MATH. SCAND. 4 (1956), 287–302

ON THE IRREDUCIBILITY OF CERTAIN TRINOMIALS

ERNST S. SELMER

1. Through a study of generalized continued fractions, I have been led to certain questions concerning the irreducibility of polynomials. Let us first consider the general problem:

The ordinary algorithm for a continued fraction may be described as a systematic replacement of two non-negative numbers, $a_1^{(r)}$ and $a_2^{(r)} \leqq a_1^{(r)}$, by two other numbers, usually $a_1^{(r+1)} = a_2^{(r)}$ and $a_2^{(r+1)} =$ the (positive) remainder by the division $a_1^{(r)}/a_2^{(r)}$. Formulated in this way, a generalization to n dimensions is immediate. Such a *division* algorithm has been extensively studied by Perron [7]. An alternative procedure, using *subtraction* instead of division, was introduced by Brun [1]: At each step, with the n numbers

$$(1.1) \qquad a_1^{(r)} \geqq a_2^{(r)} \geqq \ldots \geqq a_n^{(r)} \geqq 0 ,$$

we replace $a_1^{(r)}$ by the difference $a_1^{(r)} - a_2^{(r)}$, and rearrange the numbers according to magnitude.

Of particular interest are *periodic* expansions, characterized by

$$(1.2) \qquad \frac{a_1^{(r+s)}}{a_1^{(r)}} = \frac{a_2^{(r+s)}}{a_2^{(r)}} = \ldots = \frac{a_n^{(r+s)}}{a_n^{(r)}} = \lambda .$$

In any procedure for generalized continued fractions, the ratio λ is determined by an equation of degree n, and *this equation is irreducible if and only if the given n numbers are linearly independent.* Irreducibility and independence are then, of course, related to the *same* basic field of rationality. In what follows, we shall always assume this to be the ordinary *field of rational numbers*.

The simplest periods consist of *one step* only, that is $s = 1$ in (1.2). In Brun's algorithm, we must then have $a_1^{(r)} - a_2^{(r)} = a_n^{(r+1)}$, since otherwise the smallest number would not be involved at all in the process. The equations (1.2) then take the form

$$\frac{a_2^{(r)}}{a_1^{(r)}} = \frac{a_3^{(r)}}{a_2^{(r)}} = \ldots = \frac{a_n^{(r)}}{a_{n-1}^{(r)}} = \frac{a_1^{(r)} - a_2^{(r)}}{a_n^{(r)}} = \lambda ,$$

Received June 1, 1956.

showing that λ is a characteristic root of the $n \times n$ matrix

$$\begin{Bmatrix} 0 & 1 & 0 & 0 \ldots 0 \\ 0 & 0 & 1 & 0 \ldots 0 \\ 0 & 0 & 0 & 1 \ldots 0 \\ \cdot & \cdot & \cdot & \cdot \cdots \cdot \\ 0 & 0 & 0 & 0 \ldots 1 \\ 1 & -1 & 0 & 0 \ldots 0 \end{Bmatrix}.$$

The corresponding equation for λ takes the form

$$\lambda^n + \lambda - 1 = 0 . \tag{1.3}$$

For several reasons, I have found it natural to replace the difference $a_1^{(r)} - a_2^{(r)}$ in Brun's algorithm by $a_1^{(r)} - a_n^{(r)}$, that is to form the *largest possible difference* between any two of the numbers (1.1). For a period of one step only, the equation (1.3) is then replaced by

$$\lambda^n + \lambda^{n-1} - 1 = 0 , \tag{1.4}$$

or with $\lambda = 1/\mu$:

$$\mu^n - \mu - 1 = 0 .$$

In general, I have been led to study *the irreducibility of the polynomials*

$$x^n \pm x \pm 1 .$$

By changing the sign of x appropriately, we can always get one of the two forms

$$\begin{cases} f_1(x) = x^n - x - 1 \\ f_2(x) = x^n + x + 1 . \end{cases} \tag{1.5}$$

2. Before studying the irreducibility of these polynomials, we may mention an interesting property: For $n = 2$, the equations (1.3) and (1.4) both give the polynomial

$$\lambda^2 + \lambda - 1 , \tag{2.1}$$

corresponding to an ordinary continued fraction with all partial denominators $= 1$. It is well known that (2.1) is the quadratic polynomial with the smallest possible positive discriminant, $D = 5$.

