CYCLOTOMIC POINTS ON CURVES

F. Beukers and C.J. Smyth

Abstract. We show that a plane algebraic curve $f = 0$ over the complex numbers has on it either at most $22V(f)$ points whose coordinates are both roots of unity, or infinitely many such points. Here $V(f)$ is the area of the Newton polytope of f. We present an algorithm for finding all these points.

1. Introduction. When does a curve $f(x, y) = 0$ with complex coefficients have cyclotomic points on it? By *cyclotomic points* we mean points (x, y) with x and y both roots of unity. How do we estimate the number of cyclotomic points on a given curve? How do we actually find all these points?

In Section 2 we present an algorithm for finding the cyclotomic part of a polynomial in one variable. We do this first for polynomials with rational coefficients, and then show how the algorithm can be extended to polynomials with complex coefficients. In Section 3 we give an algorithm for finding all the cyclotomic points on a curve. This algorithm uses the algorithm of Section 2. Again, we first present an algorithm for curves with rational coefficients, and show how it can be extended to curves over more general fields. In Section 4 we state and prove our main result, giving an upper bound of $22V(f)$ for the number of cyclotomic points on the curve, when this number is finite. Here $V(f)$ is the area of the Newton polytope of f. In Section 5 we give some examples and applications of our results. Finally, in Section 6 we give a sharp version of our main result.

2. Finding the cyclotomic part of a one-variable polynomial. As a warm-up for the problem of finding cyclotomic points on curves, let us first look at the one-variable version of the problem: given a polynomial $f(x)$ of degree d, with rational coefficients, find all roots of unity ω which are zeroes of f. This is of course equivalent to finding the factor of f consisting of the product of all distinct irreducible cyclotomic polynomial factors of f, which we shall call the *cyclotomic part* of f. One way of finding the cyclotomic part of f is simply to use trial division of f by cyclotomic polynomials of degree up to that of f. Our approach here is somewhat different, and gives a more efficient algorithm. It is based on the following simple properties of roots of unity.

Lemma 1. *(i) If $g(x) \in \mathbb{C}[x], g(0) \neq 0$, is a polynomial with the property that for every zero α of g, at least one of $\pm\alpha^2$ is also a zero, then all zeroes of g are roots of unity.*

(ii) If ω is a root of unity, then it is conjugate to exactly one of $-\omega, \omega^2$ and $-\omega^2$.

Conversely, if $\alpha \neq 0$ and either α^2 or $-\alpha^2$ is conjugate to α, then α is a root of unity.

Recall that two algebraic numbers are *conjugate* if they are zeroes of the same irreducible polynomial with integer coefficients. The obvious example $\alpha = \sqrt{2}$ shows that α and $-\alpha$ can be conjugate without α being a root of unity.

The first part of (ii) was stated without proof in [Sm], where it was used to find the cyclotomic factors of a family of polynomials. The converse part of (ii) is a special case of a result of Dobrowolski[D], Lemma 2(i).

To prove (i), suppose that α is any zero of g. Then so is one of $\pm\alpha^2$, and hence so is one of $\pm\alpha^4$, one of $\pm\alpha^8$, and so on. As g has only finitely many zeroes, two of these powers must be equal. As $\alpha \neq 0$, this shows that α is a root of unity.

The second part of the lemma follows from the observation that ω is conjugate to ω^ℓ for

$$\begin{cases} \ell = 2k+1, \quad \omega^\ell = -\omega & \text{for } \omega \text{ a } 4k\text{th root of unity} \\ \ell = k+2, \quad \omega^\ell = -\omega^2 & \text{for } \omega \text{ a } 2k\text{th root of unity, } k \text{ odd} \\ \ell = 2, \quad \omega^\ell = \omega^2 & \text{for } \omega \text{ a } k\text{th root of unity, } k \text{ odd} \end{cases}$$

For the final part of (ii): if α and one of $\pm\alpha^2$ are conjugate, with minimal polynomial g, then $g(\alpha) = g(\pm\alpha^2) = 0$, which implies that $g(x)$ divides $g(x^2)$. Hence for any conjugate α' of α, $g(\pm\alpha'^2) = 0$, so that we can apply (i).

We claim that, for $f \in \mathbb{Q}[x]$, the following recursive algorithm finds Cf, the (square–free) cyclotomic part of f, which is

$$(Cf)(x) = \prod_{\substack{f(\alpha)=0 \\ \alpha \text{ root of } 1}} (x - \alpha).$$

An algorithm for finding the cyclotomic part of a polynomial, using essentially the same ideas, was given earlier by Bradford and Davenport [BD]. First of all, we can clearly assume that f is monic and not divisible by x. Define Gf by

$$(Gf)(x) = \gcd((f(x), f(x^2)f(-x^2)).$$

Then we claim that Cf is given recursively in pseudocode by

Function C
Input f, Output Cf
Local f, f_2, g, h
if $Gf = f$ then $h := f$
else
$f_2(x) := \gcd(f(x), f(-x))$
$g(x) := f_2(\sqrt{x})$
$h(x) := (CGf)(x) * (Cg)(x^2)$
fi
Return$(h/\gcd(h, h'))$

`end`

Proof of termination and correctness of the algorithm.

We work by induction on the degree of f. When f is constant we have $Gf = f$, hence the output is a constant, which is correct.

Assume now that f has positive degree and suppose the algorithm works for all polynomials of lower degree. First note that if $Gf = f$ then f has only roots of unity as zeroes by Lemma 1(i). In that case we also have $f = Cf$ and thus f is the correct output. Let us now assume that Gf has strictly lower degree than f. Suppose that α is a cyclotomic zero of f. Then, by Lemma 1(ii), α is zero of at least one of $f_2(x) = \gcd(f(x), f(-x))$ or $(Gf)(x)$. Hence $(Cf)(x)$ has the same zero set as $(CGf)(x)(Cf_2)(x)$. The latter may contain zeroes of higher multiplicity. Note that $f_2(x)$ is a polynomial in x^2, say $f_2(x) = g(x^2)$. So finding the common cyclotomic zeroes of $f(x)$ and $f(-x)$ comes down to finding the cyclotomic zeroes of g. Hence $(Cf)(x)$ also has the same zero set as $h = (CGf)(x)(Cg)(x^2)$, giving $(Cf)(x) = h/\gcd(h, h')$. Since, by assumption, the degrees of Gf and g are strictly smaller than the degree of f, our induction hypothesis guarantees that algorithm C works on Gf and g. Hence we can compute Cf.

