ACTA ARITHMETICA
XXXVI (1980)

On the representation of units by cyclotomic polynomials

by

VEIKKO ENNOLA (Turku)

Let m be a natural number, $\Phi_m(x)$ the mth cyclotomic polynomial, and $\zeta = \zeta_m$ a suitably chosen primitive mth root of unity. By a *J-field* we mean an algebraic number field which is either totally real or a totally imaginary quadratic extension of a totally real field. For the general theory of such fields we refer the reader to [4]. Clearly abelian extensions of Q (i.e. subfields of cyclotomic fields) are J-fields. Subfields, joins, and normal closures of J-fields are also J-fields.

Let K be a J-field. By S_∞ we denote the set of archimedean valuations of K. Following Győry [4], we call a non-archimedean valuation ψ of K *real* iff $\psi(\alpha) = \psi(\bar{\alpha})$ for all $\alpha \in K$, where $\bar{\alpha}$ denotes the complex conjugate of α. If K_0 denotes the maximal real subfield of K, then ψ is real if and only if ψ is either ramified or inert in the extension K/K_0. Let S be a finite set of valuations of K containing S_∞. An element α of K is called an *S-integer* (*S-unit*) iff $\psi(\alpha) \leqslant 1$ ($\psi(\alpha) = 1$) for all valuations ψ of K not contained in S.

Let $p > 3$ be a prime and put $K = Q(\zeta_p)$. Grossman [3] has investigated the diophantine equation

$$\Phi_m(\xi) = \eta \tag{1}$$

where ξ and η are units of K and ξ is not a root of unity. He showed that the equation (1) has no solutions if $m > 2$, $m \neq 3, 6$, and determined the solutions for $m = 3$ or 6. He further noted that if K is any J-field, η is a unit of K, and ξ is a non-zero number of K which is not a root of unity, then from the validity of (1) it follows that $m \leqslant m_0$ for some constant m_0 depending on the degree $[K:Q]$. From the results of Schinzel ([7], cf. also [6]) it follows that the same holds for any field K. Grossman asks whether m_0 may be found independent of $[K:Q]$ in the case when K is a J-field. The following theorem answers this question in the affirmative.

THEOREM 1. *Let ξ be a non-zero algebraic number not a root of unity such that $Q(\xi)$ is a J-field. Suppose that $m \geqslant 5$, $m \neq 6$, and that $\Phi_m(\xi)$*

is an S-unit for some finite set $S \supseteqq S_\infty$ of valuations of the field $Q(\xi, \zeta)$ such that every $\psi \in S \setminus S_\infty$ is real. Then $Q(\xi)$ is an abelian extension of Q and $m \leqslant m_0$ for some absolute constant m_0.

From the proof it should be easy to obtain a numerical value for m_0. One should also be able to find all possible solutions for the remaining values of m as in [3]. A natural question is what can be said in the case when S is a set of valuations of $Q(\xi)$ and not of $Q(\xi, \zeta)$. Obviously the theorem does not remain true in this generality. This is seen trivially by taking ξ totally real. Less trivial examples are the following ones. Take $a = 3 + \sqrt{3}$, $\xi = \sqrt{-a}$. Then $K = Q(\xi)$ is a non-normal extension of Q which is a J-field. We have

$$\Phi_8(\xi) = \xi^4 + 1 = a^2 + 1 = 13 + 6\sqrt{3},$$

$$\Phi_{16}(\xi) = \xi^8 + 1 = a^4 + 1 = 253 + 144\sqrt{3},$$

$$\Phi_{32}(\xi) = \xi^{16} + 1 = a^8 + 1 = 7(17959 + 10368\sqrt{3}).$$

Let S' denote the set of primes of K lying above $13 + 6\sqrt{3}$, $253 + 144\sqrt{3}$, 7, $17959 + 10368\sqrt{3}$, and put $S = S_\infty \cup S'$. It is not hard to check that the primes in S' are real.

