MATH. SCAND. 8 (1960), 121–126

ON THE IRREDUCIBILITY OF THE TRINOMIALS $x^n \pm x^m \pm 1$

HELGE TVERBERG

1.

In an earlier paper in this journal, Selmer [1] studied the polynomials $x^n \pm x^m \pm 1$. He gave a complete discussion, as to the possibility of factorization in the rational field, of the case $m = 1$. The purpose of this note is to extend his results to the general case $0 < m < n$.

I want to express my gratitude towards Professor Selmer, who called my attention to the problem, and whose active interest in it was of great help to me while I was working on the solution.

2.

We write

$$f(x) = x^n + \varepsilon\varepsilon_1 x^m + \varepsilon_1 ,$$

where ε and ε_1 take the values ± 1. As the roots of $f(x)$ are the inverses of the roots of $g(x) = x^n + \varepsilon x^{n-m} + \varepsilon_1$, it will suffice for our purposes to treat the cases with $n \geqq 2m$. This inequality will be assumed throughout the paper.

We further write

$$\sigma_k = \sum_{x;f(x)=0} x^k ,$$

when k is a rational integer. If we assume $f(x) = f_1(x) f_2(x)$, where $f_1(x)$ and $f_2(x)$ are monic rational polynomials of positive degree, then the corresponding power sums are denoted by σ_k' and σ_k''. The coefficients of $f_1(x)$ and $f_2(x)$ are denoted by a_i', a_i'', $i = 1, 2, \ldots$, with $\sigma_1' + a_1' = \sigma_1'' + a_1'' = 0$. Further, b_i', b_i'' denote the coefficients of the monic polynomials whose roots are the inverses of the roots of $f_1(x)$ and $f_2(x)$, and we have $\sigma_{-1}' + b_1' = \sigma_{-1}'' + b_1'' = 0$.

By a well-known lemma of Gauss, the coefficients a_i' and a_i'' are rational integers. As the constant term of $f_1(x)$ divides ε_1 and hence is equal to ± 1, we see that also the coefficients b_i' and b_i'' are rational integers. Hence, finally, so are the sums σ_k' and σ_k'' too.

Following the idea in Selmer [1], we shall consider the expression

Received April 16, 1960.

$$\sigma_k - \sigma_{-k} = (\sigma'_k - \sigma'_{-k}) + (\sigma''_k - \sigma''_{-k}) . \tag{2.1}$$

If a root of $f(x)$ is given by

$$x = R(\cos\varphi + i \sin\varphi) ,$$

the contribution from x to $\sigma_k - \sigma_{-k}$ is

$$(R^k - R^{-k}) \cos k\varphi + i(R^k + R^{-k}) \sin k\varphi .$$

As $f(x)$ is a real polynomial, we can, for our purposes, say that the contribution is $(R^k - R^{-k}) \cos k\varphi$. The same remark applies to $\sigma'_k - \sigma'_{-k}$ and $\sigma''_k - \sigma''_{-k}$.

3.

The structure of the proof of our theorem (see section 5) is quite simple. In section 4 we prove essentially that the sums $\sigma'_k - \sigma'_{-k}, \sigma''_k - \sigma''_{-k}$ have to be small in absolute value when $k \leqq m$. In section 5 this "smallness" is applied, in conjunction with a congruence condition induced by Newton's formulae, to prove that the sums in question have to vanish when $k < m$, and an application of a lemma on $\sigma_m - \sigma_{-m}$, due to Selmer, yields the final result.

4.

In this section we prove three lemmas.

Lemma 1. *When* $n > 2m$, $\sigma_m - \sigma_{-m} = \varepsilon m$. *If both* $f_1(x)$ *and* $f_2(x)$ *have roots with* $R \neq 1$, *then*

$$0 < |\sigma'_m - \sigma'_{-m}| < m, \qquad 0 < |\sigma''_m - \sigma''_{-m}| < m .$$

Proof. The first statement follows trivially from Newton's equations for the power sums. The second statement follows from the central result in [1], namely, that the two addends on the right hand side of (2.1) have the same sign.

Lemma 2.

$$\sum_{x;f(x)=0} |R^m - R^{-m}| \leqq 2m .$$

Proof. When $n = 2m$, the equation $f(x) = 0$ is quadratic in x^m, and it is easily verified that the sum in question is equal to $m(1-\varepsilon_1)$.

