Department
of
PURE MATHEMATICS

No. 23 (October, 1982) ISSN 0332-5047

On cubic factors of certain trinomials

By

Helge Tverberg

UNIVERSITY OF BERGEN
Bergen, Norway

No. 23 (October, 1982) ISSN 0332-5047

On cubic factors of certain trinomials

By

Helge Tverberg

On cubic factors of certain trinomials.

HELGE TVERBERG

1. Introduction.

Let $f \in Z[x]$ be a trinomial of the form $x^n + Ax^m + E$, where $3 < n > m > 0 \neq A$, and $E = \pm 1$. Assume that f has an irreducible cubic factor, $g = x^3 + ax^2 + bx + c \in Z[x]$. We shall say that f is special, and in this paper we determine all special trinomials. A. Bremner [1] did this for $E = 1$, stating that his methods can probably be used also for $E = -1$. We have used a different method, however, and thus obtain a (largely) independent verification of his results. He relies (mostly) on a p-adic method of Skolem, whereas we (mostly) make use of the properties of the zeros of f.

We refer to [1] for further background.

2. The theorem, and some particular cases of it.

The special trinomials can be normalized in a certain sense. For if g divides f then $-g(-x)$ divides $(-1)^n f(-x)$, $cx^3 g(1/x)$ divides $Ex^n f(1/x)$ and $-cx^3 g(-1/x)$ divides $(-x)^n Ef(-1/x)$. Consider the following list of special trinomials, chosen so that $n \geq 2m$ and $A > 0$: $f_1 = x^4 + 2x + 1$, $f_2 = x^5 + x + 1$, $f_3 = x^7 + 2x^2 - 1$, $f_4 = x^7 + 2x^3 + 1$, $f_5 = x^8 + 3x^3 - 1$, $f_6 = x^{12} + 1040x^4 - 1$, $f_7 = x^{13} + 3x^4 - 1$, $f_8 = x^{14} + 4x^5 - 1$, $f_9 = x^{33} + 67x^{11} + 1$, $f_{10,j} = x^6 + 4(j^4 - j)x^2 - 1$, $j = -1, \pm 2, \pm 3, \ldots$ Of these, only f_6 is not given in [1].

We can now state our

THEOREM. Every special trinomial is, or becomes after normalization, one of the trinomials f_1, ..., f_9, $f_{10,j}$.

It will be convenient to treat the cases with $n \leqq 6$ or $|A| \leqq 2$ separately. One finds easily that f_1, $f_2 = (x^3 - x^2 + 1)(x^2 + x + 1)$ and the $f_{10,j}$, with factors $x^3 \pm 2jx^2 + 2j^2x \pm 1$, are (up to normalization) all the special trinomials with $n \leqq 6$. Note that, by normalization, we can always assume $n \geqq 2m$ and we assume that, and also $n > 6$, from now on. (The other normalizing assumption $A > 0$, which we could make only because it so happens that no special trinomial has n and m even, $A < 0$ and $E = 1$ will never be used, however.)

If $|A| = 1$ we rely on Ljunggren's result (th. 3 in [3]) which implies that f factorizes into $x^{2d} + A^m E^n x^d + 1$ and an irreducible polynomial, with $d = (m,n)$. The first factor divides $x^{6d} - 1$, but no root of unity has degree 3, so g must equal the other factor, and hence $3 = n - 2d$, so that $d = 1$ or 3. But $d \neq 1$, as $n > 6$, and hence $n = 9$, $m = 3$, which violates Ljunggren's further condition, $n + m \equiv 0 \pmod{3d}$, for factorization.

If $|A| = 2$, we use Schinzel's result [4]. His th. 3 (corrected in [5]) describes explicitly those irreducible factors of a trinomial $x^n + Ax^m + E$ which have no roots of unity as zeros. They are polynomials in x^k, of degrees $3k$ or $4k$, and we obtain the normalized special trinomials

$$f_3 = x^7 + 2x^2 - 1 = (x^3 - x^2 + 1)(x^3 + x - 1)(x + 1),$$

$$f_4 = x^7 + 2x^3 + 1 = (x^3 - x^2 + 1)(x^4 + x^3 + x^2 + 1).$$

In what follows we add $|A| > 2$ to our assumptions.