In general, the polynomials (1.5) *have very small discriminants.* I have obtained the expressions

$$D(f_1(x)) = (-1)^{\frac{1}{2}(n-1)(n-2)} \cdot [n^n + (-1)^n (n-1)^{n-1}]$$
$$D(f_2(x)) = (-1)^{\frac{1}{2}n(n-1)} \cdot [n^n + (-1)^{n-1} (n-1)^{n-1}] .$$

For the first values of n, this yields:

$$n = 2: \quad D(f_1) = +5, \quad D(f_2) = -3 ,$$

representing the smallest possible quadratic discriminants of both signs.

$$n = 3: \quad D(f_1) = -23, \quad D(f_2) = -31\ ,$$

which are the two smallest negative discriminants in the cubic case.

$$n = 4: \quad D(f_1) = -283, \quad D(f_2) = +229\ .$$

According to Delone and Faddeev [2], there exists one negative quartic discriminant with a smaller absolute value than $D(f_1)$, namely $D = -275$. In the case of totally complex quartic fields, many discriminants smaller than $D(f_2)$ are known (the smallest one being $D = 117$). However, the fields listed by Delone and Faddeev all have a quadratic subfield. Dr. H. J. Godwin has computed the small totally complex quartic fields, whether or not subfields exist. He has kindly informed me that $D(f_2) = 229$ is really the *least* discriminant in the latter case. His results are submitted for publication to the Proc. Cambridge Phil. Soc.

$$n = 5: \quad D(f_1) = 2869\ ,$$

while $f_2(x)$ is reducible (cf. (3.1) below). The minimal discriminants of quintic fields have been calculated by Hunter [4]. In the case of 4 complex roots, the minimum is $D = 1609$, and there are at least 6 more fields with a smaller discriminant than $D(f_1)$.

For $n \geqq 6$, no results on minimal discriminants are available.—I owe all references to such discriminants to Dr. J. W. S. Cassels.

3. For large n, all zeros of the polynomials (1.5) will clearly have a modulus close to 1. As we shall see later (cf. fig. 1, p. 292), a modulus $= 1$ can occur only for $x = e^{\pm 2\pi i/3}$, corresponding to a rational factor $x^2 + x + 1$. It is easily seen that this is possible only for $f_2(x)$, in the case $n \equiv 2 \pmod 3$. The first such factorizations are given by

$$\begin{aligned} (3.1) \qquad x^5 + x + 1 &= (x^2 + x + 1)(x^3 - x^2 + 1) \\ x^8 + x + 1 &= (x^2 + x + 1)(x^6 - x^5 + x^3 - x^2 + 1)\ . \end{aligned}$$

The general form of the second factor is clear.

The main purpose of the present paper is to prove the following

Theorem 1. *The polynomials*

$$f_1(x) = x^n - x - 1$$

are irreducible for all n. The polynomials

$$f_2(x) = x^n + x + 1$$

are irreducible for $n \not\equiv 2$ (*mod* 3), *but have a factor* x^2+x+1 *for* $n \equiv 2$ (mod 3). *In the latter case, the second factor of* $f_2(x)$ *is irreducible.*

This result does not seem to follow from any of the *existing* irreducibility criteria. The Eisenstein-Schönemann theorem and its generalizations (cf. Ore [6]) clearly fail. However, by studying reducibility modulo a prime p, Serret [11] and Ore [6] have shown that the polynomial

$$x^p - x + a$$

is *irreducible when* p *is a prime such that* $p \nmid a$. This result contains as a special case the irreducibility of my polynomials $f_1(x)$ when n is a prime. However, similar methods seem to fail for composite degrees.

Criteria by *primality* of certain values of the function are clearly insufficient in the case of arbitrary degree (but see Section 7 below).

Other general criteria, which also fail in my case, are listed in the expository article by Dorwart [3], and in Part 8, problems 116–129, of Pólya and Szegö [10].

An important criterion, typical of one approach to the problem, is given by Perron [8]: The polynomial (with integer coefficients)

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$$

is irreducible if

$$|a_1| > 1 + |a_2| + |a_3| + \ldots + |a_n| .$$

Applied to $f(x) = x^n + ax \pm 1$, where we substitute $x = 1/z$, this shows that $f(x)$ is irreducible for $|a| \geqq 3$. When $|a| = 2$ and $f(\pm 1) \neq 0$, we can still conclude irreducibility according to Perron. When $|a| = 2$ and $f(x)$ has a rational factor $x+1$ or $x-1$, the second factor of $f(x)$ will be irreducible (this is not contained among Perron's statements, but follows easily from his method). To sum up, we have the following

THEOREM 2 (*Perron*). *The polynomial*

$$f(x) = x^n + ax \pm 1$$

is irreducible for $|a| \geqq 3$. *When* $|a| = 2$, $f(x)$ *is either irreducible or has a factor* $x \pm 1$. *In the latter case, the second factor of* $f(x)$ *is irreducible.*

Combined with my Theorem 1, this settles the problem of irreducibility of the polynomials

$$f(x) = x^n + ax \pm 1$$

for *all* (integer) values of a.

The only criterion for irreducibility of a *trinomial*

$$g(x) = x^n + qx^p + r, \qquad 1 \leqq p \leqq n-1 ,$$

is given by Nagell [5]: $g(x)$ is irreducible if

1° $|q| > 1 + |r|^{n-1}$.

2° If $h|n$, $h > 1$, then $|r|$ is not a h^{th} power. In particular, we must have $|r| > 1$.