In connection with the result of Schinzel it is also natural to consider representations by the homogenized cyclotomic polynomial $\Phi_m(x, y) = y^{\varphi(m)}\Phi_m(x/y)$. In this case we can prove

THEOREM 2. *Let ξ and η be non-zero algebraic numbers such that $Q(\xi, \eta)$ is a J-field. Let $S \supseteqq S_\infty$ be a finite set of valuations of the field $Q(\xi, \eta, \zeta)$ such that every $\psi \in S \setminus S_\infty$ is real. Suppose that ξ and η are S-integers and that $\Phi_m(\xi, \eta)$ is an S-unit. Then either $\bar\eta/\xi$ is a root of unity or there exist absolute constants $m_1 < m_2$ such that $m \leqslant m_2$ and for $m \geqslant m_1$ $Q(\bar\xi/\xi, \eta/\xi, \bar\eta/\xi)$ is an abelian extension of Q.*

In the case when $\bar\eta/\xi$ is a root of unity, writing $\bar\eta = \xi\theta^2$, $\omega = \eta\theta$, we have $\Phi_m(\bar\omega, \omega) = \theta^{\varphi(m)}\Phi_m(\xi, \eta)$. It is easy to construct examples where ω is an S-unit for a suitable S showing that there is no absolute bound for m, but excluding this case the question still remains open whether there then is such a bound.

Finally, taking into account the close connection between the nature of $\Phi_m(\xi, \eta)$ and the existence of a primitive divisor of the expression $\xi^m - \eta^m$ (see [6] and [7]), one is led to ask whether there exists an absolute constant m_0 such that the expression $\xi^m - \eta^m$ has a primitive divisor for $m \geqslant m_0$ when $(\xi, \eta) = 1$, ξ/η is not a root of unity, and $Q(\xi, \eta)$ is a J-field.

Proof of the theorems. We shall use an idea of Newman (cf. [2]) combined with results of Győry [4] and the recent results of Conway and Jones [1] on relations between roots of unity. We begin with a proof of the first part of Theorem 1. Put $\varepsilon_k = \xi - \zeta^k$ ($(k, m) = 1$). Let ψ be any valuation of the field $Q(\xi, \zeta)$ which does not belong to S. Since $\psi(\Phi_m(\xi)) = 1$ and $\Phi_m(x)$ is a monic polynomial with integral coefficients, we have $\psi(\xi) \leqslant 1$. Therefore clearly $\psi(\varepsilon_k) = 1$ for each k, so that the ε_k are S-units. From [4], p. 154, Th. 1, it follows that $\varrho_k = \bar\varepsilon_k/\varepsilon_k$ is a root of unity for each k. From the assumption of our theorem $\varphi(m) \geqslant 3$. Therefore it is possible to choose ζ so that ε_1 is not purely imaginary. From the equations $\bar\varepsilon_1 = \varrho_1\varepsilon_1$, $\bar\varepsilon_{-1} = \varrho_{-1}\varepsilon_{-1}$ we obtain

$$(2)\qquad \begin{aligned}(\varrho_1 - \varrho_{-1})\varepsilon_1 &= (1 + \varrho_{-1})(\zeta - \zeta^{-1}),\\ (\varrho_1 - \varrho_{-1})\varepsilon_{-1} &= (1 + \varrho_1)(\zeta - \zeta^{-1}).\end{aligned}$$

Since ε_1 is not purely imaginary, $\varrho_1 \neq -1$, whence $\varrho_1 \neq \varrho_{-1}$. Thus ε_1 belongs to a cyclotomic field so that $Q(\xi)$ is an abelian extension of Q. This proves the first part of Theorem 1. The second part is clearly contained in Theorem 2, whence in what follows we shall only be concerned with the proof of that.

As above we now denote $\varrho_k = (\bar\xi - \zeta^{-k}\bar\eta)/(\xi - \zeta^k\eta)$ for any k with $(k, m) = 1$, where again the ϱ_k are roots of unity. We assume that $\bar\eta/\xi$ is not a root of unity otherwise there is nothing to prove. We always suppose that m is sufficiently large. Take any r with $(r, m) = 1$, $r \not\equiv \pm 1 \bmod m$. We have

$$(3)\qquad \begin{aligned}\bar\xi - \zeta^{-1}\bar\eta - \varrho_1(\xi - \zeta\eta) &= 0,\\ \bar\xi - \zeta\bar\eta - \varrho_{-1}(\xi - \zeta^{-1}\eta) &= 0,\\ \bar\xi - \zeta^{-r}\bar\eta - \varrho_r(\xi - \zeta^r\eta) &= 0,\\ \bar\xi - \zeta^r\bar\eta - \varrho_{-r}(\xi - \zeta^{-r}\eta) &= 0.\end{aligned}$$