3. Location of the zeros of g.

We prove that g has one zero inside the unit circle and hence two outside (as $|c| = 1$ and f has no zero on the circle when $|A| > 2$). To see this let first $g(w) = 0$, with $|w| < 1$. Then

$$|w^m + A^{-1}E| = |w|^n|A|^{-1} \leqq |w|^{2m}|A|^{-1} < |A|^{-1}$$

so that $|w|^m < 2|A|^{-1}$ and hence

$$|w|^m \leqq |A|^{-1} + |w|^n|A|^{-1} \leqq |A|^{-1} + 4|A|^{-3} .$$

If $|w| > 1$ instead, we get

$$|w|^m \leqq |w|^{n-m} = |A + Ew^{-m}| < |A| + 1 .$$

This shows that if g has two zeros inside the unit circle, then (with $B = |A|$)

$$1 = |c|^m \leqq (B^{-1} + 4B^{-3})^2(B + 1) = (1 + 4B^{-2})^2(B^{-1} + B^{-2}) .$$

But this is absurd, as $(1 + 4B^{-2})^2 \leqq 169/81$ and $B^{-1} + B^{-2} \leqq 4/9$ for $B \geqq 3$.

With g having one zero, denote it by t, inside the unit circle, there are either two more real zeros, u and v, or a conjugate pair $z, \bar{z}$, outside it. We'll now exclude the first possibility.

Firstly u and v must be of opposite signs. For if, say, $1 < u < v$, then the equation $u^{n-m} + Eu^{-m} = v^{n-m} + Ev^{-m}$ $(= -A)$ is inconsistent with the fact that $d/dx(x^{n-m} + Ex^{-m}) > (n - m) - m \geqq 0$, for $x > 1$. Now let $u > 1$ and $v < -1$. Then

$|u^{n-m} - v^{n-m}| = |v^{-m} - u^{-m}| < 2$. This implies that $n - m$ is even, that $|u - |v|| < 2(n - m)^{-1} < 1$ and that $|u^3 - |v|^3| < 3 \cdot 2 \cdot (n - m)^{-1} < 2$. Note also that the equation $u^{n-m} + Eu^{-m} = |v|^{n-m} + E(-1)^m|v|^{-m}$, which holds as $n - m$ is even, gives $u = |v|$ for m even, and $E(u - |v|) < 0$ for m odd.

Consider now $-a = t + u + v$. We find, as $0 < |t| < 1$, that $u + v \neq 0$. Thus m (and hence n , too,) is odd, and the inequality $E(u - |v|) < 0$ holds. Furthermore $E = c$, which is a consequence of the fact that f/g has only complex zeros, so that $E/c = f(0)/g(0) > 0$. If, namely, the evendegreed polynomial f/g has a real zero, it has at least two (distinct or coincident). Now $(g, f/g) = 1$, as g is irreducible and can not divide f' , which has at most two real zeros $\neq 0$. Thus two real zeros for f/g would mean at least five real zeros (out of which at most two are coincident) for f , and hence the impossible number of four distinct real zeros for f' .

We consider $-a$ again. As $c = E$ it can now be written as $u + v - E/uv = E(E(u - |v|) + u^{-1}|v|^{-1})$, which shows that $|a| < 1$, as $-1 < E(u - |v|) < 0$ and $0 < u^{-1}|v|^{-1} < 1$. Thus $a = 0$ and so $-(t^3 + u^3 + v^3) = b(t + u + v) + 3E = 3E$, which is inconsistent with $|t^3 + u^3 + v^3| = |t^3 + (u^3 - |v|^3)| < 1 + 2$.

It has thus been shown that the zeros of g are t, z and $\bar{z}$, where $-1 < t < 1$, and $|z| = R > 1$.

4. The case $n \neq 3m$.

The distinction indicated by this heading seems unmotivated right now, but its importance will soon become clear.

The equation $z^{n-m} + A = -Ez^{-m}$ shows that $|R^{n-m} - |A|| \leq R^{-m}$,

and we also have $||t|^{-m} - |A|| \leqq |t|^{n-m}$, as $A + Et^{-m} = -t^{n-m}$. Thus $|R^{n-m} - |t|^{-m}| \leqq R^{-m} + |t|^{n-m}$, which, as $|t| = R^{-2}$, gives

$$(*) \qquad |R^{n-3m} - 1| \leqq R^{-3m} + R^{-2n} .$$

For the discussion of (*) , it is useful to observe that $m \geqq 2$. For g and f/g have both at least one zero inside the unit circle, while f has m zeros inside it (as $|A| > 2$). Now for $m = 2$, $n \geqq 7$, the LHS of (*) is at least $R - 1$, while for $m \geqq 3$ it is only at least $1 - R^{-1}$. Using this (remember $n \geqq 2m$) one finds that (*) implies $R < 1.272$. Put $1.272 = R_0$.

