[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.)

Moreover, we introduce the following notation from [11]: Let $a \in \Omega \setminus \{0\}$, then

$$E(a, \Omega) = \begin{cases} 0 & \text{if } a = \zeta_N \text{ for some } N, \\ \text{maximal } n \text{ such that } a = v^n,\ v \in \Omega_n & \text{otherwise.} \end{cases}$$

We quote the following result ([11], Lemma 2, (12))

(1.1) For any field Ω, with $a \in \Omega \setminus \{0\}$, if $a = b^m$, $b \in \Omega' \subseteq \Omega_m$, then $m \cdot E(b, \Omega') | E(a, \Omega)$.

(In fact, in [11] this result was given for Ω an algebraic number field, but the proof given there remains valid for any field Ω.)(*)

This paper is constructed as follows: In Section 2 we show that any $F(x) \in \Omega[x]$ of finite order can be written as: $F(x) = G(x^n)$ with $G(x) \in \Omega[x]$ of dimension 1, irreducible over Ω iff $F(x)$ is irreducible over Ω. (This result improves [11], Lemma 3.) So it is sufficient to determine all polynomials of finite order and dimension 1. This is done in Section 3, for $\Omega = Q$. In Section 4 the irreducibility of $\Phi_M(x^m/a)$, $\Theta_{M,s}(x^m/a)$ and $\Psi_{M,s}(x^m/a)$ is investigated. Finally, in Section 5 we treat some examples and mention an application to Number Theoretic Transforms ([2], [5]).

2. A property of polynomials of finite order. Our aim in this section is to show that in searching polynomials of finite order we can limit ourselves to the search of those having dimension 1. Our results are obtained from the following lemma:

(2.1) LEMMA. *Let $v \in \bar{\Omega}$ and let $v^N \in \Omega$. If v has dimension d over Ω_N then $v^d \in \Omega_N$ and $m(v, \Omega_N; x) = x^d - v^d$.*

Proof. This is a slightly different formulation of Satz I in Hasse [4]. ∎

Then the main result of this section is

(2.2) THEOREM. *Let $F(x) \in \Omega[x]$ divide $x^N - q$ $(q \in \Omega)$. Then there exists $G(x) \in \Omega[x]$, $n | N$ such that $F(x) = G(x^n)$, and $G(x)$ has all its zeroes in $\Omega_{N/n}$. $F(x)$ and $G(x)$ have the same number of irreducible factors over $\Omega[x]$. Moreover, $N/n | (N, E(q, \Omega))$.*

Proof. Let d be the dimension of the zeroes of $F(x)$ over Ω_N. Then (2.1) implies that their minimal polynomials over Ω_N, hence certainly over Ω, are in fact polynomials in x^d. This in turn implies that $F(x)$ is a polynomial in x^d, $F(x) = F_1(x^d)$, $F_1(x) \in \Omega[x]$, say, and $F(x)$ and $F_1(x)$ have the same number of irreducible factors over $\Omega[x]$.

Repeating the same argument, we find polynomials $F_0(x) = F(x), F_1(x), F_2(x), \ldots$ in $\Omega[x]$ and $d_0 = d, d_1, d_2, \ldots$ such that

$$F_i(x) = F_{i+1}(x^{d_i}), \qquad F_i(x) | x^{N/d_0 d_1 \ldots d_i - 1} - q,$$

(*) Editors note. It is tacitly assumed $E(\alpha, \Omega) = 0$ if $\alpha = v^n$, $v \in \Omega_n$ for infinitely many n.

the dimension of the zeroes of $F_i(x)$ over $\Omega_{N/d_0 \ldots d_{i-1}}$ is d_i, until finally for some m we have $d_m = 1$. Then with $n = d_0 \ldots d_{m-1}$, $G(x) = F_m(x)$ we have the first part of (2.2).

Finally, if v is a zero of $F(x)$, then $q = v^N = [v^n]^{N/n}$, and since v^n is a zero of $G(x)$ we have $v^n \in \Omega_{N/n}$. Then the last conclusion of (2.2) follows from (1.1). ∎

(2.3) Remark. If in (2.2) $F(x)$ has order N, then $G(x)$ has order N/n and hence dimension 1.