Nagell remarks that his result is clearly weaker than the above criterion of Perron in the case $p = n-1$. It could also be noted that Nagell's *first* condition *coincides* with Perron's criterion for $p = 1$ (immediately seen if x is replaced by r/z). In this case, Nagell's second condition is consequently redundant. However, his first condition fails for my polynomials (1.5).

In a series of papers from 1935 to 1937, Petterson has discussed and extended many of the general irreducibility criteria. All results are also contained in his thesis [9], where in particular (pp. 95–96) the conditions are applied to the polynomial

$$x^m + EM(x)x + a \quad (a \neq 0) .$$

To get the types (1.5), we must put $EM(x) = a = \pm 1$, in which case it is easily seen that Petterson's criteria all fail.

4. To prove Theorem 1, we must study the distribution in the complex plane of the roots of the equations

$$\text{(4.1)} \qquad x^n \mp (x+1) = 0 .$$

It will turn out that this distribution is very *regular*.

Substituting in (4.1)

$$x = re^{i\varphi} = r(\cos\varphi + i \sin\varphi) ,$$

and separating the real and imaginary parts, we find

$$\text{(4.2)} \qquad r^n \cos n\varphi = \pm (r\cos\varphi + 1), \quad r^n \sin n\varphi = \pm r \sin\varphi ,$$

or, by taking the sum of the squares on both sides:

$$\text{(4.3)} \qquad \cos\varphi = \frac{r^{2n} - r^2 - 1}{2r} .$$

This may be considered as the equation, in polar coordinates (r, φ), of a curve in the complex plane, containing all the roots of (4.1). A typical curve, for $n = 5$, is drawn in fig. 1. When $0 \leqq \varphi \leqq \pi$, r is a decreasing function of φ for increasing φ. The extreme values of r, for $\varphi = 0$ and $\varphi = \pi$, are denoted by R_n and r_n, respectively. Both values are close to 1 when n is large, and we find the approximations

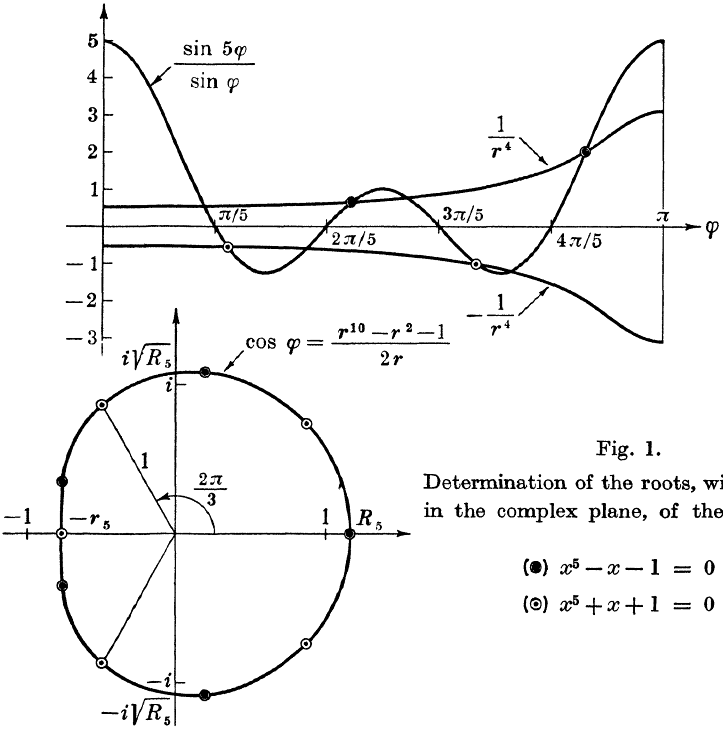

Fig. 1.
Determination of the roots, with location in the complex plane, of the equations

(●) $x^5 - x - 1 = 0$,
(⊙) $x^5 + x + 1 = 0$.

$$R_n \approx 1 + n^{-1} \ln 2, \qquad r_n \approx 1 - n^{-1} \ln n\,. \tag{4.4}$$

For $\varphi = \pm \pi/2$, we have $r = R_n^{1/2} > 1$. The curve (4.3) cuts through the unit circle $r = 1$ for $\cos\varphi = -\frac{1}{2}$, $\varphi = \pm 2\pi/3$. We made use of this fact at the beginning of Section **3** above.

The *arguments* φ of the roots of (4.1) can be easily determined graphically. From the second equation (4.2), we get

$$\frac{\sin n\varphi}{\sin \varphi} = \pm \frac{1}{r^{n-1}}\,. \tag{4.5}$$

When r is determined as a function of φ by the graph of (4.3), both sides of (4.5) may be represented graphically for $0 \leqq \varphi \leqq \pi$. The arguments of the roots are then found among the *intersections* of the two curves. A closer examination reveals that we must use those intersections which lie to the *left* on each of the (positive or negative) "waves" of $\sin n\varphi / \sin \varphi$, as illustrated for $n = 5$ in fig. 1.

