Some Remarkable Polynomials

by Michael Filaseta
University of South Carolina

filaseta@math.sc.edu
http://www.math.sc.edu/~filaseta

$$f(x) = 1 + 2x - 2x^2 + 4x^3 + 4x^4 + 2x^6 + 4x^7 - 4x^8 + 8x^9 + 8x^{10} - 2x^{12} - 4x^{13} + 4x^{14} - 8x^{15} - 8x^{16} + 4x^{18} + 8x^{19} - 8x^{20} + 16x^{21} + 16x^{22} + 4x^{24} + 8x^{25} - 8x^{26} + 16x^{27} + 16x^{28}$$

$f(x)$ has 25 terms

$f(x)^2$ has 23 terms

$f(x)$ has more terms than its square

Notation:

$$Q(n) = \min_{\substack{f \in \mathbb{Z}[x] \\ \#\text{ of terms } = n}} \{\#\text{ of terms of } f^2\}$$

$$f(x) = 1 + 2x - 2x^2 + 4x^3 + 4x^4 + 2x^6 + 4x^7 - 4x^8 + 8x^9 + 8x^{10} - 2x^{12} - 4x^{13} + 4x^{14} - 8x^{15} - 8x^{16} + 4x^{18} + 8x^{19} - 8x^{20} + 16x^{21} + 16x^{22} + 4x^{24} + 8x^{25} - 8x^{26} + 16x^{27} + 16x^{28}$$

$$Q(25) \le 23$$

Early Contributors:

P. Erdős, R. Freud, G. Hajós, L. Kalmár, L. Rédei, A. Rényi, W. Verdenius

Later Contributors:

D. Coppersmith, J. Davenport, A. Schinzel

Some Problems Considered:

- Does $Q(n)/n \to 0$? Yes.
- What happens if $f \notin \mathbb{Z}[x]$?
- What happens with f^2 replaced by f^k?

Problem (Rényi, 1947): Does $Q(n) \to \infty$?

Is it possible that there are f with an arbitrary number of terms and with f^2 having ≤ 100 terms?

Schinzel (1987): Yes.

$$\log\log n \ll Q(n) \ll n^{1-c} \quad \text{for some } c > 0$$

$$\begin{aligned} f(x) = 1 &+ 2x - 2x^2 + 4x^3 + 4x^4 + 2x^6 + 4x^7 \\ &- 4x^8 + 8x^9 + 8x^{10} - 2x^{12} - 4x^{13} \\ &+ 4x^{14} - 8x^{15} - 8x^{16} + 4x^{18} + 8x^{19} \\ &- 8x^{20} + 16x^{21} + 16x^{22} + 4x^{24} \\ &+ 8x^{25} - 8x^{26} + 16x^{27} + 16x^{28} \end{aligned}$$

What is the smallest n for which $Q(n) < n$?

Unknown.

Where did the above example come from?

$$w(x) = 1 + 2x - 2x^2 + 4x^3 + 4x^4$$

$$h(x) = w(x)^2 = 1 + 4x + 28x^4 + 32x^7 + 16x^8$$

$f_k(x) = w(x) \cdot w(x^k)$ has 25 terms if $k \geq 5$

$f_k(x)^2 = h(x) \cdot h(x^k)$ has 25 terms if $k \geq 9$

What if $5 \leq k \leq 8$?

$f_5(x)^2$ has 25 terms

$f_6(x)^2$ and $f_8(x)^2$ have 23 terms

$f_7(x)^2$ has 21 terms

$$f(x) = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35}$$

$$f_0(x) = 1$$
$$f_{j+1}(x) = f_j(x) + x^k$$

where $k > \deg f_j$ is minimal with $f_j(x) + x^k$ reducible

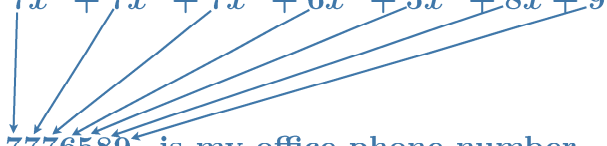
$$f(x) = f_7(x)$$

Why is $f_7(x)$ interesting?