(2.4) Remark. (2.2) includes [11], Lemma 3. That (2.2) may lead to stronger conclusions is shown by the following example: With the assumptions as in (2.2), take $\Omega = Q$, $q = -2^6$, $N = 6$. Then $q = (1+i)^{12}$ and $(1+i) \in Q_{12}$, so by (1.1) this implies $12 | E(q, Q)$ and Lemma 3 of [11] allows no conclusion. However, since $q = (2i)^6$, $2i \notin Q_6$, $(2i)^2 \in Q_6$ it follows from (2.2) that $F(x)$ is a polynomial in x^2.

3. The irreducible polynomials over Q of dimension 1. From now on, we take $\Omega = Q$. Let us denote by $S(N)$ $(N \in N)$ the set of square free $s \in Z$ such that $\sqrt{s} \in Q_N$. We have the following well-known theorem (see e.g. [10], Lemma 3):

(3.1) *Let $N = 2^m M$ with M odd.*

(i) *If $m = 0$ or $m = 1$ then $S(N)$ consists of the numbers $(-1|t)t$ with $t \in N$, t squarefree and $t | M$.*

(ii) *If $m = 2$ then $S(N)$ consists of all $t \in Z$ with t squarefree, $t | M$.*

(iii) *If $m \geqslant 3$ then $S(N)$ consists of all $t \in Z$ with t squarefree, $t | 2M$.*

If $F(x) \in Q[x]$ has order N and dimension 1, $F(x) | x^N - q$ $(q \in Q)$ say, then $x^N - q$ also has dimension 1. First we shall determine for which N, q this is the case.

(3.2) LEMMA. *$x^N - q$ $(q \in Q)$ has dimension 1 iff one of the following holds:*

(i) *N odd, $q = a^N$ with $a \in Q$,*

(ii) *N even, $q = a^N s^{N/2}$ with $a \in Q$ $s \in S(N)$,*

(iii) *$N = 4M$ with M odd, $q = -a^{4M}(2s)^{2M}$ with $a \in Q$, $s \in S(N)$.*

Proof. This is an equivalent formulation of [10], Lemma 4. ∎

In the next theorem we show that there are other irreducible polynomials in $Q[x]$ of dimension 1 besides $\Phi_M(x/a)$ (M odd, $a \in Q$). We shall denote the Galois group of Q_N over Q by $\mathrm{Gal}(Q_N/Q)$ and its order by $\Phi(N)$ (where Φ is the Euler function). Let $M \in N$ be odd, $s \in S(2M) \setminus \{1\}$, $t \in S(4M)$. Define v and η by

$$v := \zeta_M \sqrt{s}, \qquad \eta := \zeta_{4M}(1+i)\sqrt{t}$$

and let

$$\Theta_{M,s}(x) = m(v, Q; x), \qquad \Psi_{M,t}(x) = m(\eta, Q; x).$$

Then we have

(3.3) THEOREM. (i) *$\Theta_{M,s}(x)$ is irreducible, of order $2M$, degree $\Phi(2M) = \Phi(M)$, dimension 1. Moreover $\Theta_{M,s}(x)\Theta_{M,s}(-x) \equiv \Phi_M(x^2/s)$.*

(ii) *$\Psi_{M,t}(x)$ is irreducible, of order $4M$, degree $\Phi(4M) = 2\Phi(M)$, and dimension 1. Moreover $\Psi_{M,t}(x)\Psi_{M,t}(-x) \equiv \Phi_M(x^4/-4t^2) \equiv \Phi_{4M}(x^2/2t)$.*

Proof. (i) Clearly $v \in Q_{2M}$ and v has order $2M$. It follows that $\Theta_{M,s}(x)$ is irreducible of order $2M$ and dimension 1. If $\sigma \in \mathrm{Gal}(Q_{2M}/Q)$ maps v to $\pm v$ then σ fixes v^2. This implies that σ fixes ζ_M^2, a primitive Mth root of unity. Since $Q_{2M} = Q_M$ it follows that $\sigma = 1$.

We have shown: $\Theta_{M,s}(x)$ has degree $\Phi(2M) = \Phi(M)$ and $\Theta_{M,s}(x)$ and $\Theta_{M,s}(-x)$ $(= m(-v, Q; x))$ are distinct.

Since both v and $-v$ are zeros of $\Phi_M(x^2/s)$ of degree $2\Phi(M)$, we have $\Theta_{M,s}(x)\Theta_{M,s}(-x) \equiv \Phi_M(x^2/s)$.