We note that this 'cyclotomic part' algorithm can be easily extended to find the cyclotomic part of a polynomial $f(x)$ whose coefficients are algebraic, lying in some number field K. To do this, simply compute $\gcd(f(x), CNf(x))$, where N is the norm $N_{K(x)/\mathbb{Q}(x)}$. Finally, we can extend the algorithm to any $f \in \mathbb{C}[x]$. Suppose that not all coefficients of f are algebraic, with its coefficients lying in some extension field F of the algebraic numbers $\overline{\mathbb{Q}}$. Scaling f so that $f(0) = 1$, we can find an automorphism $\sigma \in \mathrm{Gal}(F/\overline{\mathbb{Q}})$ so that $f^\sigma \neq f$ for the image f^σ of f under σ. As $f^\sigma(0) = 1$, $\gcd(f, f^\sigma)$ has lower degree than f, while having the same cyclotomic zeroes. Thus we can reduce the degree of our polynomial until all its coefficients are algebraic.

3. Finding cyclotomic points on curves.

3.1 Definitions.

We now address the problem of finding cyclotomic points on the curve $f(x, y) = 0$. We simply call these *the cyclotomic points of* f. We can allow f to be in $\mathbb{C}[x, x^{-1}, y, y^{-1}]$, so that it is a Laurent polynomial. For $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$ we define the *support* of f, to be $\mathrm{supp}(f) = \{(i, j) \in \mathbb{Z}^2 \mid a_{ij} \neq 0\}$. Let $\mathcal{N}(f)$ be the convex hull of $\mathrm{supp}(f)$, called the *Newton polytope* of f, with area $V(f)$. The set of differences $\{\underline{j} - \underline{j}' \mid \underline{j}, \underline{j}' \in \mathbb{Z}^2\}$ generates a sublattice $\mathcal{L}(f)$ of $\mathbb{Z}^2$, the *exponent lattice* of f. For f not equivalent to a constant, this lattice is a rank 1 or rank 2 $\mathbb{Z}$-module. If the lattice is the whole of $\mathbb{Z}^2$, $\mathcal{L}(f)$ is said to be *full*. We define the extension field of $\mathbb{Q}$ generated by all ratios $a_{ij}/a_{i'j'}$ of non-zero coefficients of f to be the *coefficient field of* f.

We say that two Laurent polynomials are *equivalent* if their ratio is a non-zero scalar multiple of a monomial $x^a y^b$. Two equivalent Laurent polynomials clearly have the same cyclotomic points, and the same coefficient field. This allows us to assume that f is a (true) polynomial, and also that at least one of its coefficients is rational. Note that its coefficient field is then simply the extension field of $\mathbb{Q}$ generated by its coefficients.

We let ω_n denote a primitive nth root of unity.

We now consider how to find the cyclotomic points of f for various different classes of f.

3.2 $\mathcal{L}(f)$ of rank 1.

In this case it is clear that f is equivalent to a Laurent polynomial of the form $c(x^k y^\ell)$, where $k, \ell \in \mathbb{Z}$ and c is a polynomial in one variable. If f has a cyclotomic point (x, y), then c must have a zero ω which is a root of unity. We can use the algorithm of Section 2 to find the cyclotomic part of c, and so find all such zeroes ω. Thus to find all cyclotomic points on the curve, we only have to solve the equations $x^k y^\ell = \omega$ for every zero ω of c. If $(k, \ell) = 1$, then from $kk_1 + \ell\ell_1 = 1$ we obtain the general solution $(x, y) = (\omega^{k_1} t^\ell, \omega^{\ell_1} t^{-k})$, where t is any root of unity. If $g = (k, \ell) > 1$ we can consider $c(x^{k/g} y^{\ell/g})$, and we are reduced to the relatively prime case. Thus in this case we have no cyclotomic points of f if c has no cyclotomic part, and infinitely many such points otherwise.

3.3 $\mathcal{L}(f)$ full of rank 2 : General form of the algorithm.

Our strategy for finding the cyclotomic points of f when $\mathcal{L}(f)$ is full of rank 2 is the following. We first identify a finite set $\{f_i\}$ of polynomials with the property that each cyclotomic point on f is also on some f_i, and such that no f_i has a common component with f.

We then claim that the following algorithm will find all the cyclotomic points of f.

1. For each i compute the y-resultant of f and f_i, and form the product $R(x)$ of these resultants. Calculate $CR(x)$ using the algorithm of Section 2.

2. For each zero ω of $CR(x)$, find zeroes ω' of the cyclotomic part of $f(\omega, y)$, using the algorithm for a polynomial having coefficients in the relevant field, as described in Section 2. Then the points (ω, ω') are the cyclotomic points of f.

Now, as is well known, the y-resultant of two polynomials like f and f_i can be expressed in the form $h_i f_i + h_i^* f$ for some $h_i, h_i^* \in \mathbb{C}[x, y]$. Thus the zeroes of its cyclotomic part includes the x-coordinates of all cyclotomic points on both curves. If all the f_i have the stated properties, this resultant will be a polynomial in x only, and so the algorithm will find every one of the finite number of cyclotomic points.

We now separate the proof into two main cases, depending on whether or not the coefficient field of f is a subfield of the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$. However for ease of exposition we look first at the case where the coefficient field of f is rational. We assume throughout this section that f is a polynomial, irreducible over its coefficient field. If it is reducible, factorise it over that field and apply the algorithm separately to each irreducible factor. It may be that some of these factors have their lattices of rank 1, in which case 3.2 above should be applied.

3.4 $\mathcal{L}(f)$ full of rank 2, f with rational coefficients.

We must find a set of polynomials f_i with the properties stated. To do this, let (x, y) be a cyclotomic point of f. Then there is a root of unity ω such that both x and y are powers of ω, say $x = \omega^a$ and $y = \omega^b$. We can, by replacing ω by a power of itself, assume that $\gcd(a, b) = 1$. Thus $f(\omega^a, \omega^b) = 0$ and so, by Lemma 1, also at least one of $f(\omega^a, -\omega^b), f(-\omega^a, \omega^b), f(-\omega^a, -\omega^b), f(\omega^{2a}, \omega^{2b}), f(\omega^{2a}, -\omega^{2b}), f(-\omega^{2a}, \omega^{2b})$ or $f(-\omega^{2a}, -\omega^{2b})$ is also zero. Note that we are also using the fact that a and b are not both even. Thus our cyclotomic point (x, y) of f also lies on at least one of the seven other curves $f_i = 0 (i = 1, \cdots, 7)$, where $f_1(x, y) = f(x, -y), f_2(x, y) = f(-x, y), f_3(x, y) = f(-x, -y), f_4(x, y) = f(x^2, y^2)$, and $f_i(x, y) = f_{i-4}(x^2, y^2)$ for $i = 5, 6, 7$.

