PANORAMAS OF MATHEMATICS
BANACH CENTER PUBLICATIONS, VOLUME 34
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 1995

SOLVED AND UNSOLVED PROBLEMS ON POLYNOMIALS

ANDRZEJ SCHINZEL

Institute of Mathematics, Polish Academy of Sciences
Śniadeckich 8, 00-950 Warszawa, Poland
E-mail: schinzel@impan.gov.pl

We shall tell about problems concerning polynomials in one variable over an arbitrary field K considered during the last hundred years.

In 1895 Vahlen proved for the rational field $\mathbb{Q}$ the following theorem, which in 1897 was extended by Capelli [1] to all fields of characteristic 0.

CAPELLI'S THEOREM. *A binomial $x^n - a$ is reducible over a field K if and only if either $a = b^p$, p prime, $p \mid n$, $b \in K$ or $a = -4b^4$, $4 \mid n$, $b \in K$.*

(The theorem also is true for fields of positive characteristic as shown by Rédei [11]).

COROLLARY. *Every binomial over $\mathbb{Q}$ has at least one irreducible factor with at most three non-zero coefficients.*

R e m a r k. The equality $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$ shows that the number three in the corollary is best possible.

In 1922 Ritt [13] introduced the following

DEFINITION. Let $f \in \mathbb{C}[x]$. The polynomial f is called *prime*, if its degree $\partial f > 1$ and

$$f = g(h) \Rightarrow \partial g = 1 \quad \text{or} \quad \partial h = 1.$$

Of course, every polynomial is a composition ($\circ$) of prime polynomials. Is the decomposition unique? The question should be made precise. First of all, for

---

1991 *Mathematics Subject Classification*: 12.
Lecture given at the Banach Center Colloquium on 25th February 1993.
The paper is in final form and no version of it will be published elsewhere.

a linear polynomial l we have

$$g \circ h = (g \circ l) \circ (l^{-1} \circ h).$$

Next, the composition of polynomials in not, in general, commutative. On the other hand, we have the following example

$$\begin{aligned} g_1 &= x^v p(x)^n, & h_1 &= x^n, \\ g_2 &= x^n, & h_2 &= x^v p(x^n). \end{aligned} \tag{1}$$

For the above polynomials we have $g_1 \circ h_1 = g_2 \circ h_2$ and we can choose a polynomial p so that the polynomials g_1, h_1, g_2, h_2 are prime, thus there is no uniqueness of decomposition.

The two theorems given below were proved by Ritt for polynomials over $\mathbb{C}$.

First Ritt's Theorem. *If polynomials f_i an g_j for $1 \le i \le r$, $1 \le j \le s$ are prime and*

$$f = f_1 \circ f_2 \circ \ldots \circ f_r = g_1 \circ g_2 \ldots \circ g_s,$$

then $r = s$ and the vector $[\partial f_1, \ldots, \partial f_r]$ is a permutation of $[\partial g_1, \ldots, \partial g_s]$.

Ritt's proof was analytic, using Riemann surfaces. In 1969 Fried and MacRae [7] gave an algebraic proof valid for an arbitrary field K under the assumption that $\partial f \not\equiv 0 \bmod \operatorname{char} K$, reducing the theorem to the Jordan–Hölder theorem about finite groups. In 1974 Dorey and Whaples [4] showed that without the above assumption the theorem is not true in general. Much deeper is second Ritt's theorem.

Second Ritt's Theorem. *If $g_1 \circ h_1 = g_2 \circ h_2$, $\partial g_1 = \partial h_2 = m > \partial h_1 = \partial g_2 = n$, $(m, n) = 1$ then up to transformations by linear functions we either have* (1) *or $g_1 = D_m = h_2$, $g_2 = D_n = h_1$, where the polynomials D_k are given by the formula*

$$D_k(x + x^{-1}) = x^k + x^{-k}.$$

The author in his lectures on polynomials [15] presented a proof of this theorem for polynomials over an algebraically closed field K satisfying the condition

$$\operatorname{char} K = 0 \qquad \text{or} \qquad \operatorname{char} K > \max\{m, n\} \tag{2}$$

and indicated the changes necessary if K is not algebraically closed. Recently Zannier [21] has proved the above theorem for algebraically closed K without condition (2). He has assumed only that $g_1' g_2' h_1' h_2' \not\equiv 0$.