(ii) Here we have $\eta \in Q_{4M}$ and η has order $4M$. Moreover, note that $\eta^2 = 2t\zeta_{4M}^{2+M}$ and ζ_{4M}^{2+M} is a primitive $4M$-th root of 1. Now essentially the same reasoning as in (i) will prove (ii). ∎

Remark. The polynomials in (3.3) are not new. If M is odd, $M = nM^*$ with M^* the squarefree part of M, then

$$\Theta_{M,s}(x) = \Psi_{M^*,|s|}\left((x/\sqrt{s})^n\right)\cdot(\sqrt{s})^{\Phi(M)},$$

$$\Psi_{M,s}(x) = \Psi_{4M^*,2|t|}\left((x/\sqrt{2|t|})^n\right)(2|t|)^{\Phi(M)}$$

where $\Psi_{n,m}(x)$ are polynomials as defined in [9], Theorem 1. It follows from the said theorem that $\Theta_{M,s}(x)$ and $\Psi_{M,t}(x)$ have integer coefficients and satisfy the formulae given in (3.3). Their irreducibility could then be deduced from the irreducibility of $\Phi_M(x)$ and $\Phi_{4M}(x)$ and from the lemma of Capelli (see [12], p. 289), which implies that the number of irreducible factors of $f(g(x))$ for $f(x)$ irreducible does not exceed the degree of $g(x)$.

Now we come to the main result of our paper:

(3.4) THEOREM. *There are exactly three families of irreducible polynomials in $Q[x]$ of finite order and dimension 1:*

(i) *$\Phi_M(x/a)$ with M odd, $a \in Q$ of order M, degree $\Phi(M)$,*

(ii) *$\Theta_{M,s}(x/a)$ with M odd, $a \in Q$, $s \in S(2M)\setminus\{1\}$, of order $2M$ and degree $\Phi(2M)$.*

(iii) *$\Psi_{M,t}(x/a)$ with M odd, $a \in Q$, $t \in S(4M)$, of order $4M$ and degree $\Phi(4M)$.*

Proof. Suppose $F(x) \in Q[x]$ is irreducible of order N, dimension 1, and let $F(x)|x^N - q$ $(q \in Q)$ say. Then $x^N - q$ also has dimension 1, and we can use (3.2):

(i) N odd, $q = a^N$ $(a \in Q)$. Since $x^N - a^N \equiv \prod_{d|N} \Phi_d(x/a)$ with $\Phi_d(x/a)$ irreducible of order d we must have $F(x) \equiv \Phi_N(x/a)$.

(ii) N even, $q = a^N s^{N/2}$ $(a \in Q, s \in S(N))$. If $4|N$ or $s = 1$ then

$$x^N - a^N s^{N/2} = (x^{N/2} - a^{N/2} s^{N/4})\,(x^{N/2} + a^{N/2} s^{N/4}),$$

contradicting the fact that $F(x)$ has order N. So we may assume that $N = 2M$, M odd and $s \in S(2M)\setminus\{1\}$. Since $x^{2M} - a^{2M}s^M \equiv \prod_{d|M} \Phi_d(x^2/a^2 s)$ with $\Phi_d(x^2/a^2 s)$ of order $2d$ we must have $F(x)|\Phi_M(x^2/a^2 s)$. Now use (3.3).

(iii) $N = 4M$, M odd, $q = -a^{4M}(2t)^{2M}$ $(a \in Q, t \in S(4M))$. Since $x^{4M} + a^{4M}(2t)^{2M} \equiv \prod_{d|M} \Phi_d(x^4/-a^4(2t)^2)$ with $\Phi_d(x^4/-a^4(2t)^2)$ of order $4d$ we must have $F(x)|\Phi_M(x^4/-a^4(2t)^2)$. Now use (3.3). ∎

(3.5) COROLLARY. *Any irreducible polynomial over $Q[x]$ of finite order is of the form $\Phi_M(x^m/a)$, $\Theta_{M,s}(x^m/a)$ or $\Psi_{M,t}(x^m/a)$ for some $m \in N$ and some M, s, t, a as in* (3.4).

Proof. Consequence of (2.2), (2.3) and (3.4). ∎

4. The irreducible polynomials over $Q[x]$ of finite order. To complete our investigation we shall state in this section under which conditions the polynomials in (3.5) are reducible. The interested reader can find the proofs in the appendix.

