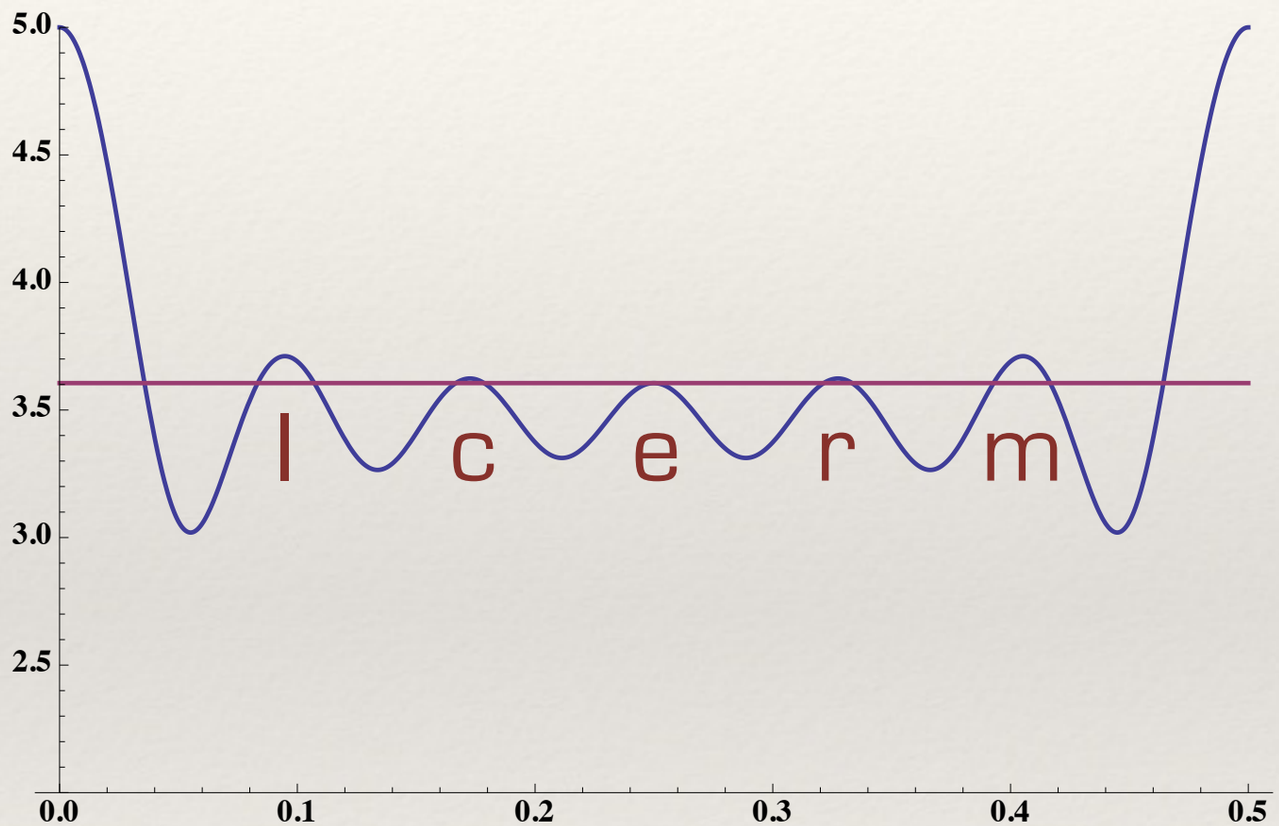
Come on Down!
An Invitation to Barker Polynomials



Michael Mossinghoff
Davidson College

Introduction to Topics
Summer@ICERM 2014
Brown University

Engineers

Barker Sequences

- $a_0,\ a_1,\ \ldots,\ a_{n-1}$: finite sequence, each ± 1.
- For $0 \leq k \leq n-1$, define the kth *aperiodic autocorrelation* by

$$c_k = \sum_{i=0}^{n-k-1} a_i a_{i+k}.$$

- $k = 0$: *peak* autocorrelation.
- $k > 0$: *off-peak* autocorrelations.
- Goal: make off-peak values <u>small</u>.
- *Barker sequence*: $|c_k| \leq 1$ for $k > 0$.

Engineering Motivation

- $\{a_i\} \leftrightarrow$ binary digital signal.
- $c_k \leftrightarrow$ output when two signals are out of phase by k units.
- Peak at $k = 0$ facilitates synchronization.
- R. H. Barker (1953): *Group synchronization of binary digital systems.*
- Want c_0 large compared to other c_k.

Example

++++−−+−

$$
\begin{aligned}
c_0 &= 7 \\
c_1 &= 0 \\
c_2 &= -1 \\
c_3 &= 0 \\
c_4 &= -1 \\
c_5 &= 0 \\
c_6 &= -1
\end{aligned}
$$

