Power-spectral Numbers

by

Walter A. Kehowski, Ph.D.
Glendale Community College, AZ 85302
walter.kehowski@gccaz.edu
Recall that modular arithmetic in $\mathbb{Z}_{12}$ is the set of equivalence classes of remainders modulo 12 endowed with operations of addition, subtraction, multiplication and, when possible, division. For example, it is easy to see that

$$8 + 9 = 5,$$
$$5 \cdot 7 = 1,$$
$$2 \cdot 6 = 0, \quad 3 \cdot 4 = 0.$$ 

Consider

$$2^{57} = 8.$$ 

But what about $2^{57}$? Since $2^2 = 4$, $2^3 = 8$, $2^4 = 4$, $\ldots$, it is clear that $2^{\text{even}} = 4$ and $2^{\text{odd}} = 8$. Is there any way that operations in $\mathbb{Z}_{12}$ can be “simplified”? 
$12 = (2)^2(3)$.
Spectral basis: \{9, 4\}.
Index=1.
Observe that, in $\mathbb{Z}_{12}$, we have

\[
9 + 4 = 1, \\
9 \cdot 4 = 0, \\
9^2 = 9, \\
4^2 = 4.
\]

Furthermore, any $x \in \mathbb{Z}_{12}$ can be uniquely decomposed as

\[
x = (x \mod 4) \cdot 9 + (x \mod 3) \cdot 4,
\]

and

\[
x^r = (x^r \mod 4) \cdot 9 + (x^r \mod 3) \cdot 4,
\]

for all positive integers $r$. If $x$ is invertible, then $r$ can be negative as well.
The Spectral Basis Theorem

The elements 9 and 4 in $\mathbb{Z}_{12}$ comprise what is called the *spectral basis* for $\mathbb{Z}_{12}$, or for convenience, the spectral basis of 12. It is a fact that any integer $n$ with at least two prime factors has a spectral basis.

**Theorem 1**

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, $k > 1$, be a positive integer with at least two prime factors. Then there exist elements $s_1, s_2, \ldots, s_k$ of $\mathbb{Z}_n$ with the following properties:

\begin{align*}
  s_1 + s_2 + \cdots + s_k &= 1 \quad (1) \\
  s_i^2 &= s_i, 1 \leq i \leq k, \quad (2) \\
  s_is_j &= 0, i \neq j, \quad (3) \\
  x = (x^r \mod p_1^{e_1}) \cdot s_1 + \cdots + (x^r \mod p_k^{e_k}) \cdot s_k, (r \geq 0). \quad (4)
\end{align*}

We call \{s_1, s_2, \ldots, s_k\} the spectral basis of $\mathbb{Z}_n$, or, for convenience, the spectral basis of $n$. 
Proof of the Spectral Basis Theorem, 1/2

Define the map \( \psi : \mathbb{Z} \to M, M := \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}} \), by

\[
\psi(x) = (\psi_1(x), \psi_2(x), \ldots, \psi_k(x)), \quad \psi_i(x) = x \mod p_i^{e_i}.
\]

Let us first find the image of \( \psi \). Given \( \gamma = (\tilde{\gamma}_1, \ldots, \tilde{\gamma}_k) \), there exists \( x \in \mathbb{Z} \) such that \( \psi(x) = \gamma \) if and only if \( x \equiv \tilde{\gamma}_i \mod p_i^{e_i} \) for all \( i = 1, \ldots, k \). Since the primary factors of \( n \) are pairwise relatively prime, by the Chinese Remainder Theorem the system of congruences has a solution, and so \( \psi \) is a ring epimorphism.

