(\theta+1,\theta,1) > 1.21$, hence $1.21^{k-d} \leq 216$. Hence $k-d \leq 28$. Now apply Lemma 3.5 with $A=(\theta+1)^k$, $B=\theta^k$, $a=(\theta+1)^{d-k}$, $b=\theta^{d-k}$ to obtain

$$H(\theta+1,\theta,1)^k \leq 216H((\theta+1)^{d-k},\theta^{d-k},1), \tag{5}$$

$$\leq 216H(\theta+1,\theta,1)^{2(k-d)}, \tag{6}$$

$$\leq 216H(\theta+1,\theta,1)^{56}. \tag{7}$$

So, $1.21^{k-56} \leq 216$ and we get $k < 56+29 = 85$. □

Proposition 4.3. *Let t be a complex number with absolute value* 1 *and suppose that $|1+t| \leq 1$. Suppose there exists $n \in \mathbf{N}$ such that $(t+1)^n - t^n - 1 = 0$. Then there exists $m \in \mathbf{Z}$ such that*

$$|n\,\mathrm{Arg}(t) + m\pi| \leq \tfrac{\pi}{3}|1+t|^n.$$

Proof. Suppose we have a complex number z of absolute value 1 such that $z = 1+w$ with $|w| \leq 1$. A small geometrical picture then easily shows that $|\mathrm{Arg}(z)| \leq (\pi/3)|w|$. This principle applied to $z = -t^n$ yields $|\mathrm{Arg}(-t^n)| \leq (\pi/3)|1+t|^n$. Our proposition now follows immediately. □

Proposition 4.4. *Let the notations be as in Theorem* 4.1. *Suppose there exist two integers k, l with $l > k > 1$ such that $(\theta+1)^n - \theta^n - 1 = 0$ for $n = l, k$. Assume in addition that $|\theta| = 1$ and $|\theta+1| < 0.5$. Then $l < 10^{14}$.*

Proof. We already know that $k < 85$ and θ is a non-trivial zero of $(X+1)^k - X^k - 1$. According to the above lemma we have the inequality

$$|l\,\mathrm{Arg}(\theta) + m\pi| \leq \tfrac{\pi}{3}|1+\theta|^l < \tfrac{\pi}{3}\left(\tfrac{1}{2}\right)^l$$

for some $m \in \mathbf{Z}$. Note that we can assume $|m| \leq l$. Let us now apply Lemma 3.4 with $\log\alpha_1 = \mathrm{i}\,\mathrm{Arg}(\theta)$, $\log\alpha_2 = \mathrm{i}\pi$ and $b_1 = l, b_2 = -m$. We can take $D < k$, $A = 3$ and $b' \leq 2l/3k$. Let us assume that $l > 10^{10}$. Then Lemma 3.4 implies that

$$\log|l\,\mathrm{Arg}(\theta) + m\pi| \geq -30.9k^4(\log(2l/3k))^2 \cdot 9.$$

Together with the upper bound and the fact that $4 \leq k < 85$ this gives us

$$15 \cdot 10^9(\log(l/6)^2 > \log(\pi/3) + l\log(2).$$

From this we obtain $l < 10^{14}$. □

Proof of Theorem 4.1. Suppose our equation has two solutions $n = k$, l with $l > k > 1$. We already know that $k < 85$. Since for given k the non-trivial factor of p_k is irreducible, we can take for θ any non-trivial zero of p_k. In particular we can take the zero with the properties $|\theta| = 1$ and $|\theta+1| < 0.5$. We then know that $l < 10^{14}$

and, moreover,

$$|l\,\mathrm{Arg}(\theta) - m\pi| \leq \tfrac{\pi}{3}\left(\tfrac{1}{2}\right)^{l}$$

for some $m \in \mathbf{Z}$. In particular, this implies

$$\left|\frac{\mathrm{Arg}(\theta)}{\pi} - \frac{m}{l}\right| \leq \frac{1}{3l^2}.$$

A theorem of Legendre tells us that m/l is a convergent of the continued fraction of $\mathrm{Arg}(\theta)/\pi$. So for each $k < 85$ we must find θ such that $(\theta+1)^k - \theta^k - 1 = 0$, $|\theta| = 1$ and $|\theta + 1| < 0.5$ and check all denominators of the convergents of the continued fraction of $\mathrm{Arg}(\theta)/\pi$. This is a small task on a computer. The outcome of it establishes the proof of our theorem. □

References

[1] F. Beukers and H.P. Schlickewei, The equation $x + y = 1$ in finitely generated groups, Acta Arith. 78 (1996) 189–199.

[2] F. Beukers and D. Zagier, Lower bounds for points on hypersurfaces, Acta Arith., to appear.

[3] M. Laurent, M. Mignotte and Y. Nesterenko, J. Number Theory 55 (1995) 285–321.

[4] D. Zagier, Algebraic numbers close to both 0 and 1, Math. Comput. 61 (1993) 485–491.