(4.1) *Let M be odd, $m \in N$, $a \in Q$. Then $\Phi_M(x^m/a)$ is reducible iff one of the following holds:*

(i) *For some prime p, some $b \in Q$ we have $p \nmid M$, $p|m$, $a = b^p$,*

(ii) *$2|m$ and $a = b^2 s$ for some $b \in Q$, $s \in S(2M)\setminus\{1\}$,*

(iii) *$4|m$ and $a = -b^4(2t)^2$ for some $b \in Q$, $t \in S(4M)$.*

(4.2) *Let M be odd, $m \in N$, $a \in Q$, $s \in S(2M)\setminus\{1\}$, $t \in S(4M)$*

$\Theta_{M,s}(x^m/a)$ is reducible iff $p \nmid M$, $p|m$, $a^2 s = (b^2 s)^p$ for some prime p, some $b \in Q$,

$\Psi_{M,t}(x^m/a)$ is reducible iff $p \nmid M$, $p|m$, $a^4(2t)^2 = (b^4(2t)^2)^p$ for some prime p, some $b \in Q$.

We wish to remark that $\Phi_M(x^m/a)$ divides $x^N - q$ (M odd, a, $q \in Q$) iff $mM|N$ and $q = a^{N/m}$.

This fact together with (3.3), (3.4), (4.1) and (4.2) could then be used to find the complete factorisation of any binomial $x^N - q$ $(q \in Q)$ over $Q[x]$.

5. An application. We can use the polynomials of type (iii) in (3.5) to find factors of $x^{4M} + 2^{2M}$ (M odd): Indeed, (3.3) implies $\Psi_{M,1}(x)|x^{4M} + 2^{2M}$. We have computed some of these $\Psi_{M,1}(x)$. The result is:

$$\Psi_{1,1}(x) = x^2 + 2x + 2,$$
$$\Psi_{3,1}(x) = x^4 + 2x^3 + 2x^2 + 4x + 4,$$
$$\Psi_{5,1}(x) = x^8 + 2x^7 + 2x^6 - 4x^4 + 8x^2 + 16x + 16,$$
$$\Psi_{7,1}(x) = x^{12} + 2x^{11} + 2x^{10} - 4x^8 - 8x^7 - 8x^6 - 16x^5 - 16x^4 + 32x^2 + 64x + 64,$$
$$\Psi_{9,1}(x) = x^{12} + 4x^9 + 8x^6 + 32x^3 + 64,$$
$$\Psi_{15,1}(x) = x^{16} + 2x^{15} + 2x^{14} + 4x^{13} + 8x^{12} + 16x^{11} + 24x^{10} + 32x^9 + 48x^8 + 64x^7 + 96x^6 + 128x^5 + 128x^4 + 128x^3 + 128x^2 + 256x + 256.$$

(Note that $\Psi_{9,1}(x) = 2^4\,\Psi_{3,1}(x^3/2)$ in accordance with (1) of the appendix.)

The polynomial $x^{\Phi(4M)}\Psi_{M,1}(x^{-1})$ is in $Z[x]$ and divides $2^{2M}x^{4M}+1$. As a consequence, the numbers $M_{M,n}=2^{\Phi(4M)n}\Psi_{M,1}(2^{-n})$ are in Z and divide $2^{2M(2n+1)}+1$ (M odd, $n\in N$).

These numbers $M_{M,n}$ could then be used to define new families of Number Theoretic Transforms with 2 as a root of unity (see [2], [5]). (This problem was in fact the motivation for this work.)

Appendix. Let us make the following observation:

If for some $a, b\in Q$, $n\in N$, we have

$$a=b^n, \quad a^2 s=(b^2 s)^n \quad \text{or} \quad a^4(2t)^2=\left(b^4(2t)^2\right)^n$$

then we have

(1) $\Phi_{Mn}(x/b)\mid\Phi_M(x^n/a)$, $\Theta_{Mn,s}(x/b)\mid\Theta_{M,s}(x^n/a)$ or $\Psi_{Mn,t}(x/b)\mid\Psi_{M,t}(x^n/a)$

respectively.

Moreover, under these assumptions, we have $\equiv$ instead of $\mid$ in (1) iff $n\mid M$.