It remains only to check that f does not divide any of the f_i. Now, it is easy to see that, if $f | f_1$, then f is equivalent to a polynomial in $\mathbb{Q}[x, x^{-1}, y^2, y^{-2}]$, in which case $\mathcal{L}(f)$ would not be full. Similarly, if $f | f_2$, then f is equivalent to a polynomial in $\mathbb{Q}[x^2, x^{-2}, y, y^{-1}]$, while if $f | f_3$, f is equivalent to a polynomial in $\mathbb{Q}[xy, 1/xy, x/y, y/x]$, so that, again, $\mathcal{L}(f)$ would not be full. Also note that if any of f_1, f_2, f_3 were to divide any other one of f_1, f_2, f_3, the same contradiction would apply.

Next, suppose $f | f_4$. Then, as $f_4(x, y) \in \mathbb{Q}[x^2, y^2]$, we have that each of f_1, f_2 and f_3 also divide f_4. Hence $f f_1 f_2 f_3 | f_4$, clearly impossible by degree considerations (say, in x) . Exactly the same argument applies to f_5, f_6 and f_7. This completes the proof that the f_i have the required properties, and so our algorithm works for f with rational coefficients.

3.5 $\mathcal{L}(f)$ full of rank 2, f with coefficients in $\mathbb{Q}^{\mathrm{ab}}$.

We now define the f_i in the case of f having coefficients lying in a cyclotomic field $\mathbb{Q}(\omega_N)$. We take f irreducible over $\mathbb{Q}^{\mathrm{ab}}$, with constant term 1. We choose N to be minimal in the following strong sense. For any roots of unity ω' and ω'', $f(\omega' x, \omega'' y)$ has the same number of cyclotomic points as f. So, take N to be the smallest integer such that, for some roots of unity ω' and ω'', $f(\omega' x, \omega'' y)$ has all its coefficients in $K = \mathbb{Q}(\omega_N)$. We then replace f by this polynomial. When we have found the cyclotomic points on this new f, it is easy to go back and find those on the original f.

We need to separate the two cases of N odd and N a multiple of 4.

Case I: N odd. Take σ to be an automorphism of K taking ω_N to ω_N^2. We keep f_1, f_2, f_3 as in 3.4, but replace the polynomials f_4, f_5, f_6, f_7 of 3.4 by $f_4^\sigma, f_5^\sigma, f_6^\sigma, f_7^\sigma$. (Of course this has no effect if $K = \mathbb{Q}$.) We then claim that any cyclotomic point of f also lies on one of these new $f_i = 0$ for $i = 1, \cdots, 7$. Take a cyclotomic point $P = (\omega_m^r, \omega_m^s)$ of f, with $\gcd(r, s) = 1$. If $4 \nmid m$ then we can extend σ to an automorphism of $K(\omega_m)$, which takes ω_m to one of $\pm\omega_m^2$. Hence P also lies on one of f_4, f_5, f_6 or f_7. On the other hand, if $4 | m$, we put $4k = \mathrm{lcm}(m, N)$. Then the automorphism, τ say, of $K(\omega_m) = \mathbb{Q}(\omega_{4k})$ mapping $\omega_{4k} \mapsto \omega_{4k}^{2k+1}$ takes $\omega_m \mapsto \omega_m^{2k+1} = -\omega_m$ and $\omega_N \mapsto \omega_N^{2k+1} = \omega_N$. Thus P also lies on one of f_1, f_2 or f_3.

For this case, it follows that we can take $f_1, \cdots, f_7$ to be the set of f_i. The argument of the previous paragraph carries over to show that none of them has a common component with f.

Case II: $4 | N$. We take the point P as in Case I, again put $4k = \mathrm{lcm}(m, N)$, and use the same automorphism τ. Then τ takes $\omega_m \mapsto \omega_m^{2k}\omega_m = \pm\omega_m$ and $\omega_N \mapsto \omega_N^{2k}\omega_N = \pm\omega_N$. We now consider separately the four possibilities for these signs. Firstly, they cannot both be + signs, from the definition of k.

If

$$\tau(\omega_m) = \omega_m \qquad \tau(\omega_N) = -\omega_N$$

then P also lies on f^τ. Note that $f^\tau \neq f$, by the minimality of N, so that they have a proper intersection.

If

$$\tau(\omega_m) = -\omega_m \qquad \tau(\omega_N) = \omega_N$$

then P lies on one of f_1, f_2 or f_3. , As $\mathcal{L}(f)$ is full, each has proper intersection with f, as we saw in 3.4.

Finally if

$$\tau(\omega_m) = -\omega_m \qquad \tau(\omega_N) = -\omega_N$$

then P lies on one of f_1^τ, f_2^τ or f_3^τ. Suppose that for instance f and $f^\tau(-x,y)$ have a common component, so that $f^\tau(-x,y) = f(x,y)$. Then we would have $f(\omega_N x, y)^\tau = f^\tau(-\omega_N x, y) = f(\omega_N x, y)$, so that $f(\omega_N x, y) \in \mathbb{Q}(\omega_N^2)[x, x^{-1}, y, y^{-1}]$, contradicting the minimality of N. The same argument applies to $f^\tau(x,-y)$ and to $f^\tau(-x,-y)$.

Thus for Case II P lies on one of the seven curves $f_1, f_2, f_3, f^\tau, f_1^\tau, f_2^\tau$ and f_3^τ, which we take to be our set $\{f_i\}$. Note that the definition of these curves depends only on N, not on m. Since, by assumption, f has at least one rational coefficient, none of $f^\tau, f_1^\tau, f_2^\tau$ or f_3^τ has a common component with f.

3.6 $\mathcal{L}(f)$ full of rank 2, f with coefficients in $\mathbb{C}$.

Take f to be absolutely irreducible, with constant term 1, and f having coefficient field, L say, not a subfield of $\mathbb{Q}^{\mathrm{ab}}$. Choose an automorphism $\sigma \in \mathrm{Gal}(L/\mathbb{Q}^{\mathrm{ab}})$ which does not fix f. Then since all roots of unity belong to $\mathbb{Q}^{\mathrm{ab}}$, f and f^σ have the same cyclotomic points. Further, f and f^σ have no common component. Thus in this case we can take the set of f_i to be the single polynomial f^σ.

3.7 $\mathcal{L}(f)$ of rank 2, but not full.

