THE PERIOD OF $\frac{1}{P}$ AND OF THE FIBONACCI SEQUENCE MOD $P$

Jody Radowicz

SENIOR HONORS THESIS
Submitted in Partial fulfillment of Requirements of the
College Scholars Program
North Central College

May 31, 2002

Approved: David Schmitz Date: 5/31/02
Thesis Director

Approved: Steve Renk Date: 5/30/02
Second Reader
Chapter 1

The Period of $\frac{1}{n}$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\frac{1}{n}$</th>
<th>Decimal Representation of $\frac{1}{n}$</th>
<th>$T(\frac{1}{n})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/1</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1/2</td>
<td>0.5</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1/3</td>
<td>0.33333333333333333333333333333333...</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1/4</td>
<td>0.25</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1/5</td>
<td>0.2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1/6</td>
<td>0.16666666666666666666666666666666...</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1/7</td>
<td>0.1428571428571428571428571428571428...</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>1/8</td>
<td>0.125</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1/9</td>
<td>0.11111111111111111111111111111111...</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1/10</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1/11</td>
<td>0.09090909090909090909090909090909...</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>1/12</td>
<td>0.08333333333333333333333333333333...</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>1/13</td>
<td>0.0769230769230769230769230769230769...</td>
<td>6</td>
</tr>
<tr>
<td>14</td>
<td>1/14</td>
<td>0.0714285714285714285714285714285714...</td>
<td>6</td>
</tr>
<tr>
<td>15</td>
<td>1/15</td>
<td>0.06666666666666666666666666666666...</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>1/16</td>
<td>0.0625</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>1/17</td>
<td>0.0588235294117647058823529411764705...</td>
<td>16</td>
</tr>
<tr>
<td>18</td>
<td>1/18</td>
<td>0.0555555555555555555555555555555555...</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>1/19</td>
<td>0.0526315789473684210526315789473684...</td>
<td>18</td>
</tr>
<tr>
<td>20</td>
<td>1/20</td>
<td>0.05</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>1/21</td>
<td>0.0476190476190476190476190476190476...</td>
<td>6</td>
</tr>
</tbody>
</table>

Figure 1 a.k.a. "The Chart that Starts It All"

Initial Observations

Above, Figure 1 contains the decimal representations and periods of $\frac{1}{n}$ for $1 \leq n \leq 21$.

Before we get into exactly what a period of a decimal is, let's notice some patterns about the decimal representations of $\frac{1}{n}$. The big question is "Is there a way to determine the period of $\frac{1}{n}$ for all integers $n$?" This is the question to focus on throughout our quest, as our ultimate goal is to determine the period of $\frac{1}{n}$ for all $n$. The first thing that one notices is that some of the
decimals, such as $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{10}$, terminate and some of them do not. "Why is this?" one wonders. It has to do with the fact that decimal representation is in base 10. In fact, we will prove that for any number $n$ whose only prime factors are 2 and 5, $\frac{1}{n}$ will terminate. We begin by recounting elementary yet extremely useful points from arithmetic.

**Fundamental Theorem of Arithmetic:** Every integer greater than 1 can be expressed in the form $p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ with $p_1, p_2, \ldots, p_n$ distinct prime numbers and $a_1, a_2, \ldots, a_n$ positive integers. This form, called the prime factorization of the integer, is unique except for the arrangement of the $p_i^{a_i}$.

**Definition:** $a$ divides $b$ (denoted by $a \mid b$) if and only if there exists an integer $q$ such that $b = aq$, in other words, if $\frac{b}{a}$ is an integer.

**Lemma 1:** For any $d \in \mathbb{N}$, the integer $5^d$ does not end in 0.

**Proof:**

Suppose for contradiction that $5^d$ ends in 0.

Then $10 \mid 5^d$ which implies that $10q = 5^d$ for some $q \in \mathbb{N}$, i.e., $2 \cdot 5 \cdot q = 5^d$.

This would imply that $2 = 5$ by the Fundamental Theorem of Arithmetic.

This contradiction proves that $5^d$ does not end in 0. ■
Remark: The proof that powers of 2 do not end in 0 is completely analogous to the above proof for powers of 5.

Proposition 1: The decimal representation of $\frac{1}{n}$ terminates if and only if $n = 2^i 5^j$ for some nonnegative integers $i, j$.

Proof:

(*) First note that since multiplying any number by $10^m$ results in the decimal point moving $m$ places to the left (if $m < 0$) or to the right (if $m > 0$), any integer multiplied by a power of 10 still has a terminating decimal representation.

($\Rightarrow$)

Without loss of generality, assume the decimal $\frac{1}{n}$ terminates after $m$ digits.

Therefore, $\frac{1}{n} = 0.n_1 n_2 n_3 n_4 n_5 n_6 \ldots n_m$.

Multiply each side of the equation by $10^m$ to get $\frac{10^m}{n} = \underbrace{n_1 n_2 n_3 n_4 n_5 n_6 \ldots n_m}_{m} \cdot 0 \in \mathbb{Z}$.

From this, it follows that $n$ divides $10^m$, which means that $n | 2^m \cdot 5^m$.

Hence by the Fundamental Theorem of Arithmetic, the only possible prime factors of $n$ are 2 and 5, which implies that $n = 2^i \cdot 5^j$.

Now, let us prove the other direction.

($\Leftarrow$)

Let $n = 2^i 5^j$. 

Case 1: \( i \geq j \)

\[
\frac{1}{n} = \frac{1}{2^i \cdot 5^j} = \frac{5^{i-j}}{2^i \cdot 5^j} \cdot \frac{5^{i-j}}{10^j} = 5^{i-j} \cdot 10^{-j}. 
\]

Since \( i \geq j \), \( i - j \geq 0 \). In other words, \( 5 \) is raised to a positive exponent. Therefore, \( 5^{i-j} \) is an integer. By (*) , the decimal representation of \( \frac{1}{n} \) terminates.

Case 2: \( i < j \)

The proof of Case 2 is completely analogous to Case 1. ■

Definition: The length of a terminating decimal is the total number of digits before and after the decimal point excluding the non-place-holding zeros on the far left or far right of the decimal. To avoid excessive wordiness, we will say that the length of \( \frac{1}{n} \) is the length of the decimal representation of \( \frac{1}{n} \).

Example 1: The length of .5 is one.

Example 2: The length of .125 is three.

Example 3: The length of 200 is three.

Example 4: The length of 32.6 is three.

If \( \frac{1}{n} \) terminates, then we can use the prime factorization of \( n \) to determine its length.

Corollary 1: If \( n = 2^i 5^j \), then the length of \( \frac{1}{n} \) is \( \text{Max}\{i, j\} \).

Proof:
If \( \frac{1}{n} = 0.a_1a_2...a_N \) where \( a_N \neq 0 \), then \( N \) is the smallest exponent of 10 such that 
\[
10^N \left( \frac{1}{n} \right) \in \mathbb{Z}.
\]
On the other hand, 
\[
10^N \left( \frac{1}{n} \right) = 10^N \left( \frac{1}{2^i5^j} \right) = \frac{10^N}{2^i5^j} \in \mathbb{Z} \text{ if and only if } N \geq i \text{ and } N \geq j.
\]
Therefore, the length of \( \frac{1}{n} \) is the smallest integer greater than or equal to both \( i \) and \( j \), i.e. \( \text{Max}\{i, j\} \).

