References

[1] H. L. Montgomery and R. C. Vaughan, *Hilbert's inequality*, Journ. London Math. Soc. (2), 8 (1974), pp. 73–82.

[2] K. Ramachandra, *Progress towards a conjecture on the mean value of Titchmarsh series*, in: *Recent progress in analytic number theory* (Edited by H. Halberstam and C. Hooley), Vol. 1, Academic Press, 1981, pp. 303–318.

[3] — *Progress towards a conjecture on the mean value of Titchmarsh series, II*, Hardy-Ramanujan Journal 4 (1981), pp. 1–12.

[4] — *Some remarks on a theorem of Montgomery and Vaughan*, Journ. Number Theory 11 (1979), pp. 465–471.

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD
BOMBAY 400005, INDIA

Received on 11.5.1983
and in revised form on 20.6.1984 (1359)

On positive definite quadratic polynomials

by

R. J. Cook (Sheffield) and S. Raghavan (Bombay)

1. Introduction. It is well known that an indefinite quadratic form in 21 or more variables takes on arbitrarily small values at integer points (see Davenport and Ridout [8] for a full list of references). An analogous problem for positive definite quadratic forms has been considered by Davenport and Lewis in their interesting paper [7] which contains the following

Theorem 1 (Davenport and Lewis). *There exists an integer n_0 (absolute) with the following property:*

Let $Q(\boldsymbol{x}) = Q(x_1, \ldots, x_n)$ be a positive definite quadratic form with real coefficients and suppose that $n \geqslant n_0$. Then, if $x_1^*, \ldots, x_n^*$ are integers with $\max|x_i^*|$ sufficiently large, there exist integers $x_1, \ldots, x_n$, not all zero, such that

$$|Q(\boldsymbol{x}+\boldsymbol{x}^*) - Q(\boldsymbol{x}^*)| < 1. \tag{1}$$

In the course of their proof, Davenport and Lewis have however overlooked the (trivial) solution $\boldsymbol{x} = -2\boldsymbol{x}^*$ for (1); indeed, their proof of Theorem 1 assumes that (1) has no nonzero solutions and proceeds then to obtain a contradiction. The object of this note is to show that the very same analytic arguments used by them not only remove this lacuna but can also be adapted to yield many more integer solutions $\boldsymbol{x}$ of (1).

In (1), the term 1 can be replaced by an arbitrary $\varepsilon > 0$, and the result can then be regarded as a recurrence theorem. The quadratic form Q returns to the neighbourhood of values it has taken. Examples such as $\theta(x_1^2 + \ldots + x_n^2)$ show that it is not possible to obtain a theorem of the form "Q takes values close to all sufficiently large real numbers X" without some additional condition, such as incommensurability of the coefficients of Q.

Theorem 2. *There exists an integer $n_0 \leqslant 995$ and a constant $\tau > 0$ with the following property:*

Let $F(\boldsymbol{x})$ be a positive definite quadratic form with real coefficients and suppose that $n \geqslant n_0$. Then, if $x_1^*, \ldots, x_n^*$ are integers with $\max|x_i^*|$ sufficiently large, then there exist at least $[|\boldsymbol{x}^*|^\tau]$ integer points $\boldsymbol{x} \in \boldsymbol{Z}^n$ such that

$$|F(\boldsymbol{x}+\boldsymbol{x}^*) - F(\boldsymbol{x}^*)| < 1. \tag{2}$$

Davenport and Lewis did not attempt to give a bound for n_0, but inequalities (73) and (83) of [7] suggest a large value like 17401; the value 995 in Theorem 2 seems to be just about optimal with the present techniques although still far from the "anticipated value of 5".

We shall use $|x|$ to denote $\max|x_i|$ rather than the Euclidean norm; this does not really affect Theorem 2.

Recently, we have considered the values of indefinite quadratic polynomials (see [3] and [4]) and there are earlier results on inhomogenous forms due to Watson [10]. Let $x=(x_1, \ldots, x_n)$. We say that the real quadratic polynomial

$$F(x)=Q(x)+\Lambda(x)+C \tag{3}$$

is *positive definite* if the quadratic part $Q(x)$ is positive definite.