In 1933 D. H. Lehmer [9] asked (in an equivalent formulation) the following question. Let $f \in \mathbb{Z}[x]$ be monic and assume that $f(0) \ne 0$ and f is not a product of cyclotomic polynomials. Does there exist a constant $C > 1$ (independent of f) such that

$$M(f) = \prod_{f(\xi)=0} \max\{1, |\xi|\} \ge C$$

(multiple zeros counted multiply)?

Lehmer indicated a possible value of C, as the unique real greater than 1 root of the equation

$$f_0(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 = 0,$$

approximately equal to 1.17. One sees that f_0 is a reciprocal polynomial, i.e.

$$f_0(x^{-1}) = \pm x^{-\partial f_0} f_0(x).$$

This is not an accident, since Smyth proved in [19] that if f is not reciprocal then $M(f) \geq \vartheta_0$, where $\vartheta \approx 1.32$ is a unique real root of $x^3 - x - 1 = 0$.

For reciprocal polynomials an essential progress was achieved by E. Dobrowolski, who proved in [3] that for all $\varepsilon > 0$ and $\partial f \geq n_0(\varepsilon)$

$$M(f) \geq 1 + (c - \varepsilon)\left(\frac{\log\log \partial f}{\log \partial f}\right)^3,$$

where $c = 1$.

The value of c has been improved. The present record belongs to R. Louboutin [10] and is $c = 9/4$.

Lehmer's problem is related to the following problem proposed in [18] by Zassenhaus and the author. Is it true under the same conditions on f as before that

$$\max_{f(\xi)=0} |\xi| > 1 + \frac{C}{\partial f},$$

where $C > 0$ is an absolute constant?

Combining the theorems of Smyth and Louboutin we infer that

$$\max_{f(\xi)=0} |\xi| > 1 + \left(\frac{9}{2} - \varepsilon\right)\frac{1}{\partial f}\left(\frac{\log\log \partial f}{\log \partial f}\right)^3.$$

Recently, A. Dubickas [5] has proved that

$$\max_{f(\xi)=0} |\xi| > 1 + \left(\frac{64}{\pi^2} - \varepsilon\right)\frac{1}{\partial f}\left(\frac{\log\log \partial f}{\log \partial f}\right)^3.$$

Let us return now to the chronological order of problems. In 1947 Rényi [12] found an example of a polynomial $f \in \mathbb{Q}[x]$ complete, i.e. with all coefficients different from zero, of degree 28 and such that f^2 has only 28 non-zero coefficients.

Denoting the number of non-zero coefficients of a polynomial g by $N(g)$ we may conclude from Rényi's example that there exist $f \in \mathbb{Q}[x]$ such that $N(f^2) < N(f)$.

In 1949 Erdős [6] proved that there exists an infinite sequence of polynomials $f_n \in \mathbb{Q}[x]$ such that $N(f_n) \to \infty$ and $N(f_n^2) < N(f_n)^c$, where $c < 1$. The same year Verdenius [20] showed that one can take $c = \log 8/\log 13 \approx 0.81\ldots$

In 1991 D. Coppersmith and J. Davenport [2] proved that for every $l > 1$ and a suitable sequence of polynomials $f_n \in \mathbb{Q}[x]$ with $N(f_n) \to \infty$ we have

$$N(f_n^l) \ll N(f_n)^{c_l},$$

where $c_l < 1$ is effectively computable (unfortunately $c_2 > \log 8/\log 13$). Moreover they proved that for every $F \in \mathbb{C}[x]$, $\partial F > 1$ there exists an infinite sequence of polynomials $f_n \in \mathbb{C}[x]$ such that $N(f_n) \to \infty$ and

$$N(F(f_n)) \ll N(f_n)^{c_F},$$

where $c_F < 1$.