The possible *real* roots of (4.1) are $x = R_n$ and $x = -r_n$. It is immediately seen that R_n is always a zero of $f_1(x)$ (cf. (1.5)), while $-r_n$ is a zero of $f_1(x)$ for even n, but of $f_2(x)$ for odd n.

5. We are now able to prove Theorem 1. For this purpose, we introduce the following *function of the roots*: Let $f(x)$, of degree n, have the zeros x_j (all $\neq 0$). We define

$$S(f(x)) = \sum_{j=1}^{n} \left(x_j - \frac{1}{x_j}\right), \tag{5.1}$$

that is, *the sum of the roots less the sum of their reciprocals.*—Clearly, S is *additive* by any factorization of $f(x)$. As a symmetric function of the roots, S is *rational*, and *integer* if the constant term of $f(x)$, in normalized form, is ± 1. In the latter case, any factorization of $f(x)$ must yield an *integer partition* of $S(f(x))$, since a rational factor of $f(x)$ must then also have a constant term ± 1.

For both functions $f_1(x)$ and $f_2(x)$ of (1.5), we find

$$S(f_k(x)) = 1, \qquad k = 1, 2\,. \tag{5.2}$$

On the other hand, by substituting $x_j = re^{i\varphi}$, $x_j^{-1} = r^{-1}e^{-i\varphi}$ in (5.1), and summing *in pairs* over conjugate imaginary roots, we get

$$\sum{}' \left(x_j - \frac{1}{x_j}\right) = \sum_{0<\varphi<\pi} 2\frac{r^2-1}{r}\cos\varphi\,. \tag{5.3}$$

For possible *real* roots, with $\cos\varphi = \pm 1$, the factor 2 must be omitted.

For the polynomials $f_k(x)$, the sum (5.3) will contain *negative* terms only in the interval $\pi/2 < \varphi < 2\pi/3$, where $\cos\varphi < 0$, $r > 1$ (cf. fig. 1). It is not difficult to conclude from (4.4) that the negative part of the sum will always be < 1 in absolute value (but this fact is not needed for completion of the proof). Consequently, any factorization of $f_k(x)$ must yield the integer partition

$$1 = 0 + 1 \tag{5.4}$$

of the sum (5.2).

If we leave aside for a moment the possible factor x^2+x+1 of $f_2(x)$ (where $r=1$, $S=0$), one factor of $f_k(x)$ must contain some terms of *both signs* in the sum (5.3). As the negative terms all have $r>1$, we must *compensate* for this by taking some roots from the interval $2\pi/3 < \varphi \leqq \pi$, where $r<1$, since the *product* of the roots must be ± 1. However, this is not possible without "*over-compensation*" for the sum S, which becomes >0. A partition of the type (5.4), and thereby a factorization of $f_k(x)$, consequently becomes impossible.

To carry through this idea in precise mathematical terms, we substitute for $\cos\varphi$ in (5.3) the expression (4.3):

$$2\frac{r^2-1}{r}\cos\varphi = 2\frac{r^2-1}{r}\cdot\frac{r^{2n}-r^2-1}{2r}$$
$$= \frac{1}{r^2}-r^2+r^{2n-2}(r^2-1) \geqq \frac{1}{r^2}-1\,,$$

since $r^{2n-2}(r^2-1)\geqq r^2-1$, with *equality only for* $r=1$, that is, for a possible factor x^2+x+1. If we remember that the sum (5.3) is taken over conjugate imaginary roots *in pairs*, we get the following inequality for the sum S for any *factor* of $f_k(x)$:

$$(5.5)\qquad S = \sum\left(x_j-\frac{1}{x_j}\right) \geqq \tfrac{1}{2}\sum\left(\frac{1}{r^2}-1\right).$$

The sum is now taken over *all* roots (real or complex) separately.

On the other hand, the product of the modulus over the same roots must give unity:

$$\prod r = 1, \quad\text{or}\quad \prod\frac{1}{r^2} = 1\,.$$

The *geometric mean* of all r^{-2} is consequently $=1$. Since this is always $\leqq$ the *arithmetic mean* (again with equality only for all $r=1$), it follows for the sum in (5.5) that

$$S \geqq 0\,.$$

Equality can occur only for the factor x^2+x+1. This concludes the proof of Theorem 1.

6. Whenever a new method has been developed, one tries to apply it also to cases other than those for which it was originally designed. In this instance, however, it seems that my method is "tailor-made" for the polynomials $f_1(x)$ and $f_2(x)$, and for these only. After a series of attempts to generalize to other polynomials, especially of the type x^n+ax+b, I feel convinced that my method will lead to no new proofs of irreducibility. (The case $b=\pm1$ is already covered by Theorem 2, and for $|b|>1$, all arguments are destroyed by the fact that the sum S may become *fractional*).