Next, let us find the kernel of \( \psi \). The kernel is all \( x \in \mathbb{Z} \) such that \( x \equiv 0 \mod p_i^{e_i} \) for all \( i \), that is, if and only if \( x \) is divisible by \( n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \). Consequently, the kernel of \( \psi \) is the ideal \( n\mathbb{Z} \) and the induced map \( \bar{\psi} : \mathbb{Z}/n\mathbb{Z} \to M \) is an isomorphism.
The direct sum $M := \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$, has canonical projections $\pi_i : M \to \mathbb{Z}_{p_i^{e_i}}$ given by $\pi_i(n_1, \ldots, n_k) = n_i$ that satisfy

\[
\pi_1 + \cdots + \pi_k = \text{Id}, \\
\pi_i^2 = \pi_i, \\
\pi_i \pi_j = 0, (i \neq j).
\]

What elements $s_i$ of $\mathbb{Z}_n$ correspond to the projections $\pi_i$ of $M$? Define $h_i := n/p_i^{e_i}$. Since $h_1, \ldots, h_k$ are pairwise relatively prime, there exists integers $a_1, \ldots, a_k$ in $\mathbb{Z}_n$ such that

\[
a_1 h_1 + \cdots + a_k h_k = 1 \quad \text{in } \mathbb{Z}_n.
\]

It can be shown that $s_i := a_i h_i = (h_i^{-1} \mod p_i^{e_i}) h_i$ have the properties

\[
s_1 + \cdots + s_k = 1, \\
s_i^2 = s_i, \\
s_i s_j = 0, (i \neq j).
\]
Power-spectral numbers

**Definition 2**
A positive integer is *power-spectral* if its spectral basis consists of primes or powers.

**Examples 3**

1. \{3, 4\} is the spectral basis for 6.
2. \{9, 4\} is the spectral basis for 12.
3. \{7, 8\} is the spectral basis for 14.
4. \{9, 16\} is the spectral basis for 24.
5. \{15^2, 2^6\} is the spectral basis for 288 = (2)^5\,(3)^2.
6. \{15^2, 20^2, 24^2\} is the spectral basis for 600 = (2)^3\,(3)(5)^2.
Theorem 4
The number $2p^k$ has spectral basis $\{p^k, p^k + 1\}$.

Corollary 5
The number $2M_p$ has spectral basis $\{M_p, 2^p\}$.

Examples 6
1. $\{3, 2^2\}$ is the spectral basis for $2 \cdot 3$.
2. $\{7, 2^3\}$ is the spectral basis for $2 \cdot 7$.
3. $\{31, 2^5\}$ is the spectral basis for $2 \cdot 31$.
4. $\{127, 2^7\}$ is the spectral basis for $2 \cdot 127$. 
Theorem 7
Let $M_p$ be a Mersenne prime with Mersenne exponent $p$. Then the following numbers are power-spectral.

1. $2M_p$ has spectral basis $\{M_p, 2^p\}$ or, equivalently, $\{M_p, M_p + 1\}$.

2. $2^p M_p$ has spectral basis $\{M_p^2, 2^p\}$ or, equivalently, $\{M_p^2, M_p + 1\}$.

3. $2^{p+1} M_p$ has spectral basis $\{M_p^2, 2^{2p}\}$ or, equivalently, $\{M_p^2, (M_p + 1)^2\}$

4. $2^{2p+1} M_p^2$ has spectral basis $\{M_p^2 (M_p + 2)^2, (M_p^2 - 1)^2\}$.
It is easily shown that $2^a + 1$ can be prime if and only if $a$ is a power of 2. The number $F_i = 2^{2^i} + 1$, $i \geq 0$, is called a Fermat number and a Fermat prime when it is prime. The only known Fermat primes are $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$.

