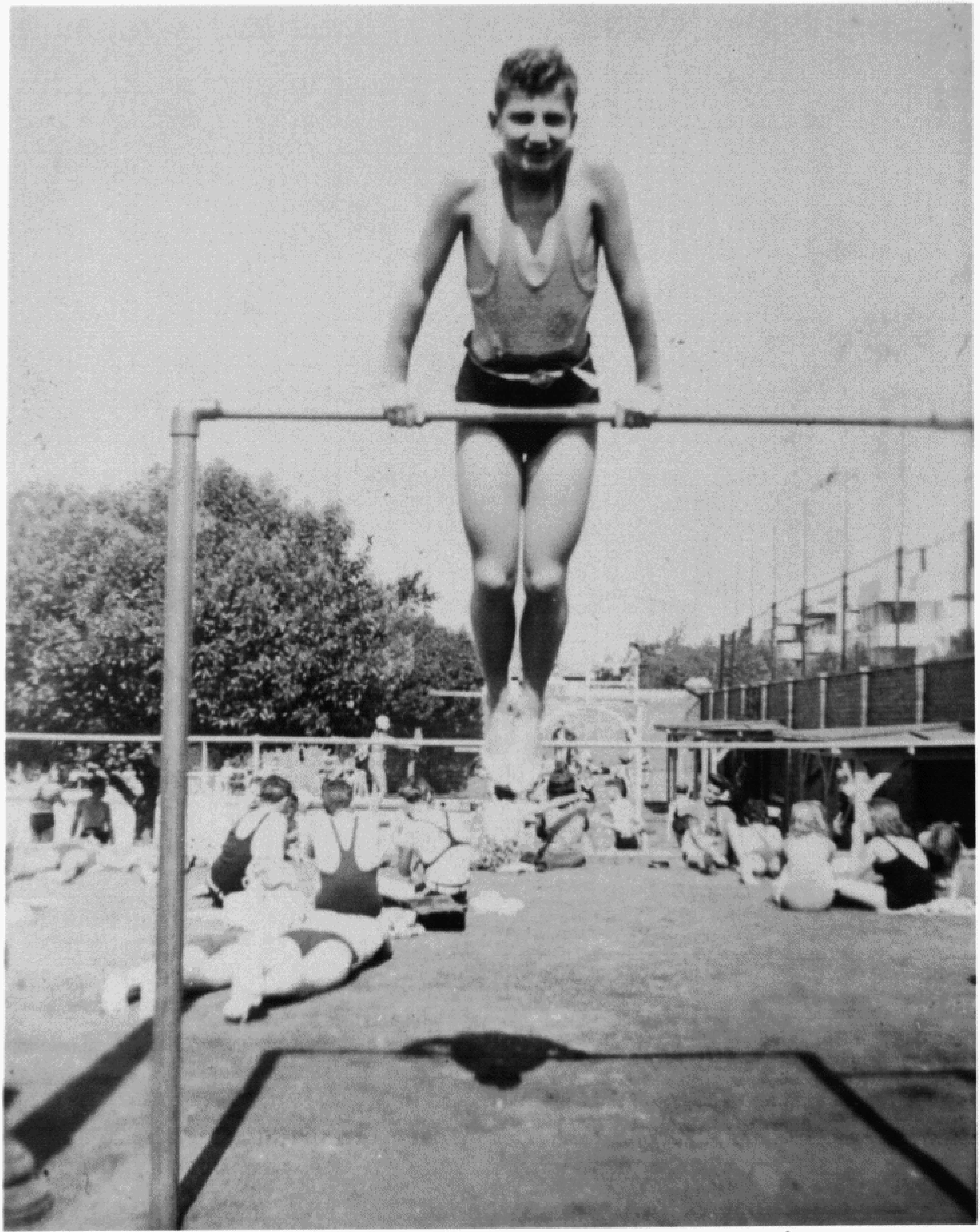


DAVID (YOUVILLE BATHS)

Three Highly Computational Problems in Diophantine Number Theory (I guess)

Peter Borwein

-

http://www.cecm.sfu.ca/~pborwein.