Let us consider the polynomials

$$x^n\pm x^2\pm 1\,.$$

When n is even, all four combinations of signs will here lead to essentially different cases. For simplicity, we shall only deal with the combinations

$$f(x) = x^n\pm(x^2+1)\,.$$

Treating these as we did with $f_k(x)$ in Section 4 above, we find

$$\cos 2\varphi = \frac{r^{2n} - r^4 - 1}{2r^2} .$$

Because of 2φ, it is here natural to replace the sum (5.1) by

$$\sum \left(x_j^2 - \frac{1}{x_j^2} \right) .$$

Exactly as in Section 5, we find that this sum is $\geqq 0$ for any factor of $f(x)$, with equality only for a possible factor with all $r = 1$. However, the corresponding sum for $f(x)$ itself (for $n > 4$) has the value 2, not 1. We can therefore not conclude irreducibility, only the existence of *at most two* irreducible factors.

A similar argument, with all inequalities reversed, holds for $x^n \pm (x^2 - 1)$. More generally, we can show that the polynomials

$$(6.1) \qquad F(x) = x^n \pm x^m \pm 1, \qquad 1 \leqq m \leqq \tfrac{1}{2}n ,$$

have at most m irreducible factors, in addition to a possible factor with all $r = 1$. This result is contained as a part of

THEOREM 3. *The following results hold for the factorization of the trinomials* (6.1):

1° *All possible roots with modulus* 1 *are roots of a rational factor, typified by*

$$x^{2d} + x^d + 1 \mid x^n + x^m + 1 = (x^d)^{n_1} + (x^d)^{m_1} + 1 ,$$

if

$$n = n_1 d, \quad m = m_1 d, \quad (n_1, m_1) = 1, \quad n_1 + m_1 \equiv 0 \pmod 3 ,$$

and all those cases resulting from changing the sign of x^d.

2° *Apart from a possible factor of the above type, there are at most m irreducible factors, all of degree > 5 for $n > 7$.*

3° *If $F(x)$ is irreducible or has a factor $x^{2d} \pm x^d + 1$ and a second, irreducible factor, then $F(x^2)$ has the same property.*

4° *All polynomials $F(x)$ have this property for $n \leqq 20$ (and hence for $n \leqq 40$ when n and m are both even).*

7. We shall only indicate the proof of Theorem 3.—The result 1° is established by forming an expression for $\cos m\varphi$ similar to (4.3), and examining the case $r = 1$. The arguments are tedious but straightforward. It should be noted that the factor

$$x^{2d} \pm x^d + 1 = \frac{x^{3d} \mp 1}{x^d \mp 1}$$

may itself be *reducible*, cf. (11.2). Changing the sign of x^d is *not* the same as changing the sign of x itself, if d is even.

A proof of the first statement under 2° is already sketched in Section 6. The second statement may be proved as follows: Since $F(0)=\pm 1$ and $F(\pm 1)=\pm 1$ or ± 3, we get a very limited choice of values $\psi(0)$ and $\psi(\pm 1)$ for a possible factor $\psi(x)$ of $F(x)$. For each set of values, $\psi(x)$ is uniquely determined mod (x^3-x). A closer examination shows that a possible quadratic factor of $F(x)$ must have one of the forms

$$x^2 \pm x \pm 1 .$$

The constant term $+1$ gives a factor with all $r=1$. The term -1 is impossible, since the roots then *differ too much from* 1 *in absolute value* to be roots of $F(x)$.

Similarly, the possible cubic factors of $F(x)$ are given by

$$x^3 \pm x^2 \pm 1 \qquad \text{or} \qquad x^3 \pm x \pm 1 ,$$

all with one real root. The same argument shows that this root can not satisfy $F(x)=0$ for $n>5$. An exception for $n=5$ is given by (3.1).

In the same way, by factorizing $F(i)$ in the field $K(i)$, we get a limited choice of values $\psi(i)$. For each choice, $\psi(x)$ is uniquely determined mod (x^2+1). Combining this with the earlier modulus (x^3-x), we get a limited (but rather large) number of alternatives mod (x^5-x) for a possible factor $\psi(x)$ of $F(x)$. Using the same principle, we find that the resulting factors of degree 4 or 5 (apart from $x^4 \pm x^2+1$) can not occur for $n>18$, and hence not for $n>7$ by 4° of Theorem 3. An exception (a factor of degree 5) occurs for $n=7$, $m=2$, cf. 1°.

The statement 3° is proved in Section 11 below. Because of this result, the cases when n and m are both even could be left out in the numerical computations.

To prove the result 4°, I have mainly used a *primality criterion* of Pólya and Szegö [10, Part 8, Problem 127]: Since all the roots of the polynomials (6.1) have an absolute value <1.5 for $n>2$, the criterion shows that $F(x)$ *is irreducible if* $F(k)$ *is a prime for an integer argument* k *such that* $|k|>1$. Replacing x by $1/x$, we can argue similarly with $k^n F(1/k)$. More generally, the criterion can be extended to the case $a^n F(b/a)$, provided that all the roots of $F(x)$ have a modulus $<(|b|-\frac{1}{2})/|a|$.