**Theorem 8**

If $F_i = 2^{f_i} + 1$ is a Fermat prime with exponent $f_i = 2^i$, $i \geq 0$, then

1. $2^{f_i}F_i$ has spectral basis $\{F_i, 2^{2f_i}\}$.
2. $2^{f_i+1}F_i$ has spectral basis $\{F_i^2, 2^{2f_i}\}$.
3. $2^{2f_i+1}F_i^2$ has spectral basis $\{(F_i - 2)^2F_i^2, (F_i^2 - 1)^2\}$. 
Consider the number $20439 = 3^3 \cdot 757$. Let us verify that \( \{757, 3^9\} \) is the spectral basis for 20439. Clearly, 
\[
757 + 3^9 = 20440 \equiv 1 \mod 20439 \text{ and } 757 \cdot 3^9 \equiv 0 \mod 20439.
\]
Further,
\[
757^2 - 757 = 757 \cdot 756 = 757 \cdot 2^2 \cdot 3^3 \cdot 7 \\
= 2^2 \cdot 7 \cdot (3^3 \cdot 757) \equiv 0 \mod 20439.
\]
\[
(3^9)^2 - 3^9 = 3^9(3^9 - 1) = 3^9 \cdot 2 \cdot 13 \cdot 757 \\
= 2 \cdot 3^6 \cdot 13 \cdot (3^3 \cdot 757) \equiv 0 \mod 20439.
\]

Are 757 and $3^9$ related? The key is the decomposition of the identity.
Cyclotomic primes, 2/3

\[ 757 + 3^9 = 3^3 \cdot 757 + 1 \]
\[ 3^9 - 1 = 3^3 \cdot 757 - 757 \]
\[ 3^9 - 1 = (3^3 - 1)(757) \]
\[ 757 = \frac{3^9 - 1}{3^3 - 1} \]

Definition 9
The number \( \Phi_{re}(p) = \frac{p^{re} - 1}{p^{re-1} - 1} \), where \( p \) and \( r \) are primes and \( e \geq 1 \), when prime, is called a cyclotomic prime.

**NOTE:** \( \Phi_{re}(x) = \frac{x^{re} - 1}{x^{re-1} - 1} \) can be prime when \( x \) is composite but we are only interested in the case when \( x \) is prime.
Theorem 10
The number \( p^{re-1} \Phi_{re}(p) \) has spectral basis \( \{ \Phi_{re}(p), p^{re} \} \), where \( \Phi_{re}(p) \) is a cyclotomic prime.

Proof.
The decomposition of the identity follows from the requirement that \( \Phi_{re}(p) \) is prime. Let’s verify the projection property for \( q = \Phi_{re}(p) \). Observe that

\[
q^2 - q = q(q - 1) = q \left( \frac{p^{re} - 1}{p^{re-1} - 1} - 1 \right)
= q \left( \frac{p^{re} - p^{re-1}}{p^{re-1} - 1} \right)
= p^{re-1} q \left( \frac{p^{re-re-1} - 1}{p^{re-1} - 1} \right)
\equiv 0 \pmod{p^{re-1} q}.
\]

Exercise: \( (p^{re})^2 \equiv p^{re} \pmod{p^{re-1} q} \).
Power-spectral numbers $9p^{2s}q^{2t}, 1/3$

Of natural interest are primes solutions to $q^t = 2p^s \pm 1$ with $s, t \geq 1$. For example, **Sophie-Germain primes** are primes of the form $q = 2p + 1$ and **Cunningham primes** are of the form $q = 2p - 1$. It is open question whether or not there are infinitely many primes of the form $q = 2p \pm 1$.

**Theorem 11 (Pell equation)**

*The equations* $x^2 - 2y^2 = \pm 1$ *have infinitely many integer solutions. The only prime solution to* $x^2 - 2y^2 = 1$ *is* $(x, y) = (3, 2)$. *The only prime solutions to* $x^2 - 2y^2 = -1$ *known so far are*

$$(7)^2 = 2(5)^2 - 1$$

$$(41)^2 = 2(29)^2 - 1$$

$$(63018038201)^2 = 2(44560482149)^2 - 1$$

$$(19175002942688032928599)^2 = 2(13558774610046711780701)^2 - 1$$
Theorem 12 (Ljungren, 1942)

The only positive integer solutions to \( y^2 = 2x^4 - 1 \) are \((x, y) = (1, 1)\) and \((13, 239)\), and the only prime solution is \((13, 239)\).