PREPARED FOR CMS SESSION JUNE 2004

Abstract: A number of classical and not so classical problems in number theory concern finding polynomials with integer coefficients that are of small norm. These include old chestnuts like the Merit Factor problem, Lehmer's Conjecture and Littlewood's (other) Conjecture.

Let

$$\mathcal{Z}_n := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \mathbb{Z} \right\}$$

denote the set of algebraic polynomials of degree at most n with integer coefficients and let $\mathcal{Z}$ denote the union.

Let

$$\mathcal{L}_n := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \{-1, 1\} \right\}$$

denote the set of polynomials of degree at most n with coefficients from $\{-1, 1\}$. Call such polynomials **Littlewood polynomials**.

P4. Littlewood's Problem in L_∞.
Find the polynomial in $\mathcal{L}_n$ that has smallest possible supremum norm on the unit disk. Show that there exist positive constants c_1 and c_2 so that for any n is it is possible to find $p_n \in \mathcal{L}_n$ with

$$c_1\sqrt{n} \leq |p_n(z)| \leq c_2\sqrt{n}$$

for all complex z with $|z| = 1$.

Littlewood, in part, based his conjecture on computations of all such polynomials up to degree twenty.

Odlyzko has now done 200 MIPS years of computing on this problem

P5. Erdős's Problem in L_∞. *Show that there exists a positive constant c_3 so that for all n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_D \geq (1 + c_3)\sqrt{n}$.*

Merit Factor Problems. How small can the L_4 norm of Littlewood polynomial be. The L_4 norm computes algebraically from the coefficients. If

$$p(z) := \sum_{k=0}^{n} a_k z^k$$

is a polynomial with real coefficients then

$$p(z)p(1/z) = \sum_{k=-n}^{n} c_k z^k$$

where, for $-n \leq k \leq n$, the **acyclic autocorrelation coefficients**

$$c_k = \sum_{j=0}^{n-k} a_j a_{j+k} \quad \text{and} \quad c_{-k} = c_k$$

and

$$\|p(z)\|_4^4 = \|p(z)p(1/z)\|_2^2 = \sum_{k=-n}^{n} c_k^2.$$

The *merit factor* is defined by

$$MF(p) = \frac{\|p\|_2^4}{\|p|_4^4 - \|p\|_2^4}.$$

The merit factor is a useful normalization. It tends to give interesting sequences integer limits and makes the expected merit factor of a polynomial with ± 1 coefficients 1. The Rudin-Shapiro polynomialsRudin-Shapiro polynomials have merit factors that tend to 3.

P6. The Merit Factor Problem.

Find the polynomial in $\mathcal{L}_n$ that has smallest possible L_4 norm on the unit disk. Show that there exists a positive constant c_4 so that for all n and all $p_n \in \mathcal{L}_n$ we have

$$L_4(p_n) \geq (1 + c_4)\sqrt{n}.$$

Equivalently show that the Merit Factor is bounded above.

P7. Barker Polynomial Problem.

For $n > 12$ *and* $p_n \in \mathcal{L}_n$ *show that*

$$L_4(p_n) > ((n+1)^2 + 2n)^{1/4}.$$

Equivalently show that at least one non trivial autocorrelation coefficient is strictly greater than 1 in modulus.

This is much weaker than the Merit Factor Problem.

• Find sequences that have analysable Merit Factors

Theorem . *For q an odd prime, the Turyn type polynomials*

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q} \right) z^k$$

where $[\cdot]$ denotes the nearest integer, satisfy

$$\|R_q\|_4^4 = \frac{7q^2}{6} - q - \frac{1}{6} - \gamma_q$$

and

$$\gamma_q := \begin{cases} h(-q)\big(h(-q) - 4\big) & \text{if } q \equiv 1, 5 \pmod 8 \\ 12\big(h(-q)\big)^2 & \text{if } q \equiv 3 \pmod 8, \\ 0 & \text{if } q \equiv 7 \pmod 8. \end{cases}$$

Thus these polynomials have merit factors asymptotic to 6. Golay, Høholdt and Jensen, and Turyn (and others) show that the merit factors of cyclically permuted character polynomials associated with non-principal real characters (the Legendre symbol) vary asymptotically between 3/2 and 6.