When $n > 2m$, we write the sum as follows, making use of lemma 1:

$$\begin{aligned}\sum |R^m - R^{-m}| &= \sum_{R\leqq 1} (R^{-m} - R^m) + \sum_{R>1} (R^m - R^{-m}) \\ &= \sum_{R\leqq 1} (R^{-m} - R^m)(1+\varepsilon \cos m\varphi) + \sum_{R>1} (R^m - R^{-m})(1-\varepsilon \cos m\varphi) + m \\ &= \Sigma_1 + \Sigma_2 + m .\end{aligned}$$

In order to get the desired upper bounds for $\sum_1$ and $\sum_2$, we must examine more closely the equation $f(x)=0$. Separating its real and imaginary parts, we get

$$\begin{aligned} R^n \cos n\varphi + \varepsilon_1 \varepsilon R^m \cos m\varphi + \varepsilon_1 &= 0 , \\ R^n \sin n\varphi + \varepsilon_1 \varepsilon R^m \sin m\varphi &= 0 , \end{aligned}$$

and, by elimination:

$$F(R, \cos m\varphi) = R^{2n} - R^{2m} - 1 - 2\varepsilon R^m \cos m\varphi = 0 . \tag{4.1}$$

Elimination of $\cos m\varphi$ between (4.1) and the equation

$$\frac{\partial F}{\partial R}(R, \cos m\varphi) = 0$$

yields

$$(2n-m)R^{2n} = m(R^{2m}-1) .$$

When $n > m$, this equation has no real solutions R. As $F(0, \cos m\varphi) = -1$ and $F(\infty, \cos m\varphi) = \infty$, we are thus assured that equation (4.1) defines R as a positive-valued real function of $\cos m\varphi$. We then have, for $R \leqq 1$

$$\begin{aligned} (R^{-m} - R^m)(1 + \varepsilon \cos m\varphi) &= (R^{-m} - R^m) \frac{R^{2n} - (R^m - 1)^2}{2R^m} \\ &\leqq \tfrac{1}{2}(R^{-m} - R^m)R^{2n-m} , \end{aligned}$$

where we have substituted for $\cos m\varphi$ from (4.1).

By elementary calculus, we find

$$\max_{R \leqq 1}[(R^{-m} - R^m)R^{2n-m}] = \frac{m}{n-m}\left(1 - \frac{m}{n}\right)^{n/m} < \frac{m}{n-m} e^{-1} < 2e^{-1}\frac{m}{n} < \frac{m}{n}$$

(for the second inequality, remember that $n > 2m$), and this is what we need to estimate $\sum_1$.

When we gave the upper bound for $(R^{-m} - R^m)(1 + \varepsilon \cos m\varphi)$, we did not make full use of the fact that R is the modulus of a root of $f(x)$, as we applied just equation (4.1). We shall not need more to find an upper bound when $R > 1$. Taking (4.1) into account, the expression $n(R^m - R^{-m})(1 - \varepsilon \cos m\varphi)$ can be regarded as a function $G(\cos m\varphi)$. For a fixed value of m, we get a family G_m of functions as n takes the values $2m, 2m+1, 2m+2, \ldots$. The corresponding functions R, as defined by (4.1), share the property

$$R > 1 \Leftrightarrow \varepsilon \cos m\varphi > -\tfrac{1}{2} . \tag{4.2}$$

This is seen by noticing that the above inequalities are both equivalent to $F(1, \cos m\varphi) < 0$. We shall now see that the family G_m is a monotonous family on the domain $\varepsilon \cos m\varphi > -\frac{1}{2}$. This enables us to find a common upper bound for *all* members of the family G_m.

Let $R_n > 1$ satisfy

$$R_n^{2n} - R_n^{2m} - 1 - 2\varepsilon R_n^m \cos m\varphi = 0 .$$

Then

$$R_n^{2n-2} - R_n^{2m} - 1 - 2\varepsilon R_n^m \cos m\varphi < 0 ,$$

which means that $R_{n-1} > R_n$. Furthermore

$$\begin{aligned} R_{n-1}^{2(n-1)} &= 1 + R_{n-1}^m (R_{n-1}^m + 2\varepsilon \cos m\varphi) \\ &> 1 + R_n^m (R_n^m + 2\varepsilon \cos m\varphi) = R_n^{2n} . \end{aligned}$$

The inequality is correct because $R_{n-1} > R_n$ and the expressions $R_{n-1}^m + 2\varepsilon \cos m\varphi$, $R_n^m + 2\varepsilon \cos m\varphi$ are both positive by property (4.2).

Hence, by the above inequality,

$$\begin{aligned} (n-1)(R_{n-1}^m - R_{n-1}^{-m}) &= 2(n-1) \sum_{r=0}^{\infty} \frac{(m \log R_{n-1})^{2r+1}}{(2r+1)!} \\ &= m \log R_{n-1}^{2n-2} \sum_{r=0}^{\infty} \frac{(m \log R_{n-1})^{2r}}{(2r+1)!} \\ &> m \log R_n^{2n} \sum_{r=0}^{\infty} \frac{(m \log R_n)^{2r}}{(2r+1)!} = n(R_n^m - R_n^{-m}) . \end{aligned}$$

As $(1 - \varepsilon \cos m\varphi) \geqq 0$, we have now proved the monotony of the family G_m.