There remains the question whether for every sequence f_n one can give a similar bound from below. In 1987 the author [16] gave the estimate

$$N(f^l) \geq l + 1 + (\log 2)^{-1} \log\left(1 + \frac{\log(N(f)-1)}{l \log 4l - \log l}\right)$$

for $l > 1$, $f \in \mathbb{C}[x]$, $N(f) \geq 2$. There is a great distance between the above upper and lower bounds for $N(f^l)$ already for $l = 2$. Erdős thinks that his estimate is closer to the truth.

Perhaps for every non-constant F the inequality holds

$$N(F(f)) \geq \varphi_F(N(f)),$$

for some function φ_F satisfying the condition $\lim_{x\to\infty} \varphi_F(x) = \infty$.

Such function is unknown even for quite simple polynomials F, e.g. $F(x) = x^3 - x$.

We have begun the lecture from binomials, we shall finish with trinomials. Let us consider a field K and a trinomial of the form

$$x^n + Ax^m + B, \qquad \text{where } A, B \in K^* \text{ and } n > m > 0.$$

We observe that the trinomial is reducible over K if and only if the trinomial $Bx^n + Ax^{n-m} + 1$, or what comes to the same $x^n + AB^{-1}x^{n-m} + B^{-1}$ is reducible over K.

Since either $n \geq 2m$, of $n \geq 2(n-m)$ we may assume without loss of generality that $n \geq 2m$. Let us fix the following notation

$$\operatorname{char} K := \pi \geq 0, \qquad n_1 := n/(n,m), \qquad m_1 := n/(n,m)$$

and let $\mathbf{y}$ denote a vector of independent variables. Assume that $\pi \nmid mn(n-m)$.

We shall state two theorems about reducibility of trinomials.

THEOREM 1. *Let $n \geq 2m > 0$; $A, B \in K(\mathbf{y})^*$, where $A^{-1}B^{n-m} \notin K$. The trinomial $x^n + Ax^m + B$ is reducible over $K(\mathbf{y})$ if and only if either*

(i) *$x^n + Ax^m + B$ has over $K(\mathbf{y})$ a proper factor of degree ≤ 2*

or

(ii) *there exists an integer l such that $\langle \frac{n}{l}, \frac{m}{l} \rangle := \langle \nu, \mu \rangle \in S_0$, where*

$$S_0 := \prod_p \{\langle 2p, p\rangle\} \cup \{\langle 6,1\rangle, \langle 6,2\rangle, \langle 7,1\rangle, \langle 8,2\rangle, \langle 8,4\rangle, \langle 9,3\rangle, \langle 10,2\rangle, \langle 10,4\rangle, \langle 12,2\rangle, \langle 12,3\rangle, \langle 12,4\rangle, \langle 15,5\rangle\}$$

and

$$A = u^{\nu-\mu} A_{\nu,\mu}(v), \qquad B = u^{\nu} B_{\nu\mu}(v),$$

where $u, v \in K(\mathbf{y})$, p runs over all primes and $A_{\nu,\mu}$, $B_{\nu,\mu}$ are given in Table 1 (below).