It is trivial to see that Theorem 2 holds also for positive definite quadratic polynomials $F(x)$.

2. A preliminary diagonalization. Let $F(x)$ be a positive definite quadratic polynomial, where

$$Q(x)=\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_{ij}x_i x_j \quad (\alpha_{ij}=\alpha_{ji}), \tag{4}$$

$$\Lambda(x)=\sum_{j=1}^{n}\lambda_j x_j; \tag{5}$$

and let $B(x, y)$ be the bilinear form associated with Q. Then

$$F(x+x^*)-F(x^*)=Q(x)+2B(x^*, x)+\Lambda(x)=Q(x)+\sum_{j=1}^{n}\nu_j x_j \tag{6}$$

say, where

$$\nu_j=\lambda_j+2\sum_{i=1}^{n}\alpha_{ij}x_i^*. \tag{7}$$

We may relabel the variables so that $\max|\nu_j|=|\nu_1|$ and, replacing x by $-x$ if necessary, we may also suppose that $\nu_1<0$. Let

$$P=-\nu_1, \quad B_2=-\nu_2, \quad \ldots, \quad B_n=-\nu_n \tag{8}$$

and

$$\begin{aligned} G(x)=F(x+x^*)-F(x^*)&=Q(x)-Px_1-B_2x_2-\ldots-B_nx_n \\ &=Q(x)-L(x) \end{aligned} \tag{9}$$

say. We need to show that there are many integer points x with $|G(x)|<1$. Since Q is positive definite, the matrix A is non-singular and, from (7), we have $x^*=A^{-1}(\nu-\lambda)/2$ where ν, λ are column vectors with $\nu_1, \ldots, \nu_n$ and $\lambda_1, \ldots, \lambda_n$ as entries respectively. Now λ and A^{-1} depend only on $F(x)$ so P and $|x^*|$ are of comparable size. We shall suppose P to be fixed, but arbitrarily large, and use the notation $f \ll g$ to mean $|f|<cg$ for some number c independent of P.

Under a linear substitution of rank 6

$$x=y_1z^1+\ldots+y_6z^6=Ty, \tag{10}$$

we have

$$G(x)=Q(x)-L(x)=\Phi(y)-\Psi(y)=H(y) \tag{11}$$

say, where

$$\Phi(y)=\sum_{i=1}^{6}\sum_{j=1}^{6}\varphi_{ij}y_iy_j, \quad \varphi_{ij}=B(z^i, z^j), \tag{12}$$

and

$$\Psi(y)=\sum_{j=1}^{6}\psi_j y_j, \quad \psi_j=L(z^j). \tag{13}$$

Since T has rank 6, distinct values of y give distinct values of x, so it is now sufficient to prove that for some $\tau>0$ there are at least $[P^\tau]$ solutions of the inequality

$$|H(y)|<1. \tag{14}$$

Our first lemma is a generalized version of Dirichlet's box principle, this version is essentially the lemma of Birch and Davenport [2].

LEMMA 1. *Suppose that $m<n$, and let $L_1, \ldots, L_m$ be m real linear forms in n variables, say*

$$L_i(x)=\sum_{j=1}^{n}\gamma_{ij}x_j, \quad 1\leqslant i\leqslant m. \tag{15}$$

Then, for any $Z\geqslant 2$, there exists an integer vector $z\neq 0$ such that

$$|z|\leqslant Z^m, \tag{16}$$

and

$$|L_i(z)|\ll Z^{m-n}\sum_{j=1}^{n}|\gamma_{ij}|, \quad 1\leqslant i\leqslant m. \tag{17}$$

We take $z^1=(1, 0, \ldots, 0)$ so that $\varphi_{11}=\beta_{11}$ and $\lambda_1=-P$. Having chosen $z^1, \ldots, z^{j-1}$, we choose z^j by applying Lemma 1 with $m=j$, $Z=P^{\theta(j)/j}$, $L_i(z)=B(z^i, z)$ for $i=1, \ldots, j-1$ and $L_j(z)=L(z)$, where $\theta(j)=C_j/n$ with $C_1=0$ and

$$C_2=4.0080563954\ldots, \quad C_3=6.030266299\ldots,$$

$$C_4=8.056630741\ldots, \quad C_5=10.091195104\ldots, \quad C_6=12.13402140609\ldots$$