There is no $f_8(x)$.

The sequence of $f_j(x)$ ends here.

$$f(x) = 7x^6 + 7x^5 + 7x^4 + 6x^3 + 5x^2 + 8x + 9$$



7776589 is my office phone number

7776589 is prime

Theorem (A. Cohn): *Let $d_n d_{n-1} \dots d_1 d_0$ be the decimal representation of a prime. Then*

$$d_n x^n + d_{n-1} x^{n-1} + \cdots + d_1 x + d_0$$

is irreducible over the integers.

Theorem (A. Cohn): *Let $d_n d_{n-1} \dots d_1 d_0$ be the decimal representation of a prime. Then*

$$d_n x^n + d_{n-1} x^{n-1} + \cdots + d_1 x + d_0$$

is irreducible over the integers.

Results by J. Brillhart, A. Odlyzko, F.:

- The theorem is true in any base.
- Can replace primes with kp where p is prime and $k \leq 9$ (sort-of).
- The coefficients being digits can be relaxed.

$$f(x) = 7x^6 + 7x^5 + 7x^4 + 6x^3 + 5x^2 + 8x + 9$$

$$f(10) = 7776589$$

Theorem (F.): *Let*

$$f(x) = d_n x^n + d_{n-1} x^{n-1} + \cdots + d_1 x + d_0$$

with $f(10)$ prime and $0 \leq d_j \leq 10^{30}$. Then $f(x)$ is irreducible over the integers.

Comment: If $n \leq 31$, then $0 \leq d_j \leq 10^{30}$ can be replaced by $d_j \geq 0$.

$$f(x) = x^{32} + 130x^2 + 560328675401014156716157263772 0x + 610910410476130955598601060595 29$$

$f(10)$ is prime and $f(x)$ is reducible

$f(x)$ is (necessarily) divisible by $x^2 - 20x + 101$

Prime Bits:

$37 = (100101)_2$ is prime

so $x^5 + x^2 + 1$ is irreducible

$$f(x) = \sum_{k=0}^{n} b_k x^k \in \mathbb{Z}[x], f(2) \text{ prime}, 0 \le b_k \le 4$$

$$\Longrightarrow f(x) \text{ is irreducible}$$

Prime Bits:

$37 = (100101)_2$ is prime

so $x^5 + x^2 + 1$ is irreducible

$$f(x) = \sum_{k=0}^{n} b_k x^k \in \mathbb{Z}[x], f(2) \text{ prime}, 0 \le b_k \le ?$$

$$\Longrightarrow f(x) \text{ is irreducible}$$

Problem: What's best possible here?

$$f(x) = x^{10} + 7x^5 + 10x^4 + 10x^3 + 10x^2 + 3$$

$f(2) = 1531$ is prime, $(x^2 - 3x + 3) | f(x)$

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

Cyclotomic polynomials are the irreducible factors of $x^n - 1$.

Theorem (L. Kronecker): *If $F(x) \in \mathbb{Z}[x]$ is monic, is irreducible, and has all its roots on $\{z : |z| = 1\}$, then $F(x)$ is a cyclotomic polynomial.*

Mahler Measure: $M(p(x)) = |a_n| \prod_{\substack{1 \le j \le n \\ |\alpha_j| > 1}} |\alpha_j|,$

where

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

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

Mahler Measure: $M(p(x)) = |a_n| \prod_{\substack{1 \le j \le n \\ |\alpha_j| > 1}} |\alpha_j|,$

where

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

$M(L) = 1.1762808182599175\ldots$

$L(x)$ is Lehmer's polynomial (D. H. Lehmer).