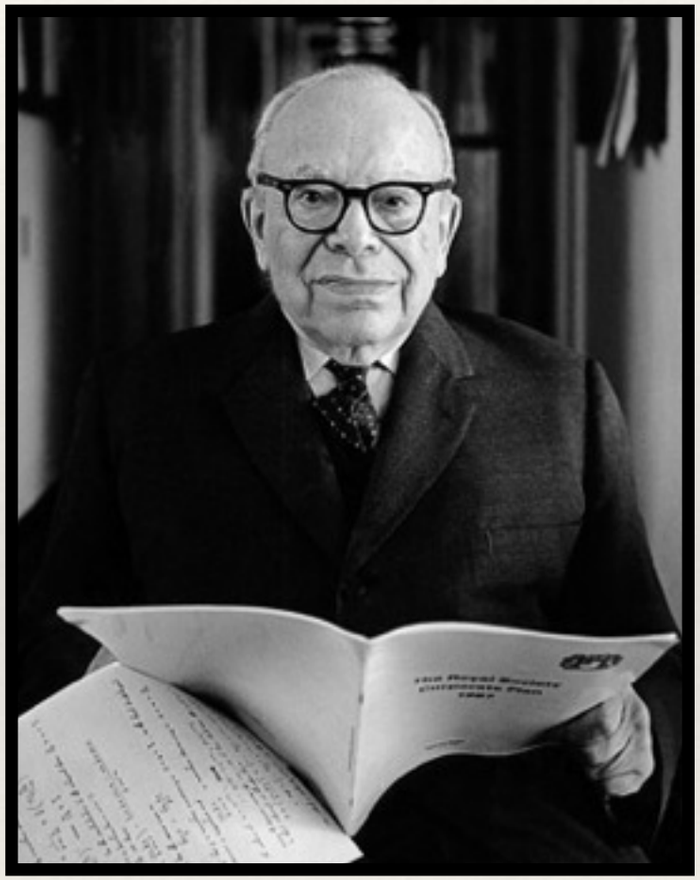
Solution: Barker Sequences

n	Sequence
1	$+$
2	$++$
3	$++-$
4	$+++-$
5	$+++-+$
7	$+++--+-$
11	$+++---+--+-$
13	$+++++--++-+-+$

Open Problem

- Barker (1953): Do any Barker sequences exist with length $n > 13$?
- Turyn and Storer (1961): If n is odd then $n \leq 13$.
- Are there any with even length $n > 4$?

Analysts



- Let $f(z) = \sum_{k=0}^{n-1} a_k z^k = a_{n-1} \prod_{k=1}^{n-1} (z - \beta_k)$.

- Let $\|f\|_p$ denote the L_p norm of f:

$$\|f\|_p = \left(\int_0^1 |f(e^{2\pi i t})|^p \, dt \right)^{1/p}.$$

- Limit as $p \to \infty$: *sup norm*: $\|f\|_\infty = \sup_{|z|=1} |f(z)|$.

- Limit as $p \to 0^+$: *Mahler measure*:

$$M(f) = \exp\left(\int_0^1 \log |f(e^{2\pi i t})| \, dt \right).$$

- Jensen's formula in complex analysis produces

$$M(f) = |a_{n-1}| \prod_{k=1}^{n-1} \max\{1, |\beta_k|\}.$$

- $p \leq q$ implies $\|f\|_p \leq \|f\|_q$.

- Parseval's formula: $\|f\|_2^2 = \sum_{k=0}^{n-1} |a_k|^2$.

- Erdős conjecture (1962):

  There exists $\epsilon > 0$ so that if $n \geq 2$ and $f(x) = \pm 1 \pm x \pm \cdots \pm x^{n-1}$ then $\dfrac{\|f\|_\infty}{\sqrt{n}} > 1 + \epsilon$.

- Stronger form: $\dfrac{\|f\|_4}{\sqrt{n}} > 1 + \epsilon$.

Quick Calculation

$$\|f\|_4^4 = \|f(z)\overline{f(z)}\|_2^2$$

$$= \|f(z)f(1/z)\|_2^2$$

$$= \left\| \sum_{k=-(n-1)}^{n-1} \left(\sum_{i-j=k} a_i a_j \right) z^k \right\|_2^2$$

$$= \left\| \sum_{k=-(n-1)}^{n-1} c_k z^k \right\|_2^2$$

$$= n^2 + 2\sum_{k=1}^{n-1} c_k^2.$$

- Golay defined the *merit factor* of a sequence $\mathbf{a}$ of length n over $\{-1, +1\}$ by

$$\mathrm{MF}(\mathbf{a}) = \frac{n^2}{2\sum_{k=1}^{n-1} c_k^2}.$$

- Engineering: peak energy vs. sidelobe energy.
- Barker sequence of length n has MF $\approx n$.
- Best known merit factor for binary seq.: 14.083.
- Problem: find long $\{-1,1\}$ sequences with large merit factor.
- Equivalent formulation, building $f(z)$ from $\mathbf{a}$:

$$\mathrm{MF}(f) = \frac{\|f\|_2^4}{\|f\|_4^4 - \|f\|_2^4} = \frac{1}{\left(\|f\|_4/\sqrt{n}\right)^4 - 1}.$$

Periodic Barker Sequences

Periodic Barker Sequences

- The k*th periodic autocorrelation*:

$$\gamma_k = \sum_{i=0}^{n-1} a_i a_{(i+k \bmod n)}.$$

- Example:

$$\gamma_2 = a_0 a_2 + a_1 a_3 + \cdots + a_{n-3} a_{n-1}$$
$$+ a_{n-2} a_0 + a_{n-1} a_1$$
$$= c_2 + c_{n-2}.$$

$$\gamma_1 = -1. \quad \gamma_4 = -1.$$
$$\gamma_2 = -1. \quad \gamma_5 = 1.$$
$$\gamma_3 = -1. \quad \gamma_6 = -1.$$

- In the same way, $\gamma_k = c_k \pm c_{n-k}$ for $0 < k < n$.
- *Periodic Barker sequence*: $|\gamma_k| \leq 1$ for $k > 0$.

Theorem: Every Barker sequence with length $n > 2$ is a periodic Barker sequence.