We obtain non-zero integer vectors z^j $(1 \leqslant j \leqslant 6)$ satisfying

$$|z^j| \leqslant P^{\theta(j)}, \tag{18}$$

$$|B(z^i, z^j)| \ll P^{\theta(j)(1-n/j)+\theta(i)}, \quad 1 \leqslant i < j, \tag{19}$$

and

$$|L(z^j)| \ll P^{\theta(j)(1-n/j)+1}. \tag{20}$$

For $n \geqslant 995$, we have

$$\max_{1 \leqslant i \leqslant j} \theta(j)(1-n/j)+\theta(i) < -2 \quad \text{for} \quad 2 \leqslant j \leqslant 6 \tag{21}$$

and we note that

$$\theta(2)+\ldots+\theta(6) = \Omega/n \tag{22}$$

where $\Omega = 40.32016994707\ldots$

Let T be the $n \times 6$ integer matrix whose jth column is z^j. The transformation $x = Ty$ takes $G(x)$ to a polynomial $H(y)$ which is almost diagonal:

$$H(y) = \sum_{j=1}^{6} \mu_j y_j^2 + \sum\sum_{i \neq j} \varepsilon_{ij} y_i y_j - Py_1 - \sum_{2}^{6} \varepsilon_j y_j \tag{23}$$

where $\mu_j \geqslant c = c(Q) > 0$ for every j, since $z^j \neq \mathbf{0}$ and Q is positive definite. Indeed, we have

$$1 \ll \mu_j = B(z^j, z^j) \ll P^{2\theta(j)}, \quad 1 \leqslant j \leqslant 6, \tag{24}$$

$$\varepsilon_{ij} = B(z^i, z^j) = o(P^{-2}), \quad i \neq j, \tag{25}$$

and

$$\varepsilon_j = L(z^j) = o(P^{-1}), \quad 2 \leqslant j \leqslant 6. \tag{26}$$

For any solution $y_1, \ldots, y_6$ of the inequality

$$|\mu_1 y_1^2+\ldots+\mu_6 y_6^2 - Py_1| < 1/2 \tag{27}$$

we have

$$\mu_1 y_1^2 < Py_1 + 1/2$$

and $\mu_1 > 0$, so for $P \geqslant 1$ and any solution of (27) in integers $y_1, \ldots, y_6$ we have

$$0 < y_1 \ll P.$$

Then

$$\mu_2 y_2^2+\ldots+\mu_6 y_6^2 \ll Py_1 \ll P^2$$

and so

$$y_j \ll P\mu_j^{-1/2} \quad \text{for} \quad i \leqslant j \leqslant 6. \tag{28}$$

From (25) and (26) we now have

$$\varepsilon_{ij} y_i y_j = o(1) \quad \text{and} \quad \varepsilon_j y_j = o(1); \tag{29}$$

so, if P is sufficiently large, it is trivial to see that, in view of (24) and (25), T has rank 6 and further $|H(y)| < 1$. Recalling the remarks preceding inequality (14), it is clearly sufficient to prove the following Proposition 1, in order to establish Theorem 2.

PROPOSITION 1. *Let $\mu_j \gg 1$ for $j = 1, \ldots, 6$. There exists a constant $\tau > 0$ such that, for all large P, the inequalities*

$$|\mu_1 y_1^2+\ldots+\mu_6 y_6^2 - Py_1| < 1/2, \tag{30}$$

$$1 \leqslant y_j \leqslant P\mu_j^{-1/2}, \quad 1 \leqslant j \leqslant 6, \tag{31}$$

have at least $[P^\tau]$ solutions in integers $y_1, \ldots, y_6$.

3. The analytical argument. The next stage is to use the Hardy–Littlewood method to show that if the inequalities (30) and (31) do not have enough solutions, then we have good Diophantine approximations to the numbers $\mu_j\alpha$, $j = 1, \ldots, 6$, from some real α.