Suppose that $\mathcal{L}(f)$ has a basis $(a,c),(b,d)$ with index $I = |ad - bc|$ in $\mathbb{Z}^2$. Put $u = x^a y^c, v = x^b y^d$, so that f is equivalent to $f^*(u,v)$ for some Laurent polynomial f^* with {* full. For convenience define an $SL_2(\mathbb{Z})$-action of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on monomials $x^i y^j$ by $(x^i y^j)^A = x^{ai+bj} y^{ci+dj}$, and so on pairs of monomials by this action on each coordinate. Then we can write the relations connecting x, y with u, v as $\binom{x}{y}^A = \binom{u}{v}$. Now, putting A into Smith Normal Form ([N], p. 26) yields two matrices U and W in $SL_2(\mathbb{Z})$ with $WAU = D$ say, where $D = \mathrm{diag}(d_1, d_2)$, and d_1 and d_2 are positive integers with $d_1 | d_2$. Also $d_1 d_2 = I$. Hence

$$\begin{pmatrix} x \\ y \end{pmatrix}^{W^{-1}D} = \begin{pmatrix} u \\ v \end{pmatrix}^U = \begin{pmatrix} u^* \\ v^* \end{pmatrix} \qquad (*)$$

say. Now, as $\mathcal{L}(f^*)$ is full, we can find all cyclotomic points (u,v) of f^*. Then, letting u_1, u_2 be all possible primitive d_1th, d_2th roots of u^*, v^*, respectively, each cyclotomic point (u,v) of f^* gives I points

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}^W$$

of f. Hence the cyclotomic points of f can be obtained from those of f^*. Also, we see that f has I times as many cyclotomic points as f^*.

4. Sharp and almost-sharp bounds for the number of cyclotomic points on a curve.

4.1 The main Theorem.

We now obtain good upper bounds on the number of cyclotomic points of f. Define f to be *reciprocal* if it is equivalent to $\bar{f}(x^{-1}, y^{-1})$, where $\bar{}$ denotes complex conjugation.

Theorem. *Let $f \in \mathbb{C}[x, x^{-1}, y, y^{-1}]$, having Newton polytope of area $V(f)$. Then f has either at most $22V(f)$ cyclotomic points, or infinitely many. In the latter case f has a factor $x^i y^j - \omega$ for some root of unity ω and some integers i, j not both* 0.

If all of the absolutely irreducible factors of f are non-reciprocal, then f has at most $4V(f)$ cyclotomic points.

If none of the coefficient fields of the absolutely irreducible factors of f is a subfield of $\mathbb{Q}^{\mathrm{ab}}$, then f has at most $2V(f)$ cyclotomic points.

Finally, the constant 22 *above cannot be replaced by any constant smaller than* 16. *The constants* 4 *and* 2 *are best possible.*

A result of Liardet [Li] tells us that if a plane curve over $\mathbb{C}$ has infinite intersection with the division group of a finitely generated multiplicative group, then the curve has an irreducible component which is the translate of a subtorus. Our result contains an alternative proof of the special case when the finitely generated group is the trivial group. This was in fact first proved by Ihara, Serre and Tate, independently (see [La]). Quantitative (though large) bounds on the number of such points, when this number is finite, follow from a general result of Schmidt [Sc] on the number of maximal torsion cosets on a variety. Our theorem gives an almost sharp quantative upper bound in the curve case. A far more general conjecture of Lang, proved in 1995 by McQuillan [M], incorporating conjectures of Mordell and Manin–Mumford, describes the intersections of a semi-abelian variety A over $\mathbb{C}$ with the division group of a finitely generated subgroup of A. See Hindry and Silverman [HS], especially p.439, for a very readable, up-to-date account of results in this area.

4.2 Lemmas for the proof.

For the proof of the theorem, we need the following two lemmas. The first one is a particularly important ingredient in our proof.

Recall that for two convex sets S_1, S_2 in $\mathbb{R}^n$, their Minkowski sum $S_1 + S_2$ is defined to be $\{\underline{x}_1 + \underline{x}_2 \mid \underline{x}_1 \in S_1, \underline{x}_2 \in S_2\}$. Also, let V be the n-volume function.

Lemma 2. *If the curves $f = 0$ and $g = 0$ have no common component, then the number of points of $\mathbb{C}^{*2}$ common to both curves is at most*

$$V(\mathcal{N}(f) + \mathcal{N}(g)) - V(f) - V(g).$$

In particular, if in addition the polynomial g has the same support as $f(x^k, y^k)$ for some positive integer k, then the number of such points is at most $2kV(f)$.

Proof. The first statement of the lemma is a based on a slight strengthening, due to Fulton [F] p. 122, of a result of D. N. Bernstein, A.G. Kouchnirenko, and A.G. Khovanskii which, in the two variable case, gives an upper bound for the number of points of $\mathbb{C}^{*2}$ on two plane algebraic curves $f = 0, g = 0$ without common component. More precisely, they give a bound $2V(f, g)$ for the sum of the intersection numbers of the points on both curves. Here $V(f, g)$ is the *mixed volume* of $\mathcal{N}(f)$ and $\mathcal{N}(g)$. The theory of mixed volumes is discussed in [E], p.82, but for our purposes we can just use the fact that $2V(f, g) = V(\mathcal{N}(f) + \mathcal{N}(g)) - V(f) - V(g)$. (A very accessible account of this kind of result is given in [St].)

For the second part, we have $\mathcal{N}(g) = k\mathcal{N}(f)$, so that

$$V(\mathcal{N}(f) + \mathcal{N}(g)) - V(f) - V(g) = ((1 + k)^2 - 1 - k^2)V(f) = 2kV(f).$$

Lemma 3. *(i) If $\mathcal{B}_1, \cdots, \mathcal{B}_k$ are convex bodies in $\mathbb{R}^n$, then*

$$V(\mathcal{B}_1 + \cdots + \mathcal{B}_k) \geqslant V(\mathcal{B}_1) + \cdots + V(\mathcal{B}_k).$$

(ii) If $g = g_1 g_2 \cdots g_k$, where g and the g_i are in $\mathbb{C}[x, y]$, then

$$\mathcal{N}(g) = \mathcal{N}(g_1) + \cdots + \mathcal{N}(g_k).$$

Proof. (i) By the Brunn-Minkowski inequality ([E], p.97), we have that

$$V(\mu\mathcal{B}_1 + (1 - \mu)\mathcal{B}_2)^{\frac{1}{n}}$$

is a convex function of $\mu, 0 \leqslant \mu \leqslant 1$. Putting $\mu = 1/2$ and taking the nth power gives the result for $k = 2$, from which the general case follows immediately. (In fact this proof gives a stronger result, namely (i) with V replaced by $V^{1/n}$ throughout, but we do not need this for our purposes.)

(ii) It is enough to do the case $k = 2$. This follows from the fact that if $g = g_1 g_2$ then each extreme point of $\mathcal{N}(g)$ is a sum of an extreme point of $\mathcal{N}(g_1)$ and an extreme point of $\mathcal{N}(g_2)$.