We now know that if the only prime factors of \( n \) are 2 and 5, then the decimal representation of \( \frac{1}{n} \) terminates, and the length of the decimal is directly related to the exponents in the prime factorization of \( n \). What do you suppose happens if \( n \) is divisible by primes other than 2 and 5? Since we just determined why the decimals that terminate do so, we will now focus on nonterminating decimals. By Proposition 1, we know for nonterminating decimals, \( \frac{1}{n} \), \( n \) must have prime factors other than 2 and 5. In the next proposition, we will show that these nonterminating decimals consist of the same sequence of digits repeating indefinitely.

**Proposition 2:** If the prime factorization of \( n \) contains a prime other than 2 or 5, then the decimal representation of \( \frac{1}{n} \) repeats and is nonterminating.

**Proof:**

Let \( n \) be such that its prime factorization contains some prime not equal to 2 or 5.
The conversion of \( \frac{1}{n} \) into its decimal representation involves long division. According to the division algorithm, for all \( a, b \in \mathbb{Z} \) where \( b \neq 0 \), there exists unique integers \( q, r \) where \( 0 \leq r < b \) such that \( a = b \cdot q + r \).

Let’s look at \( \frac{1}{13} \) to get an idea of the proof.

\[
\begin{array}{c|cccc}
\text{13} & 1.00 \\
\hline
\text{13) } & -91 \\
\text{} & -91 \\
\text{} & 90 \\
\text{} & -78 \\
\text{} & 120 \\
\text{} & -117 \\
\text{} & 30 \\
\text{} & -26 \\
\text{} & 40 \\
\text{} & -39 \\
\text{} & 1 \\
\end{array}
\]

When dividing by \( n \), there are only \( n \) possible remainders, 0 to \( n - 1 \). (In our example, since we are always dividing by 13, the possible remainders are 0 to 12.) However, if at some step in the long division, the remainder is 0, then the decimal would terminate. Since \( n \) is not of the form \( 2^a \cdot 5^b \), Proposition 1 implies \( \frac{1}{n} \) does not terminate. So, really, we are dealing with just \( n - 1 \) remainders, 1 to \( n - 1 \). Because the decimal does not terminate, the long division will continue on indefinitely. Thus, we will have infinitely many remainders (not unique). Since we have only \( n - 1 \) distinct remainders, the Pigeon-Hole Principle states that once we have done \( n \) divisions, one of the remainders is guaranteed to be a duplicate of a previous one. In our example with \( n = 13 \), the first repeat remainder is equal to 1 (which is equal to our very first “remainder”, the 1
in the dividend with which we started the division). Since the division algorithm states that \( q \) and \( r \) are unique, \( n \) is going to divide the repeated remainder exactly the same way that it divided the first remainder. Because we are simply adding zeros to the remainders to continue the long division, once the remainders repeat, so will the quotients. Therefore, the decimal representation of \( \frac{1}{n} \) is guaranteed to repeat. ■

Those decimals that eventually repeat will have a period length.

**Definition:** Let \( \alpha \in \mathbb{R} \) with \( 0 \leq \alpha < 1 \) and let \( \sum_{n=1}^{\infty} a_n 10^{-n} = 0.a_1a_2a_3... \) be a decimal representation of \( \alpha \). This decimal representation is **periodic** (or repeating) if there exist positive integers \( T \) and \( N \) such that \( a_n = a_{n+T} \) \( \forall n \geq N \). The minimal such \( T \), call it \( T(\alpha) \), for which \( a_n = a_{n+T} \) \( \forall n \geq N \) is known as the **period length** of \( \alpha \).

**Remark:** In the case of decimals that terminate, the period length of the decimal is designated as 1 because technically, the trailing zeros repeat.

The period is the actual sequence of digits that repeats, but since in this report we are not concerned with the sequence as much as the length of the sequence, we will use the term "period" to refer to the period length. In other words, the **period of \( \frac{1}{n} \)**, denoted \( T(\frac{1}{n}) \), is the smallest number of digits in the decimal (representation of) \( \frac{1}{n} \) occurring in the repeated sequence. An irrational number such as \( \pi \) or \( \sqrt{2} \) has an infinite period because its decimal representation never repeats and does not terminate.
Example 1: The period of $\frac{1}{3} = .333\ldots$ is 1 because the repeating pattern of digits consists of only one number (3).

Example 2: The period of $\frac{1}{7} = .142857142857\ldots$ is 6 because the shortest repeated sequence is 142857 which has length 6.

Example 3: The period of $\frac{1}{11} = .090909\ldots$ is 2 because the repeating sequence consists of two digits (09).

Example 4: The period of $.5$ is 1 because $.5 = .500000\ldots$.

Referring to Figure 1, when $n$ is prime, the repeated sequence of digits in the decimal representation of $\frac{1}{n}$ begins directly to the right of the decimal point ($\frac{1}{3} = .333\ldots$). Yet when $n$ is a composite number (i.e. has factors other than 1 and itself), the repeated sequence of digits begins directly after the decimal point for some $\frac{1}{n}$ like $\frac{1}{21}$ and $\frac{1}{7}$ and not for some others like $\frac{1}{6}$. So what is special about 9 and 21 compared to all other composite numbers that are less than 21? Note that the only factor of 9 is 3, and 21 also has a factor of 3. However, 12 has a factor of 3, and its fraction does not begin to repeat until the hundredths place. So, instead, we focus on the prime factors that 9 and 21 do not contain. It turns out that 9 and 21 are the only composite numbers less than or equal to 21 that are not divisible by 2 or 5.

Lemma 2: If $a/bc$ and $\text{gcd}(a, c) = 1$, then $a/b$. (See [3], p. 28)

Lemma 3: If a composite number $n$ is not divisible by 2 or 5, then the repeated sequence of digits in the decimal $\frac{1}{n}$ will begin directly after the decimal point.
Proof:

Let $r$ be the period of $\frac{1}{n}$. Since we do not know when the repeating sequence of digits begin in the decimal representation of $\frac{1}{n}$, we only know that the number of non-repeating digits directly to the right of the decimal point, is some integer.

Let us consider some examples.

Example 1: (1) $\frac{1}{n} = 0.123$  
(2) $10^r \left( \frac{1}{n} \right) = 123.123$

Example 2: (1) $\frac{1}{n} = 0.8123$  
(2) $10^r \left( \frac{1}{n} \right) = 812.3123$

Example 3: (1) $\frac{1}{n} = 0.8888123$  
(2) $10^r \left( \frac{1}{n} \right) = 888.8123$

Subtracting equation (1) from equation (2) for each example, one gets $123$, $811.5$, and $887.9235$ for Example 1, Example 2, and Example 3, respectively. It is important to note that in every case, subtracting equation (1) from equation (2) results in a terminating decimal. In other words, $10^r \left( \frac{1}{n} \right) - \frac{1}{n} = t$, for some $t, q \in \mathbb{Z}$. Also, as Example 1 demonstrates, the repeated sequence of digits in $\frac{1}{n}$ begins directly after the decimal point if and only if $10^r \left( \frac{1}{n} \right) - \frac{1}{n}$ is an integer.

Without loss of generality, it can be assumed that $\frac{t}{q}$ is in lowest terms.

Let $s \in \mathbb{N}$ be large enough such that $10^s \left( \frac{t}{q} \right)$ is an integer.

Therefore, $\frac{10^s t}{q} \in \mathbb{Z}$ which implies that $q \mid 10^s t$. 


Because \( \frac{t}{q} \) is in lowest terms, \( \gcd(t, q) = 1 \), and so \( q \mid 10^i \) by Lemma 2. Therefore, \( q = 2^i \cdot 5^j \)
where \( i, j \in \mathbb{N} \).