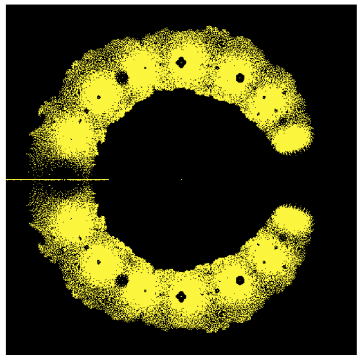
Is this the minimum Mahler measure > 1 for polynomials in $\mathbb{Z}[x]$?

Can these Mahler measures be arbitrarily close to 1?

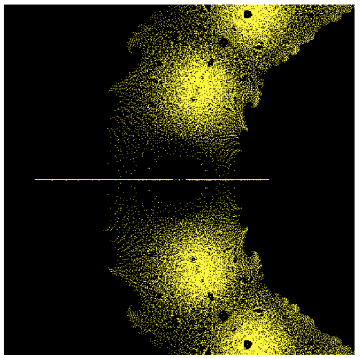
$$f(x) = x^{59} + x^{58} + x^{54} + x^{51} + x^{48} + x^{47} + x^{46} + x^{45} + x^{41} + x^{37} + x^{36} + x^{35} + x^{34} + x^{31} + x^{28} + x^{25} + x^{24} + x^{23} + x^{22} + x^{18} + x^{14} + x^{13} + x^{12} + x^{11} + x^{8} + x^{5} + x + 1$$

$f(x)$ is a 0,1-polynomial

A. Odlyzko and B. Poonen (1993) investigated the zeroes of 0,1-polynomials

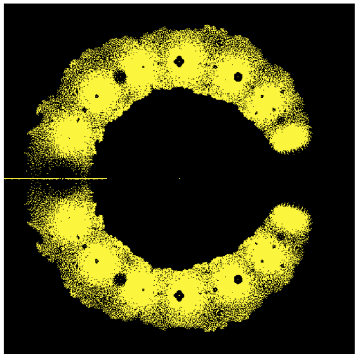


All roots with degrees ≤ 15

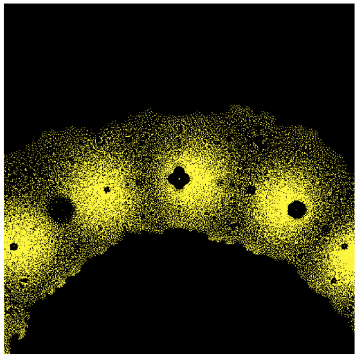


Same roots near -1

Images from: http://www.cecm.sfu.ca/organics/papers/odlyzko/support/polyform.html



All roots with degrees ≤ 15



Same roots near i

Images from: http://www.cecm.sfu.ca/organics/papers/odlyzko/support/polyform.html

$$f(x) = x^{59} + x^{58} + x^{54} + x^{51} + x^{48} + x^{47} + x^{46} + x^{45} + x^{41} + x^{37} + x^{36} + x^{35} + x^{34} + x^{31} + x^{28} + x^{25} + x^{24} + x^{23} + x^{22} + x^{18} + x^{14} + x^{13} + x^{12} + x^{11} + x^{8} + x^{5} + x + 1$$

Based on their computations, Odlyzko and Poonen conjectured that if a 0,1-polynomial has a root with multiplicity > 1, then the root is a cyclotomic root of unity.

M. Mossinghoff resolved the conjecture with the above counterexample.

$$f(x) = x^{59} + x^{58} + x^{54} + x^{51} + x^{48} + x^{47} + x^{46} + x^{45} + x^{41} + x^{37} + x^{36} + x^{35} + x^{34} + x^{31} + x^{28} + x^{25} + x^{24} + x^{23} + x^{22} + x^{18} + x^{14} + x^{13} + x^{12} + x^{11} + x^{8} + x^{5} + x + 1$$

If a 0,1-polynomial has a factor $w(x)^2$ that is the square of a non-cyclotomic irreducible polynomial, what might be a good possibility for $w(x)$?