As shown in Section 8 below, the criterion of Pólya and Szegö can be extended to cover the case $|F(k)|=t \cdot p$, where p is a prime and t is a *small* factor.

The cases $F(x^2)$ are completely settled by the result 3°. Some information regarding $F(x^3)$ can also be obtained, cf. Section 9.

By combining these different principles, I have been able to establish the result 4° of Theorem 3. For $14 < n \leqq 20$, $F(\pm 2)$ and $2^n F(\pm \frac{1}{2})$ are the only values which can be examined directly by Lehmer's factor table and list of primes to 10^7. In spite of this limitation, it was only in three cases necessary to seek information outside these tables, namely for

$$F(x) = x^{17}+x^5+1, \qquad x^{18}+x^7+1, \qquad x^{19}-x^4+1 .$$

The primality of $3^n F(-\frac{1}{3})$ in each of the cases was established by Dr. C.-E. Fröberg on the electronic computer SMIL in Lund, Sweden.

It would be of great interest if it could be proved that the last statement of Theorem 3 holds for *all* polynomials $F(x)$, or if a *counterexample* could be found. As it is, I have only been able to settle completely the case $m=1$.

8. As already mentioned, the criterion of Pólya and Szegö can be extended to cover the case

$$(8.1) \qquad |F(k)| = t \cdot p, \qquad t < p, \qquad p \text{ prime},$$

when t is a *small* factor.

Let $M > 1$ be an upper bound for the absolute values of the roots of $F(x)$. For a polynomial $x^n \pm x^m \pm 1$ $(m < n)$, M is given by the positive real root of the equation

$$M^n = M^m + 1 .$$

Here clearly $M \approx 1$ for large n. We shall treat only this case; the same principle applies for greater values of M.

Let $F(x) = A_0 x^n + A_1 x^{n-1} + \ldots$ have a factor $\varphi(x) = a_0 x^q + a_1 x^{q-1} + \ldots$ $(q \leqq \frac{1}{2}n)$, with roots $\alpha_1, \alpha_2, \ldots, \alpha_q$, and let k denote a rational integer such that $|k| > 1$. Then

$$|\varphi(k)| = |a_0| \cdot |k-\alpha_1| \cdot |k-\alpha_2| \ldots |k-\alpha_q| \geqq (|k|-M)^q ,$$

which is impossible by (8.1) if

$$(8.2) \qquad t < (|k|-M)^q .$$

This irreducibility criterion is due to Weisner [12]. However, it is useless in the most important case $|k|=2$, and can be improved.

Following the idea of Pólya and Szegö, we take into account the fact that $\varphi(\pm 1) \neq 0$. Let $\varepsilon = \pm 1$, with the same sign as k. Then

$$|\varphi(\varepsilon)| = |a_0| \cdot |\varepsilon-\alpha_1| \cdot |\varepsilon-\alpha_2| \ldots |\varepsilon-\alpha_q| \geqq 1 .$$

With this additional condition, it can be shown that we get a (theoretical) minimum for $|\varphi(k)|$ when $|a_0| = 1$, and when all the roots of $\varphi(x)$ have the property

$$|\alpha_i| = M, \quad |\varepsilon - \alpha_i| = 1, \qquad i = 1, 2, \ldots, q .$$

This gives

$$|k - \alpha_i| = \left(k^2 - (|k|-1)M^2\right)^{\frac{1}{2}} ,$$

which may be substituted for $|k| - M$ in (8.2), thereby improving the criterion.

For the polynomials (6.1), I knew that $q \geqq 4$ for $n > 5$. A factorization (8.1) consequently showed irreducibility if

$$t < \left(k^2 - (|k|-1)M^2\right)^2 .$$

This criterion proved very useful also for $|k| = 2$. To indicate the strength of the condition, we may mention that the inequality is then always satisfied for $t \leqq 7$ when $n \geqq 9$.

9. When n and m are both *even*, the polynomials (6.1) are of the type

$$F(x) = f(x^2) .$$

In this section, we will study such polynomials in general, under the assumption that $f(x)$ is *irreducible*, and shall establish some obvious criteria for the irreducibility of $f(x^2)$.

Let $f(x)$ be of degree n, with the highest term x^n. It is easily seen that the only possible factorization of $f(x^2)$ must have the form

$$(9.1) \qquad F(x) = f(x^2) = (-1)^n g(x) g(-x) ,$$

where $g(x)$ is *irreducible*. With

$$g(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n ,$$

we get

$$(9.2) \quad F(x) = f(x^2) = (x^n + a_2 x^{n-2} + a_4 x^{n-4} + \ldots)^2 - \\ - (a_1 x^{n-1} + a_3 x^{n-3} + \ldots)^2 .$$

