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 \( \pm 1 \).
- For \( 0 \leq k \leq n-1 \), define the \( k^{th} \) 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 small.
- Barker sequence: \( |c_k| \leq 1 \) for \( k > 0 \).
Engineering Motivation

- \{a_i\} ↔ binary digital signal.
- \(c_k\) ↔ output when two signals are out of phase by \(k\) units.
- Peak at \(k = 0\) facilitates synchronization.
- Want \(c_0\) large compared to other \(c_k\).
Example

\[ c_0 = 7 \]
\[ c_1 = 0 \]
\[ c_2 = -1 \]
\[ c_3 = 0 \]
\[ c_4 = -1 \]
\[ c_5 = 0 \]
\[ c_6 = -1 \]
### Barker Sequences

<table>
<thead>
<tr>
<th>$n$</th>
<th>Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>+</td>
</tr>
<tr>
<td>2</td>
<td>++</td>
</tr>
<tr>
<td>3</td>
<td>+++-</td>
</tr>
<tr>
<td>4</td>
<td>++++-</td>
</tr>
<tr>
<td>5</td>
<td>++++-+</td>
</tr>
<tr>
<td>7</td>
<td>++++++-</td>
</tr>
<tr>
<td>11</td>
<td>++++++-+-+++</td>
</tr>
<tr>
<td>13</td>
<td>++++++-+-+++</td>
</tr>
</tbody>
</table>
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 $n > 4$?
• 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 \( \frac{\|f\|_\infty}{\sqrt{n}} > 1 + \epsilon \).
- Stronger form: \( \frac{\|f\|_4}{\sqrt{n}} > 1 + \epsilon \).
Quick Calculation

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

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

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

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

$$= n^2 + 2 \sum_{k=1}^{n-1} c_k^2.$$
• Golay defined the *merit factor* of a sequence $a$ of length $n$ over $\{-1, +1\}$ by

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

• 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 $a$:

$$
MF(f) = \frac{\|f\|_2^4}{\|f\|_4^4 - \|f\|_2^4} = \frac{1}{(\|f\|_4/\sqrt{n})^4 - 1}.
$$
Periodic Barker Sequences
Periodic Barker Sequences

- The $k$th periodic autocorrelation:
  \[ \gamma_k = \sum_{i=0}^{n-1} a_i a(i+k \mod n). \]

- Example:
  \[ \begin{align*}
  \gamma_2 &= a_0 a_2 + a_1 a_3 + \cdots + a_{n-3} a_{n-1} \\
  &+ a_{n-2} a_0 + a_{n-1} a_1 \\
  &= c_2 \gamma_1 + c_{n-2} \gamma_2.
  \end{align*} \]
  \[ \gamma_1 = -1, \quad \gamma_4 = -1. \]

- 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 $a, b = \pm1$ then $ab \equiv a + b - 1 \pmod{4}$.
- $c_k \equiv \sum_i (a_i + a_{i+k}) - (n-k) \pmod{4}$.
- $c_k - c_{k+1} \equiv a_{n-1-k} + a_k - 1 \pmod{4}$.
- $c_{n-1-k} - c_{n-k} \equiv a_{n-1-k} + a_k - 1 \pmod{4}$.
- $c_k - c_{k+1} \equiv c_{n-1-k} - c_{n-k} \pmod{4}$.
- $c_k - c_{k+1} = c_{n-1-k} - c_{n-k}$.
- $\gamma_k = \gamma_{k+1}$ 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 \( c_k \equiv n - k \mod 2 \).
- 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 periodic 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

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

- **Open problem**: Show that if \( H \) is an \( n \times n \) circulant Hadamard matrix with \( \pm1 \) 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 \( H \).
- \( (HH^T)J_n = (nI_n)J_n = nJ_n \).
- \( H(H^TJ_n) = H(eJ_n) = e^2J_n \).
- So \( n = 4m^2 \).
Restriction 2: Self-Conjugacy

- *a* is semiprimitive mod *b*: \( a^j ≡ -1 \mod b \) 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

- $\nu_p(m) = \text{multiplicity of } p \text{ in factorization of } m$.
- $m_q = q\text{-free and squarefree part of } m: m_q = \prod_{\substack{p|m \\ p \neq q}} p$.
- $b(p, m) = \max_{q|m, q \neq p} \{\nu_p(q^{p-1} - 1) + \nu_p(\text{ord}_{m_q}(q))\}$.
- $F(m) = \gcd\left( m^2, \prod_{p|m} p^{b(p,m)} \right)$.

- **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 \( p \equiv 1 \mod 4 \).

• 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

- \( m = 689 = 13 \cdot 53 \).

- \( p = 13: \nu_{13}(53^{12} - 1) + \nu_{13}(\text{ord}_{13}(53)) = 1 \).

- \( p = 53: \nu_{53}(13^{52} - 1) + \nu_{53}(\text{ord}_{53}(13)) = 1 \).