Table 1

ν, μ	$A_{\nu,\mu}$	$B_{\nu,\mu}$
$2p$, p	$-\left(\frac{1+\sqrt{1-4v}}{2}\right)^p - \left(\frac{1-\sqrt{1-4v}}{2}\right)^p$	v^p
6, 1	$8v(v^2+1)$	$(v^2+4v-1)(v^2-4v-1)$
6, 2	$4(v+1)$	$-v^2$
7, 1	$-(2v+1)^4(4v^2-3v+1) \times (v^3-2v^2-v+1)$	$v(2v-1)(2v+1)^5(3v-2)(v^2-v-1)$
8, 2	$-v^2+8v-8$	$(2v-2)^2$
8, 4	$2v^2-8v+4$	v^4
9, 3	$v^3-81v+243$	$27(v-3)^3$
10, 2	$4v^3-8v+4$	$-(v^2-4v+2)^2$
10, 4	$v^5(-v^3+8v-8)$	$-4v^8(v-1)^4$
12, 2	$1024(v-4)^8(2v-3)(v^2-6v+6) \times (v^2-2v+2)$	$1024(v-4)^{10}(v^3-8v+8)^2$
12, 3	$-729v(v-1)^7(2v-1)(3v^2-6v+2) \times (3v^2-3v+1)$	$729(v-1)^9(3v^3-3v+1)^3$
12, 4	$512(2v-1)(2v^2+2v-1)(2v^2-2v+1)$	$1024(2v^2-4v+1)^4$
15, 5	$5(5v-5)^7(5v^4-5v^3-5v^2+5v-1) \times (5v^4-10v^3+100v^2-5v+1)$	$(5v-5)^{10}(5v^2-5v+1)^5$

There is an analogy between this theorem and Capelli's theorem. There was one exceptional case there, here there are twelve. However Capelli's theorem is true over an arbitrary field, the above theorem only over an arbitrary field of rational functions.

THEOREM 2. *Let $n \geq 2m > 0$, $[K : \mathbb{Q}] < \infty$; $A, B \in K^*$. The trinomial $x^n + Ax^m + B$ is reducible over K if and only if either one of the conditions* (i), (ii) *holds with K in place of $K(\mathbf{y})$ or*

(iii) *there exists an integer l such that $\langle \frac{n}{l}, \frac{m}{l} \rangle := \langle \nu, \mu \rangle \in S_1$, where*

$$S_1 = \{\langle 7,2\rangle, \langle 7,3\rangle, \langle 8,1\rangle, \langle 9,1\rangle, \langle 14,2\rangle, \langle 21,7\rangle\}$$

and $A = u^{\nu-\mu} A_{\nu,\mu}(v,w)$, $B = u^{\nu} B_{\nu,\mu}(v,w)$, where $u \in K$, $\langle v, w\rangle \in E_{\nu,\mu}(K)$, while the polynomials $A_{\nu,\mu}$, $B_{\nu,\mu}$ and the elliptic curve $E_{\nu,\mu}$ are given in Table 2 (below) or

(iv) *there exists an integer l such that $\langle \frac{n}{l}, \frac{m}{l} \rangle := \langle \nu, \mu \rangle \in \mathbb{Z}^2$ and $A = u^{\nu-\mu} A_0$, $B = u^{\nu} B_0$, $u \in K$, $\langle A_0, B_0\rangle \in F_{\nu,\mu}(K)$ and $F_{\nu,\mu}(K)$ is a certain finite (possibly empty) set.*

Table 2

ν, μ	$E_{\nu,\mu}$	$A_{\nu,\mu}$	$B_{\nu,\mu}$
7, 2	$w^2 = v^3 + 16v^2 + 64v + 80$	$2v^2 - 8v - 48 + w(2v-4)$	$-(4v+12+w) \times (v^2+12v+32+4w)$
7, 3	$w^2 = v^3 - 675v + 13662$	$(-v^3+27v^2+3753v - 34803 + w(6v-666)) \times (v-39)$	$6(v-39)^2(-v^2-12v + 693 + 6w)(9v^2+162v - 4455 - w(v+33))$
8, 1	$w^2 = v^3 - 10v + 12$	$-8v^3+20v^2+8v-32 + w(3v^2-12v-10)$	$(w-3v+5)(-3v^2+15v - 17 + w(2v-5))$
	$w^2 = v^3 - 20v - 16$	$128(w-2v-8)^4 \times (v+2)(v^2+12v+4) \times (2w-v^2+4v+4) \times (4w-v^2-12)$	$64(w-2v-8)^4(9v^4+8v^3 - 8v^2+288v+272 - w(v^3+18v^2+76v+24)) \times (v^4+24v^3+152v^2 + 96v+16+w(v^3-22v^2 - 52v-72))$
9, 1	$w^2 = v^3 + 18v - 36$	$81(w-2v-9)^4((v^7+27v^6 + 351v^5+639v^4-675v^3 - 5589v^2+6318v - 7290)w + (-9v^8-66v^7 - 936v^6+1890v^5+4995v^4 - 5670v^3+14580v^2 - 72900v+37179))$	$27(w-2v-9)^5((5v^7-603v^6 - 765v^5+5661v^4+3213v^3 + 29889v^2-28674v + 10206)w + (-v^9+63v^8 + 1719v^7-4959v^6 - 10611v^5+1917v^4 + 111456v^3-145800v^2 + 207036v-61236))$