Clearly $f(x^2)$ is irreducible if

$$(9.3) \qquad (-1)^n f(0) \quad \textit{is not a perfect square} .$$

Let k be a rational integer. From (9.2), we see that $F(k) = f(k^2)$ is a *difference between two squares*, which is impossible if $f(k^2) \equiv 2 \pmod 4$. For even k, this is already contained in (9.3), but we get a criterion for the irreducibility of $f(x^2)$ for odd k:

$$f(1) \equiv 2 \pmod 4 .$$

More information can be obtained from a (purely) *imaginary* value of the argument. Then $F(ik) = f(-k^2)$ is real, and $|f(-k^2)|$ is a *sum* of two squares. Consequently, $f(x^2)$ is irreducible if $|f(-k^2)|$ is *exactly divisible by an odd power of a prime* $4h+3$. In particular, this is the case if

$$(9.4) \qquad |f(-k^2)| \equiv 3 \pmod 4, \quad \text{or} \quad \equiv 6 \pmod 8) .$$

The criteria (9.3-4) are necessary to establish Theorem 4 of Section 10 below, and thereby the result 3° of Theorem 3.

We can prove similar results for a polynomial

$$F(x) = f(x^3) .$$

With the same assumptions for $f(x)$, a possible factorization must have the form

$$F(x) = f(x^3) = g(x)G(x) = g(x)g(\varrho x)g(\varrho^2 x), \qquad \varrho = e^{2\pi i/3} .$$

In particular, $f(0)$ must be a *perfect cube* (always satisfied for the polynomials (6.1)). Further, $f(k^3)$ can be written as

$$(X+Y+Z)(X+Y\varrho+Z\varrho^2)(X+Y\varrho^2+Z\varrho) = X^3+Y^3+Z^3-3XYZ ,$$

with integers X, Y and Z. This cubic form is never exactly divisible by 3, and $f(x^3)$ is consequently irreducible if

$$f(1) \quad \text{or} \quad f(-1) \equiv \pm 3 \pmod 9) .$$

This condition was useful when examining the polynomials (6.1).

10. When $f(x)$ is a *trinomial*, we can obtain additional information regarding the irreducibility of $f(x^2)$. By operating modulo 4, we can prove the following

THEOREM 4. *Let*

$$f(x) = x^n + ax^m + b \qquad (m < n)$$

be an irreducible trinomial satisfying the conditions

$$(10.1) \qquad 2^3 \nmid a, \quad 2 \nmid b, \quad n \neq 2m ,$$

or

$$(10.2) \qquad a \equiv 1 \text{ or } 2 \pmod 4), \quad 2|b .$$

Then $f(x^2)$ is also irreducible.

PROOF. We know that $f(x^2)$ must have the form (9.2). Multiplying out, we get

$$f(x^2) = x^{2n} + ax^{2m} + b = x^{2n} + A_2 x^{2n-2} + A_4 x^{2n-4} + \ldots ,$$

where

$$\begin{aligned}
A_2 &= 2a_2 - a_1{}^2 \\
A_4 &= a_2{}^2 + 2a_4 - 2a_1a_3 \\
A_6 &= 2a_2a_4 + 2a_6 - a_3{}^2 - 2a_1a_5 \\
A_8 &= a_4{}^2 + 2a_2a_6 + 2a_8 - 2a_1a_7 - 2a_3a_5 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

All coefficients $a_N = 0$ for $N > n$.

Let first a be *odd*. If $A_2 = 0$, both a_1 and a_2 are even, and so also A_4. Consequently $A_4 = a$ is impossible, and we must have $A_4 = 0$, a_4 even. If also $A_6 = 0$, both a_3 and a_6 are even. We conclude similarly that $A_8 \neq a$, $A_8 = 0$, a_8 even. Continuing the argument, we see that $A_{4k} \neq a$, and that a factorization of $f(x^2)$ is impossible if n and m have the *same parity*. More generally, we have clearly established the irreducibility of $f(x^2)$ if

$$(10.3) \qquad f(x) = x^n + (2h+1)x^{n-2k} + \ldots$$

is irreducible.

When n and m have opposite parity, the case $a \equiv +1 \pmod 4$ can be excluded by similar arguments. If $A_2 = a$, both a_1 and a_2 are odd, and so also A_4, which is impossible (always if b is even; as a consequence of $n \neq 2m$ if b is odd). If $A_2 = A_4 = 0$, $A_6 = a$, we get a_1, a_2 and a_4 even, a_3 and a_6 odd, which again is impossible (either $n < 6$, and so $a_6 = 0$; or $n \geqq 6$, but then A_{12} is odd), etc.

If $a \equiv -1 \pmod 4$, we must have b odd by (10.2). It follows from (9.3) that $b \equiv (-1)^n \pmod 8$ (since otherwise $f(x^2)$ is certainly irreducible). For a sufficiently large odd integer k, we then have

$$\begin{aligned}
(10.4) \quad |f(-k^2)| = (-1)^n f(-k^2) &= k^{2n} + (-1)^{m+n} a k^{2m} + (-1)^n b \\
&\equiv 2 + (-1)^{m+n} a \pmod 8 .
\end{aligned}$$

When n and m have *opposite* parity, and $a \equiv -1 \pmod 4$, we get $|f(-k^2)| \equiv 3 \pmod 4$, and the irreducibility of $f(x^2)$ follows from (9.4).