• A really interesting observation made here!!!

P8. Lehmer's Problem (1933). *Show that a (non-cyclotomic) polynomial* p *with integer coefficients has Mahler measure at least* 1.1762.... *(This latter constant is the Mahler measure of* $1 + z - z^3 - z^4 - z^5 - z^6 - z^7 + z^9 + z^{10}$*.)*

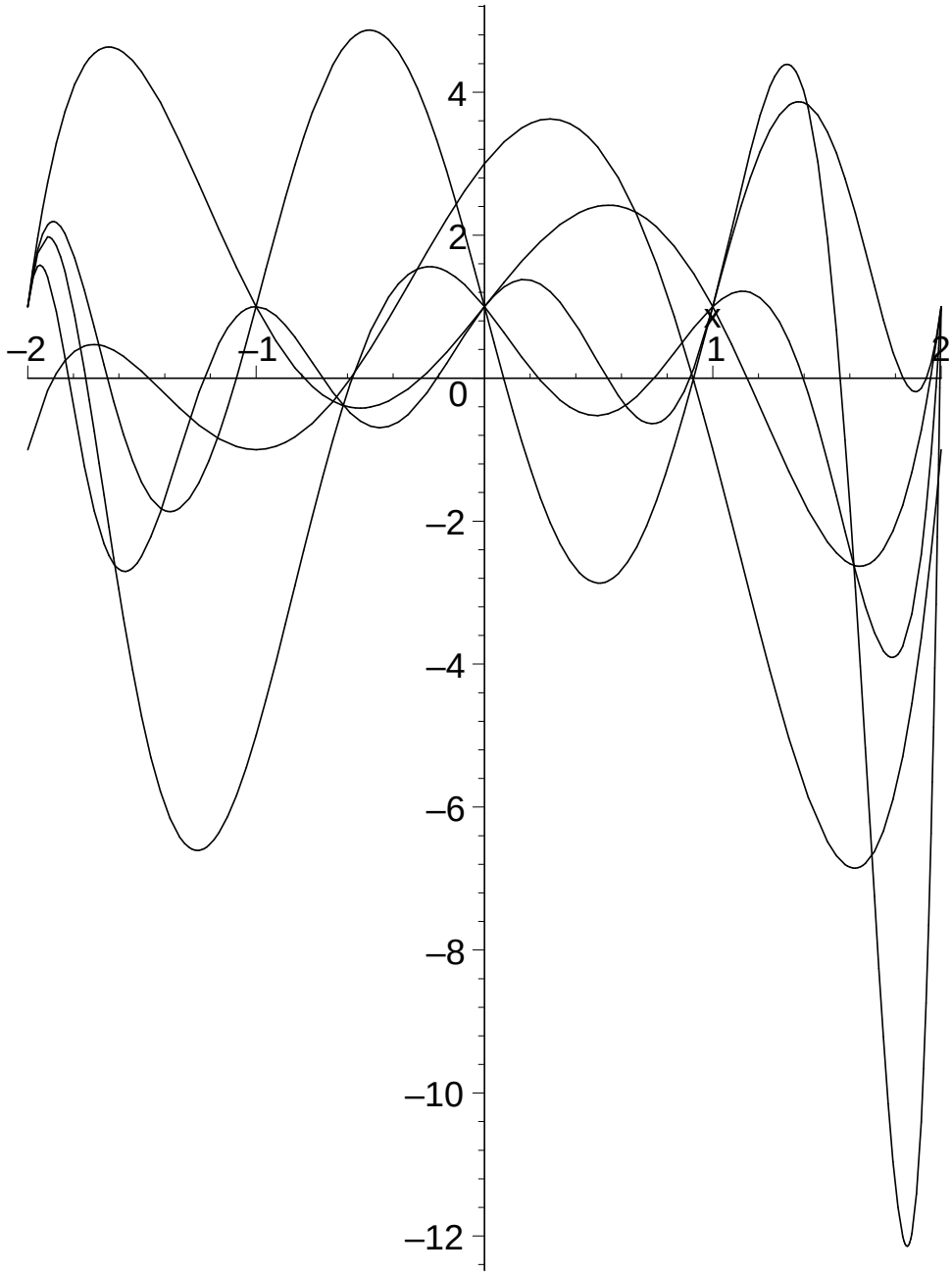
A conjecture of similar flavour is

P12. Conjecture of Schinzel and Zassenhaus (1965). *There is a constant* c *so that any non-cyclotomic polynomial* p_n *of degree* n *with integer coefficients has at least one root of modulus at least* c/n*.*

This conjecture is made in Schinzel and Zassenhaus [1965]. It is easy to see that P8 implies P12. The best partial is due to Smyth. If p is a non-reciprocal polynomial of degree n then at least one root ρ satisfies