Note that, from Lemma 3(ii), the term $V(\mathcal{N}(f) + \mathcal{N}(g))$ in Lemma 2 is simply $V(fg)$.

We now prove the theorem. We separate the proof into various cases.

4.3 $\mathcal{L}(f)$ *of rank* 1.

Here $V(f) = 0$ and, from 3.2, f has either no cyclotomic points, or it has a factor of the form $x^i y^j - \omega$, and infinitely many cyclotomic points. Hence the theorem is true in this case.

4.4 $\mathcal{L}(f)$ *full, of rank* 2, f *with coefficients in* $\mathbb{Q}^{\mathrm{ab}}$, *irreducible over* $\mathbb{Q}^{\mathrm{ab}}$.

In this case we know from 3.4 that in Case I (N odd) any cyclotomic point of f lies on one of the seven f_i given there. We can therefore apply Lemma 2, with f defining our curve, and $g = f_i$, noting that for $i = 1, 2, 3$, f_i has the same support as f, while for $i = 4, 5, 6, 7$, f_i has the same support as $f(x^2, y^2)$. Hence we have

$$V(f, f_i) = \begin{cases} 2V(f) & \text{for } i = 1, 2, 3 \\ 4V(f) & \text{for } i = 4, 5, 6, 7 \end{cases}$$

Summing these bounds over all i, we have that the number of cyclotomic points on f cannot exceed $(3 \times 2 + 4 \times 4)V(f) = 22V(f)$.

For Case II P lies on one of the seven curves $f_1, f_2, f_3, f^\tau, f_1^\tau, f_2^\tau$ and f_3^τ. Note that the definition of these curves depends only only on N, not on m. Also, each of these curves has the same support as f. Hence from Lemma 2 we see that f has at most $14V(f)$ cyclotomic points in this case.

4.5 $\mathcal{L}(f)$ *non-full.*

We saw in Section 3.7 that the number of cyclotomic points of f is I times the number on the curve defined by a certain polynomial f^* having a full lattice. Since we now know that our theorem holds for f^*, and noting that $V(f) = IV(f^*)$, we see that the proof in 4.4 applies with $\mathcal{L}(f)$ nonfull as well.

4.6 f *with complex coefficients, absolutely irreducible and non-reciprocal.*

If (x, y) is a cyclotomic point, then its complex conjugate $(\bar{x}, \bar{y}) = (x^{-1}, y^{-1})$ is a cyclotomic point of $f^\dagger$, where $f^\dagger(x, y) = \bar{f}(x^{-1}, y^{-1})$. Since f and $f^\dagger$ are inequivalent, they can have no common component. Now the Newton polytope of $f^\dagger$ is a 180° rotation of that of f. Thus the Minkowski sum $\mathcal{N}(f) + \mathcal{N}(f^\dagger)$ is what is called the *difference body* of $\mathcal{N}(f)$, namely the set $\{\underline{x}_1 - \underline{x}_2 \mid \underline{x}_1, \underline{x}_2 \in \mathcal{N}(f)\}$. It was proved by Rademacher [R] that for any convex body S in the plane, its difference body has area $\leqslant 6V(S)$, with equality iff S is a triangle. [In n dimensions the corresponding bound is $\binom{2n}{n}V(S)$, with equality iff S is an n-simplex. See Rogers and Shephard [RS] for a surprisingly simple proof of this general upper bound.] Thus as $V(f) = V(f^\dagger)$, we have $2V(f, f^\dagger) \leqslant (6 - 1 - 1)V(f) = 4V(f)$, and so, by Lemma 2, f has at most $4V(f)$ cyclotomic points.

4.7 f *with complex coefficients, absolutely irreducible, and coefficient field not in* $\mathbb{Q}^{\mathrm{ab}}$.

Take f^σ as in 3.6. Then f and f^σ have the same cyclotomic points. Also, as $f \neq f^\sigma$, and f^σ has the same support as f, we have from Lemma 2 that f has at most $2V(f)$ cyclotomic points.

4.8 f reducible.

We can now show that the irreducibility restrictions in 4.4, 4.6 and 4.7 can be removed. For instance, for 4.4, write $f = f_1 \cdots f_k$ as a product of factors irreducible over $\mathbb{Q}^{ab}$. If all of these factors have rank 2 lattices, then we have from 4.3 and Lemma 3(i), (ii) that the number of cyclotomic points on f is at most

$$22(V(f_1) + \cdots + V(f_k)) \leqslant 22V(\mathcal{N}(f_1) + \cdots + \mathcal{N}(f_k)) = 22V(f).$$

If any of the factors have lattices of rank 1, then from 4.2 they have either no cyclotomic points or infinitely many, so the result stated in the theorem is again true. The same argument applies for 4.6 and 4.7.

The results of the theorem concerning the constants follow from the examples in the next section.

4.9 Remarks.

1. In the proof we showed that if the minimal N (in the sense defined above) such that the coefficient field of f is $\mathbb{Q}(\omega_N)$ where N is divisible by 4, then f has at most $14V(f)$ cyclotomic points.

2. The constant 22 in the theorem seems at first sight probably to be a construct of the particular method of proof, and so unlikely to be best possible. This may indeed be the case. However, it is interesting to note that there is another proof, using cubes and cube roots of unity instead of squares and ± 1, which also gives the constant 22! For this proof, we intersect $f = 0$ with the 9 curves defined by the polynomials $f(x^3, y^3)$ and $f(\omega_3^i x, \omega_3^j y)(i, j = 0, 1, 2)$ with $(i, j) \neq (0, 0)$. Now it is easy to check that every root of unity ω is conjugate either to ω^3 or to $\omega_3\omega$ or to $\omega_3^2\omega$. Thus any cyclotomic point of f must also lie on one of these other curves, and so, using Lemma 2, we obtain the upper bound $(6 + 8 \times 2)V(f) = 22V(f)$ for the total number of cyclotomic points of f.

3. We compare the bound $22V(f)$ of our theorem with what could be obtained using Bezout's theorem. Suppose for instance that $f \in \mathbb{Q}[x, y]$, irreducible over $\mathbb{Q}$, and of degree d. Then from 3.4 f_1, f_2 and f_3 each has degree d too, while f_4, f_5, f_6 and f_7 each has degree $2d$. Hence, by Bezout, the number of projective points (counted with multiplicity) of both f and f_i is $\deg f . \deg f_1$, which is $d^2 (i = 1, 2, 3)$ and $2d^2 (i = 4, 5, 6, 7)$, giving a total of at most $11d^2$ points. Now this is also what we get from our theorem in the worst case that $\mathcal{N}(f)$ is as large as possible for a polynomial of degree d, namely $V(f) = \frac{1}{2}d^2$. Hence our result at worst gives the same as Bezout, but often gives a significant improvement.