Table 2 continued

ν, μ	$E_{\nu,\mu}$	$A_{\nu,\mu}$	$B_{\nu,\mu}$
14, 2	$w^2 = v^3 - 6v + 5$	$4(v-2)^7(4v^4 - v^3 - 34v^2 + 51v - 18 + w(v^3 + 6v^2 - 18v + 8))$	$-(v-2)^8(v^3 - 12v + 14 + w(2v-6))^2$

$\nu = 21, \mu = 7$

$E_{\nu,\mu}: \quad w^2 = v^3 - 1715v + 33614$

$$\begin{aligned} A_{\nu,\mu} = {} & 3764768(w - 7v - 343)^7 \times (-70v^{13} - 52822v^{12} + 19467098v^{11} + 3451790790v^{10} \\ & - 68568103744v^9 - 7533659832748v^8 + 155066962439572v^7 + 6992189738638860v^6 \\ & + 111845300294417242v^5 - 2615541950886590670v^4 - 18520719744403646 9646v^3 \\ & - 21674061456637587473 14v^2 - 17859482834686233287988v \\ & - 18838244084537504480336)w + (v^{15} + 2625v^4 + 91584v^{13} - 411648706v^{12} \\ & - 8059651761v^{11} + 1191725696763v^{10} + 27401291878562v^9 - 2107086579531888v^8 \\ & - 82212564592345537v^7 + 2560864878174600039v^6 + 6443661255627895322 8v^5 \\ & - 65304473170056903528 2v^4 - 20619925798094466268271v^3 \\ & - 39964825892126689494688 3v^2 - 17492015250159665074110 86v \\ & - 96422978975763738021865 12). \end{aligned}$$

$B_{\nu,\mu} = 14^7(w - 7v - 343)^{14}(21v^2 - 686v - 7203 - (v + 49)w)^7$

As to Table 2 the curve $E_{7,2}$ is not in Weierstrass normal form, since to have it reduced would require $\operatorname{char} K \neq 3$. In the case $\langle \nu, \mu \rangle = \langle 8, 1 \rangle$ we have a double choice. The polynomial $A_{21,7}$ has been computed by Prof. J. Browkin using the programme GP-PARI, some other polynomials by Dr. A. Pokrzywa, using the programme Mathematica.

Table 3. Sporadic trinomials over $\mathbb{Q}$

The table contains all reducible trinomials $x^n + Ax^m + B$, $n \geq 2m$, $A, B \in \mathbb{Z} \setminus \{0\}$ known to the author, which satisfy neither (vi) nor (vii) nor (viii) and have the following properties: 1) for every greater than 1 divisor d of (n, m) $x^{n/d} + Ax^{m/d} + B$ is irreducible, 2) (A^n, B^{n-m}) is free from $n(n-m)$th powers, 3) if $n - m$ is odd then $A > 0$, if n, m both odd, then $B > 0$.