$$\rho \geq 1 + \frac{\log \phi}{n}$$

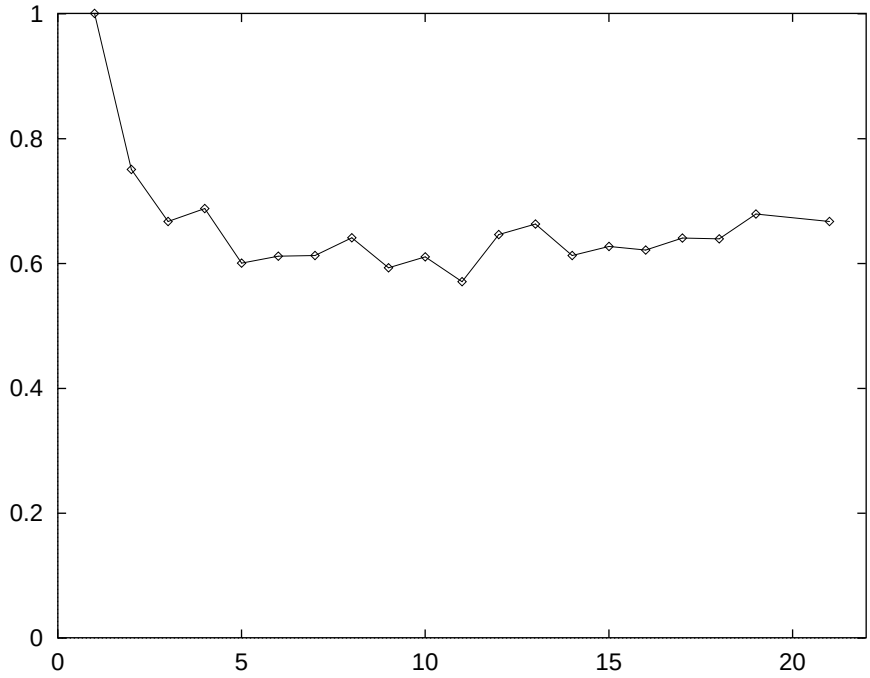
where $\phi = 1.3247\ldots$ is the smallest Pisot number, namely the real root of $z^3 - z - 1$.


4
2
–2
–1
1
2
x
0
–2
–4
–6
–8
–10
–12

P9. Mahler's Problem. *For each n find the polynomials in $\mathcal{L}_n$ that have largest possible Mahler measure. Analyse the asymptotic behaviour as n tends to infinity.*

P10. Multiplicity of Zeros of Height One Polynomials. *What is the maximum multiplicity of the vanishing at 1 of a polynomial in $\mathcal{F}_n$?*

P11. Muliplicity of Zeros in $\mathcal{L}_n$. *What is the maximum multiplicity of the vanishing at 1 of a polynomial in $\mathcal{L}_n$?*


1
0.8
0.6
0.4
0.2
0
0
5
10
15
20