Since \( \frac{10^r - 1}{n} = \frac{t}{q} \), it follows that \( (10^r - 1)q = nt \).

Therefore, \( q \mid nt \Rightarrow q \mid n \) since \( \gcd(t, q) = 1 \).

But from the hypothesis, \( n \) does not have any prime factors equal to 2 or 5.

Therefore, \( i = j = 0 \) and \( q = 1 \).

This implies that \( 10^r \left( \frac{1}{n} \right) - \frac{1}{n} \) is equal to the integer \( t \).

Therefore, the decimal \( \frac{1}{n} \) begins to repeat directly after the decimal point. ■

In order to delve deeper into our search for a formula that determines the period of all decimal representations of \( \frac{1}{n} \), we will need to touch on a few topics from abstract algebra. First, the definition of a group needs to be understood, as this will be a backbone for many of the later proofs.

**Definition:** A nonempty set \( G \) is said to be a group if in \( G \) there is defined a binary operation \( * \) such that:

(a) \( a, b \in G \) implies that \( a * b \in G \).

(b) Given \( a, b, c \in G \), then \( a * (b * c) = (a * b) * c \).

(c) There exists an identity element \( e \in G \) such that \( a * e = e * a = a \) for all \( a \in G \).

(d) For every \( a \in G \) there exists an inverse element \( b \in G \) such that \( a * b = b * a = e \).
Example: $G = \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3 = \{0, 1, 2\}$ is a group under mod 3 addition. Let us illustrate this by verifying the 4 conditions:

(a) To the left, the Cayley table for $G$ organizes the results (in white) of the operation on each pair of elements (in gray). For instance,

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

(because we are working with the group of integers mod 3).

\[ 1 + 0 = 0 + 1 = 1 \quad 0 + 2 = 2 + 0 = 2 \quad 1 + 2 = 2 + 1 = 0 \]

(b) \( 0 + (1 + 2) = (0 + 1) + 2 \) Other choices for \( a, b, c \) can be easily verified.

(c) From (a), 0 is obviously the identity element.

(d) By looking at the Cayley table, 0 is its own inverse and the inverse of 1 is 2.

Therefore, $G$ is a group.

Definition: If $G$ is finite, and \( a \in G \), then the order of \( a \) is the least positive integer \( m \) such that \( a^m = e \).

Lemma 4: If $G$ is a finite group and if \( k \) is the order of \( g \in G \), then \( g^n = e \) if and only if \( k \mid n \).

Proof:

Since \( k \) is the order of \( g \), \( g^k = e \).

By the division algorithm, there exist integers \( q \) and \( r \) with \( 0 \leq r < k \) such that \( n = q \cdot k + r \).

If \( g^n = e \), then \( e = g^n = g^{qk+r} = (g^k)^q \cdot g^r = g^r \).

Since \( 0 \leq r < k \) and \( k \) is the smallest positive power such that \( g^k = e \) by the definition of order, \( g^r = e \) implies that \( r = 0 \). Therefore, \( n = q \cdot k \Rightarrow k \mid n \).
Conversely, if \( k \mid n \), then \( n = q \cdot k \). Thus, \( g^n = g^{qk} = (g^k)^q = e^q = e \). 

To help us with calculating the period of \( \frac{1}{n} \), we will work in the particular group described in the next definition.

**Definition:** The group of multiplicatively invertible integers mod \( m \) is denoted by \((\mathbb{Z}/m\mathbb{Z})^*\) and is equivalent to the group of all positive integers less than \( m \) whose greatest common divisor with \( m \) is 1 (i.e. those integers relatively prime to \( m \)). The group operation in \((\mathbb{Z}/m\mathbb{Z})^*\) is multiplication.

**Example 1:** \((\mathbb{Z}/3\mathbb{Z})^* = \{1, 2\} \).

**Example 2:** \((\mathbb{Z}/6\mathbb{Z})^* = \{1, 5\} \).

**Definition:** Let \( a, m \in \mathbb{Z} \) with \( m > 0 \) and \( \gcd(a, m) = 1 \). The order of \( a \) mod \( m \) is the least positive integer \( n \) for which \( a^n \equiv 1 \mod m \). According to the definition of order of an element of a group, the order of \( a \) mod \( m \) is exactly the same as the order of \( a \) in the group \((\mathbb{Z}/m\mathbb{Z})^*\).

**Example:** The order of 2 mod 7 is 3 because 3 is the least positive integer such that \( 2^3 = 2 \cdot 2 \cdot 2 = 8 \equiv 1 \mod 7 \).
So far, we have broken the integers into three groups: i) those such that $\frac{1}{n}$ will terminate; ii) those such that $\frac{1}{n}$ will begin to repeat immediately to the right of the decimal point and iii) those such that $\frac{1}{n}$ will eventually begin to repeat. But we still do not have a general formula for determining the period of the decimal representation of $\frac{1}{n}$. What is worse is that generally, as $n$ gets larger, so do the periods and so does the time it takes to count all of the digits by hand. Sure, we could write a computer program to count the digits for us, but that would be a very inefficient use of cpu cycles as we have potentially $n-1$ remainders to work through for each $\frac{1}{n}$ and we would have to use a data type with arbitrary precision. Here is where abstract algebra comes to the coder’s rescue. It can be proven (in fact, we will prove it directly below!) that when $n$ is relatively prime to 2 and 5 (i.e. $n$ is of type (ii) described above), the period of the decimal representation of $\frac{1}{n}$ is equivalent to the order of $10$ mod $n$. In fact, the beautiful theorem below is what this coder used to collect data on thousands of integers (See Appendix A).

**Theorem 1:** If the $n$ is not divisible by 2 or 5, then $T(\frac{1}{n}) = \text{order of } 10 \in (\mathbb{Z}/n\mathbb{Z})^\times$.

**Proof:**

Let $S$ be the set of all $r$ such that for all $i \geq 0$, $a_i = a_{i+r}$, i.e. $S = \{ r \in \mathbb{N} | a_{i+r} = a_i \ \forall i \}$. Let $T = \{ R \in \mathbb{N} | 10^R \equiv 1 \mod n \}$, the set of all natural number such that $n$ divides $10^R - 1$.

Note that by the well ordering principle, $S$ and $T$ each have a minimal element. The minimal element of $S$ is equal to the period of $\frac{1}{n}$ and the minimal element of $T$ is the order of
10 \in (\mathbb{Z}/n\mathbb{Z})^\times.\text{ In order to prove the minimal elements of two sets are equal, we must show that the sets are equal. And this will be done by showing that } S \subseteq T \text{ and } T \subseteq S.\n
(\Rightarrow)\n
Let \gcd(n, 2) = 1 \text{ and } \gcd(n, 5) = 1.\n
Recall that the decimal \( \frac{1}{n} \) can be represented by \( 0.a_1a_2a_3... \).\n
Now recall that the period of \( \frac{1}{n} \) is the minimal number \( T(\frac{1}{n}) \) such that \( a_i = a_{i+T(\frac{1}{n})} \ \forall i \geq 0 \) by Lemma 3. Note that since \( a_i = a_{i+T(\frac{1}{n})} \) is true for all \( i \) greater than or equal to 0, the repeating sequence of digits in the decimal representation of \( \frac{1}{n} \) begins directly after the decimal point.

Let \( r \in S \).

Using the same reasoning as in the proof of Lemma 3, we see that \( (10^r - 1) \cdot \frac{1}{n} \) is an integer, which we will denote by \( t \).