Number	*Trinomial*	*Factor*	*Discoverer*
1	$x^8 + 3x^3 - 1$	$x^3 + x - 1$	Łutczyk
2	$x^8 + 2^3 \cdot 3x^3 + 2^5$	$x^3 - 2x^2 + 4$	Nicolas
3	$x^8 + 2^2 \cdot 3^3x^3 + 3^5$	$x^3 + 3x^2 + 9x + 9$	Nicolas
4	$x^8 + 3 \cdot 5 \cdot 7^3 \cdot 59x^3 - 2^3 \cdot 7^5 \cdot 11^3$	$x^3 - 7x^2 - 98x + 2156$	Author
5	$x^9 - 2^2 \cdot 19x + 2^5 \cdot 3$	$x^4 - 2x^2 - 4x + 6$	Author
6	$x^9 + 2^5x^2 - 2^6$	$x^3 - 2x^2 + 4x - 4$	Nicolas

Table 3 continued

Number	*Trinomial*	*Factor*	*Discoverer*
7	$x^9 + 3^4x^2 - 2 \cdot 3^3$	$x^3 + 3x + 3$	Nicolas
8	$x^9 + 3^6x^2 - 2 \cdot 3^6$	$x^3 - 3x^2 + 9$	Browkin
9	$x^9 + 3^5x^4 + 2^2 \cdot 3^6$	$x^3 - 3x^2 + 18$	Browkin
10	$x^9 + 2^4 \cdot 3^5x^4 - 2^8 \cdot 3^6$	$x^3 + 6x^2 + 36x + 72$	Nicolas
11	$x^{10} + 3^3 \cdot 11x - 3^5$	$x^3 + 3x - 3$	Author
12	$x^{10} + 2^6 \cdot 3^3 \cdot 5^6 \cdot 11x - 2^7 \cdot 3^5 \cdot 5^5 \cdot 19$	$x^4 - 60x^2 - 300x + 5400$	Browkin
13	$x^{10} + 3x^3 - 2^3$	$x^4 + x^3 - x - 2$	Morain
14	$x^{10} + 2^5x^3 - 2^6$	$x^5 - 2x^4 + 8x - 8$	Morain
15	$x^{10} + 3^2 \cdot 11x^3 + 2 \cdot 3^3$	$x^3 + 3x + 3$	Nicolas
16	$x^{11} + 2^2 \cdot 3x + 2^3$	$x^5 - 2x^4 + 2x^3 - 2x^2 + 2$	Nicolas
17	$x^{11} + 2^3 \cdot 3^3 \cdot 23x^2 - 2^4 \cdot 3^5$	$x^3 + 6x - 6$	Browkin
18	$x^{11} + 2^2 \cdot 23x^3 + 2^3 \cdot 3$	$x^3 + 2x^2 + 4x + 2$	Morain
19	$x^{11} + x^4 + 2^2$	$x^5 - x^3 - x^2 + 2$	Jonassen
20	$x^{11} - 3^3 \cdot 5^2 \cdot 23x^5 + 3^8 \cdot 5^4$	$x^3 - 15x - 45$	Browkin
21	$x^{12} + 2^6 \cdot 3^2x + 2^4 \cdot 23$	$x^3 + 2x^2 + 4x + 2$	Browkin–Author
22	$x^{12} + 2^5 \cdot 3^4 \cdot 13x + 2^4 \cdot 3^4 \cdot 23$	$x^3 + 6x + 6$	Browkin
23	$x^{12} + 2^6x^5 - 2^8$	$x^3 - 2x^2 + 4x - 4$	Morain
24	$x^{13} + 2^8 \cdot 3x + 2^{10}$	$x^3 + 2x^2 + 4x + 4$	Browkin
25	$x^{13} + 2^8 \cdot 3 \cdot 53x - 2^{12} \cdot 7$	$x^3 - 4x^2 + 8x - 4$	Browkin–Author
26	$x^{13} + 2^8 \cdot 3 \cdot 5^6 \cdot 53x + 2^{11} \cdot 5^7 \cdot 13$	$x^3 + 20x + 100$	Browkin
27	$x^{13} - 2^6 \cdot 3 \cdot 5^5 \cdot 53x^3 + 2^8 \cdot 5^8 \cdot 11$	$x^3 + 20x - 100$	Browkin
28	$x^{13} + 3x^4 - 1$	$x^3 + x^2 - 1$	Coray