- If $a, b = \pm 1$ then $ab \equiv a + b - 1 \bmod 4$.
- $c_k \equiv \sum_i (a_i + a_{i+k}) - (n-k) \bmod 4$.
- $c_k - c_{k+1} \equiv a_{n-1-k} + a_k - 1 \bmod 4$.
- $c_{n-1-k} - c_{n-k} \equiv a_{n-1-k} + a_k - 1 \bmod 4$.
- $c_k - c_{k+1} \equiv c_{n-1-k} - c_{n-k} \bmod 4$.
- $c_k - c_{k+1} = c_{n-1-k} - c_{n-k}$.
- $\gamma_k = \gamma_{k+1}$ for $0 < k < n-1$.

Theorem: Every Barker sequence with length $n > 2$ is a periodic Barker sequence.

- So $\gamma_k = \gamma$ for $0 < k < n$.
- If $|\gamma| = 2$ then $c_k = c_{n-k} = \pm 1$ for each k.
- But $c_k \equiv n - k \bmod 2$.
- So $|\gamma| = 2$ is impossible if $n > 2$.
- Thus $|\gamma| \leq 1$.

- Note: The converse is false!

Theorem: Every Barker sequence with length $n > 2$ is a periodic Barker sequence.

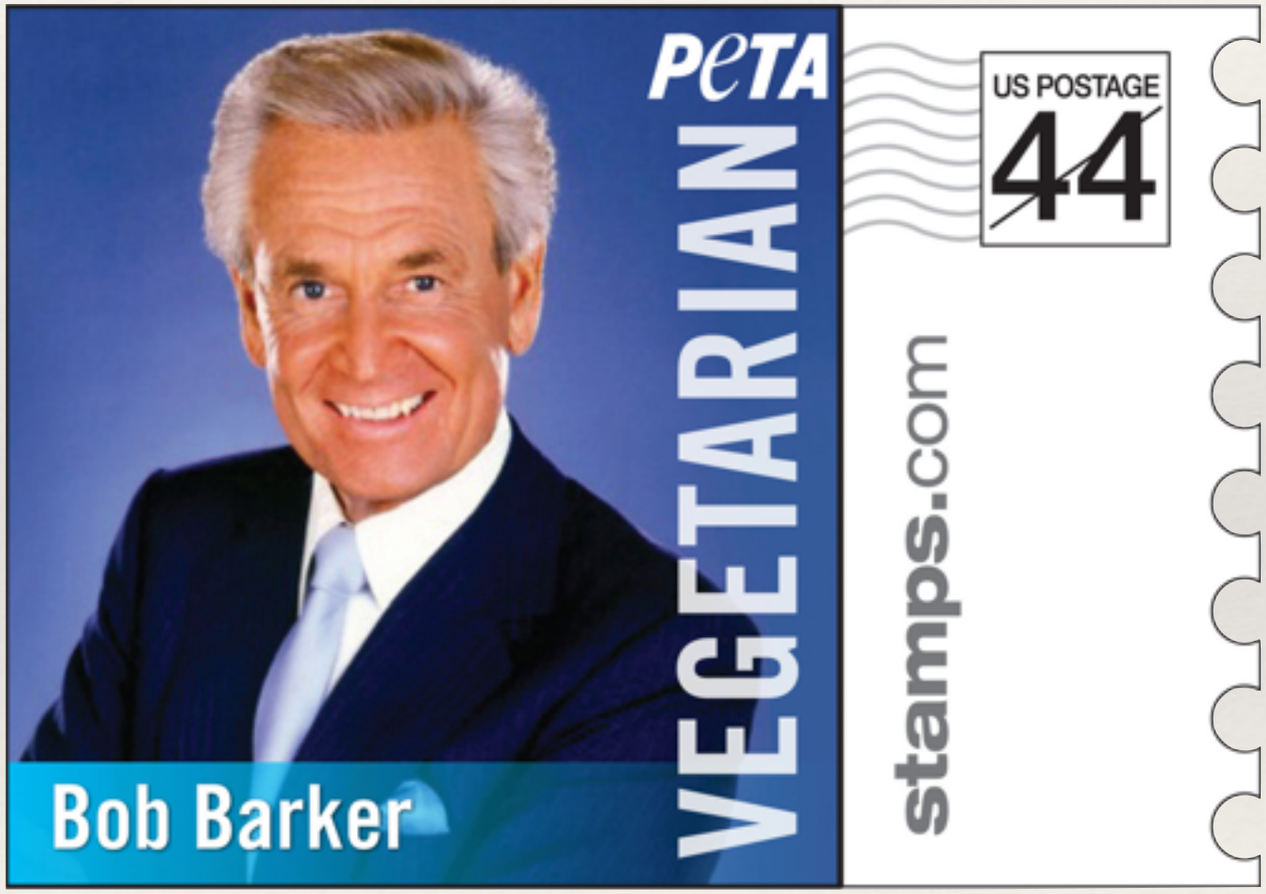
- Thus: the off-peak <u>periodic</u> autocorrelations of a Barker sequence of even length are all 0.
- I.e., $(a_0, ..., a_{n-1})$ is orthogonal to all cyclic shifts of itself.
- The *circulant matrix* made from this sequence is *Hadamard*.

Examples

$$\begin{bmatrix} + & + & + & - \\ - & + & + & + \\ + & - & + & + \\ + & + & - & + \end{bmatrix}, \quad [+].$$

- <u>Open problem</u>: Show that if H is an $n \times n$ circulant Hadamard matrix with ± 1 entries, then $n \leq 4$.
- This implies that no more Barker sequences exist.

Restrictions



Restriction 1

- **Theorem** (Turyn, 1965): If $n > 2$ is the order of a circulant Hadamard matrix, then $n = 4m^2$. Further, m is odd, and not a prime power.
  - Let $J_n = n \times n$ matrix of all 1's.
  - Let $e =$ sum of entries of a row of H.
  - $(HH^T)J_n = (nI_n)J_n = nJ_n$.
  - $H(H^T J_n) = H(eJ_n) = e^2 J_n$.
  - So $n = 4m^2$.