Thus, \( 10^r = nt + 1 \equiv 1 \mod n \), which shows that \( r \in T \). Therefore \( S \subseteq T \).

We now prove \( T \subseteq S \).

Let \( R \in T \).

\[ \therefore 10^R = 1 \mod n. \]

For some \( q \in \mathbb{Z}, 10^R - n \cdot q + 1 \Rightarrow 10^R - 1 = n \cdot q \Rightarrow (10^R - 1) \frac{1}{n} = \boxed{q}. \]

\[ 10^R \cdot \frac{1}{n} - \frac{1}{n} = \boxed{q} \Rightarrow 10^R \cdot \frac{1}{n} = q + \frac{1}{n} = \boxed{q | \text{digits} \ | \text{digits} ...} \]

\[ \Rightarrow \frac{1}{n} = \boxed{q | \text{digits} \ | \text{digits} ...}. \frac{00...0}{n} \boxed{q | \text{digits} \ | \text{digits} ...}. \]
But since the repeated sequence of digits in the decimal representation of \( \frac{1}{n} \) begins directly to the right of the decimal point, \( \frac{00...0[q]}{R} \) must equal \( \left[ \text{digits} \right] \left[ \text{digits} \right] ... \left[ \text{digits} \right] \).

Therefore, \( R \) is equal to the period of \( \frac{1}{n} \) or \( R \) is equal to a multiple of the period of \( \frac{1}{n} \).

\[ \therefore R \in S. \]

\[ \therefore T \subseteq S. \]

\[ \therefore T = S. \]

Therefore, \( T(\frac{1}{n}) = \text{order of } 10 \in (\mathbb{Z}/n\mathbb{Z})^* \). №

Because the period of \( \frac{1}{n} \) is the order of an element of a particular group, we can determine all of the possible orders of its elements and therefore, the possible periods of \( \frac{1}{n} \). By definition, the order of a group is the number of elements in the group. The number of elements in \( (\mathbb{Z}/n\mathbb{Z})^* \) is equal to the number of integers less than \( n \) that are relatively prime to \( n \). So, by definition of the Euler-\( \phi \) function, the order of \( (\mathbb{Z}/n\mathbb{Z})^* \) is \( \phi(n) \). Note that in the case where \( n \) is prime, \( \phi(n) = n - 1 \). Now, the order of an element in a group has to divide the order of the group (See [3], p. 69). Therefore, the period of \( \frac{1}{n} \) must divide the order of the group \( (\mathbb{Z}/n\mathbb{Z})^* \). This explains why the period of \( \frac{1}{n} \) where \( n \) is prime is equal to \( n - 1 \) or a factor of \( n - 1 \). And when \( n \) is not necessarily prime, the period of \( \frac{1}{n} \) divides \( \phi(n) \).

Reducing the Problem to Prime Powers
The prime factorization of 21 is $3^1 \cdot 7^1$. The period of $\frac{1}{21}$ is 6 and the periods of $\frac{1}{3}$ and $\frac{1}{7}$ are 1 and 6, respectively. Perhaps the period of $\frac{1}{n}$, where $n$ is a composite integer, is the product of the periods of $1/(\text{the prime factors of } n)$. However, the period of $\frac{1}{77}$ proves this conjecture wrong because the period of $\frac{1}{77}$ is 6 while the periods of $\frac{1}{7}$ and $\frac{1}{11}$ are 6 and 2, respectively. But, if the period of $\frac{1}{n}$ ($n$ is a composite number) is equal to least common multiple of its prime factors (that are relatively prime to each other), then both examples are explained. Indeed, it turns out that the period of $\frac{1}{mn}$ is equal to the least common multiple of the periods of $\frac{1}{m}$ and $\frac{1}{n}$.

This lemma is quite significant because it indicates that we can break down the “period of all $\frac{1}{n}$ dilemma” into the “period of all $1/(\text{the prime power factors of } n)$ dilemma”. Granted, even though we have greatly reduced our formula to a fraction of what existed before, we are only breaking it down into a fraction of infinity, which is still infinity.

**Lemma 5:** If $r \mid t$ and $s \mid t$ for $r, s, t \in \mathbb{Z}$, then $\text{lcm}(r, s) \mid t$.

**Proof:**

By the Fundamental Theorem of Arithmetic, we can write $r = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ and $s = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$, where some of the $\alpha_i$ or $\beta_i$ may equal 0.

Since $t = rl$ and $t = sv$ for some $l, v \in \mathbb{N}$, it follows that $t = p_1^{\max(\alpha_i, \beta_i)} p_2^{\max(\alpha_i, \beta_i)} \ldots p_n^{\max(\alpha_i, \beta_i)} \cdot u$ for some $u \in \mathbb{N}$.

By definition of least common multiple, $\text{lcm}(r, s) = p_1^{\max(\alpha_i, \beta_i)} p_2^{\max(\alpha_i, \beta_i)} \ldots p_n^{\max(\alpha_i, \beta_i)}$.

Therefore, $\text{lcm}(r, s) \mid t$. ■
Lemma 6: If \( \gcd(m, n) = 1 \), then \( T\left(\frac{1}{mn}\right) = \lcm\left(T\left(\frac{1}{m}\right), T\left(\frac{1}{n}\right)\right) \).

Proof:

Let \( r \) = order of 10 mod \( n \) and let \( s \) = order of 10 mod \( m \).

Then, \( 10^r = 1 \mod n \) and \( 10^s = 1 \mod m \).

If \( k = \lcm(r, s) \), then \( k = ar \) and \( k = bs \) for some \( a, b \in \mathbb{N} \).

Therefore, \( 10^k = 10^{ar} = \left(10^r\right)^a = 1^a \mod n = 1 \mod n \).

Similarly, \( 10^k = 10^{bs} = \left(10^s\right)^b = 1^b \mod m = 1 \mod m \).

Therefore, \( m \mid 10^k - 1 \) and \( n \mid 10^k - 1 \), whence \( mn \mid 10^k - 1 \) since \( \gcd(m, n) = 1 \).

Hence by Lemma 4, the order of 10 mod \( mn \) divides \( k \).

Now, let \( t \) = order of 10 mod \( mn \). Then, \( nm \mid 10^t - 1 \), which implies that

\[ 10^t - 1 = nmq \text{ for some } q \in \mathbb{Z}. \]

But then \( 10^t = nmq + 1 \), so \( 10^t = 1 \mod n \) and \( 10^t = 1 \mod m \).

By Lemma 4, \( r \mid t \) and \( s \mid t \), and therefore, \( \lcm(r, s) \mid t \) by Lemma 5, i.e., \( k \mid t \).

Since \( t \mid k \) and \( k \mid t \), we conclude that \( t = k \).

Therefore, \( T\left(\frac{1}{mn}\right) = \lcm\left(T\left(\frac{1}{m}\right), T\left(\frac{1}{n}\right)\right) \) by Theorem 1.