Consider (3) as a system of homogeneous linear equations in the unknowns $\bar\xi, \bar\eta, \xi, \eta$. The determinant of the coefficient matrix

$$(4)\qquad \begin{bmatrix} 1 & -\zeta^{-1} & -\varrho_1 & \varrho_1\zeta\\ 1 & -\zeta & -\varrho_{-1} & \varrho_{-1}\zeta^{-1}\\ 1 & -\zeta^{-r} & -\varrho_r & \varrho_r\zeta^r\\ 1 & -\zeta^r & -\varrho_{-r} & \varrho_{-r}\zeta^{-r}\end{bmatrix}$$

must vanish. Computing the determinant we obtain

$$(5)\qquad \begin{aligned}&(\varrho_1\varrho_{-1} + \varrho_r\varrho_{-r})(-\zeta^{r+1} - \zeta^{-r-1} + \zeta^{r-1} + \zeta^{-r+1}) -\\ &\quad - \varrho_1\varrho_r(\zeta^{2r} - 2\zeta^{r+1} + \zeta^2) - \varrho_{-1}\varrho_{-r}(\zeta^{-2r} - 2\zeta^{-r-1} + \zeta^{-2}) +\\ &\quad + \varrho_1\varrho_{-r}(\zeta^{-2r} - 2\zeta^{-r+1} + \zeta^2) + \varrho_{-1}\varrho_r(\zeta^{2r} - 2\zeta^{r-1} + \zeta^{-2}) = 0.\end{aligned}$$

Suppose that the rank of (4) is less than three. Then in particular the leading three by three minor determinant of (4) vanishes so that we have

$$(6)\qquad (\zeta - \zeta^{-1})\varrho_r + (\zeta^{-1} - \zeta^{-r})\varrho_{-1} + (\zeta^{-r} - \zeta)\varrho_1 = 0.$$

Using the language of Conway and Jones [1], let T denote the vanishing formal sum of roots of unity corresponding to the left-hand side of (6). Consider the root $\zeta\varrho_r$. If T does not involve $\zeta\varrho_r$, then there is another term on the left-hand side of (6) equal to $-\zeta\varrho_r$, and these two terms cancel out. On the other hand, if T does involve $\zeta\varrho_r$, then there is a minimal vanishing subsum T_1 of T involving $\zeta\varrho_r$. From [1], p. 235, Th. 5, it follows that the reduced exponent of T_1 divides 30. Thus in both cases there is another term on the left-hand side of (6) equal to $\alpha\zeta\varrho_r$, where $\alpha^{30} = 1$. This term cannot be $-\zeta^{-1}\varrho_r$ if m is large enough. Hence we have an equation of the form

$$\alpha\zeta\varrho_r = \zeta^{-ar-b}\varrho_u \quad (a \in \{0, 1\};\ b \in \{0, \pm 1\};\ u \in \{\pm 1\}).$$

Writing $X = \zeta^r$ we obtain from (3)

$$(7) \qquad \xi X - \bar{\eta} - \alpha^{-1}\zeta^{-1-b}\varrho_u X^{1-a}(\xi - \eta X) = 0.$$

Consider (7) as an equation in the unknown X. Since $\bar{\eta}/\xi$ is not a root of unity, (7) does not reduce to an identity. As there are only a finite number of equations (7), we obtain a contradiction for m sufficiently large choosing r suitably. Hence the rank of (4) must be three, so that all the ratios of $\xi, \bar{\eta}, \xi, \eta$ belong to a cyclotomic field. This proves the second assertion of Theorem 2.