Thus, if $R > 1$ for s roots of $f(x)$, we have

$$\begin{aligned} \Sigma_2 &\leqq (s/n) \max_{R_n \geqq 1} [n(R_n^m - R_n^{-m})(1 - \varepsilon \cos m\varphi)] \\ &\leqq (s/n) \max_{R_{2m} \geqq 1} [2m(R_{2m}^m - R_{2m}^{-m})(1 - \varepsilon \cos m\varphi)] \\ &= (s/n) \cdot 2m \cdot \max_{y \geqq 1} \left[(y - y^{-1}) \left(1 - \frac{y^4 - y^2 - 1}{2y} \right) \right] \\ &= (2ms/n) \max_{y \geqq 1} \left[\tfrac{1}{2} - \frac{(y^3 - y - 1)^2}{2y^2} \right] = (s/n)m . \end{aligned}$$

We thus have, finally,

$$\sum |R^m - R^{-m}| = \Sigma_1 + \Sigma_2 + m \leqq (n-s)(m/n) + (s/n)m + m = 2m .$$

LEMMA 3. *When* $0 < k < m$, *then*

$$|\sigma_k' - \sigma_{-k}'| = |\sigma_k'' - \sigma_{-k}''| < k .$$

PROOF. For the values of k in question, it is immediately seen by Newton's formulae that $\sigma_k - \sigma_{-k} = 0$, whence $\sigma'_k - \sigma'_{-k} = -(\sigma''_k - \sigma''_{-k})$. Now,

$$\sum_{x;f(x)=0} |R^k - R^{-k}||\cos k\varphi| \leqq \sum_{x;f(x)=0} |R^k - R^{-k}| \leqq (k/m) \sum_{x;f(x)=0} |R^m - R^{-m}| .$$

We can replace the last $\leqq$ by $<$, as $\sigma'_k - \sigma'_{-k} = 0$ quite trivially if all R's are equal to 1. Thus, taking lemma 2 into account, we have finished the proof.

5.

THEOREM. *The trinomial $f(x)$ is irreducible whenever no root of $f(x)$ has the modulus* 1. *If $f(x)$ has roots with modulus* 1, *these roots can be collected to give a rational factor of $f(x)$. The other factor of $f(x)$ is then irreducible.*

PROOF. We first show, by induction on k, that

$$\sigma'_k - \sigma'_{-k} = \sigma''_k - \sigma''_{-k} = a'_k - b'_k = a''_k - b''_k = 0$$

for $1 \leqq k < m$. We need Newton's formulae

$$\sigma'_k + a'_1 \sigma'_{k-1} + \ldots + a'_{k-1}\sigma'_1 + k a'_k = 0$$
$$\sigma'_{-k} + b'_1 \sigma'_{-(k-1)} + \ldots + b'_{k-1}\sigma'_{-1} + k b'_k = 0 .$$

By means of the induction hypothesis for smaller values of k (or directly, if $k = 1$), we conclude that

$$\sigma'_k - \sigma'_{-k} = k(b'_k - a'_k) \equiv 0 \pmod{k} . \tag{5.1}$$

By lemma 3, the congruence (5.1) leads to $\sigma'_k - \sigma'_{-k} = \sigma''_k - \sigma''_{-k} = 0$, and then the equation (5.1) gives

$$a'_k - b'_k = a''_k - b''_k = 0 .$$

The proof of the first statement of the theorem differs a little for the two cases $n > 2m$ and $n = 2m$. We start, in both cases, with the assumption that $f(x)$ is reducible.

Case 1: $n > 2m$. It is seen that the deduction of (5.1) is valid also for $k = m$, hence

$$\sigma'_m - \sigma'_{-m} \equiv 0 \pmod{m} .$$

On the other hand, by lemma 1,

$$0 < |\sigma'_m - \sigma'_{-m}| < m .$$

The assumption of reducibility thus leads to a contradiction.

Case 2: $n = 2m$. The polynomials $x^{2m} \pm x^m + 1$ have $R = 1$ for all their roots. If the polynomical $x^{2m} - \varepsilon x^m - 1$ is reducible, one concludes from the equations

$$a_1' - b_1' = a_1'' - b_1'' = \ldots = a_{m-1}'' - b_{m-1}'' = 0$$

that either $f_1(x)$ or $f_2(x)$ is symmetric, namely the one of them with $+1$ as its constant term. But it is immediately seen that if x is a root of $x^{2m} - \varepsilon x^m - 1$, x^{-1} cannot be, and the symmetry of any factor of $f(x)$ is then impossible.

The second statement of the theorem is taken from theorem 3 of [1]. The above proof needs only minor amendments to be at the same time a proof of the third and last statement.

REFERENCE

1. E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. 4 (1956), 287–302.

UNIVERSITY OF BERGEN, NORWAY