Restriction 2: Self-Conjugacy

- a is *semiprimitive* mod b: $a^j \equiv -1 \bmod b$ for some j.
- r is *self-conjugate* mod s: For each $p \mid r$, p is semiprimitive mod the p-free part of s.
- **Theorem** (Turyn): If $n = 4m^2$ is the order of a CHM, $r \mid m$, $s \mid n$, $\gcd(r, s)$ has $k \geq 1$ distinct prime divisors, and r is self-conjugate mod s, then $rs \leq 2^{k-1}n$.

Special Case: Large Primes

- **Theorem** (Turyn): If $n = 4m^2$ is the order of a CHM, $r \mid m$, $s \mid n$, $\gcd(r, s)$ has $k \geq 1$ distinct prime divisors, and r is self-conjugate mod s, then $rs \leq 2^{k-1}n$.
- Suppose p is odd and $p \mid m$. Take $r = p$, $s = 2p^2$.
- p is semiprimitive mod 2.
- r is self-conjugate mod s.
- Thus $p^3 \leq 2m^2$.
- **Corollary**: If $p^k \mid m$ and $p^{3k} > 2m^2$, then no circulant Hadamard matrix of size $n = 4m^2$ exists.

Restriction 3: *F*-Test

- $\nu_p(m) =$ multiplicity of p in factorization of m.
- $m_q = q$-free and squarefree part of m: $m_q = \prod_{\substack{p|m \\ p \neq q}} p$.
- $b(p,m) = \max_{\substack{q|m \\ q \neq p}} \left\{ \nu_p(q^{p-1} - 1) + \nu_p(\mathrm{ord}_{m_q}(q)) \right\}$.
- $F(m) = \gcd\left(m^2, \prod_{p|m} p^{b(p,m)} \right)$.
- **Theorem** (Leung & Schmidt, 2005): If $n = 4m^2$ is the order of a circulant Hadamard matrix, then $F(m) \geq m\varphi(m)$.

Prior Bounds for CHMs

- Turyn (1968): $m \geq 55$.
- Schmidt (1999): $m \geq 165$.
- Schmidt (2002): If $m \leq 10^5$ then $m \in \{11715, 16401, 82005\}$.

Restriction 4: Barker Only

- **Theorem** (Eliahou, Kervaire, Saffari, 1990): If $n = 4m^2$ is the length of a Barker sequence and $p \mid m$, then $p \equiv 1 \bmod 4$.
- Prior bounds:
  - Jedwab & Lloyd; Eliahou & Kervaire (1992): $m \geq 689$.
  - Schmidt (1999): $m > 10^6$.
  - Leung & Schmidt (2005): $m > 5 \cdot 10^{10}$.
  - No plausible value known in 2005!

Example 1

- $m = 689 = 13 \cdot 53.$
  - $p = 13$: $\nu_{13}(53^{12} - 1) + \nu_{13}(\mathrm{ord}_{13}(53)) = 1.$
  - $p = 53$: $\nu_{53}(13^{52} - 1) + \nu_{53}(\mathrm{ord}_{53}(13)) = 1.$
- $F(689) = 689.$

Example 2

- $m = 11715 = 3 \cdot 5 \cdot 11 \cdot 71.$
  - $p = 3$: $71^2 \equiv 1 \bmod 3^2$.
  - $p = 5$: $5 \mid \mathrm{ord}_{m/3}(3) = 140$.
  - $p = 11$: $3^{10} \equiv 1 \bmod 11^2$.
  - $p = 71$: $11^{70} \equiv 1 \bmod 71^2$.
- $F(11715) = 11715^2$.

Example 3

- $m = 83661685751365 = 5 \cdot 41 \cdot 2953 \cdot 138200401.$
- Survives F-test, but fails Turyn test!
  - $r = 5 \cdot 2953,\ s = 138200401^2 r^2.$
  - $5^{19576834465819410 0} \equiv -1 \bmod s/5^2.$
  - $2953^{2387418837295050} \equiv -1 \bmod s/2953^2.$
  - $rs > 2n.$

Prior Work

- M. (2009):
  If a Barker sequence of length n exists,
  then either

  $$n = 189\ 260\ 468\ 001\ 034\ 441\ 522\ 766\ 781\ 604,$$

  or $n > 2 \cdot 10^{30}$.

- Leung & Schmidt (2012):
  Three new restrictions for the CHM
  problem.

- Two apply to the Barker sequence problem.

Prior Work

- Leung & Schmidt (2012):
  If a Barker sequence of length n exists,
  then $n > 2 \cdot 10^{30}$.

One New Criterion

- **Theorem** (LS, 2012): If $p^a \mid\mid m$ with p odd, $p^{2a} > 2m$, $r \mid m/p^a$ is self-conjugate mod p, and

$$\gcd(\mathrm{ord}_p(q_1), \ldots, \mathrm{ord}_p(q_s)) > m^2/r^2p^{2a},$$

where $q_1, \ldots, q_s$ are the prime divisors of m/rp^a, then there is no CHM of order $4m^2$.