Before proceeding further with the proof of Theorem 2 we need the following

LEMMA. *Let ξ and η be non-zero complex numbers satisfying the conditions*

$$\xi = \tau\xi, \qquad \bar{\eta} = \tau\eta, \qquad \xi - \zeta^{-k}\bar{\eta} = \varrho_k(\xi - \zeta^k\eta) \qquad (k \in Z,\ (k, m) = 1),$$

where τ and the ϱ_k are roots of unity. Then either $\xi = \pm\eta$ or $m \leqslant m_3$ for some absolute constant m_3.

Proof. Determine θ_k so that $\theta_k^2 = \varrho_k\tau^{-1}$. For each k with $(k, m) = 1$ we then have

$$(8) \qquad \xi/\eta = (\theta_k\zeta^k - \theta_k^{-1}\zeta^{-k})/(\theta_k - \theta_k^{-1}),$$

and in particular we see that $\theta_k^2 \neq 1, \zeta^{-2k}$. Combining the equation (8) as it stands and with k replaced by 1 we get the relation

$$(9) \qquad -\theta_1\theta_k\zeta + \theta_1\theta_k^{-1}\zeta + \theta_1\theta_k\zeta^k - \theta_1^{-1}\theta_k\zeta^k - \\ -\theta_1^{-1}\theta_k^{-1}\zeta^{-1} + \theta_1^{-1}\theta_k\zeta^{-1} + \theta_1^{-1}\theta_k^{-1}\zeta^{-k} - \theta_1\theta_k^{-1}\zeta^{-k} = 0.$$

We suppose that $m > m_3$ for a sufficiently large absolute constant m_3 and show that then $\xi = \pm\eta$. Arguing as before we obtain a non-trivial equation of the form

$$(10) \qquad \alpha\theta_1\theta_k\zeta = \theta_1^a\theta_k^b\zeta^{ck+d} \qquad (a, b \in \{\pm 1\};\ c, d \in \{0, \pm 1\};\ \alpha^{210} = 1).$$

Consider first the possibility $b = 1$. Then we must have $c = 0$, otherwise we obtain a contradiction choosing k suitably which is possible for large enough m. From (9) we now find that the only possibility is $a = d = -1$, whence $\theta_1^2 = \alpha^{-1}\zeta^{-2}$. From (8) with $k = 1$ we get

$$\xi/\eta = (1-\alpha)\zeta/(1-\alpha\zeta^2),$$

and we have a contradiction by assuming that ζ was originally so chosen that this equation does not hold for any α with $\alpha^{210} = 1$.

Thus $b = -1$. Put $X = \zeta^k$. Combining (8) and (10) we obtain

$$(\xi/\eta)(\alpha^{-1}\theta_1^{a-1}\zeta^{d-1}X^{c+1} - X) - \alpha^{-1}\theta_1^{a-1}\zeta^{d-1}X^{c+2} + 1 = 0.$$

Since this equation must reduce to an identity, we easily find that $c = -1$ and $\xi/\eta = \pm 1$. This proves the lemma.

Consider now the relation (5). Again we have a non-trivial equation

$$(11) \qquad \alpha\varrho_1\varrho_{-1}\zeta^{r+1} = \varrho_u\varrho_v\zeta^{ar+b} \qquad (u, v \in \{\pm 1, \pm r\};\ a, b \in \{0, \pm 1, \pm 2\}; \\ \alpha^M = 1),$$

where M denotes the product of primes < 20. We cannot have $\varrho_u\varrho_v = \varrho_1\varrho_{-1}$ otherwise we get a contradiction for a suitable r. (Note that if $a = 1$ then $b = -1$, which is impossible for large m.)

Suppose first that $\varrho_u\varrho_v = \varrho_r\varrho_{-r}$. Write $X = \zeta^r$, $\tau^2 = \alpha\varrho_1\varrho_{-1}\zeta^{1-b}$ so that $\varrho_r\varrho_{-r} = \tau^2 X^{1-a}$. From (3) we have

$$(\xi X - \bar{\eta})(\xi - \bar{\eta}X) = \tau^2 X^{1-a}(\xi X - \eta)(\xi - \eta X).$$

This equation must reduce to an identity, whence necessarily $a = 1$ and

$$\xi^2 + \bar{\eta}^2 = \tau^2(\xi^2 + \eta^2), \qquad \overline{\xi\eta} = \tau^2\xi\eta.$$

Hence $(\xi + \bar{\eta})^2 = \tau^2(\xi + \eta)^2$. Choosing the sign of τ suitably we thus have either $\xi = \tau\xi$, $\bar{\eta} = \tau\eta$ or $\xi = \tau\eta$, $\bar{\eta} = \tau\xi$. However, from the lemma we infer that in both cases $\bar{\eta}/\xi$ is a root of unity, a contradiction.