Table 3 continued

Number	*Trinomial*	*Factor*	*Discoverer*
29	$x^{13} + 2^6 \cdot 3x^4 - 2^9$	$x^3 + 2x^2 + 4x + 4$	Browkin
30	$x^{13} + 3^3 \cdot 53x^4 - 2^2 \cdot 3^6$	$x^3 - 3x^2 + 6$	Browkin
31	$x^{13} + 3x^6 + 1$	$x^4 - x + 1$	Coray
32	$x^{13} + 2^4 \cdot 3x^6 - 2^8$	$x^3 - 2x^2 + 4x - 4$	Browkin
33	$x^{14} + 2^2x + 3$	$x^3 - x^2 + 1$	Bremner
34	$x^{14} + 2^2x^5 - 1$	$x^3 + x^2 - 1$	Bremner
35	$x^{14} + 2^2 \cdot 3^6x^5 + 3^{11}$	$x^4 - 3x^3 + 9x^2 - 18x + 27$	Morain
36	$x^{15} - 3^7 \cdot 5^6 \cdot 31x + 2^2 \cdot 3^8 \cdot 5^5 \cdot 29$	$x^3 + 15x - 45$	Browkin
37	$x^{15} - 2^4 \cdot 7^3 \cdot 31x^7 + 2^{11} \cdot 3 \cdot 7^5$	$x^3 - 14x - 28$	Browkin
38	$x^{16} + 7x^3 + 3$	$x^3 - x^2 + 1$	Bremner
39	$x^{16} + 2^3 \cdot 7x^3 - 3^2$	$x^3 + x^2 + x - 1$	Bremner
40	$x^{16} + 2^8x^7 + 2^{12}$	$x^4 - 2x^3 + 4x^2 - 8x + 8$	Morain
41	$x^{16} + 2^8 \cdot 7x^7 - 2^{15}$	$x^3 + 2x^2 - 8$	Bremner
42	$x^{17} + 103x + 2^3 \cdot 7$	$x^3 - x^2 + x + 1$	Bremner
43	$x^{17} + 2^{12} \cdot 103x^4 - 2^{16} \cdot 3^2$	$x^3 + 2x^2 + 4x - 8$	Browkin
44	$x^{21} + 2^{11} \cdot 13x^5 + 2^{14} \cdot 3$	$x^3 - 2x^2 + 4$	Browkin
45	$x^{22} + 2^{14} \cdot 23x - 2^{15} \cdot 13$	$x^3 + 2x^2 - 4$	Browkin
46	$x^{24} + 2^{11} \cdot 7x + 2^8 \cdot 47$	$x^3 - 2x^2 + 2$	Browkin–Author
47	$x^{26} + 2^7 \cdot 3 \cdot 53x^3 + 2^8 \cdot 47$	$x^3 - 2x^2 + 2$	Browkin–Author
48	$x^{33} + 67x^{11} + 1$	$x^3 + x + 1$	Bremner
49	$x^{39} + 2^9 \cdot 3 \cdot 157x^{13} + 2^{13}$	$x^3 + 2x + 2$	Browkin
50	$x^{46} + 2^{26} \cdot 47x^7 - 2^{31} \cdot 3^2$	$x^3 - 2x^2 + 4x - 4$	Browkin
51	$x^{51} - 2^{31} \cdot 103x^5 + 2^{34} \cdot 47$	$x^3 - 2x^2 + 4x - 4$	Browkin
52	$x^{52} + 2^{34} \cdot 3 \cdot 53x + 2^{35} \cdot 103$	$x^3 + 2x^2 + 4x + 4$	Browkin

Table 3 shows 52 reducible trinomials over $\mathbb{Q}$ that do not satisfy (i)–(iii). We propose

CONJECTURE. *For every algebraic number field K sets $F_{\nu,\mu}(K)$ can be chosen so that the set*

$$\bigcup_{\langle\nu,\mu\rangle} \bigcup_{\langle A_0,B_0\rangle\in F_{\nu,\mu}(K)} \{x^\nu + A_0x^\mu + B_0\}$$

is finite.