- \( F(689) = 689 \).
Example 2

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

- $m = 83661685751365 = 5 \cdot 41 \cdot 2953 \cdot 138200401$.
- Survives $F$-test, but fails Turyn test!
  - $r = 5 \cdot 2953$, $s = 138200401^2 r^2$.
  - $5^{195768344658194100} \equiv -1 \mod s/5^2$.
  - $2953^{2387418837295050} \equiv -1 \mod s/2953^2$.
- $rs > 2n$. 
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 $p^a \parallel m$ with $p$ odd, $p^{2a} > 2m$, $r \mid m/p^a$ is self-conjugate mod $p$, and

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

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

\[ n = 189\,260\,468\,001\,034\,441\,522\,766\,781\,604, \]
\[ m = 13 \cdot 41 \cdot 2953 \cdot 138200401, \]
\[ p = 138200401, r = 2953, \]
\[ \gcd(\text{ord}_p(13), \text{ord}_p(41)) = 959725 > 13^2 \cdot 41^2. \]
Strategy
Searching

- Focus on $F$-test: need $F(m) \geq m \varphi(m)$.

- $F(m) = \gcd\left( m^2, \prod_{p|m} p^{b(p,m)} \right)$.

- $b(p, m) = \max_{q|m, q \neq p} \left\{ \nu_p(q^{p-1} - 1) + \nu_p(\text{ord}_{m_q}(q)) \right\}$.

- Simplification 1: $m$ is squarefree.
• Simplification 2: $F(m) = m^2$ (or $m^2/3$).
  
  • Need $F(m) \geq m\varphi(m) = m^2 \prod_{p|m} \left(1 - \frac{1}{p}\right)$.

• If $F(m) \leq m^2/r$ for some $r \mid m$ then

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

• 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
  • $q^{p-1} \equiv 1 \mod p^2$ for some prime $q \mid m$, or
  • $p \mid \text{ord}_{m/q}(q)$ 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): $2^{p-1} \equiv 1 \mod p^2$.
- Mirimanoff, Vandiver, Granville, et al.: $q^{p-1} \equiv 1 \mod p^2$ for $q \leq 113$.
- Catalan’s Conjecture.
  - (Mihăilescu) If $x^p - y^q = 1$, then $q^{p-1} \equiv 1 \mod p^2$ and $p^{q-1} \equiv 1 \mod q^2$. 
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) $q^{p-1} \equiv 1 \mod p^2$.
  - (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

\[138200401 \rightarrow 13\]

\[41 \rightarrow 2953\]

CHM

\[3 \rightarrow 11 \rightarrow 71\]

\[5 \rightarrow 11\]
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 \( n > 4 \cdot 10^{33} \).

\[
\begin{align*}
5 \leftarrow & \cdots \cdots 138200401 \rightarrow 13 \\
41 \leftarrow & \cdots \cdots 2953 \\
\end{align*}
\]
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?
- $4 \cdot 10^{33} \leq n \leq 10^{50}$:

<table>
<thead>
<tr>
<th>$\Omega(m)$</th>
<th>All</th>
<th>Turyn</th>
<th>LS5</th>
<th>LS1</th>
<th>Survive</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>7</td>
<td>7</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>27</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>46</td>
<td>44</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>41</td>
<td>35</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>133</td>
<td>115</td>
<td>0</td>
<td>0</td>
<td>18</td>
</tr>
<tr>
<td>Number</td>
<td>Factors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31540455528264605</td>
<td>[5, 13, 29, 41, 2953, 138200401]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66687671978077825</td>
<td>[5, 5, 53, 193, 4877, 53471161]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>866939735715011725</td>
<td>[5, 5, 13, 53, 193, 4877, 53471161]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1293740836374709805</td>
<td>[5, 53, 97, 193, 4877, 53471161]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6468704181873549025</td>
<td>[5, 5, 53, 97, 193, 4877, 53471161]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16818630872871227465</td>
<td>[5, 13, 53, 97, 193, 4877, 53471161]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>84093154364356137325</td>
<td>[5, 5, 13, 53, 97, 193, 4877, 53471161]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2487505958525418181705</td>
<td>[5, 29, 41, 2953, 1025273, 138200401]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6467515492166087272433</td>
<td>[13, 29, 41, 2953, 1025273, 138200401]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19417213258149231605065</td>
<td>[5, 17, 613, 1974353, 188748146801]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32337577460830436362165</td>
<td>[5, 13, 29, 41, 2953, 1025273, 138200401]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>863383081390130269759645</td>
<td>[5, 41, 193, 2953, 53471161, 138200401]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1686504775565176744556405</td>
<td>[5, 13, 29, 41, 2953, 53471161, 138200401]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1890448348089674770182781</td>
<td>[53, 97, 4794006457, 76704103313]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2630496319975038327042325</td>
<td>[5, 5, 193, 24697, 53471161, 412835053]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2988996856098832119836165</td>
<td>[5, 13, 123397, 1974353, 188748146801]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3080894677428239302747085</td>
<td>[5, 5333, 612142549, 188748146801]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3770469237344599632723365</td>
<td>[5, 53, 97, 193, 4877, 2914393, 53471161]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4316915406950651348798225</td>
<td>[5, 5, 41, 193, 2953, 53471161, 138200401]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The table contains pairs of numbers and their factorizations. Each number is paired with a list of its prime factors.
### Up to $10^{100}$?

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

COME ON DOWN
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

- www.cecm.sfu.ca/~mjm/WieferichBarker.
2. Double Wieferich Prime Pairs

- \( q^{p-1} \equiv 1 \mod p^2 \) and \( p^{q-1} \equiv 1 \mod q^2 \).
- 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* \( a^{p-1} \equiv 1 \mod p^r \), *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.
4. Polyphase Barker Sequences

- Generalization of Barker sequences: allow complex numbers of unit modulus.
- Common: demand $H$th roots of unity for fixed $H$.

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

- 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


Fabulous prizes could be yours if…

Good Luck!