Corollary 2: If \( n = p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m} \) is the prime factorization of \( n \), then
\[ T\left(\frac{1}{n}\right) = \operatorname{lcm}\left( T\left(\frac{1}{p_1^{n_1}}\right), \ldots, T\left(\frac{1}{p_m^{n_m}}\right)\right). \]

**Proof:** Use induction. ■

However, the previous lemma along with the Fundamental Theorem of Arithmetic makes one wonder if our formula can be broken down even further in terms of \( T\left(\frac{1}{n}\right) \). If this is the case, and if we are able to determine the general formula for \( T\left(\frac{1}{n}\right) \) when \( n \) is equal to some prime number \( p \), then we would have our general formula for the period of \( \frac{1}{n}! \) As it turns out, we can almost simplify the formula into a powers of primes formula. There are only two cases we need to consider. As we will demonstrate in Theorem 2 below, the period of \( \frac{1}{p^r} \) where \( p \) is prime is either equal to the period of \( \frac{1}{p^{r+1}} \) or \( p \) times the period of \( \frac{1}{p^{r+1}} \). And if the period of \( \frac{1}{p^r} \) is equal to \( pT\left(\frac{1}{p^{r+1}}\right) \), we can prove that \( T\left(\frac{1}{p^r}\right) \) is equal to \( pT\left(\frac{1}{p^{r+1}}\right) \) for all \( m \geq n \).

**Theorem 2:** If \( p \) is a prime different from 2 and 5, then either

\[ T\left(\frac{1}{p^r}\right) = T\left(\frac{1}{p^{r+1}}\right) \text{ or } T\left(\frac{1}{p^r}\right) = pT\left(\frac{1}{p^{r+1}}\right). \]

**Proof:**

Let \( r = T\left(\frac{1}{p^r}\right) = \text{order of } 10 \mod p^{r+1} \) and let \( t = T\left(\frac{1}{p^t}\right) = \text{order of } 10 \mod p^u \).

Then, \( 10^r = 1 \mod p^{r+1} \) and \( 10^r = 1 \mod p^u \).

Because \( p^{r+1} | 10^r - 1 \), it follows that \( p^u | 10^r - 1 \), whence \( 10^r = 1 \mod p^u \).
Therefore, $t \mid r$ by Lemma 4.

Now, the fact that $10' = 1 \mod p^n$ implies that $10' = 1 + p^nA$ for some $A \in \mathbb{N}$.

Using the Binomial Theorem, $(10')^p = (1 + p^nA)^p = \binom{p}{0}(p^nA)^0 + \binom{p}{1}(p^nA)^1 + \binom{p}{2}(p^nA)^2 + ...$

$= 1 + pp^nA + p(p - 1)(\frac{1}{2})p^{2n}A^2 + ...$

$= 1 + p^{n+1}(A + (p - 1)(\frac{1}{2})p^nA^2 + ...)$

This shows that $10^p = 1 \mod p^{n+1}$, and so the order of $10 \mod p^{n+1}$ divides $pt$, i.e. $t \mid pt$.

Therefore, $t \mid r \mid pt$, in other words $T\left(\frac{1}{pt}\right) | T\left(\frac{1}{p^n}\right) | pT\left(\frac{1}{p^n}\right)$. But then since $p$ is prime, either

$T\left(\frac{1}{p^n}\right) = T\left(\frac{1}{pt}\right)$ or $T\left(\frac{1}{p^n}\right) = pT\left(\frac{1}{p^n}\right)$. $\blacksquare$

---

**Corollary 2:** If $p$ is a prime different from 2 and 5, and if $T\left(\frac{1}{p^n}\right) = pT\left(\frac{1}{p^{n-1}}\right)$, then

$T\left(\frac{1}{p^{n-1}}\right) = pT\left(\frac{1}{p^{n-1}}\right)$.

**Proof:**

Suppose $T\left(\frac{1}{p^n}\right) = pT\left(\frac{1}{p^{n-1}}\right)$ and let $T\left(\frac{1}{p^{n-1}}\right) = k$. Then, $T\left(\frac{1}{p^n}\right) = pk$.

Now, $k = T\left(\frac{1}{p^{n-1}}\right)$ implies that the order of $10 \mod p^{n-1}$ is $k$, and so $10^k = 1 \mod p^{n-1}$.

This means that $10^k - 1 = p^{n-1}q$ for some $q \in \mathbb{N}$.

If $p \mid q$, then $p\mid 10^k - 1$, which would imply that the order of $10 \mod p^n$ divides $k$, i.e. $pk \mid k$, a contradiction. So, $p \nmid q$. 

---

19
Now, \(10^{k} = 1 + p^{n-1}q\) implies that \((10^{k})^{n} = (1 + p^{n-1}q)^{n} = 1 + \binom{p}{1}p^{n-1}q + \binom{p}{2}(p^{n-1}q)^{2} + \ldots\) by the Binomial Theorem.

So, \(10^{pk} = 1 + p^{n}q + \binom{p}{2}(p^{n-1})^{2}q^{2} + \ldots = 1 + p^{n}q + \binom{p}{2}p^{2n-2}q^{2} + \ldots = 1 + p^{n}q + p^{n+1}A\) for some \(A \in \mathbb{Z}\). Therefore, \(10^{pk} \not\equiv 1 \pmod{p^{n+1}}\) because \(p^{n+1} \nmid p^{n}q\).

Therefore, because \(p^{n+1} \nmid 10^{pk} - 1\), the order of \(10 \pmod{p^{n+1}}\) is not \(pk\).

In other words, \(T\left(\frac{1}{p^{n+1}}\right) \neq T\left(\frac{1}{p^{k}}\right)\). Therefore, \(T\left(\frac{1}{p^{n+1}}\right) = pT\left(\frac{1}{p^{k}}\right)\) by Theorem 2.

**Corollary 3:** If \(T\left(\frac{1}{p^{n}}\right) = pT\left(\frac{1}{p^{k}}\right)\), then \(T\left(\frac{1}{p^{m-n}}\right) = p^{m-n}T\left(\frac{1}{p^{n}}\right)\) \(\forall m \geq n\).

**Proof:**

Use induction.

So, in order to simplify our search even more, we just need to determine when the period of \(\frac{1}{p^{n+1}}\) will equal \(T\left(\frac{1}{p^{n}}\right)\). Looking up again at the chart, one can see that \(T\left(\frac{1}{3}\right) = 1\) and \(T\left(\frac{1}{9}\right) = T\left(\frac{1}{3}\right) = 1\). In both of these cases, the order of \(10 \pmod{p}\) is equal to 1. However, as we calculate the period of the decimal representations of \(\frac{1}{p}\) and \(\frac{1}{p^{i}}\) for a few primes, we notice that it is the case that no other prime numbers appear to even have the case that \(T\left(\frac{1}{p^{n}}\right) = T\left(\frac{1}{p^{n-1}}\right)\). Since \(p = 3\) is the only case such that both \(p\) and \(p^{2}\) will be less than 10, perhaps this is indeed the only case where \(T\left(\frac{1}{p^{n}}\right) = T\left(\frac{1}{p^{n-1}}\right)\). In other words, for all of the prime numbers greater than 3 (excluding 5,
of course, because we proved in Proposition 1 that $\frac{1}{3}$ terminates), it appears that

$$T\left(\frac{1}{p^r}\right) = pT\left(\frac{1}{p^{r+1}}\right).$$

This is very exciting because we know that once $T\left(\frac{1}{p^r}\right) = pT\left(\frac{1}{p^{r+1}}\right)$, this formula will continue to hold for any integer exponent greater than $n$. It cannot be the case that $T\left(\frac{1}{p^r}\right) = T\left(\frac{1}{p^{r-1}}\right)$ for all $n \geq 1$. If we let $s = T\left(\frac{1}{p}\right)$, then $10^r - 1 = pq$ for some $q \in \mathbb{Z}$. Then, if $T\left(\frac{1}{p^r}\right) = T\left(\frac{1}{p^{r-1}}\right)$ for all $n \in \mathbb{N}$, then $p^n$ would divide $q$ for all $n \in \mathbb{N}$. This would imply that $q = 0$ which in turn would imply that $10^r - 1$. This result would imply that the period of a repeating decimal could be 0 (because $s$ would be 0) which is obviously not true. Therefore, $T\left(\frac{1}{p^r}\right) \neq T\left(\frac{1}{p^{r-1}}\right)$ for all $n \geq 1$. So, if we were able to determine that $T\left(\frac{1}{p^r}\right) = pT\left(\frac{1}{p^{r+1}}\right)$ for $n = 2$ and all primes $p > 3$, this would imply that $T\left(\frac{1}{p^r}\right) = p^{r-1}T\left(\frac{1}{p}\right)$ for all $n \geq 1$ and all $p$! The next logical step then became to write a computer program (See Appendix A) in Mathematica (thinking it surely had the most efficient algorithms for mathematical functions of any program we could possibly write) to compare the periods of the decimal representations of $\frac{1}{p}$ and $\frac{1}{p^r}$.