$n = 189\ 260\ 468\ 001\ 034\ 441\ 522\ 766\ 781\ 604,$

$m = 13 \cdot 41 \cdot 2953 \cdot 138200401,$

$p = 138200401,\ r = 2953,$

$\gcd(\mathrm{ord}_p(13), \mathrm{ord}_p(41)) = 959725 > 13^2 \cdot 41^2.$

Strategy

Searching

- Focus on F-test: need $F(m) \geq m\varphi(m)$.
  - $F(m) = \gcd\left(m^2, \prod_{p|m} p^{b(p,m)}\right)$.
  - $b(p,m) = \max_{\substack{q|m \\ q \neq p}} \left\{\nu_p(q^{p-1} - 1) + \nu_p(\mathrm{ord}_{m_q}(q))\right\}$.
- Simplification 1: m is squarefree.

- Simplification 2: $F(m) = m^2$ (or $m^2/3$).
  - Need $\boldsymbol{F(m) \geq m\varphi(m) = m^2 \prod_{p|m} \left(1 - \frac{1}{p}\right)}$.
  - If $\boldsymbol{F(m) \leq m^2/r}$ for some $\boldsymbol{r \mid m}$ then

$$\boldsymbol{\prod_{p|m} \left(1 - \frac{1}{p}\right)^{-1} \geq r.}$$

  - Barker: $r \geq 5$ cannot occur in the range considered.
  - CHM: only $r = 3$ is plausible.
  - Almost always need each $b(p, m) = 2$.

Searching

- For each $p \mid m$, we require either
  - $q^{p-1} \equiv 1 \bmod p^2$ for some prime $q \mid m$, or
  - $p \mid \mathrm{ord}_{m/q}(q)$ for some prime $q \mid m$.
- Former: (q, p) is a *Wieferich prime pair*.
- Latter: Requires $p \mid (r-1)$ for some prime $r \mid m$.

Wieferich Prime Pairs

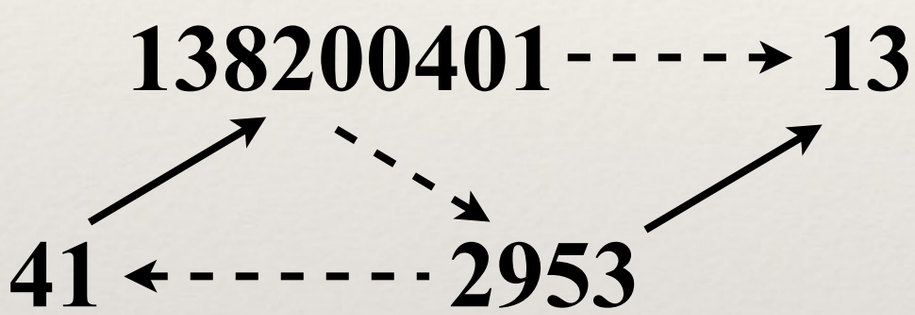
- "First case" of Fermat's Last Theorem.
  - Suppose $x^p + y^p = z^p$ with p not a factor of x, y, or z.
  - Wieferich (1909): $2^{p-1} \equiv 1 \bmod p^2$.
  - Mirimanoff, Vandiver, Granville, et al.: $q^{p-1} \equiv 1 \bmod p^2$ for $q \leq 113$.
- Catalan's Conjecture.
  - (Mihăilescu) If $x^p - y^q = 1$, then $q^{p-1} \equiv 1 \bmod p^2$ and $p^{q-1} \equiv 1 \bmod q^2$.

Search Strategy

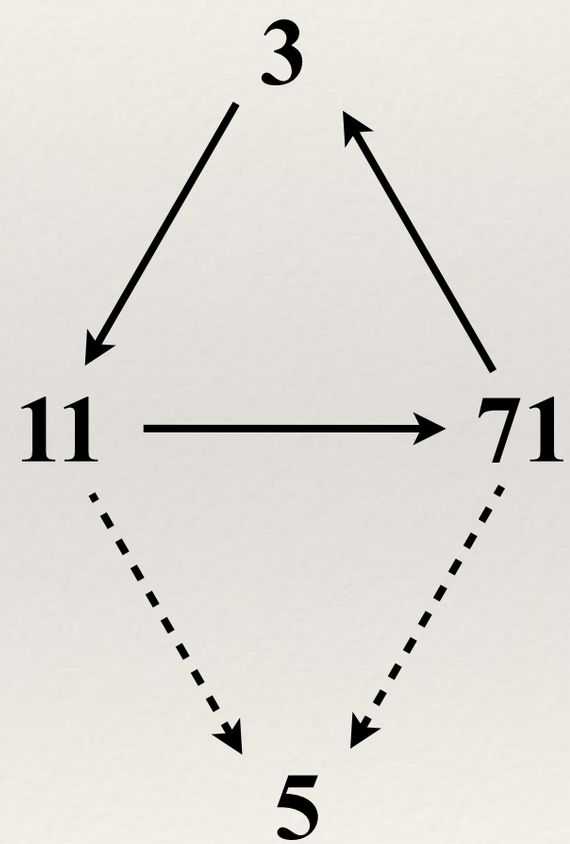
- Wish to find all permissible $m \leq M$.
- Create a directed graph, $D = D(M)$.
- Vertices: subset of primes $p \leq M$.
- Directed edge from q to p in two cases:
  - (Solid edge) $q^{p-1} \equiv 1 \bmod p^2$.
  - (Flimsy edge) $p \mid (q-1)$.
- So p is (probably) allowed if $q \mid m$ also.
- Need a subset of vertices where each indegree is positive in the induced subgraph.