The magnitude of a is at most $2R_0 + R_0^{-2} < 4$, and hence $|a| \leqq 3$. The integer $a - bc$, which equals $t^{-1} - t + (z^{-1} - \bar{z}) + (\bar{z}^{-1} - z)$ has magnitude at most $R_0^2 - R_0^{-2} + 2(R_0 - R_0^{-1}) < 1.972$, as, generally, $|w^{-1} - \bar{w}| = ||w| - |w|^{-1}|$. Thus $|ac - b| = |a - bc| = 0$, 1 or -1 . Furthermore, as g has no real zero outside (-1,1) , we have $g(1) \geqq 1$ and $g(-1) \leqq -1$, so that $-b \leqq a + c \leqq b$. Replacing g by $-g(-x)$ we can require $a \geqq 0$, too, and then we are left with the following candidates for g :

$$x^3 + x + c,\ x^3 + x^2 + (c + 1)x + c,\ x^3 + 2x^2 + 3x + 1,\ x^3 + 3x^2 + 4x + 1.$$

When $-1 < x < 0$, we have

$$x^3 + 3x^2 + 4x + 1 < x^3 + 2x^2 + 3x + 1 < x^3 + x^2 + 2x + 1 ,$$

and the latter polynomial takes a negative value for $x = -R_0^{-2}$. Thus any of these three candidates for g would have $0 > t > -R_0^{-2}$, i.e. $R > R_0$, and is hence excluded.

For $x^3 + x - 1$ we have $R > 1.21$, as $1.21^{-6} + 1.21^{-2} > 1$. Then (*) can hold only for $m = 2$, $n = 7$, and for $m = 3$, $n = 9 \pm 1$. As t^7 has a unique expression as an integral

combination of $1, t, t^2$, the only possibility for f is, in the first case, f_3. Expressing t^8 and t^{10} in terms of $1, t^2$ and t^3 we find also $f_5 = x^8 + 3x^3 - 1 = (x^3 + x - 1)(x^5 - x^3 + x^2 + x + 1)$. The candidate $x^3 + x + 1$ has been covered, too.

The final candidate for g is $x^3 + x^2 - 1$ with $R > 1.15$. Now (*) shows that $m \leqq 6$ and that $m = 2 \Rightarrow n \leqq 8$, $m = 3 \Rightarrow n \leqq 11$, $m = 4 \Rightarrow n \leqq 13$ and $m = 5 \Rightarrow n \leqq 16$. Expressing t^n in the basis $1, t, t^2(t^3, t^4)$ for $n \leqq 8(11, 13)$, and in the basis $1, t^2, t^5$ for $n \leqq 16$ we rediscover f_2, f_3 and f_4 and also get the new specimens f_7 and f_8.

4. The case $n = 3m$.

Let d be a divisor in m. Then $f_{1/d} = x^{3m/d} + Ax^{m/d} + E$ will also have an irreducible cubic factor. For $f_{1/d}(t^d) = 0$, while the polynomial $(x - t^d)(x - z^d)(x - \bar{z}^d)$ is in $Z[x]$ and is clearly irreducible, as $|t| < 1 < |z|$. This means that we can in the first instance concentrate on finding those f's for which m is a prime. We already know the case $m = 2$ and we'll see further below that the only other case is $m = 11$. Then $f = f_9 = x^{33} + 67x^{11} + 1$, $g = x^3 + x + 1$. This shows that the only possible values for m are powers of 2, or 11, as $m = 22$, say, would require $\pm A$ to be 67 <u>and</u> to have the form $4(j^4 - j)$. We start with the powers of 2.