4. The theorem may be extended to f defined over any field of characteristic 0. This is simply because the coefficient field of such an f is isomorphic to a subfield of $\mathbb{C}$.

5. Examples and applications.

Example 5.1 below shows that the constant 22 in $22V(f)$ in the theorem cannot be reduced below 16. This remains true even if we restrict our attention to curves whose degrees tend to infinity, as the examples $f(x^\ell, y^\ell) = 0$ (f as in Example 5.1) show. Of course these curves no longer have full lattices. In Section 6 below we give a strengthening of the theorem, for which this example is actually best possible. However, the upper bound in this stronger theorem is, unlike the bound $22V(f)$, not straightforward to calculate. The fact that this revised result is sharp does however show, as its proof indicates, that it essential to consider the intersection of f with all seven polynomials f_i.

Example 5.2 shows that the constant 4 in $4V(f)$ is best possible in the non-reciprocal case. For this case, the Bezout degree-type upper bound for the number of cyclotomic points of f is $2d^2$, for f a polynomial of degree d. This is because $f^\dagger$ has degree at most $2d$. Again, this example shows that the constant 2 in this degree-type bound cannot be improved. Example 5.3 shows that the constant 2 for curves with some non-cyclotomic coefficients cannot be improved. The family of curves in Example 5.4 shows that, even for curves with full lattices and arbitrarily high degree the constant in the theorem must be at least 10.

In 5.5 and 5.6 we give two applications of our results.

5.1. *A curve with the largest-known constant* 16.
Take

$$f(x,y) = xy + \frac{1}{xy} + x + \frac{1}{x} + y + \frac{1}{y} + 1.$$

Here f is reciprocal, and $V(f) = 3$, so the theorem tells us that there are at most 66 cyclotomic points of f. In fact, f has exactly 48 cyclotomic points, which we classify according to which other curve $f_i = 0$, defined in 3.4, that they also lie on.

On $f(x,-y) = 0 : (\omega_{12}^4, \omega_{12})$, (4 points)
On $f(-x,y) = 0 : (\omega_{12}, \omega_{12}^4)$, (4 points)
On $f(-x,-y) = 0 : (-\omega_{12}, \omega_{12})$, (4 points)
On $f(x^2,y^2) = 0 : (\omega_7, \omega_7^2)$, (ω_7^2, ω_7), (12 points)
On $f(x^2,-y^2) = 0 : (-\omega_{30}^3, \omega_{30})$, (8 points)
On $f(-x^2,y^2) = 0 : (\omega_{30}, -\omega_{30}^3)$, (8 points)
On $f(-x^2,-y^2) = 0 : (\omega_{30}, \omega_{30}^{11})$, (8 points).

To try to understand why this particular polynomial has so many cyclotomic points, let Z_6 be the cyclic subgroup of $SL_2(\mathbb{Z})$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, and consider its action, as defined in 3.7. As the orbit of x under Z_6 is $\{x, y^{-1}, x^{-1}y^{-1}, x^{-1}, y, xy\}$, having sum $f(x,y) - 1$, we see that for any point (x,y) on $f(x,y) = 0$, every point in the orbit of (x,y) under Z_6 will also be on the curve. In fact, since $f(x,y) = f(y,x)$, the same is true for the group $\langle Z_6, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$ of order 12. Thus, a single cyclotomic point on this curve potentially gives an orbit of twelve cyclotomic points on the curve. In fact, this is what happens: there are four orbits of twelve points each.

Given that f has so many cyclotomic points, one might expect its Mahler measure (the geometric mean of $|f|$ on $|x| = |y| = 1$) to be small. And indeed it is the two-variable polynomial with integer coefficients of smallest known Mahler measure greater than 1 ([B]).

Note that the primes $2, 3, 5$ and 7 all appear as divisors of the orders of the coordinates of cyclotomic points on this curve. In fact, this *must* happen for any f having more than $14V(f)$ cyclotomic points. For otherwise there would be a prime

$p \leqslant 7$ such that all cyclotomic points of f would also lie on $f(x^p, y^p) = 0$. Then by Lemma 2 there could be at most $2pV(f) \leqslant 14V(f)$ cyclotomic points on the curve.

5.2. *A family of curves with the maximum number of cyclotomic points for nonreciprocal curves.*

Put

$$f(x,y) = 1 + x + x^2 + \cdots + x^n + y + y^2 + \cdots + y^m.$$

We find below all points on the intersection of $f = 0$ and $f^\dagger = 0$. This shows that, as f and $f^\dagger$ have no common component, f has no reciprocal factors — presumably it is not difficult to show that it is actually irreducible, but we do not need that here — and as $V(f) = \frac{1}{2}mn$, that, by the theorem, there are at most $2mn$ cyclotomic points of f. And indeed, there are exactly $2mn$ points, as we now show.

Writing $f^\dagger(x,y) = f(1/x, 1/y)$ as $(1+x+\cdots+x^n)/x^n + (y+y^2+\cdots+y^m)/y^{m+1}$, we can eliminate $(1 + x + \cdots + x^n)$ from f and $f^\dagger$ to obtain $\frac{y^m-1}{y-1}(y^{m+1} - x^n) = 0$. By symmetry, also $\frac{x^n-1}{x-1}(x^{n+1} - y^m) = 0$. Now

(i) if $y^m = 1, y \neq 1$ then from $f = 0$ we have $x^{n+1} = 1, x \neq 1$, giving $n(m-1)$ points $(\omega_{n+1}^i, \omega_m^j), (i = 1, \cdots, n; j = 1, \cdots, m-1)$.

(ii) If $x^n = 1, x \neq 1$ we obtain by symmetry $m(n-1)$ points $(\omega_n^i, \omega_{m+1}^j), (i = 1, \cdots, n-1; j = 1, \cdots, m)$.

(iii) Finally if $y^{m+1} = x^n$ and $x^{n+1} = y^m$ we have, on eliminating y^m that $y = 1/x$ and so, from $f = 0$ that $x^{n+m+1} = 1, x \neq 1$. This gives $n + m$ points $(\omega_{n+m+1}^i, \omega_{n+m+1}^{-i}), (i = 1, \cdots, n+m)$.

Note that $\mathcal{N}(f)$ is triangular which, by Rademacher's result above, is necessary in order that f has the maximum number $4V(f)$ of cyclotomic points. Note too that $\mathcal{L}(f)$ is full, so that the constant 4 in the nonreciprocal part of the theorem cannot be improved, even if we restrict our attention to curves with full lattices whose degrees are bounded below by a number tending to infinity.