Examples

Barker



CHM



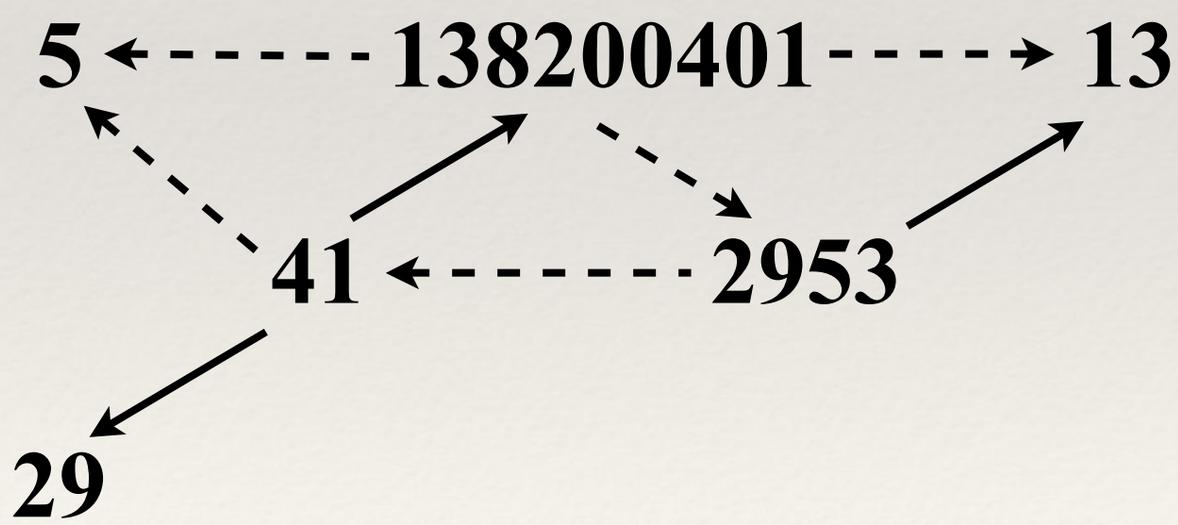
Algorithms

- Ascending Wieferich pair search.
- Graph closure.
- Cycle enumeration.
- Cycle augmentation.
- Verify flimsy links.
- Check for non-squarefree multiples.
- Turyn self-conjugacy test.
- Leung & Schmidt new criteria.

Current Result

- **Theorem** (Borwein & M., 2014): If $n > 13$ is the length of a Barker sequence, then either

$n = 3\ 979\ 201\ 339\ 721\ 749\ 133\ 016\ 171\ 583\ 224\ 100$,
or $n > 4 \cdot 10^{33}$.



Computation

- Set $M = 10^{16.5}$.
- D: 608246 vertices, 950456 solid edges, 665640 flimsy edges.
- 4656 cycles.
- Produces seven new possible $n < 4 \cdot 10^{33}$.
- Turyn test: Eliminates three.
- New Leung & Schmidt: Eliminates three.

More Results

- Existing graph produces many more integers surviving the F-test.
- How many survive the other requirements?
- $4 \cdot 10^{33} \leq n \leq 10^{50}$:

$\Omega(m)$	All	Turyn	LS5	LS1	Survive
3	7	7			0
4	27	25	0	0	2
5	46	44	0	0	2
6	41	35	0	0	6
7	11	4	0	0	7
8	1	0	0	0	1
Total	133	115	0	0	18