Theorem 13 (Crescenzo, 1975)

The only solutions to \( q^t = 2p^s \pm 1, s, t > 1 \), for primes \( p \) and \( q \) occur only for \((s, t) = (2, 2)\) and \((4, 2)\).

Theorem 14 (Solutions to \( q^t = 2p^s \pm 1 \))

The only prime solutions to \( q^t = 2p^s \pm 1, s, t \geq 1 \), occur for \((s, 1), (1, t), (2, 2), \) and \((4, 2)\).
Theorem 15

Suppose $q^t = 2p^s \pm 1$ has prime solutions, $p, q \neq 3$, for some positive integers $s$ and $t$. Then $9p^{2s}q^{2t}$ has spectral basis

$$\{p^{2s}q^{2t}, 4(p^{2s} - 1)^2, 16(p^2 \pm 1)p^{2s}\}.$$ 

Definition 16 (Ljungren’s number)

Ljungren’s number is defined to be the power-spectral number

$$3^2(13)^8(239)^4 = 23954159206871641449.$$ 

It is the unique power-spectral number of the form $9p^8q^4$ where $p$ and $q$ are prime.
Mersenne II, 1/2

Theorem 17
Let $M_p$ is a Mersenne prime with Mersenne exponent $p > 2$. Then

1. $2^{2p-1} \cdot 3 \cdot M_p^2$ has power-spectral basis
   \[
   \left\{ M_p^2 (M_p + 2)^2, M_p^2 (M_p + 1)^2, (M_p^2 - 1)^2 \right\}
   \]
   of index 2.

2. $2^{2p} \cdot 3 \cdot M_p^2$ has power-spectral basis
   \[
   \left\{ M_p^2 (M_p + 2)^2, M_p^2 (M_p + 1)^2, (M_p^2 - 1)^2 \right\}.
   \]

3. $2^{2p+1} \cdot 3 \cdot M_p^2$ has power-spectral basis
   \[
   \left\{ M_p^2 \left( M_p + 2 \right)^2, 4M_p^2 (M_p + 1)^2, (M_p^2 - 1)^2 \right\}.
   \]

The numbers 1 and 2 comprise an isospectral pair. See 22.
Theorem 18
Let $M_p$ be a Mersenne prime with Mersenne exponent $p > 2$. Then

1. $2^{2p-3} \cdot 3^2 \cdot M_p^2$ has power-spectral basis

   \[
   \left\{ M_p^2 (M_p + 2)^2, \frac{1}{4} M_p^2 (M_p + 1)^2, (M_p^2 - 1)^2 \right\}
   \]

   of index 2.

2. $2^{2p-2} \cdot 3^2 \cdot M_p^2$ has power-spectral basis

   \[
   \left\{ M_p^2 (M_p + 2)^2, \frac{1}{4} M_p^2 (M_p + 1)^2, (M_p^2 - 1)^2 \right\}
   \]

3. $2^{2p+1} \cdot 3^2 \cdot M_p^2$ has power-spectral basis

   \[
   \left\{ M_p^2 (M_p + 2)^2, 16 M_p^2 (M_p + 1)^2, (M_p^2 - 1)^2 \right\}
   \]

Furthermore, the numbers 1 and 2 comprise an isospectral pair.
See 22.
Theorem 19
Let $F_i$ be a Fermat prime with exponent $f_i = 2^i$. Then the following numbers are power-spectral.

1. $2^{2^{f_i-1}} \cdot 3 \cdot F_i^2$ has power-spectral basis
   $\{(F_i - 2)^2 F_i^2, (F_i - 1)^2 \cdot F_i^2, (F_i^2 - 1)^2\}$. with index 2.

2. $2^{2^{f_i}} \cdot 3 \cdot F_i^2$ has power-spectral basis
   $\{(F_i - 2)^2 F_i^2, (F_i - 1)^2 F_i^2, (F_i^2 - 1)^2\}$.