Following quite closely the arguments of Davenport and Lewis ([7], §§ 3–9) while assuming that $n \geqslant 995$, it is not hard to prove

PROPOSITION 2. *Suppose that*

$$1 \ll \mu_1 \ll 1, \quad 1 \ll \mu_j \quad \text{for} \quad j = 2, \ldots, 6 \tag{32}$$

and

$$P \gg \Pi := \mu_1 \ldots \mu_6. \tag{33}$$

Suppose further that inequalities (30) *and* (31) *have $O(P^\eta)$ solutions, for some non-negative constant $\eta < 3$. Then there exists a positive constant δ $(< 31/176)$ and a real number $\alpha > 0$ satisfying*

$$P^{-7\delta}\Pi^{-1/2} \ll \alpha < P^\delta \tag{34}$$

such that there exist Diophantine approximations

$$\alpha\mu_j = a_j/q_j + \beta_j, \quad 1 \leqslant j \leqslant 6, \tag{35}$$

where a_j, q_j are integers with $(a_j, q_j) = 1$,

$$1 \leqslant q_j \ll \Pi^{1/2}\mu_j^{-1/2}P^{7\delta}, \tag{36}$$

$$|\beta_j| \ll \Pi^{1/4}\mu_j^{3/4}P^{4\delta-2}. \tag{37}$$

Remarks. We note that from (22), $\Pi = \mu_1 \dots \mu_6$ satisfies

$$\Pi \ll P^{2\Omega/n} \tag{38}$$

and that inequality (49) in [7] holds for $\max|\mu_i| (\ll P^{25/n}) < P^2$. Further, since $\eta < 3$, we have $P^n = o(P^4/\Pi^{1/2})$. A proof of the estimate in Lemma 10 of [7] may also be found in Vaughan [9], Theorem 4.2. The condition $\delta < 31/176$ in Proposition 2 stems from the requirement on $\delta > 0$ in the course of proving Proposition 2, to be small enough to ensure that

$$\Pi = o(P^{(8-44\delta)/3}). \tag{39}$$

We shall enforce (39) at the end of the proof of Theorem 2.

4. Proof of Theorem 2. We shall need the following result on quadratic equations; it is part of Theorem 1 of Watson [11].

LEMMA 2. *Let $b_1, \dots, b_5, v$ be positive integers such that the equation*

$$b_1 x_1^2 + \dots + b_5 x_5^2 = v$$

has no solution in rational integers, although there are integer solutions in every p-adic field. Then for any $\varepsilon > 0$, there exists a positive number $C_1 = C_1(\varepsilon)$, depending only on ε, such that

$$v \leqslant C_1 b_1 \dots b_4 (b_1 + \dots + b_5)^{1+\varepsilon}.$$

We use Lemma 2 to replace the inequality

$$Nt < C_1 b_1 \dots b_4 (b_1 + \dots + b_5)^{3/2} \tag{40}$$

occurring on the last line of p. 102 of Davenport and Lewis [7]. Repeating the proof of Lemma 14 of [7], we obtain the following lemma.

LEMMA 3. *Given positive integers $b_1, \dots, b_5$ and any $\varepsilon > 0$, there exists a positive integer*

$$B < C_2 b_1 \dots b_5 \max_j b_j^{\varepsilon}, \tag{41}$$

where C_2 depends only on ε, such that for all positive integers t, the equation

$$b_1 x_1^2 + \dots + b_5 x_5^2 = Bt \tag{42}$$

is soluble in rational integers.

Proof of Theorem 2. As remarked earlier, it is enough to prove Proposition 1. Let Proposition 1 be false, if possible. Then, on applying Proposition 2, with an $\eta < \min(\tau, 3)$, there exist δ and a real number α satisfying (34)–(37); on noting that $1 \ll \alpha \Pi^{1/2} P^{7\delta}$ by (34), we see, further, that, for a constant $C_3 < \frac{1}{2}\alpha\Pi P^{7\delta}$, the inequality

$$|\alpha\mu_1 y_1^2 + \dots + \alpha\mu_6 y_6^2 - \alpha P y_1| < C_3 \Pi^{-1/2} P^{-7\delta} \tag{43}$$