Let next $2 \| a$ ("exactly divide"). If then $A_2 = a$, we must have a_1 even, a_2 odd, and so A_4 odd, which is impossible (always if b is even; as a consequence of $n \neq 2m$ if b is odd). Hence $A_2 = 0$, a_1 and a_2 even. If $A_4 = a$, we get a_4 odd, which again is impossible by a similar argument, etc.

Let finally $2^2 \| a$, $2 \nmid b$. We then get $|f(-k^2)| \equiv 6 \pmod 8$ by (10.4), and the irreducibility of $f(x^2)$ follows from (9.4).

This concludes the proof of Theorem 4. It is clear that the theorem can be shown valid under less restrictive conditions than (10.1-2), by further considerations modulo 4, or by the criteria of Section 9. However, the conditions imposed on a and b are then not so simple.

11. By means of Theorem 4, it is now easy to prove the result 3° of Theorem 3. We assume that

$$F(x) = f(x^2) = x^{2n} \pm x^{2m} \pm 1 ,$$

where $f(x)$ is either irreducible or has a factor

$$(11.1) \qquad e(x) = x^{2d} \pm x^d + 1, \qquad d = (n, m) ,$$

and a second, irreducible factor.

We first dispose of the case $n = 2m$. With the constant term $+1$, $F(x)$ is then itself of the form (11.1). With the constant term -1, no factor (11.1) can occur, and $F(x)$ is irreducible by (9.3).

The case of irreducible $f(x)$ is then completely covered by Theorem 4, and we must only examine the effect of a factor $e(x^2) = E(x)$.

When d is *even*, all exponents of $F(x)$, $E(x)$ and $F(x)/E(x)$ are divisible by 4, and the irreducibility of the quotient follows from (10.3).

The upper sign in (11.1) gives

$$(11.2) \quad E(x) = e(x^2) = x^{4d} + x^{2d} + 1 = (x^{2d} + x^d + 1)(x^{2d} - x^d + 1) ,$$

which for *odd* d is of the form (9.1), $E(x) = g(x)g(-x)$. This would then also be the case for $F(x)$ itself if the quotient were reducible, and the proof of Theorem 4 can be applied.

It thus only remains to consider the lower sign in (11.1) for odd d. We may assume that $m < \frac{1}{2}n$, and then get the quotient

$$\frac{F(x)}{E(x)} = \frac{x^{2n} \pm x^{2m} \pm 1}{x^{4d} - x^{2d} + 1} = x^{2n-4d} + x^{2n-6d} - x^{2n-10d} - \dots ,$$

where the term x^{2n-8d} is *missing*, cf. (3.1). The argument following (10.3) then shows that the quotient is irreducible. This completes the proof.

REFERENCES

1. V. Brun, *En generalisation av kjedebrøken* I, II (avec des résumés en français), Vid. selsk. Skrifter, Mat.-Nat. Kl., Kristiania 1919, Nr. 6, 1–29, 1920, Nr. 6, 1–24.
2. B. N. Delone and D. K. Faddeev, *Theory of irrationalities of third degree*, Acad. Sci. URSS. Trav. Inst. Math. Stekloff 11 (1940), 340 pp. (Russian.)
3. H. L. Dorwart, *Irreducibility of polynomials*, Amer. Math. Monthly 42 (1935), 369–381.
4. J. Hunter, *The minimum discriminants of quintic fields*, To appear in the Proc. Glasgow Math. Ass. 3 (1956).
5. T. Nagell, *Sur la réductibilité des trinomes*, Åttonde Skand. Mat.-Kongr. i Stockholm 14–18 Augusti 1934 (=C.R. du huitième congres des mathématiciens scandinaves tenu à Stockholm 14–18 août 1934), Lund, 1935, 273–275.

6. Ø. Ore, *Über die Reduzibilität von algebraischen Gleichungen*, Vid. selsk. Skrifter, Mat.-Nat. Kl., Kristiania, 1923, Nr. 1, 1–37.
7. O. Perron, *Grundlagen für eine Theorie des Jacobischen Kettenbruchalgorithmus*, Math. Ann. 64 (1907), 1–76.
8. O. Perron, *Neue Kriterien für die Irreduzibilität algebraischer Gleichungen*, J. reine angew. Math. 132 (1907), 288–307.
9. E. L. Petterson, *Über die Irreduzibilität ganzzahliger Polynome*, Diss., Uppsala, 1936.
10. G. Pólya und G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, Bd. II, Berlin, 1925.
11. J.-A. Serret, *Cours d'algèbre supérieure*, T. 2, 6. éd., Paris, 1910.
12. L. Weisner, *Criteria for the irreducibility of polynomials*, Bull. Amer. Math. Soc. 40 (1934), 864–870.

UNIVERSITY OF OSLO, NORWAY