If f is $x^{12} + Ax^4 + E$, then $f_{1/2} = x^6 + Ax^2 + E$ must be one of the $f_{10,j}$, i.e. $A = 4(j^4 - j)$. Furthermore $(x - t^2)(x - z^2)(x - \bar{z}^2)$, dividing $f_{1/2}$, must be

$x^3 - 2jx^2 + 2j^2x - 1$. Then $(x^2 - t^2)(x^2 - z^2)(x^2 - \bar{z}^2)$ $= -g(x)g(-x) = x^6 - 2jx^4 + 2j^2x^2 - 1$, which requires $2b - a^2 = -2j$, $b^2 - 2ac = 2j^2$, i.e. $b = a^2 \pm (a^4/2 - 2ac)^{1/2}$.

The expression for b shows that a is even, $a = 2k$, and that $2k^4 - kc$ must be a square. Now $(k, 2k^3 - c) = 1$, and so $k = \pm r^2$, $2k^3 - c = \pm s^2$, with $r, s \in Z^+$. Thus $2r^6 = s^2 + 1$ or $2r^6 = s^2 - 1$.

The equation $2r^6 = s^2 + 1$ has the solution $r = s = 1$ in Z^+ . This gives $a = \pm 2$, $b = 6$, $c = \pm 1$, $j = -4$, and $a = \pm 2$, $b = 2$, $c = \pm 1$, $j = 0$. But $f_{10,0}$ is not special. We get $f_6 = f_{10,-4}(x^2)$ $= (x^3 + 2x^2 + 6x + 1)(x^3 - 2x^2 + 6x - 1)(x^6 - 8x^2 + 32x + 1)$.

There are no further solutions, as the Diophantine equation $2r^3 = s^2 + 1$ has no solution with $r \neq 1$. For this equation gives $s + i = (1 + i)s_1$, $s - i = (1 - i)\bar{s}_1$, where the Gaussian integer s_1 is relatively prime to its conjugate $\bar{s}_1$ (note that $(s + i, s - i)$ divides $1 + i$) . Thus $s_1 = (p + iq)^3$, and so $\mathrm{Im}(s + i) = 1 = (p - q)(p^2 + 4pq + q^2)$, which implies $p = 1$, $q = 0$, $s = 1$ or $p = 0$, $q = 1$, $s = -1$.

The equation $2r^6 = s^2 - 1$ has the solution $r = 0$, $s = 1$ in Z^+ . This gives a non-special f . Euler [2] proved around 1782 (but for a false lemma) that $1 + 2r^3$ is not the square of a rational when r is a non-zero rational. As is well known, and easy to see by arithmetic in $Z[((-3)^{1/2} + 1)/2]$ his lemma becomes correct, and useful in the context, if the assumption $(x,y) = 1$ $\equiv x + y \pmod 2$ is added to it. This finishes the case $m = 4$.

Finally m cannot be 8 (or a higher power of 2) . For if $m = 8$ we find, as above, that $(x^3 + ax^2 + bx + c)(x^3 - ax^2 + bx - c)$

must equal $x^6 - 2x^4 + 6x^2 - 1$. This implies the impossibility $2b - a^2 = -2$, $b^2 - 2ac = 6$.

Now let m be an odd prime p . The polynomial $g_0 = (x - t^p)(x - z^p)(x - \bar{z}^p)$ has integral coefficients, and zeros in common with $f_{1/p} = x^3 + Ax + E$, which is irreducible. Thus $f_{1/p} = g_0$ and, in particular, $t^p + z^p + \bar{z}^p = 0$. This equation shows that $z + \bar{z} = -a - t$ is a unit, and so is $-a - z$ and $-a - \bar{z}$. Thus $(-a - t)(-a - z)(-a - \bar{z})$ $= (-a^3) + a(-a)^2 + b(-a) + c = -ab + c = \pm 1$. Replacing g by $-g(-x)$ we may assume that $c = 1$. Then $ab = 0$ or $ab = 2$. The latter case is excluded, as $t + z + \bar{z} \equiv t^p + z^p + \bar{z}^p \pmod{p}$, implies $-a \equiv 0 \pmod{p}$. Hence $ab = 0$.

If $b = 0$, $g(1) = a + 2$. But then $a > -2$, as otherwise g would have a zero in $[1,\infty)$, and similarly $g(-1) = a < 0$. Thus $a = -1$, which contradicts $a \equiv 0 \pmod{p}$. Hence $b \neq 0$ and $a = 0$.