has at most $O(P^n)$ solutions in integers $y_1, \dots, y_6$ in the box (31) and a fortiori, such y_j with $y_j = q_j z_j$ with integral z_j for $1 \leqslant j \leqslant 6$. Replacing then y_j by $q_j z_j$ in (43), we have at most $O(P^n)$ integers $z_1, \dots, z_6$ in the box (31), such that

$$|a_1 q_1 z_1^2 + \dots + a_6 q_6 z_6^2 - \alpha P q_1 z_1 + \beta_1 q_1^2 z_1^2 + \dots + \beta_6 q_6^2 z_6^2| < C_3 \Pi^{-1/2} P^{-7\delta}. \tag{44}$$

For small τ, we shall get, in the sequel, a contradiction to the last assertion, thereby upholding Proposition 1 and along with it, Theorem 2 as well.

For any $\varepsilon > 0$, there exists, by Lemma 3, a positive integer B such that

$$B \ll a_2 \dots a_6 q_2 \dots q_6 \max(a_j q_j)^{\varepsilon} \ll \alpha^5 \mu_2 \dots \mu_6 q_2^2 \dots q_6^2 \max(\alpha \mu_j q_j^2)^{\varepsilon} \ll \Pi^5 P^{76\delta} \tag{45}$$

and, moreover, for every positive integer t, the equation

$$a_2 q_2 z_2^2 + \dots + a_6 q_6 z_6^2 = Bt \tag{46}$$

is solvable in rational integers $z_2, \dots, z_6$. Further, in view of (46), (36) and (37) and from $a_2, \dots, a_6 \geqslant 1$, we have

$$\sum_{2 \leqslant j \leqslant 6} |\beta_j q_j^2 z_j^2| \leqslant \sum_{2 \leqslant j \leqslant 6} |\beta_j q_j| Bt \ll Bt \Pi^{3/4} P^{11\delta - 2} \sum_{2 \leqslant j \leqslant 6} \mu_j^{1/4}. \tag{47}$$

But, by (24),

$$\mu_j \ll P^{2\theta(6)} \quad (2 \leqslant j \leqslant 6) \tag{48}$$

and therefore, if

$$t \ll \Pi^{-25/4} P^{2 - \theta(6)/2 - 95\delta}, \tag{49}$$

then (47) entails that

$$\sum_{2 \leqslant j \leqslant 6} |\beta_j q_j^2 z_j^2| = o(\Pi^{-1/2} P^{-7\delta}). \tag{50}$$

If now

$$z_1 \ll \Pi^{-7/8} P^{1 - 14\delta}, \tag{51}$$

then we have

$$\beta_1 q_1^2 z_1^2 \ll \Pi^{1/4} P^{4\delta - 2} \Pi P^{14\delta} \Pi^{-7/4} P^{2 - 28\delta} = o(\Pi^{-1/2} P^{-7\delta}), \text{ clearly}. \tag{52}$$

For z_1 of the form Bu with integral u, condition (51) will certainly be fulfilled, if u satisfies the inequality

$$|u| < \Pi^{-47/8} P^{1 - 90\delta}, \tag{53}$$

on taking (45) into account.

Let us suppose now that t and u are positive integers subject to (49) and (53) respectively. For any such t, we may invoke a solution in integers $z_2, \ldots, z_6$ of (46) and with $z_1 = Bu$, rewrite inequality (44) as

$$|a_1 q_1 Bu^2 + t - \alpha P q_1 u| \ll B^{-1} \Pi^{-1/2} P^{-7\delta}. \tag{54}$$