3. $2^{2^{f_i+1}} \cdot 3 \cdot F_i^2$ has power-spectral basis
   $\{(F_i - 2)^2 F_i^2, 4(F_i - 1)^2 \cdot F_i^2, (F_i^2 - 1)^2\}$.

Furthermore, 1 and 2 form an isospectral pair. See 22.
Theorem 20

Let $F_i$ be a Fermat prime with Fermat exponent $f_i = 2^i$. Then

1. $2^3 \cdot 9 \cdot 5^2$ has power-spectral basis

\[ \{3^25^2, 2^35^3, 2^63^2\}. \]

2. $2^{2f_i-3} \cdot 9 \cdot F_i^2$ has power-spectral basis

\[ \left\{ (F_i - 2)^2F_i^2, \frac{1}{4}(F_i - 1)^2F_i^2, (F_i^2 - 1)^2 \right\}. \]

with index 2.

3. $2^{2f_i-2} \cdot 9 \cdot F_i^2$ has power-spectral basis

\[ \left\{ (F_i - 2)^2F_i^2, \frac{1}{4}(F_i - 1)^2F_i^2, (F_i^2 - 1)^2 \right\}. \]

4. $2^{2f_i+1} \cdot 9 \cdot F_i^2$, has power-spectral basis

\[ \left\{ (F_i - 2)^2F_i^2, 16(F_i - 1)^2F_i^2, (F_i^2 - 1)^2 \right\}. \]

Furthermore, the numbers of Theorem 2 and Theorem 3 form an isospectral pair for $i = 2, 3, 4$. See 22.
Isospectral chains, 1/3

The pair \( \{84, 42\} \) both have the same spectral basis, namely, \( \{21, 28, 36\} \). Two numbers will be called *isospectral* if they have the same spectral basis. Let’s look at the decomposition of the identity.

\[
\begin{align*}
21 + 28 + 36 &= 2 \cdot 42 + 1 \equiv 1 \pmod{42}, \\
21 + 28 + 36 &= 1 \cdot 84 + 1 \equiv 1 \pmod{84}.
\end{align*}
\]

We say that 42 has index 2 and that 84 has index 1 and that \( \{84, 42\} \) comprise an *isospectral pair*.

**Definition 21 (Isospectral pair)**

An *isospectral pair* is a pair of integers \( \{n_1, n_2\} \) such that \( n_1 = 2n_2 \), both have the same spectral basis, and of index 1 and 2, respectively.

<table>
<thead>
<tr>
<th>( n_1 )</th>
<th>( n_1 ) factored</th>
<th>{spectral basis}</th>
</tr>
</thead>
<tbody>
<tr>
<td>84</td>
<td>( (2)^2(3)(7) )</td>
<td>{21, 28, 36}</td>
</tr>
<tr>
<td>228</td>
<td>( (2)^2(3)(19) )</td>
<td>{57, 76, 96}</td>
</tr>
<tr>
<td>280</td>
<td>( (2)^3(5)(7) )</td>
<td>{105, 56, 120}</td>
</tr>
<tr>
<td>340</td>
<td>( (2)^2(5)(17) )</td>
<td>{85, 136, 120}</td>
</tr>
</tbody>
</table>
Definition 22
An isospectral chain of length $k$ is defined to be a finite sequence of pairwise isospectral numbers $n_1, \ldots, n_k$, such that $n_i$ has index $i$ and

$$n_1 + 1 = 2n_2 + 1 = \cdots = kn_k + 1,$$

or, equivalently,

$$n_1 = 2n_2 = \cdots = kn_k.$$

It will be assumed that the chain length $k$ is maximal, that is, $n_1/(k + 1)$ is not isospectral with $n_1$. 