5.3. *A family of curves with the maximum number of cyclotomic points for curves having not all coefficients belonging to a cyclotomic field.*

Let

$$f(x,y) = 1 + x + x^2 + \cdots + x^n + \theta(1 + y + y^2 + \cdots + y^m),$$

where $\theta^3 - \theta - 1 = 0$. As $\mathbb{Q}(\theta)$ has non-abelian Galois group, $\theta \notin \mathbb{Q}^{\mathrm{ab}}$. Define automorphisms $\sigma_1, \sigma_2 \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ mapping θ to its other conjugates θ_1, θ_2. Then any cyclotomic point (x, y) of f is also a cyclotomic point of f_{σ_1} and f_{σ_2}, and so of their average $1 + x + \cdots + x^n$. Hence also $1 + y + y^2 + \cdots + y^m = 0$, and so f has $nm = 2V(f)$ cyclotomic points $(\omega_{n+1}^i, \omega_{m+1}^j), (i = 1, \cdots, n; j = 1, \cdots, m)$.

A similar example, but with some transcendental coefficients, could be obtained by replacing θ by π!

5.4. *A family of curves with constant asymptotically at least* 10.

Consider the curve

$$1 + y + y^{-1} + \sum_{r=1}^{n} x^r + x^{-r} = 0.$$

We shall give as many points (x, y), with x, y roots of unity, as possible. The trick is to make a choice for y and then solve the remaining equation in roots of unity x. We count the number of solutions.

(i) $y = \omega_3, \omega_3^{-1}$. The equation for x reads

$$(x^n + \cdots + x)(1 + x^{-n-1}) = 0$$

Any common zero of both factors has $x^n = 1$ and $x^{n+1} = -1$. This is possible only if n is even, in which case $x = -1$ is the double root. The number of x-values is $2n$ or $2n - 1$ if n is odd or even respectively.

(ii) $y = \pm i$. The equation for x reads

$$x^{2n} + \cdots + x + 1 = 0$$

Hence there are $2n$ values for x.

(iii) $y = \omega_6, \omega_6^{-1}$. The equation for x is

$$(x^n + \cdots + x + 1)(1 + x^{-n}) = 0$$

Any common factor of both factors has $x^{n+1} = 1$ and $x^n = -1$. This is possible only if n is odd, in which case $x = -1$ is the double root. The number of x-values is $2n$ or $2n - 1$ if n is even or odd respectively.

(iv) $y = x^{n+1}, x^{-n-1}$. The equation for x is

$$x^{2n+2} + \cdots + x + 1 = 0$$

Hence $x^{2n+3} = 1$ and $x \neq 1$. This gives us $2n + 2$ values $x = e^{\pm 2\pi ik/(2n+3)}$ for $k = 1, \cdots, 2n + 2$. The corresponding value of y is $e^{2\pi ik(n+1)/(2n+3)}$. This may coincide with one of the previously found y if $2n+3$ is divisible by 3 and $k(n+1) \equiv 0 \pmod{2n/3 + 1}$. So, if $n \equiv 0 \pmod 3$ then we have only $2n$ new values for x, and $2n + 2$ values in the other cases.

(v) $y = -x^n, -1/x^n$. The equation for x is

$$x^{2n-2} + \cdots + x + 1 = 0$$

Hence $x^{2n-1} = 1$ and $x \neq 1$. This gives us $2n - 2$ values $x = e^{2\pi ik/(2n-1)}$ for $k = 1, \cdots, 2n - 2$. The corresponding value of y is $-e^{\pm 2\pi ikn/(2n-1)}$. This may coincide with one of the previously found y if $2n - 1$ is divisible by 3 and $kn \equiv 0 \pmod{(2n - 1)/3}$. So, if $n \equiv 2 \pmod 3$ then we have only $2n - 4$ new values for x, and $2n - 2$ values in the other cases.

Also, the two latter cases have no x-values in common, since the first consists of $(2n + 3)$-th roots unity and the second of $(2n - 1)$-th roots of unity. Note that $\gcd(2n + 3, 2n - 1) = 1$.

In total we find $10n-3$ values of x if $n \not\equiv 1 \pmod 3$ and $10n-1$ values if $n \equiv 1 \pmod 3$. To each x-value correspond two y-values. Hence we find $20n-2$ points if $n \equiv 1 \pmod 3$ and $20n-6$ points otherwise.

Here are some additional solutions. When $n \equiv 1 \pmod 6$ we have $x = \omega_6^{\pm 1}, y = -1$. We can check that these are really two extra solutions. When $n \equiv 4 \pmod 6$ we have $x = \omega_6^{\pm 1}, y = 1$. Again, we can check that these are really two extra solutions. In particular, when $n \equiv 1 \pmod 6$ we have at least $20n$ solutions. Since $V(f) = 2n$ we have at least $10V(f)$ solutions in this case.

5.5 *Application to generalised Lie-symmetries.*

In [BSW] the authors study generalised Lie-symmetries of certain partial evolution equations. It turned out that some systems do allow for infinitely many symmetries if a particular diophantine equation in roots of unity has a solution. The equations solved in [BSW] read

$$2x^2y^2 - x^2y + x^2 - xy^3 - 2xy^2 - xy + 2y^2 - y^3 + y^4 = 0$$

and

$$x^2y^2 - x^2y + x^2 - xy - xy^3 + y^2 - y^3 + y^4 = 0.$$

Using the algorithm described in Section 3 we find that their solutions sets are

$$(x, y) = (1, 1), (1, \pm i), (\pm i, -1), (\pm i, \mp i), (\omega_3, \omega_3^2)(2 \text{ points})$$

and

$$(x, y) = (1, 1), (\pm 1, \pm i), (\omega_5, \omega_5^2)(4 \text{ points}), (\omega_5, \omega_5^4)(4 \text{ points})$$

respectively.

5.6. *The zeroes of derivatives of Chebyshev polynomials.*

Put $f_\lambda(x, y) = xy + \lambda(x + y) + 1$. Here λ is a rational parameter, which we can assume is positive. We also assume $\lambda \neq 1$, so that f_λ is irreducible. We find that for all such λ there are the two cyclotomic points $(1, -1)$ and $(-1, 1)$. For $\lambda \notin \{\frac{1}{2}, 2\}$, these are the only two points. However, for $\lambda = 2$ there is (ω_3, ω_3^2) (two more points), and for $\lambda = \frac{1}{2}$ there is (ω_3, ω_3).