Mossinghoff worked with Lehmer's polynomial $L(x)$. More precisely, he took $w(x) = L(-x)$.

In other words, $f(x)$ is divisible by $L(-x)^2$.

$$f(x) = 3 + x + 4x^2 + x^3 + 5x^4 + 9x^5 + 2x^6 + 6x^7 + \cdots + 7x^{16117} + 0x^{16118} + 3x^{16119}$$

The above polynomial is the answer to a homework problem I have given: Find a polynomial in the sequence 3, $3 + x$, $3 + x + 4x^2$, $3 + x + 4x^2 + x^3$, ... (formed from the digits of π) that is reducible.

Idea: If the digits of π are random, some partial sums of

$$3 - 1 + 4 - 1 + 5 - 9 + 2 - 6 + \cdots$$

will be 0 so that $x+1$ is a factor of some polynomials in the sequence.

$$f(x) = 3 + x + 4x^2 + x^3 + 5x^4 + 9x^5 + 2x^6 + 6x^7 + \cdots + 7x^{16117} + 0x^{161198} + 3x^{16119}$$

The above polynomial is the answer to a homework problem I have given: Find a polynomial in the sequence 3, $3 + x$, $3 + x + 4x^2$, $3 + x + 4x^2 + x^3$, ... (formed from the digits of π) that is reducible.

Problem: Is $f(x)$ the reducible polynomial of least degree in this sequence?

$$f(x) = 5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3$$

Background:

A *covering of the integers* is a finite system of congruences

$$x \equiv a_j \pmod{m_j}, \quad j = 1, 2, \ldots, r,$$

with a_j and m_j integral and with $m_j \geq 1$ distinct, such that every integer satisfies at least one of the congruences.

A *covering of the integers* is a finite system of congruences

$$x \equiv a_j \pmod{m_j}, \quad j = 1, 2, \ldots, r,$$

with a_j and m_j integral and with $m_j \geq 1$ distinct, such that every integer satisfies at least one of the congruences.

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 6 \\ x &\equiv 3 \pmod{12} \end{aligned}$$

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 8 \\ x &\equiv 7 \pmod{12} \\ x &\equiv 23 \pmod{24} \end{aligned}$$

Problem: Given $c > 0$, is there a covering with minimum modulus $\geq c$?

Problem: Does there exist a covering consisting of odd moduli > 1?

Theorem (W. Sierpinski): *A positive proportion of odd positive integers k satisfy $k \times 2^n + 1$ is composite for all non-negative integers n.*

Smallest Known k: 78557 (J. Selfridge)

Polynomial Problem: Is there a $w(x) \in \mathbb{Z}[x]$ with $w(1) \neq -1$ such that $w(x)x^n + 1$ is reducible over the rationals for all $n \geq 0$?

The answer is not known.

$$f(x) = 5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3$$

Schinzel: $f(x)$ has the property that $f(x)x^n + 12$ is reducible for all $n \geq 0$.

$$f(x) = 5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3$$

Schinzel: $f(x)$ has the property that $f(x)x^n + 12$ is reducible for all $n \geq 0$.

$$\begin{aligned} n \equiv 0 \pmod 2 &\implies f(x)x^n + 12 \equiv 0 \pmod{x+1} \\ n \equiv 2 \pmod 3 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1} \\ n \equiv 1 \pmod 4 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+1} \\ n \equiv 1 \pmod 6 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2-x+1} \\ n \equiv 3 \pmod{12} &\implies f(x)x^n + 12 \equiv 0 \pmod{x^4-x^2+1} \end{aligned}$$

covering of the integers

$$f(x) = 5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3$$

Schinzel: $f(x)$ has the property that $f(x)x^n + 12$ is reducible for all $n \geq 0$.