In view of (45), inequality (54) will be satisfied by every such t and u as above for which

$$|t + a_1 q_1 Bu^2 - \alpha P q_1 u| \ll \Pi^{-11/2} P^{-83\delta}. \tag{55}$$

We know that, for any $\varrho > 0$, Dirichlet's box principle yields $[P^\varrho]$ integers u for which

$$1 \leqslant u \leqslant \Pi^{11/2} P^{83\delta+\varrho} \tag{56}$$

and further,

$$|\alpha P q_1 u - v| < \Pi^{-11/2} P^{-83\delta} \tag{57}$$

for some integer v. For each such pair u, v, let us define

$$t = v - a_1 q_1 Bu^2. \tag{58}$$

Now (39) implies that

$$\Pi^{11/2} P^{83\delta+\varrho} < \Pi^{-47/8} P^{1-90\delta} \tag{59}$$

provided that $91\Omega/(4n) < 1 - 173\delta - \varrho$ and in such an eventuality, the integers u just chosen certainly satisfy condition (53). Inequality (55) implies that

$$t - u(\alpha q_1 P - a_1 q_1 Bu) = o(1), \tag{60}$$

while by (32), (35), (37) and (38), we have

$$|\beta_1 q_1 P| \ll \Pi^{3/4} \mu_1^{1/4} P^{11\delta-1} \ll \Pi^{3/4} P^{11\delta-1} \ll P^{3\Omega/(2n)+11\delta-1} < P.$$

Thus, for the positive number $\alpha q_1 P$, we have

$$\alpha q_1 P = (a_1 P + \beta_1 q_1 P)/\mu_1 \gg a_1 P. \tag{61}$$

Since, moreover, for $n \geqslant 995$,

$$166\delta + \varrho < 173\delta + \varrho < 1 - 22\Omega/n,$$

we have

$$a_1 q_1 Bu \ll a_1 \Pi^{11} P^{166\delta+\varrho} = o(a_1 P) \tag{62}$$

which implies, for $a_1 \neq 0$, that $t > 0$; if $a_1 = 0$, then $t = v$ and (57) ensures that $v > 0$. Also,

$$\begin{aligned} t &\ll \alpha q_1 Pu + a_1 q_1 Bu^2 \\ &\ll \alpha q_1 u(P + q_1 Bu) \end{aligned} \tag{63}$$

$$\begin{aligned} &\ll \alpha q_1 uP, && \text{by (32), (36), (45) and (53),} \\ &\ll \Pi^6 P^{1+91\delta+\varrho}, && \text{by (32), (34), (36) and (56).} \end{aligned}$$

The validity of (49) may therefore be ensured, provided that

$$\Pi^6 P^{1+186\delta+\varrho} \ll \Pi^{-25/4} P^{2-\theta(6)/2}$$

or if

$$P^{49\Omega/(2n)+186\delta+\varrho} < P^{1-\theta(6)/2}. \tag{64}$$

For $n \geqslant 995$, we have $\Omega = 40.32016994\ldots$ and (64) is fulfilled for $\varrho = 7/10^3$ and $\delta = 1/10^6$; indeed, for this choice of ϱ and δ

$$6\Omega < (8 - 44\delta)n, \qquad 91\Omega/(4n) < 1 - 173\delta - \varrho,$$

$$22\Omega/n < 1 - 166\delta - \varrho, \qquad 49\Omega/n < 2 - (\theta(6)/2) - 186\delta - \varrho,$$

guaranteeing the validity of (39), (59), (62), (64) and hence of (49). For these values of ϱ and δ, we have therefore $[P^\varrho]$ pairs of positive integers t, u satisfying (49), (53) and (55), and consequently, (43) has at least $[P^\varrho]$ solutions y in the box (31). Proposition 1 is thus proved with $\tau = 7/10^3$ and so is Theorem 2.

Acknowledgement. This paper was begun whilst R. J. Cook held a visiting fellowship at the Tata Institute of Fundamental Research, Bombay and the Centre for Advanced Studies in Mathematics, Chandigarh. He is grateful to those institutions for their hospitality, to the Indian National Science Academy and the Royal Society for their financial assistance.