For $K = \mathbb{Q}$ the conjecture implies that Table 3 cannot be indefinitely extended. To disprove the conjecture over $\mathbb{Q}$ seems very hard. In particular, author's results from [14] show that for every pair $\langle a, b\rangle \in \mathbb{Q}^2$ there exist only finitely many trinomials x^n+ax^m+b reducible, but not satisfying (i), while the recent results of Győry and the author [8] show that for every fixed polynomial f there exist only finitely many trinomials over $\mathbb{Q}$ divisible by f, but satisfying neither (i) nor (ii).

Finally, we shall note two simple consequences of the conjecture.

CONSEQUENCE 1. *For every algebraic number field K there exists a constant $C_1(K)$ such that, if $n > 2m$, $A, B \in K^*$ and the trinomial $x^n + Ax^m + B$ is reducible over K then either $x^{n_1} + Ax^{m_1} + B$ has a proper factor of degree ≤ 2 or $n_1 \le C_1(K)$.*

Remark. For $K = \mathbb{Q}$ we have $C_1(\mathbb{Q}) \ge 52$.

CONSEQUENCE 2. *For every algebraic number field K there exists a constant $C_2(K)$ such that every trinomial over K has at least one irreducible factor with at most $C_2(K)$ non-zero coefficients.*

Remark. For $K = \mathbb{Q}$ we have $C_2(\mathbb{Q}) \ge 8$.

References

[1] A. Capelli, *Sulla riduttibilita delle equazioni algebriche, Nota prima*, Rend. Accad. Fis. Mat. Soc. Napoli (3), 3 (1897), 243–252.

[2] D. Coppersmith and J. Davenport, *Polynomials whose powers are sparse*, Acta Arith. 58 (1991), 79–87.

[3] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.

[4] F. Dorey and G. Whaples, *Prime and composite polynomials*, J. Algebra 28 (1974), 88–101.

[5] A. Dubickas, *On a conjecture of A. Schinzel and H. Zassenhaus*, Acta Arith. 63 (1993), 15–20.

[6] P. Erdős, *On the number of terms of the square of a polynomial*, Nieuw. Arch. Wiskunde (2) 23 (1949), 63–65.

[7] M. Fried and R. E. MacRae, *On the invariance of the chain of fields*, Illinois J. Math. 13 (1969), 165–171.

[8] K. Győry and A. Schinzel, *On a conjecture of Posner and Rumsey*, J. Number Theory 47 (1994), 63–78.

[9] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. 34 (1933), 461–479.
[10] R. Louboutin, *Sur la mesure de Mahler d'un nombre algébrique*, C. R. Acad. Sci. Paris, Sér. I 296 (1983), 539–542.
[11] L. Rédei, *Algebra, Erster Teil*, Akademische Verlaggesellschaft, Leipzig, 1959.
[12] A. Rényi, *On the minimal number of terms in the square of a polynomial*, Hungar. Acta Math. 1 (1947), 30–34 = Selected papers, vol. 1, Budapest 1976, 42–47.
[13] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc., 23 (1922), 51–66.
[14] A. Schinzel, *Reducibility of lacunary polynomials I*, Acta Arith. 16 (1969), 123–159.
[15] A. Schinzel, *Selected topics on polynomials*, The University of Michigan Press, Ann Arbor, 1982.
[16] A. Schinzel, *On the number of terms of a power of a polynomial*, Acta Arith. 49 (1987), 55–70.
[17] A. Schinzel, *On reducible trinomials*, Dissertationes Math. 329 (1993).
[18] A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Michigan Math. J. 12 (1965), 81–85.
[19] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), 169–175.
[20] W. Verdenius, *On the number of terms of the square and the cube of polynomials*, Indag. Math. 11 (1949), 459–465.
[21] U. Zannier, *Ritt's second theorem for arbitrary characteristic*, J. Reine Angew. Math. 445 (1993), 175–203.