Theorem (Schinzel): *If there is an $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -1$ and $f(x)x^n + 1$ reducible for all $n \geq 0$, then there is a covering of the integers consisting of all odd moduli > 1.*

$$f(x) = 5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3$$

Schinzel: $f(x)$ has the property that $f(x)x^n + 12$ is reducible for all $n \geq 0$.

Theorem (F.): *There exists an $f(x) \in \mathbb{Z}^+[x]$ with $f(x)x^n + 4$ reducible for all $n \geq 0$.*

Comment: The proof is constructive but it would produce a very messy $f(x)$.

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

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{n-1}}{(n-1)!} + \frac{x^n}{n!} + \cdots$$

I. Schur: $f(x)$ is irreducible over the rationals.

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

Theorem (Schur): *Let n be an integer ≥ 1, and let $a_0, a_1, \ldots, a_n$ be arbitrary integers with $|a_0| = |a_n| = 1$. Then*

$$a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + a_2 \frac{x^2}{2!} + a_1 x + a_0$$

is irreducible over the rationals.

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

Theorem (F.): *Let n be an integer ≥ 1, and let $a_0, a_1, \ldots, a_n$ be arbitrary integers with $|a_0| = 1$ and $0 < |a_n| < n$. Then*

$$a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + a_2 \frac{x^2}{2!} + a_1 x + a_0$$

is irreducible over the rationals unless

$$(a_n, n) \in \{(\pm 5, 6), (\pm 7, 10)\}.$$

$$f(x) = x^2 + 1 \quad \text{and} \quad g(x) = x^4 + 1$$

Dirichlet's theorem asserts that a linear polynomial $w(x)$ which is irreducible over the integers (i.e., a polynomial $w(x) = ax + b$ with a and b relatively prime integers) is such that $w(m)$ is prime for infinitely many integers m.

The analogous result for an arbitrary irreducible polynomial $w(x) \in \mathbb{Z}[x]$ is believed to be true (if the $\gcd(w(m) : m \in \mathbb{Z}) = 1$), but it is unknown if there even exists an irreducible polynomial of degree > 1 that takes on infinitely many prime values.

The polynomial $f(x)$ above represents the simplest unknown case. Is it true that for infinitely many integers m, the number $m^2 + 1$ is prime?

$$f(x) = x^2 + 1 \quad \text{and} \quad g(x) = x^4 + 1$$

Theorem (H. Iwaniec): *There are infinitely many integers m such that either $f(m)$ is a prime or $f(m)$ is the product of two primes.*

Theorem (J.-M. Deshouillers & H. Iwaniec): *There are infinitely many integers m such that $f(m)$ has a prime factor $> m^{6/5}$.*

$$f(x) = x^2 + 1 \quad \text{and} \quad g(x) = x^4 + 1$$

Is it even true that for $w(x) \in \mathbb{Z}[x]$ an arbitrary irreducible polynomial (with $\gcd(w(m) : m \in \mathbb{Z}) = 1$), there are infinitely many integers m such that $w(m)$ is squarefree (i.e., not divisible by the square of a prime)?

This is unknown for $\deg w \geq 4$.

The polynomial $g(x)$ above represents the simplest unknown case here. Is it true that for infinitely many integers m, the number $m^4 + 1$ is squarefree?

$f(x) = x^2 + 1$ and $g(x) = x^4 + 1$

Theorem (P. Erdős & C. Hooley): *There exist infinitely many integers m such that $g(m)$ is cube-free (i.e., not divisible by the cube of a prime).*

The polynomial $g(x)$ is interesting for yet another reason. It is the simplest example of an irreducible polynomial over the rationals that is also reducible modulo every prime.

$f(x) = x^2 + 1$ and $g(x) = x^4 + 1$

Comment: Such polynomials imply that commonly used polynomial factoring algorithms run slowly, in non-polynomial time. However, these algorithms are preferred over polynomial time algorithms in part because polynomials that have "few" factors over the integers and "many" factors modulo all primes are provably rare.