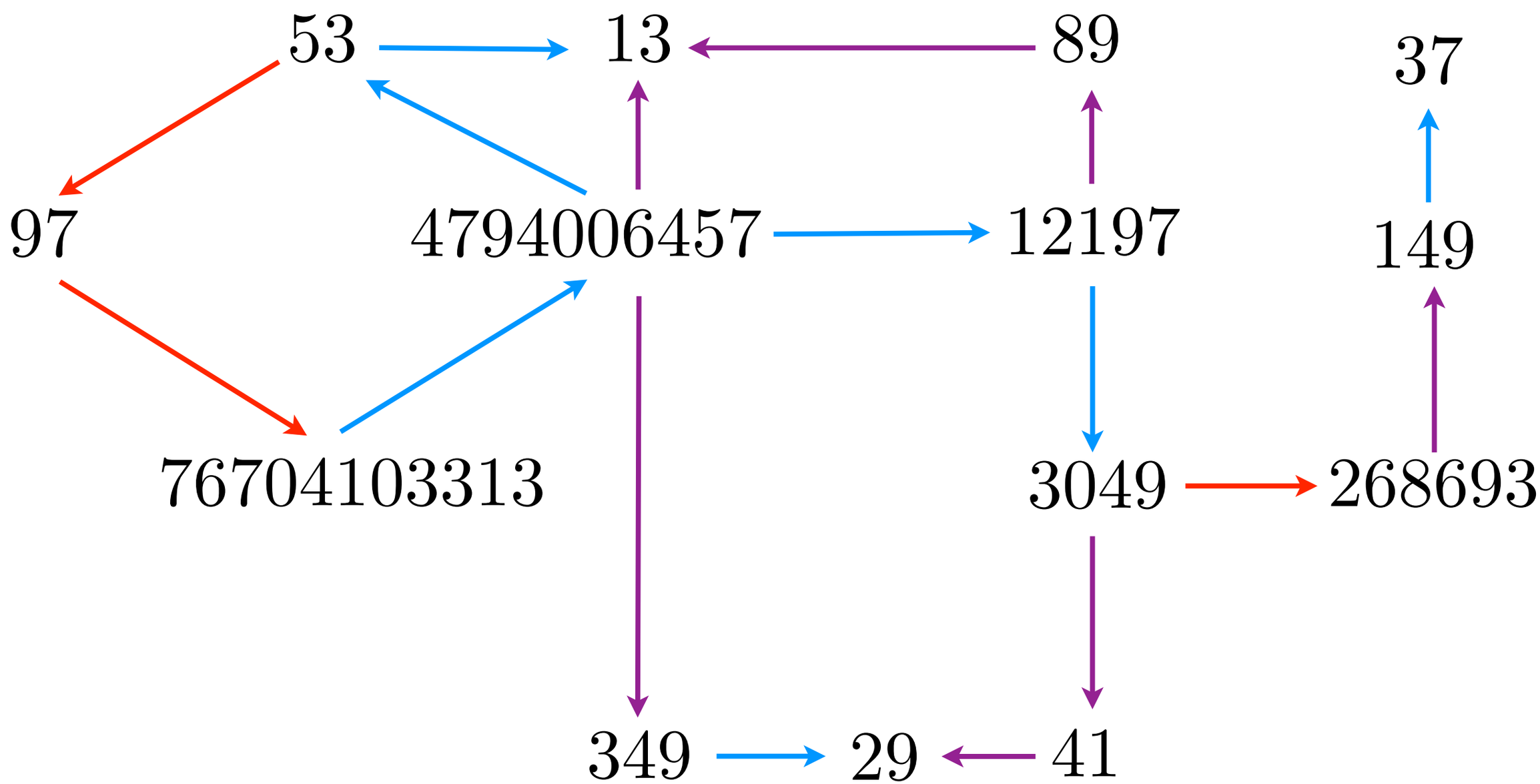
31540455528264605	[5, 13, 29, 41, 2953, 138200401]
66687671978077825	[5, 5, 53, 193, 4877, 53471161]
86693973571501172 5	[5, 5, 13, 53, 193, 4877, 53471161]
129374083637470980 5	[5, 53, 97, 193, 4877, 53471161]
64687041818735490 25	[5, 5, 53, 97, 193, 4877, 53471161]
168186308728712274 65	[5, 13, 53, 97, 193, 4877, 53471161]
84093154364356137325	[5, 5, 13, 53, 97, 193, 4877, 53471161]
248750595852541818170 5	[5, 29, 41, 2953, 1025273, 138200401]
646751549216608727243 3	[13, 29, 41, 2953, 1025273, 138200401]
194172132581492316050 65	[5, 17, 613, 1974353, 188748146801]
323375774608304363621 65	[5, 13, 29, 41, 2953, 1025273, 138200401]
863383081390130269759645	[5, 41, 193, 2953, 53471161, 138200401]
1686504775565176744556405	[5, 13, 29, 41, 2953, 53471161, 138200401]
1890448348089674770182781	[53, 97, 4794006457, 76704103313]
2630496319975038327042325	[5, 5, 193, 24697, 53471161, 412835053]
2988996856098832119836165	[5, 13, 123397, 1974353, 188748146801]
3080894677428239302747085	[5, 5333, 612142549, 188748146801]
3770469237344599632723365	[5, 53, 97, 193, 4877, 2914393, 53471161]
4316915406950651348798225	[5, 5, 41, 193, 2953, 53471161, 138200401]

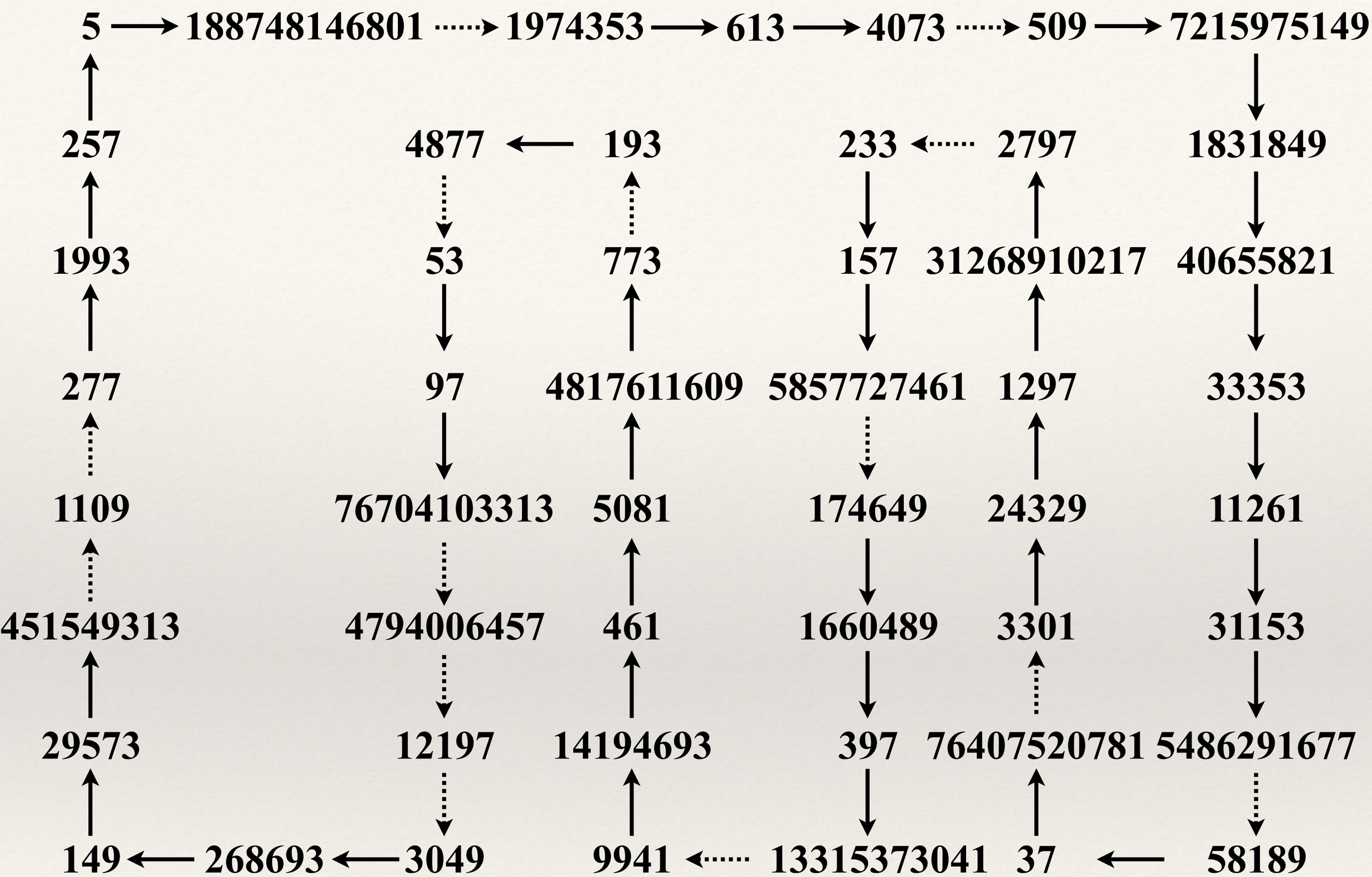
Up to 10^{100} ?

