Some Polynomial Factoring Problems From Past West Coast Number Theory Conferences

by Michael Filaseta

University of South Carolina

Joint Work with

A. Borisov, T.-Y. Lam, O. Trifonov

Classes of polynomials having one non-cyclotomic irreducible factor, Acta Arith. **90** (1999), 121–153.

Conjecture (F., 1986):

Let n be an integer ≥ 2, and let

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

Then $f'(x)$ is irreducible over the rationals.

Examples:

$$\begin{aligned} n = 2: &\quad f'(x) = 2x + 1 \\ n = 3: &\quad f'(x) = 3x^2 + 2x + 1 \\ n = 4: &\quad f'(x) = 4x^3 + 3x^2 + 2x + 1 \\ \vdots &\qquad\qquad \vdots \end{aligned}$$

1986: true if $n = p - 1 \geq 2$ or if $n = p^r$

Conjecture (T.-Y. Lam):

Let n and k be integers with $n \geq 2$ and $1 \leq k \leq n-1$, and let

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

Then $f^{(k)}(x)$ is irreducible over $\mathbb{Q}$.

Examples:

$$\frac{f^{(n-1)}(x)}{(n-1)!} = nx + 1 = \binom{n}{1}x + \binom{n-1}{0}$$

$$\frac{f^{(n-2)}(x)}{(n-2)!} = \binom{n}{2}x^2 + \binom{n-1}{1}x + \binom{n-2}{0}$$

$$\frac{f^{(n-3)}(x)}{(n-3)!} = \binom{n}{3}x^3 + \binom{n-1}{2}x^2 + \binom{n-2}{1}x + \binom{n-3}{0}$$

Conjecture (J. Lagarias & E. Gutkin, 1991):

Let n be an integer ≥ 4, and let

$$p(x) = (n-1)(x^{n+1}-1) - (n+1)(x^n - x).$$

Then

- *$p(x)$ is $(x-1)^3$ times an irreducible polynomial if n is even*
- *$p(x)$ is $(x-1)^3(x+1)$ times an irreducible polynomial over $\mathbb{Q}$ if n is odd.*

Comment: In connection to a problem concerning billiards, Eugene Gutkin was interested in showing that the polynomials $p(x)$ have no roots in common other than from the indicated cyclotomic factors.

Theorem 1. *Let* $\varepsilon > 0$. *For all but* $O(t^{1/3+\varepsilon})$ *positive integers* $n \le t$, *the derivative of the polynomial* $1 + x + x^2 + \cdots + x^n$ *is irreducible.*

Theorem 2. *Fix a positive integer* k. *For all but* $o(t)$ *positive integers* $n \le t$, *the* k*th derivative of* $1 + x + x^2 + \cdots + x^n$ *is irreducible.*

Theorem 3. *Fix a positive integer* m. *If* n *is sufficiently large and* $f(x) = 1 + x + x^2 + \cdots + x^n$, *then the polynomial* $f^{(n-m)}(x)$ *is irreducible.*

Theorem 4. *Let* $\varepsilon > 0$. *For all but* $O(t^{4/5+\varepsilon})$ *positive integers* $n \le t$, *the polynomial*

$$p(x) = (n-1)(x^{n+1} - 1) - (n+1)(x^n - x),$$

is such that $p(x)$ *is* $(x-1)^3$ *times an irreducible polynomial if* n *is even and* $p(x)$ *is* $(x-1)^3(x+1)$ *times an irreducible polynomial if* n *is odd.*

Joint Work with Ognian Trifonov

(West Coast Number Theory Conference, 1997)

In 1951, Grosswald investigated the irreducibility over the rationals of the Bessel polynomials

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j.$$

He conjectured that $y_n(x)$ is irreducible for every positive integer n. Establishing the irreducibility of $y_n(x)$ for "all" n was also the last problem he posed at a West Coast Number Theory Conference.

Theorem 5. *Let n be a positive integer, and let $a_0, a_1, \dots, a_n$ be arbitrary integers with*

$$|a_0| = |a_n| = 1.$$

Then

$$\sum_{j=0}^{n} a_j \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

is irreducible.

Theorem 1. *Let $\varepsilon > 0$. For all but $O(t^{1/3+\varepsilon})$ positive integers $n \le t$, the derivative of the polynomial*

$$f(x) = 1 + x + x^2 + \cdots + x^n$$

is irreducible.

Basic Ideas of Proof:

- Write $f(x)$ and $f'(x)$ in a "nice" form.

$$f(x) = \frac{x^{n+1} - 1}{x - 1}$$

$$f'(x) = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}$$

- Work with $w(x) = x^{n+1} - (n+1)x + n$.

  We want to show that its non-cyclotomic part is irreducible.

$$w(x) = x^{n+1} - (n+1)x + n$$

- Suppose $w(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are monic in $\mathbb{Z}[x]$ and $g(1) \neq 0$. We want to show $h(x)$ must equal $(x-1)^2$ for "most" n.

- Define
$$A = \sum_{g(\beta)=0} \left(\beta - \frac{1}{\beta}\right), \; B = \sum_{h(\gamma)=0} \left(\gamma - \frac{1}{\gamma}\right)$$
and observe that $nAB \in \mathbb{Z}$.

  The expression B has the property that $B = 0$ if and only if $h(x) = (x-1)^2$. If $B \neq 0$, then nAB is a non-zero integer. We show that typically this does not happen by finding upper and lower bounds for $n|AB|$ that are inconsistent for most n.

- Consider the complex roots of $w(x)$.

The complex roots α satisfy

$$1 \leq |\alpha| \leq 1 + \frac{5 \log n}{n}.$$

From

$$A = \sum_{g(\beta)=0} \left(\beta - \frac{1}{\beta}\right) = \sum_{g(\beta)=0} \left(\beta - \frac{1}{\overline{\beta}}\right),$$

we deduce that

$$|A| \leq 10 \log n.$$

Similarly, $|B| \leq 10 \log n$. Therefore,

$$n|AB| \leq 100n(\log n)^2.$$

$$w(x) = x^{n+1} - (n+1)x + n$$

- If $p|(n+1)$, consider the p-adic roots of $w(x)$.

$$n + 1 = p^\ell m$$
$$\implies w(x) \equiv (x^m - 1)^{p^\ell} \pmod{p}$$

The p-adic roots of $w(x)$ form clusters of roots around the p-adic mth roots of unity. Considering the Newton polygon of $w(x+\zeta)$ where $\zeta^m = 1$, one shows that around each $\zeta \neq 1$, there are ℓ clusters of roots satisfying:

(i) The roots in each cluster all belong to the same irreducible p-adic factor of $w(x)$.

(ii) There are a multiple of p roots in each cluster.

One uses (i) and (ii) to show that $\nu_p(A)$ and $\nu_p(B)$ are positive. Hence, $p^2|nAB$.

- If $p|n$, consider the p-adic roots of $w(x)$.

  In a similar fashion, one deduces here that at least one of $\nu_p(A)$ and $\nu_p(B)$ is positive so that $p|nAB$.

- Set up the inequalities on $n|AB|$ (if $B \neq 0$).

$$\Bigg(\prod_{p|(n+1)} p\Bigg)^2 \Bigg(\prod_{p|n} p\Bigg) \leq n|AB| \leq 100n(\log n)^2$$

- For most n the expression on the left is about n^3.