Conjecture 1: For $p > 5$, $T\left(\frac{1}{p^r}\right) = pT\left(\frac{1}{p}\right)$.

And then comes along the prime number 487—a counterexample to our conjecture. The period of the decimal representation of $\frac{1}{487}$ is equal to 486, as is the period of $\frac{1}{487}$. As disappointing as the counterexample was, the questions soon became focused on “Why???” and “Does anyone else know this?” The latter was easy enough to answer with a quick jog to the Prime Curios homepage (see [5]) where we discovered that Helmut Richter was looking at the
smallest numbers of the form $10^k - 1$ divisible by $p$. If you recall the proofs above, $k$, in this case, is equal to the order of $10 \in (\mathbb{Z}/p\mathbb{Z})^*$ which in turn is equal to $T(\frac{1}{p})$. He also stumbled upon the fact that the smallest number of the form $10^k - 1$ that 487 divides evenly into is also divisible by its square, $487^2$. In fact, he went even further and noted that the next time this occurs is when $p = 56,598,313$.

Unfortunately, we have been unable to determine the reason that for $p = 3$, 487, and 56,598,313, $T(\frac{1}{p})$ is equal to $T(\frac{1}{p^2})$. As a result, the search for an all-inclusive formula to determine the period of the decimal representation of $\frac{1}{n}$ is temporarily stalled. However, not all hope is lost as we will see in the next chapter, the Fibonacci sequence also can be considered to have the property of a period in relation to a prime number $p$ and its square. Perhaps it can offer some insight into our dilemma.
Chapter 2

The Period of the Fibonacci sequence mod \( n \)

Definition: The Fibonacci sequence is a recursive sequence of numbers \( f_1, f_2, f_3, \ldots \) where \( f_1 = 1, f_2 = 1 \), and if \( m \) is a positive integer, then \( f_{m+2} = f_m + f_{m+1} \).

<table>
<thead>
<tr>
<th>The Fibonacci Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 1 2 3 5 8 13 21 34</td>
</tr>
<tr>
<td>55 89 144 233 377 610 987 1597 2584</td>
</tr>
<tr>
<td>4181 6765 10946 17711 28657 46368 75025 121393 196418</td>
</tr>
<tr>
<td>317811 514229 832040 1346269 2178309 3524578 5702887 9227465 14930352</td>
</tr>
<tr>
<td>24157817 39088169 63245986 102334155 165580141 267914296</td>
</tr>
</tbody>
</table>

Figure 2: The first 42 terms of the Fibonacci sequence

In other words, once you have the first two numbers, to get any other number in the Fibonacci sequence (called a Fibonacci number), simply add the previous two Fibonacci numbers. Looking at the chart above, one can see that the first two numbers listed are \( f_1 \) and \( f_2 \) and the sequence wraps around to continue on the next line.

As we will prove below, the Fibonacci sequence will become periodic if it is reduced mod \( n \). One can “mod the Fibonacci sequence” by reducing each element of the sequence mod \( n \). In what follows, we will use the notation \( \overline{f_i} \) to denote \( f_i \mod n \), with the modulus \( n \) being understood.
Example: If the Fibonacci sequence is reduced mod 3, the first five Fibonacci numbers are
\[ f_1 \equiv 1 \pmod{3}, f_2 \equiv 1 \pmod{3}, f_3 \equiv 2 \pmod{3}, f_4 \equiv 0 \pmod{3}, \text{ and } f_5 \equiv 2 \pmod{3}, \]
in other words, \( \{1, 1, 2, 0, 2\} \).

Lemma 7: If \( f_i \) and \( f_{i+1} \) are consecutive Fibonacci numbers, then \( \gcd(f_i, f_{i+1}) = 1 \) for all \( i \geq 0 \).

Proof:

Case \( i = 1 \): \( f_1 = 1 \) and \( f_2 = 1 \). \( \gcd(f_1, f_2) = \gcd(1, 1) = 1. \checkmark \)

Assume as an induction hypothesis that \( \gcd(f_{k-1}, f_k) = 1 \) for \( k \geq 2 \).

If \( \gcd(f_k, f_{k+1}) \neq 1 \), then \( \gcd(f_k, f_{k+1}) = a \) for some \( a \in \mathbb{Z} \) such that \( a > 1 \).

Therefore, \( f_k = aq \) and \( f_{k+1} = ar \) for some \( q, r \in \mathbb{N} \).

By the definition of the Fibonacci sequence, \( f_{k-1} + f_k = f_{k+1} \), and so \( f_{k-1} = f_{k+1} - f_k \).

So, \( f_{k-1} = ar - aq = a(r - q) \). \( \Rightarrow a \mid f_{k-1} \).

Thus, \( (f_{k-1}, f_k) \geq a > 1 \), a contradiction.

Therefore, \( \gcd(f_k, f_{k+1}) \) must be 1.

By the principle of mathematical induction, \( \gcd(f_i, f_{i+1}) = 1 \) for all \( i \geq 0 \).

Now, if we define \( f_0 = 0 \), then the Fibonacci sequence is defined for all \( m \geq 0 \), and the first three Fibonacci numbers can be represented by the \( 2 \times 2 \) matrix \( A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} f_0 & f_1 \\ f_1 & f_2 \end{pmatrix} \).
Lemma 8: For any \( m \geq 0 \), \( A^m = \begin{pmatrix} f_{m-1} & f_m \\ f_m & f_{m+1} \end{pmatrix} \).

Proof:

Case \( m = 1 \). \( A^1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} f_0 & f_1 \\ f_1 & f_2 \end{pmatrix} \). \( \checkmark \)

Assume true for \( m - 1 = k \). So, \( A^k = \begin{pmatrix} f_{k-1} & f_k \\ f_k & f_{k+1} \end{pmatrix} \).

\[
A^{k+1} = A^1 \cdot A^k = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} f_{k-1} & f_k \\ f_k & f_{k+1} \end{pmatrix} = \begin{pmatrix} 0 \cdot f_{k-1} + 1 \cdot f_k & 0 \cdot f_k + 1 \cdot f_{k+1} \\ f_k + f_{k+1} & f_{k-1} + f_k \end{pmatrix} = \begin{pmatrix} f_k & f_{k+1} \\ f_{k+1} & f_{k+2} \end{pmatrix}
\]

by the definition of the Fibonacci sequence.

Therefore, \( A^{k+1} = \begin{pmatrix} f_k & f_{k+1} \\ f_{k+1} & f_{k+2} \end{pmatrix} \) which implies that \( A^m = \begin{pmatrix} f_{m-1} & f_m \\ f_m & f_{m+1} \end{pmatrix} \ \forall m \in \mathbb{N} \) by induction. \( \blacksquare \)

Just like one can mod the integers by \( n \), mod \( n \) arithmetic can also be performed on a matrix. Reducing a matrix \( M \mod n \) is equivalent to reducing \( \mod n \) each entry in \( M \) individually. We will use the notation \( \overline{M} \) to denote \( M \mod n \), with the modulus \( n \) being understood.