References

[1] B. J. Birch and H. Davenport, *On a theorem of Davenport and Heilbronn*, Acta Math. 100 (1958), pp. 259–279.
[2] – – *Indefinite quadratic forms in many variables*, Mathematika 5 (1958), pp. 8–12.
[3] R. J. Cook, *Indefinite quadratic polynomials*, Glasgow Math. J. 24 (1983), pp. 133–138.
[4] R. J. Cook and S. Raghavan, *Indefinite quadratic polynomials of small signature*, Monatsh. Math. 97 (1984), pp. 169–176.
[5] H. Davenport, *Indefinite quadratic forms in many variables*, Mathematika 3 (1956), pp. 81–101.
[6] – *Analytic Methods for Diophantine Equations and Diophantine Inequalities*, Ann Arbor 1962.
[7] H. Davenport and D. J. Lewis, *Gaps between the values of positive definite quadratic forms*, Acta Arith. 22 (1972), pp. 87–105.
[8] H. Davenport and D. Ridout, *Indefinite quadratic forms*, Proc. London Math. Soc. 9 (1959), pp. 544–555.
[9] R. C. Vaughan, *The Hardy-Littlewood Method*, Cambridge 1981.

[10] G. L. Watson, *Indefinite quadratic polynomials*, Mathematika 7 (1960), pp. 141–144.
[11] – *Quadratic Diophantine equations*, Phil. Trans. Roy. Soc. London 253A (1960), pp. 227–254.

UNIVERSITY OF SHEFFIELD
SHEFFIELD
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
BOMBAY

Received on 9.9.1983
and in revised form on 13.2.1984 (1373)

ACTA ARITHMETICA
XLV (1986)

Factorisation of x^N-q over Q

by

HENK HOLLMANN (Issy les Moulineaux)

1. Introduction. It is well known that the cyclotomic polynomials $\Phi_n(x)$ ($n\in N$) are the irreducible factors of binomials x^N-1 ($N\in N$) over $Q[x]$. In this paper, we determine the irreducible factors of binomials x^N-q ($q\in Q$, $N\in N$) over $Q[x]$.

It turns out that besides polynomials of the form $\Phi_n(x^m/a)$ there are exactly two other families of polynomials in $Q[x]$ which divide some binomial. In fact, under certain conditions on n and s there are irreducible polynomials $\Theta_{n,s}(x)$ and $\Psi_{n,s}(x)$ such that

$$\Theta_{n,s}(x)\Theta_{n,s}(-x)\equiv\Phi_n(x^2/s) \quad \text{and} \quad \Psi_{n,s}(x)\Psi_{n,s}(-x)\equiv\Phi_n(x^4/-4s^2)$$

(here $f(x)\equiv g(x)$ stands for $f(x)=cg(x)$ for some constant c, a convention used throughout this paper) and the polynomials of the form $\Theta_{n,s}(x^m/a)$ and $\Psi_{n,s}(x^m/a)$ constitute the other two families.

The polynomials $\Theta_{n,s}(x)$ and $\Psi_{n,s}(x)$ are not new, they can be obtained from certain polynomials defined in [9].

We shall use the following notation:

Let Ω be a field, $\bar{\Omega}$ its algebraic closure. ζ_N is a primitive root of 1 of degree N and $\Omega_N=\Omega(\zeta_N)$.

For $v\in\bar{\Omega}$, Ω' a field such that $\Omega\subseteq\Omega'\subseteq\bar{\Omega}$, we denote the minimal polynomial of v over Ω' by $m(v,\Omega';x)$. Its degree is the *degree* (or *dimension*) *of v over Ω'*. The *order of v over Ω'* is the smallest $N>0$ such that $v^N\in\Omega'$. (If no such N exists then the order is taken to be ∞.) Let $F(x)\in\Omega[x]$. The *order of $F(x)$ over Ω* is the smallest $N>0$ such that $F(x)$ divides some x^N-q with $q\in\Omega$. (Again taken to be ∞ if no such N exists.) Remark that if $F(x)$ has order N over Ω then $F(x^n)$ has order nN over Ω (note that $F(x^n)|x^M-b$ ($b\in\Omega$) implies $n|M$) and $F(x)|x^M-b$ ($b\in\Omega$) implies by a standard argument that $N|M$. We shall make a frequent use of these results in the text.

Let $F(x)\in\Omega[x]$ have order N over Ω. The *dimension of $F(x)$ over Ω* is the dimension of any of its zeroes over Ω_N. (Note that this is a proper definition: If v is any zero of $F(x)$ then the other zeroes all have the form $\zeta_N{}^i v$ for some i.)