### Maximal isopectral chains of length 3.

<table>
<thead>
<tr>
<th>$n_1$</th>
<th>$n_1$ factored</th>
<th>{Multiple iso-spectrals}</th>
</tr>
</thead>
<tbody>
<tr>
<td>10980</td>
<td>$(2)^2(3)^2(5)(61)$</td>
<td>{2745, 2440, 2196, 3600}</td>
</tr>
<tr>
<td>35280</td>
<td>$(2)^4(3)^2(5)(7)^2$</td>
<td>{11025, 7840, 7056, 9360}</td>
</tr>
<tr>
<td>36180</td>
<td>$(2)^2(3)^3(5)(67)$</td>
<td>{9045, 10720, 7236, 9180}</td>
</tr>
<tr>
<td>43380</td>
<td>$(2)^2(3)^2(5)(241)$</td>
<td>{10845, 9640, 8676, 14220}</td>
</tr>
</tbody>
</table>

### Maximal isopectral chains of length 4.

<table>
<thead>
<tr>
<th>$n_1$</th>
<th>$n_1$ factored</th>
<th>{Multiple iso-spectrals}</th>
</tr>
</thead>
<tbody>
<tr>
<td>488880</td>
<td>$(2)^4(3)^2(5)(7)(97)$</td>
<td>{91665, 108640, 97776, 69840, 120960}</td>
</tr>
<tr>
<td>1525680</td>
<td>$(2)^4(3)^2(5)(13)(163)$</td>
<td>{286065, 339040, 305136, 352080, 243360}</td>
</tr>
<tr>
<td>2870280</td>
<td>$(2)^3(3)^2(5)(7)(17)(67)$</td>
<td>{358785, 637840, 574056, 410040, 675360, 214200}</td>
</tr>
<tr>
<td>4930272</td>
<td>$(2)^5(3)^2(17)(19)(53)$</td>
<td>{1078497, 1095616, 1160064, 1037952, 558144}</td>
</tr>
</tbody>
</table>
Isotropic numbers, 1/4

- Recall that $42 = 2 \cdot 3 \cdot 7$ is the first number of index 2 with spectral basis $\{21, 28, 36\}$. Since $\{1 \cdot 21, 2 \cdot 14, 6 \cdot 6\}$, we call $\{1, 2, 6\}$ the spectral coefficients of 42.
- Consider the product of twin primes $3 \cdot 5 = 15$, with spectral basis $\{10, 6\}$. Observe that $10 = 2 \cdot 5$ and $6 = 3 \cdot 2$ so that the spectral coefficients of 15 are $\{2, 2\}$.

**Definition 23 (Isotropic number)**
A number is isotropic if all its spectral coefficients are equal.

**Theorem 24**
The product of twin primes is isotropic.

**Proof.**
Let $p$ and $q = p + 2$ be prime. Then $aq + ap = pq + 1$ so that $a = (pq + 1)/(p + q) = (p^2 + 2p + 1)/(2p + 2) = (p + 1)^2/(2(p + 1)) = (p + 1)/2$. It can shown that $\{aq, ap\}$ is in fact the spectral basis for $pq$. □
Theorem 25
If $p$ and $q$ are primes or prime powers, and if

$$a = (pq + 1)/(p + q)$$

is an integer, then $pq$ is isotropic with spectral coefficient $a$.

<table>
<thead>
<tr>
<th>Powerful isotropic numbers with two factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1728 (2)$^6$(3)$^3$ {513, 1216}</td>
</tr>
<tr>
<td>675  (3)$^3$(5)$^2$ {325, 351}</td>
</tr>
<tr>
<td>7092899 (11)$^3$(73)$^2$ {5675385, 1417515}</td>
</tr>
<tr>
<td>7138196909 (29)$^3$(541)$^2$ {6589127353, 549069557}</td>
</tr>
</tbody>
</table>
Theorem 26 (Isotropic number theorem)

Let \( n = P_1 \cdots P_k \) be a product of distinct primes or prime powers. Let \( \bar{P}_i = n/P_i \) and suppose that

\[
a = (n + 1)/(\bar{P}_1 + \cdots + \bar{P}_k)
\]

is an integer. Then \( n \) is isotropic with spectral coefficient \( a \) and spectral basis \( \{a\bar{P}_1, \ldots, a\bar{P}_k\} \).