Example: For the matrix \( M = \begin{pmatrix} 5 & 14 \\ 8 & 13 \end{pmatrix} \), \( M = \begin{pmatrix} 5 & 0 \\ 1 & 6 \end{pmatrix} \mod 7 \) because \( 5 \equiv 5 \mod 7 \), \( 14 \equiv 0 \mod 7 \), \( 8 \equiv 1 \mod 7 \), and \( 13 \equiv 6 \mod 7 \).
Analogous to the fact that 10 is the key to finding the period of $\frac{1}{2}$, the matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ is the (code-friendly) answer to finding the period of the Fibonacci sequence mod $n$. Recall that 10 is an element of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ as long as $n$ is relatively prime to 2 and 5. Analogously, $A \mod n$ is an element of the ring $GL_2(\mathbb{Z}/n\mathbb{Z})$ of invertible $2 \times 2$ matrices whose entries are elements of the group $\mathbb{Z}/n\mathbb{Z}$. A ring is like a special group in that it has all of the properties of a group and then some.

**Definition:** A nonempty set $R$ is said to be a ring if in $R$ there are two operations $+$ and $\cdot$ such that:

(a) $a,b \in R$ implies that $a+b \in R$. (We say the ring is “closed under addition”.)

(b) $a+b = b+a$ for $a,b \in R$. (Commutativity of addition)

(c) $(a+b)+c = a+(b+c)$ for $a,b,c \in R$. (Associativity of addition)

(d) There exists an element $0 \in R$ such that $a+0 = a$ for every $a \in R$. (0 is the identity element.)

(e) Given $a \in R$, there exists a $b \in R$ such that $a+b = 0$. (In other words, $b$ is the inverse of $a$.)

(Note so far that $R$ is simply a commutative group under addition.)

(f) $a,b \in R$ implies that $a \cdot b \in R$. (We say the ring is “closed under multiplication”.)

(g) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for $a,b,c \in R$. (Associativity of multiplication)

(h) $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$, for $a,b,c \in R$. (Distributive property)

Now, a matrix is said to be invertible if it has a multiplicative inverse. A quick way to prove that a matrix has an inverse is to check its determinant. If the determinant is not equal to
zero, then the matrix is invertible (See [4], p. 395). We can easily see that the determinant of \( A \) is 
\(-1\), and \(-1\) will never equal 0 in \( \mathbb{Z}/n\mathbb{Z} \) for \( n \geq 2 \). (In other words, \(-1 \not\equiv 0 \mod n\).) Therefore, \( \overline{A} \) will always be an element of the group \( GL_2(\mathbb{Z}/n\mathbb{Z}) \) for any \( n \geq 2 \). It is important to note that the matrix that results from reducing mod \( n \) the product of matrices with integer entries is congruent mod \( n \) to the matrix that results from multiplying the matrices with each reduced mod \( n \). In other words, \( \overline{M} \cdot \overline{L} = \overline{M} \cdot \overline{L} \). Two matrices are said to be congruent mod \( n \) if their corresponding entries are equivalent to each other mod \( n \). The example below illustrates that the matrix \( (M \cdot L) \mod 7 \) is congruent to the matrix \( (M \mod 7) \cdot (L \mod 7) \).

Example: Let \( M = \begin{pmatrix} 5 & 14 \\ 8 & 13 \end{pmatrix} \) and \( L = \begin{pmatrix} 1 & 3 \\ 10 & 11 \end{pmatrix} \).

Therefore, \( (M \cdot L) = \begin{pmatrix} 145 & 169 \\ 138 & 167 \end{pmatrix} \equiv \begin{pmatrix} 5 & 1 \\ 5 & 6 \end{pmatrix} \mod 7 \).

Now, we check that \( M \) and \( L \) are in the group \( GL_2(\mathbb{Z}/7\mathbb{Z}) \) by computing their determinants.

\[
\det(M) = \det\begin{pmatrix} 5 & 14 \\ 8 & 13 \end{pmatrix} = -47 \equiv 2 \mod 7 \quad \text{and} \quad \det(L) = \det\begin{pmatrix} 1 & 3 \\ 10 & 11 \end{pmatrix} = -19 \equiv 2 \mod 7.
\]

Both \( \det(M) \) and \( \det(L) \) are not equal to zero. Therefore, \( M \) and \( L \) are in \( GL_2(\mathbb{Z}/7\mathbb{Z}) \).

\[
M = \left( \begin{array}{cc} 5 & 0 \\ 1 & 6 \end{array} \right) \mod 7 \quad \text{and} \quad L = \left( \begin{array}{cc} 1 & 3 \\ 3 & 4 \end{array} \right) \mod 7, \quad \text{so} \quad (M \mod 7) \cdot (L \mod 7) = \left( \begin{array}{cc} 5 & 15 \\ 19 & 27 \end{array} \right) = \left( \begin{array}{cc} 5 & 1 \\ 5 & 6 \end{array} \right) \mod 7.
\]

Using congruent matrices is important from a programming perspective because considering the matrices to be elements of the group \( GL_2(\mathbb{Z}/n\mathbb{Z}) \) keeps the entries of their product small and therefore, much more memory-friendly. Also, since the group \( GL_2(\mathbb{Z}/n\mathbb{Z}) \) is
finite, the matrix \( \overline{A} \) has a finite order. Just like the definition of the order of an element of a group, the order of \( \overline{A} \) is the smallest positive integer \( m \) such that \( (\overline{A})^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \).

Theorem 3: The Fibonacci sequence mod \( n \) is periodic. Moreover,

a) the period starts at the beginning of the sequence with 0 and 1, and

b) the period length, denoted by \( T(n) \), is equal to the order of the matrix \( \overline{A} \) in \( GL_2(\mathbb{Z}/n\mathbb{Z}) \).

Proof:

In order for the Fibonacci sequence mod \( n \) to terminate, there would have to be two consecutive terms, \( \overline{f}_j \) and \( \overline{f}_{j+1} \), that are equal to 0. Then, by the definition of the Fibonacci sequence, for every \( i > j + 1 \), \( \overline{f}_i \) would equal 0. However, if \( \overline{f}_j = 0 \) and \( \overline{f}_{j+1} = 0 \), then \( n | f_j \) and \( n | f_{j+1} \), and thus \( \gcd(\overline{f}_j, \overline{f}_{j+1}) \geq n \neq 1 \) which contradicts Lemma 7.

Therefore, the Fibonacci sequence mod \( n \) does not terminate. Reminded of the decimal representation of \( \frac{1}{n} \), if the Fibonacci sequence mod \( n \) does not terminate, then does it repeat?

Since \( \overline{A} \) has finite order in the finite group \( GL_2(\mathbb{Z}/n\mathbb{Z}) \), there exists some integer \( m \) such that

\[
(A)^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\]

But \( (\overline{A})^m = \overline{A^m} = \begin{pmatrix} f_{m-1} & f_m \\ f_m & f_{m+1} \end{pmatrix} \). Therefore, the repeating sequence of digits begins with \( \overline{f}_m = 0 \) and \( \overline{f}_{m+1} = 1 \). Thus, the Fibonacci sequence mod \( n \) is periodic. In addition, the sequence begins to repeat when \( \overline{A}^{m+1} = \overline{A} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \). This implies that \( \{0, 1\} \) is included in the
repeating sequence of digits and therefore starts every repeating sequence of digits. This proves (a).