Now $g = x^3 + bx + 1$. Put $s_k = t^k + z^k + \bar{z}^k$, $k = 0, 1, \ldots$, and note that $s_0 = 3, s_1 = 0, s_2 = -2b, s_3 = -3$, $s_4 = 2b^2$ and $s_5 = 5b$, while $s_p = 0$. This shows that $p > 5$, and then $E = 1$, as $s_{3p} \equiv s_3 \pmod{p}$ implies $-3E \equiv -3 \pmod{p}$.

We first eliminate the case $|b| > 1$. Inspired by Bremner (p. 146 of [1]), we put $-t^{3p} = (1 + bt)^p$ etc.. Then $-s_{3p} = s_0 + \binom{p}{1}bs_1 + \ldots + b^p s_p$ or, equivalently,

$$p^2(p - 1)/2 = 2\binom{p}{4}b^3 + 5\binom{p}{5}b^3 + \binom{p}{6}b^3 s_6 + \ldots + \binom{p}{k}b^{k-3}s_k + \ldots .$$

This equation shows that $(b,p) = 1$ and that b^3 divides $(p - 1)/2$. Let q be a prime dividing b . Then q clearly divides $2\binom{p}{4}b^3/((p - 1)/2)$, and $5\binom{p}{5}b^3/((p - 1)/2)$. If q does

not divide $\binom{p}{k}b^{k-3}s_k/((p-1)/2))$, for some $k \geq 6$, then q^{k-3} must divide $k(k-1)$, as $\binom{p}{k} = p(p-1)\binom{p-2}{k-2}/k(k-1)$. But then $2^{k-3} \leq q^{k-3} \leq k$, contradicting $k \geq 6$. Thus $q(p-1)/2$ divides only the RHS of our equation.

We are left with $g = x^3 + x + 1$ (as $x^3 - x + 1$ has a zero in $(-\infty, -1)$). Then, as observed by Bremner, g divides $x^{46} - 47(77x^2 + 13x - 27) - 1$. This means that, with $p = 46k + r$, $0 < r < 46$, we have

$$0 = s_p = (1 + 47(77t^2 + 13t - 27))^k t^r + \ldots = s_r + \sum_{i=1}^{k} 47^i \binom{k}{i} A_i$$

where the A_i are rational integers. Thus $s_r \equiv 0 \pmod{47}$, which (one calculates) happens only for $r = 11$, with $s_{11} = 0$. This gives the special trinomial f_9.

To see that $s_{46k+11} \neq 0$ for $k > 0$, observe that $A_1 = 77s_2 + 13s_1 - 27s_0 = -73$, and that $\binom{k}{i} = \binom{k-1}{i-1}k/i$ for $i > 1$. This shows that 47 divides $47^i\binom{k}{i}A_i$ to a higher power than it does $47k\,A_1$, as 47^{i-1} does not divide i for $i > 1$.

It remains to prove that m cannot be 121 (or a higher power of 11). Assume f to be, say, $x^{363} + 67x^{121} + 1$. Then $g_0 = (x - t^{11})(x - z^{11})(x - \bar{z}^{11})$ is a cubic factor in $x^{33} + 67x^{11} + 1$, and hence equals $x^3 + x + 1$. But g divides $g_0(x^{11}) = x^{33} + x^{11} + 1$, which is, however, not a special trinomial.

REMARK

The result of this section, in the case of odd m, can also be expressed as follows: The Fermat equation $x^m + Y^m + Z^m = 0$ has a solution (x,y,z), with x,y and z conjugate cubic units, only in the case $m = 11$. This closeness to the Fermat problem

also shows up in the fact that 11 divides the Fermat quotient $\frac{1}{11}(3^{10} - 1)$, which can be shown to be related to the solvability just mentioned. These quotients are important in the Fermat problem. Also if we modify our problem, asking for three linear factors $x - a$, $x - b$ and $x - c$, where $abc \neq 0$, and not requiring $|E|$ to be 1, we get the Fermat problem in the case $n = 3m$, with m odd.

REFERENCES

1. A. Bremner, On trinomials of type $x^n + Ax^m + 1$, Math. Scand. 49 (1981), 145-155.
2. L. Euler, Opera postuma, 1, 243-244, St. Petersburg 1862.
3. W. Ljunggren, On the irreducibility of certain trinomials and quadrinomials, Math. Scand. 8 (1960), 65-70.
4. A. Schinzel, Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationels, Colloq. Math. 9 (1962), 291-296.
5. A Schinzel, private communication.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BERGEN
5000 BERGEN
NORWAY