Googol It!

$\Omega(m)$	All	Turyn	LS5	LS1	Survive
2	1	1			0
3	10	10			0
4	48	44	1	0	3
5	185	117	3	0	65
6	701	226	0	2	473
7	2560	326	0		2234
8	8440	321	0		8119
9	22406		0		22406
10	43523		0		43523
11	59673		0		59673
12	55200		0		55200
13	32627		0		32627
14	11266		0		11266
15	2029		0		2029
16	168		0		168
17	21		0		21
Total	238858	1045	4	2	237807

999955077567410874517360407849459812612282402438





2755436158671341757525976576782219699454042358570021561225598389919508345186220260398
1353657973423771968503535527683497044835982229074063017919271703666418112788377048594
1134914837028968297708935740501989512681479798109896011095835642528310561451080108805

Projects

1. Finding New Plausible Values

- Barker: $M = 10^{16.5}$. For second-largest: need $7 \cdot 10^{16}$; third-largest: $9 \cdot 10^{17}$.
- CHM: $M = 10^{13}$. Goal: $M = 5 \cdot 10^{14}$?
- This would add to the 1371 known values that cannot presently be eliminated.
- Use more care to construct graph, e.g., separate case for double Wieferich prime pairs.
- Look for faster methods to compute new Leung & Schmidt tests.

References

- M., *Wieferich pairs and Barker sequences*, Des. Codes Cryptogr. **53** (2009), no. 3, 149-163.
- P. Borwein & M., *Wieferich pairs and Barker sequences, II*, LMS J. Comput. Math. **17** (2014), 24-32.
- K. H. Leung & B. Schmidt, *New restrictions on possible orders of circulant Hadamard matrices*, Des. Codes Cryptogr. **64** (2012), no. 1-2, 143-151.
- www.cecm.sfu.ca/~mjm/WieferichBarker.

2. Double Wieferich Prime Pairs

- $q^{p-1} \equiv 1 \bmod p^2$ and $p^{q-1} \equiv 1 \bmod q^2$.
  - Fix q: can determine residues mod q^2 that p must satisfy.
  - Only need to test about $1/q$ of p's.
- Useful in Barker and CHM searches.
- Could be useful in concert with prior project.
- Keller & Richstein, *Solutions of the congruence* $a^{p-1} \equiv 1 \bmod p^r$, Math. Comp. **74** (2005), no. 250, 927-936: $q < 10^6$, $p < \max(10^{11}, q^2)$.

3. Large Merit Factors

- Experiment with sequences over $\{-1,+1\}$ to find families w. large merit factor (> 6.34).
- Likely hard to find, but last major jump found after experiments by undergraduate students.
- Jedwab, Katz & Schmidt, *Advances in the merit factor problem for binary sequences*, arXiv:1205.0626v2 (2013).

4. Polyphase Barker Sequences

- Generalization of Barker sequences: allow complex numbers of unit modulus.
- Common: demand Hth roots of unity for fixed H.
- Now $c_k = \sum_{i=0}^{n-k-1} \overline{a_i} a_{i+k}$.
- Require $|c_k| \leq 1$ for each k.
- Known to exist for $n \leq 70$ and 72, 76, 77.

4. Polyphase Barker Sequences

- Some polyphase sequences have merit factor $\approx c\sqrt{n}$.
- Experiment with these families, and try variants.
- Perhaps look at other measures of flatness, e.g., Mahler measure.

References

- J. Jedwab, *What can be used instead of a Barker sequence?*, Finite Fields and Applications, Amer. Math. Soc., 2008, pp. 153–178. (Survey.)
- Rapajic & Kennedy, *Merit factor based comparison of new polyphase sequences*, IEEE Commun. Lett. **2** (1998), no. 10, 269-270. (Interesting polyphase seqs.)
- K.-U. Schmidt (arXiv, 2013), Mercer (IEEE Trans. Info. Th., 2013). (Analysis of merit factors for polyphase seqs.)

Miscellaneous References

- Barker sequence problem stated as a problem on irreducible polynomials: Borwein, Choi & Jankauskas, *On a class of polynomials related to Barker sequences*, Proc. Amer. Math. Soc. 140 (2012), no. 8, 2613–2625.
- Analytic formulations: Borwein & M., *Flat polynomials and Barker sequences*, Number Theory and Polynomials, London Math. Soc. Lecture Note Ser., vol. 352, Cambridge Univ. Press, 2008, pp. 71–88.

Fabulous prizes could be yours if…

Good Luck!