Isotropic numbers with more than two factors

<table>
<thead>
<tr>
<th>( n )</th>
<th>( a )</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>(2)(3)(5)</td>
</tr>
<tr>
<td>429</td>
<td>(3)(11)(13)</td>
</tr>
<tr>
<td>858</td>
<td>(2)(3)(11)(13)</td>
</tr>
<tr>
<td>861</td>
<td>(3)(7)(41)</td>
</tr>
<tr>
<td>1722</td>
<td>(2)(3)(7)(41)</td>
</tr>
<tr>
<td>2300</td>
<td>(2)^2(5)^2(23)</td>
</tr>
</tbody>
</table>
Isotropic numbers of immediate interest are those with $a = 1$, called\footnote{cancelable}, since the spectral basis is found by deletion of prime factors.

<table>
<thead>
<tr>
<th>Isotropc numbers $a = 1$</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>(2)(3)(5)</td>
</tr>
<tr>
<td>858</td>
<td>(2)(3)(11)(13)</td>
</tr>
<tr>
<td>1722</td>
<td>(2)(3)(7)(41)</td>
</tr>
<tr>
<td>66198</td>
<td>(2)(3)(11)(17)(59)</td>
</tr>
</tbody>
</table>

A search on the Online Encyclopedia of Integer Sequences, https://oeis.org/, reveals the following:

A007850 \textbf{Giuga numbers}: composite numbers $n$ such that $p$ divides $n/p - 1$ for every prime divisor $p$ of $n$.

30, 858, 1722, 66198, 2214408306, 24423128562, …

It is easy to show that ever Giuga number is cancelative.

\textbf{Conjecture 1}

\textit{A number is cancelative if and only if it is Giuga.}
Recall that the Fibonacci sequence is defined recursively by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$. Since $F_m | F_n$ whenever $m | n$, $F_n$ can be prime only when $n$ is prime.

**Lemma 27**

Let $p$ be a prime such that $F_p$ is prime. Then

$$F_p \equiv \left( \frac{5}{p} \right) \pmod{p},$$

where $(5|p)$ is the Legendre symbol defined by

$$\left( \frac{5}{p} \right) = \begin{cases} 1 & \text{if } p \equiv 1, 4 \pmod{5}; \\ -1 & \text{if } p \equiv 2, 3 \pmod{5}. \end{cases}$$
Theorem 28

Let \( p \neq 5 \) be a prime such that \( F_p \) is prime. Then \( pF_p \) has spectral basis

\[
\begin{align*}
\{F_p, pF_p - F_p + 1\} & \quad \text{whenever } p \equiv 1, 4 \pmod{5}, \\
\{(p - 1)F_p, F_p + 1\} & \quad \text{whenever } p \equiv 2, 3 \pmod{5}.
\end{align*}
\]
Recall that the Lucas sequence is defined recursively by $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$, $n \geq 2$. Since $L_m | L_n$ whenever $m | n$ and $n/m$ is odd, $L_n$ can be prime only when $n$ is prime or a power of 2.

**Lemma 29**

1. Let $p$ be a prime such that $L_p$ is prime. Then $L_p \equiv 1 \mod p$.
2. If $L_{2m}$ is prime, then $L_{2m} \equiv -1 \mod p$.

**Theorem 30**

1. If $p$ is a prime such that $L_p$ is prime, then $pL_p$ has spectral basis $\{L_p, pL_p - L_p + 1\}$.
2. If $L_{2m}$ is prime, then $2^m L_{2m}$ has spectral basis $\{(2^m - 1)L_{2m}, L_{2m} + 1\}$.

**NOTE:** $L_{2m}$ is known to be prime only for $m = 1, 2, 3, 4$, just like the Fermat primes.