We are interested in this family of curves because we can use them to prove the following. For a natural number n, let $U_n(X)$ be the nth Chebyshev polynomial of the second kind, defined by

$$U_n(z + z^{-1}) = \frac{z^{n+1} - z^{-(n+1)}}{z - z^{-1}}.$$

Proposition. *The polynomial $U_n'(X)$ has no zeroes of the form $2\cos 2\pi q \neq 0$ for any rational q.*

This result is applied in [DS]. Curiously, as remarked there, this result is in contrast to the situation for the Chebyshev polynomials $T_n(X)$ of the first kind.

For as $T'_n(X) = nU_{n-1}(X)$, *all* zeroes of $T'_n(X)$ are of the form $2\cos 2\pi q$ for some rational values of q.

To prove the proposition, note first that

$$z^{n-1}(z^2-1)^3 U'_n(z+z^{-1}) = n(z^{2n+4}-1) - (n+2)(z^{2n+2}-z^2).$$

When is the right-hand side zero for z a root of unity? Putting $\frac{n+2}{n} = \lambda > 1$, $x = z^2$ and $y = -z^{2n+2}$, we see that $f_\lambda(x,y) = 0$. Now the two points $(1,-1)$ and $(-1,1)$ on $f_\lambda = 0$ have $z = \pm 1$ or $z = \pm i$. In the latter case $X = z + z^{-1} = 0$, which is excluded in the proposition. (In fact, 0 is a root of U'_n for n even.) One can check directly that $U'_n(\pm 2) \neq 0$. It remains only to consider the case $\lambda = 2, n = 2$. In this case $(x,y) = (z^2, -z^6) = (\omega_3, \omega_3^2)$, which is impossible.

6. Improving the theorem.

Let f and g be in $\mathbb{C}[x,x^{-1},y,y^{-1}]$. The improvement of our theorem which we now give is based on the the following simple remark. If the ideal $[f,g]$ of $\mathbb{C}[x,x^{-1},y,y^{-1}]$ is equal to $[f^*,g^*]$ for some f^*,g^* in $\mathbb{C}[x,x^{-1},y,y^{-1}]$, then by Lemma 2 the number of cyclotomic points on $f=0$ and $g=0$ is at most $2V(f^*,g^*)$. We therefore define $V^*(f,g)$ to be the minimum of all $V(f^*,g^*)$ with f^*,g^* in $\mathbb{C}[x,x^{-1},y,y^{-1}]$ and $[f,g] = [f^*,g^*]$. Then the first part of our theorem (the other parts already being sharp) can be restated as follows, using the polynomials f_i of Section 3. To avoid complications, we state the result only for f with rational coefficients, and irreducible over $\mathbb{Q}$.

Theorem*. *Let $f \in \mathbb{Q}[x,x^{-1},y,y^{-1}]$ be irreducible over the rationals, with area $V(f) > 0$. Then f has at most $2\sum_{i=1}^{7} V^*(f,f_i)$ cyclotomic points.*

Because of the difficulty of computing the $V^*(f,f_i)$, the bound in this theorem is not as useful for practical purposes as the bound in the original theorem. However, it is a sharp result, as we now use Example 5.1 to show. We compute the $V^*(f,f_i)$ for this example, with $f(x,y) = xy + \frac{1}{xy} + x + \frac{1}{x} + y + \frac{1}{y} + 1$. We have, after some area computations, that

$2V^*(f,f_i) \leqslant 2V((f+f_i, f-f_i) = 4$ for $i = 1,2,3$

$2V^*(f,f_4) \leqslant 2V(f,f_4) = 12$

$2V^*(f,f_i) \leqslant 2V(f, f_i - ff_{i-4}) = 8$ for $i = 5,6,7$.

Thus the improved theorem gives at most 48 cyclotomic points! Incidentally, apart from showing that the result is sharp, it proves that the above three inequalities are actually equalities, so that we have in fact computed all the $V^*(f,f_i)$ exactly for this example.

Acknowledgement. The authors are grateful for the hospitality of the Newton Institute, Cambridge, in June 1998, where this collaboration was begun.

References

[B] David W. Boyd, Speculations concerning the range of Mahler's measure, Canad. Math. Bull. **24** (1981), 453–469.

[BD] R.J. Bradford and J.H. Davenport, Effective tests for cyclotomic polynomials, Symbolic and algebraic computation (Rome, 1988), 244–251, Lecture Notes in Comput. Sci., **358**, Springer, Berlin-New York, 1989.

[BSW] Frits Beukers, Jan A. Sanders and Jing Ping Wang, One symmetry does not imply integrability, J. Diff. Eq., **146** (1998), 251–260.

[D] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith. **34** (1979), 391–401.

[DS] A. Dubickas and C.J. Smyth, The Lehmer constants of an annulus, J. Th. Nombres Bordeaux (to appear 2001).

[E] H.G. Eggleston, "Convexity", C.U.P., Cambridge 1958.

[F] William Fulton, "Introduction to Toric Varieties", Princeton University Press, Princeton 1993.

[HS] Marc Hindry and Joseph H. Silverman, "Diophantine Geometry: an Introduction", Springer-Verlag, New York 2000.

[La] Serge Lang, Division points on curves, Ann. Mat. Pura Appl. (4) **70** (1965), 229–234.

[Li] P. Liardet, Sur une conjecture de Serge Lang, Astérisque **24–25** (1975), 187–209.

[M] Michael McQuillan, Division points on semi-abelian varieties, Inv. Math. **120** (1995), 143–159.

[N] Morris Newman, "Integral Matrices", Academic Press, New York and London 1972.

[R] H. Rademacher, Über den Vektorenbereich eines konvexen ebenen Bereiches, Jber. Deutsch. Math.-Verein. **34** (1925), 64–79.

[RS] C.A. Rogers and G. C. Shephard, The difference body of a convex body, Arch. Math. **8** (1957), 220–233.

[Sc] W. M. Schmidt, Heights of points on subvarieties of $\mathbb{G}_m^n$, Number theory (Paris, 1993–1994), 157–187, London Math. Soc. Lecture Note Ser., **235**, Cambridge Univ. Press, Cambridge, 1996.

[Sm] C.J. Smyth, Salem numbers of negative trace, Math. Comp. **69** (2000), 827–838.

[St] Bernd Sturmfels, Polynomial equations and convex polytopes, Amer. Math. Monthly, **105** (1998), 907–922.

Department of Mathematics
Rijksuniversiteit te Utrecht
3508 TA Utrecht
The Netherlands
email: beukers@math.uu.nl

Department of Mathematics and Statistics,
University of Edinburgh,
JCMB, King's Buildings,
Mayfield Road,
Edinburgh EH9 3JZ, UK.
email: chris@maths.ed.ac.uk