To see this, first remark that the zeroes of the irreducible polynomials on the left-hand sides of (1) are also zeroes of the polynomials on the right-hand sides of (1). Then inspect their degrees, and use $\Phi(nM)=n\Phi(M)$ iff $n\mid M$.

This observation shows that the conditions stated in (4.1) and (4.2) are sufficient.

On the other hand, suppose $\Phi_M(x^m/a)$ reducible. By (2.2) and (2.3), there exists $n\mid m$ such that $\Phi_M(x^n/a)$, of order nM, is reducible of dimension 1. As a consequence, $x^{Mn}-a^M$ also has dimension 1 and since M is odd, (3:2) now shows that we have one of the following:

(i) n odd, $a=b^n$ ($b\in Q$). Then (1) implies $n\nmid M$, so we have (i) of (4.1).

(ii) n even, $a=b^n s^{n/2}$ ($b\in Q$, $s\in S(Mn)$).

If $s=1$ or $n/2\nmid M$ then again we have (i) of (4.1). Let us therefore assume $s\neq 1$, $n/2\mid M$. Then $S(Mn)=S(2M)$ and we find $s\in S(Mn)\setminus\{1\}$, $a=[b^{n/2}s^{(n/2-1)/2}]^2\cdot s$ and we have (ii) of (4.1).

(iii) $n=4k$, $a=-b^{4k}(2t)^{2k}$ ($b\in Q$, $t\in S(4kM)$), with k odd.

If $k\nmid M$ then again we have (i) of (4.1). Let us therefore assume $k\mid M$. Then $S(4kM)=S(4M)$, so $t\in S(4M)$, $a=-[b^k(2t)^{(k-1)/2}]^4(2t)^2$ and we have (iii) of (4.1).

The case $\Theta_{M,s}(x^m/a)$ reducible can be treated along the same lines: Again we can find $n\mid m$ such that $\Theta_{M,s}(x^n/a)$, of order $2nM$, is reducible of dimension 1, and hence we find that $x^{2Mn}-a^{2M}s^M$ has dimension 1. Then we use (3.2). Note that $-1\notin S(2M)$, so that (iii) of (3.2) is not possible. We find $a^2 s=b^{2n}t^n$ ($b\in Q$, $t\in S(Mn)\setminus\{1\}$).

Since $s\neq 1$ and s and t squarefree in Z, n must be odd and $s=t$. Then the first part of (4.2) follows.

The second part of (4.2), concerning $\Psi_{M,t}(x)$, can be proved by a similar argument.

Acknowledgements. The author wishes to thank Pierre Duhamel for his encouragement and S. Harari for his help in preparing the manuscript.

He also wishes to thank two unknown referees, whose numerous remarks allowed to simplify considerably this paper.

References

[1] E. Artin, *Theory of algebraic numbers*, G. Striker, Göttingen 1957.
[2] P. Duhamel, H. Hollmann, *Number Theoretic Transforms with 2 as a root of unity*, Electronics Letters, Vol. 18, n° 22, pp. 978–980, Oct. 1982.
[3] H. Hasse, *Zahlentheorie*, Akademie Verlag, Berlin 1949.
[4] – *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II, § 9, II Auflage, Würzburg–Wien 1965, pp. 42.
[5] H. Hollmann, P. Duhamel, *Longer NTT's with 2 as a root of unity*, ICASSP 1983, pp. 159–162.
[6] M. Kraïtchik, *On the factorisation of* $2^n\pm 1$, Scripta Mathematica 18 (1952), pp. 39–52.
[7] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.
[8] P. Samuel, *Théorie Algébrique des nombres*, Hermann, Paris 1967.
[9] A. Schinzel, *On primitive prime factors of* a^n-b^n, Proc. Cambridge Phil. Soc. 58 (1962), pp. 555–562.
[10] – *A refinement of a theorem of Gerst on power residues*, Acta Arith. 17 (1970), pp. 162–168.
[11] – *Reducibility of lacunary polynomials III*, ibid. 34 (1978), pp. 227–266.
[12] N. G. Tschebotarëw, *Grundzüge der Galois'schen Theorie*, Groningen–Djakarta, 1950.

CNET/PAB/RPE/ETP
38-40, RUE DU GÉNÉRAL LECLERC
92131 ISSY LES MOULINEAUX
FRANCE

Received on 6.10.1983
and in revised form on 3.8.1984 (1376)