Suppose next that $u = \pm 1$ and $v = r$. Then $a \in \{0, 1, 2\}$. Writing $X = \zeta^r$ we have from (11) $\varrho_r = \alpha\varrho_{-u}\zeta^{1-b}X^{1-a}$, and then (3) implies

$$\xi X - \bar{\eta} = \alpha\varrho_{-u}\zeta^{1-b}X^{2-a}(\xi - \eta X).$$

This equation could only reduce to an identity for $a = 2$, but even then we get a contradiction because $\bar{\eta}/\xi$ is not a root of unity. The remaining case $u = \pm 1$, $v = -r$ is dealt with similarly. This completes the proof of Theorem 2.

References

[1] J. H. Conway and A. J. Jones, *Trigonometric diophantine equations* (*On vanishing sums of roots of unity*), Acta Arith. 30 (1976), pp. 229–240.

[2] V. Ennola, *A note on a cyclotomic diophantine equation*, ibid. 28 (1975), pp. 157–159.

[3] E. H. Grossman, *On the solutions of diophantine equations in units*, ibid. 30 (1976), pp. 137–143.

[4] K. Győry, *Sur une classe des corps de nombres algébriques et ses applications*, Publ. Math. (Debrecen) 22 (1975), pp. 151–175.

[5] — *Representation des nombres entiers par des formes binaires*, to appear in Publ. Math. (Debrecen).

[6] L. P. Postnikova and A. Schinzel, *Primitive divisors of the expression a^n-b^n in algebraic number fields*, Mat. Sbornik 75 (1968), pp. 171–177 (in Russian).

[7] A. Schinzel, *Primitive divisors of the expression A^n-B^n in algebraic number fields*, J. Reine Angew. Math. 268/269 (1974), pp. 27–33.

Received on 30. 7. 1977 (973)

ACTA ARITHMETICA
XXXVI (1980)

Rosser's sieve

by

Henryk Iwaniec (Warsaw–Pisa)

1. Introduction. Statement of the results. Let there be given a finite integer sequence $\mathscr{A}$ and a sequence P of primes. A basic problem of the sieve is to estimate, for any real number $z \geqslant 2$ the sum (sifting function)

$$S(\mathscr{A}, P, z) = \sum_{\substack{a \in \mathscr{A} \\ (a, P(z)) = 1}} 1$$

where $P(z) = \prod_{p<z,\, p\in P} p$. The sequence $\mathscr{A}$ can be almost arbitrary. The only knowledge we need about $\mathscr{A}$ is a good approximation formula (in an average sense) for the number of those elements from $\mathscr{A}$ which are divisible by the squarefree number $d|P(z)$;

$$\mathscr{A}_d = \{a \in \mathscr{A};\ a \equiv 0 \,(\operatorname{mod} d)\}.$$

We assume that $|\mathscr{A}_d|$ may be written in the form

$$|\mathscr{A}_d| = \frac{\omega(d)}{d} X + R(\mathscr{A}, d), \tag{1.1}$$

where $\frac{\omega(d)}{d} X$ is considered as a main term and $R(\mathscr{A}, d)$ is an error term. The arithmetic function $\omega(d)$ is multiplicative and for each prime number $p \in P$ it satisfies

$$0 < \omega(p) < p. \tag{1.2}$$

Since we need the formula (1.1) only for $d|P(z)$ we are free to define $\omega(p) = 0$ for $p \notin P$.

Our next assumption is about dimension. There exists a parameter $\varkappa \geqslant 0$ (dimension) and a constant $K \geqslant 2$ such that for all $z > w \geqslant 2$ we have

$$\prod_{w \leqslant p < z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} < \left(\frac{\log z}{\log w}\right)^{\varkappa} \left(1 + \frac{K}{\log w}\right). \tag{1.3}$$