Also, the period length is $k$ if and only if $k$ is the smallest positive integer such that

\[ f_k = 0 \quad \text{and} \quad f_{k+1} = 1. \]

In other words, $k$ is the smallest integer such that \( (\overline{A})^k = \begin{pmatrix} f_k & f_{k+1} \\ f_k & f_{k-1} \end{pmatrix}. \) Since \( f_{k-1} = f_{k+1} - f_k \), this implies that \( f_{k-1} = 1 - 0 = 1. \) Therefore, the period length of the Fibonacci sequence mod $n$ is the smallest positive integer such that \( (\overline{A})^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \) Therefore, the period, $T(n)$ is equal to the order of the matrix $\overline{A}$ in $GL_2(\mathbb{Z}/n\mathbb{Z}).$ 

See the chart below for the first 42 terms of the Fibonacci sequence mod $n$ for each $n$ from 2 to 15. Note that, in order to fit the first 42 Fibonacci numbers for each $n$, the sequence wraps to the next line. Also note the period of each Fibonacci sequence mod $n$, denoted $T(n)$, is located to the right of each separate sequence.
### The Fibonacci Sequence mod $n$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$T(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>6</td>
<td>24</td>
</tr>
<tr>
<td>7</td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>24</td>
</tr>
<tr>
<td>10</td>
<td>60</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>12</td>
<td>24</td>
</tr>
<tr>
<td>13</td>
<td>28</td>
</tr>
<tr>
<td>14</td>
<td>48</td>
</tr>
<tr>
<td>15</td>
<td>40</td>
</tr>
</tbody>
</table>

Figure 3: The Fibonacci Sequence Mod $n$ for $n = 2$ to $15$

### Reducing the Fibonacci sequence problem to Prime Powers

Once again we can determine the period of the Fibonacci sequence mod $n$ by looking the periods correlating to the prime factors of $n$. In fact, the next few results are each analogous to results from the section on reducing the problem of determining the period of $\frac{1}{n}$ to the prime powers of $n$. 

30
Lemma 9: If \( \gcd(m, n) = 1 \), \( A \equiv B \mod m \), and \( A \equiv B \mod n \), then \( A \equiv B \mod mn \).

Proof:

Since \( A \equiv B \mod m \) is the result of reducing the entries of \( A \mod m \), the lemma with matrices is analogous to the integer case. ■

Lemma 10: If \( \gcd(m, n) = 1 \), then \( T(mn) = \text{lcm}(T(m), T(n)) \).

Proof:

Let \( r = \text{order of } \bar{A} \in GL_2(\mathbb{Z}/n\mathbb{Z}) \) and let \( s = \text{order of } \bar{A} \in GL_2(\mathbb{Z}/m\mathbb{Z}) \).

Then, \( (\bar{A})^r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/n\mathbb{Z}) \) and \( (\bar{A})^s = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/m\mathbb{Z}) \).

If \( k = \text{lcm}(r, s) \), then \( k = ar \) and \( k = bs \) for some \( a, b \in \mathbb{N} \).

Therefore, \( (\bar{A})^k = (\bar{A})^{ar} = (\bar{A})^s = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/n\mathbb{Z}) \) and \( (\bar{A})^k = (\bar{A})^{bs} = (\bar{A})^r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/m\mathbb{Z}) \).

Therefore, \( (\bar{A})^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/m\mathbb{n}\mathbb{Z}) \) and \( \bar{A}^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/m\mathbb{Z}) \) whence \( (\bar{A})^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/mn\mathbb{Z}) \) since \( \gcd(m, n) = 1 \) by Lemma 9.

By Lemma 4, it follows that the order of \( \bar{A} \in GL_2(\mathbb{Z}/mn\mathbb{Z}) \) divides \( k \), i.e.,

\( T(mn) \mid \text{lcm}(T(m), T(n)) \).
Now, let $t = \text{order of } \tilde{A} \in GL_2(Z/mn\mathbb{Z})$, i.e. $(\tilde{A})' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(Z/mn\mathbb{Z})$.

Then, $(\tilde{A})' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(Z/m\mathbb{Z})$ and $(\tilde{A})' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(Z/n\mathbb{Z})$.

By Lemma 4, it follows that $r \mid t$ and $s \mid t$. Therefore, $\text{lcm}(r, s) \mid t$ by Lemma 5.

In other words, $(T(m), T(n)) \mid T(mn)$, which together with the first part of the proof, proves that $T(mn) = \text{lcm}(T(m), T(n))$.

Corollary 4: If $p_1^\alpha_1 p_2^\alpha_2 \ldots p_m^\alpha_m$ is the prime factorization of $n$, then $T(n) = \text{lcm}(T(p_1^{\alpha_1}), \ldots, T(p_m^{\alpha_m}))$.

Proof: Use induction. ■

Theorem 4: For any prime $p$ and for any $r \geq 1$, either $T(p^{r+1}) = T(p^r)$ or $T(p^{r+1}) = pT(p^r)$.

Proof:

Let $s = T(p^{r+1}) = \text{order of } \tilde{A} \in GL_2(Z/p^{r+1}\mathbb{Z})$ and let $t = \text{order of } \tilde{A} \in GL_2(Z/p^r\mathbb{Z}) = T(p^r)$.

Then, $(\tilde{A})' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(Z/p^{r+1}\mathbb{Z})$ and $(\tilde{A})' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(Z/p^r\mathbb{Z})$.

Now, $(\tilde{A})' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(Z/p^{r+1}\mathbb{Z})$ implies that $p^{r+1}$ divides each entry of $A' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. In other words, there exists a $2 \times 2$ matrix $B$ with integer entries such that $A' = p^{r+1}B + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

As shown in Lemma 8, the entries $f_\theta$ of $A'$ satisfy the relations $a_{12} = a_{21}$ and $a_{11} + a_{21} = a_{22}$.
So, \( A' = \begin{pmatrix} p'^{r+1}a + 1 & p'^{r+1}b \\ p'^{r+1}b & p'^{r+1}(a+b) + 1 \end{pmatrix} \) for some \( a, b \in \mathbb{Z} \).

It is now clear that \( A' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p'^r \), i.e., \( A' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/p'^r\mathbb{Z}) \). Therefore, \( t | s \).

Let \( A' = \begin{pmatrix} 1 + p'a & p'b \\ p'b & 1 + p'(a+b) \end{pmatrix} \).

Claim: Now we will prove by induction that \( (A')^l = \begin{pmatrix} 1 + lp'a & lp'b \\ lp'b & 1 + lp'(a+b) \end{pmatrix} \mod p'^{r+1} \) for every \( l \in \mathbb{N} \).

Case 1: \( l = 1 \).

\[
(A')^1 = \begin{pmatrix} 1 + p'a & p'b \\ p'b & 1 + p'(a+b) \end{pmatrix} \]

Let \( k = l - 1 \). Assume it has been shown that \( (A')^k = \begin{pmatrix} 1 + kp'a & kp'b \\ kp'b & 1 + kp'(a+b) \end{pmatrix} \mod p'^{r+1} \). Then,

\[
(A')^{k+1} = (A')^k \cdot A'
\]

\[
\begin{pmatrix} 1 + kp'a & kp'b \\ kp'b & 1 + kp'(a+b) \end{pmatrix} \begin{pmatrix} 1 + p'a & p'b \\ p'b & 1 + p'(a+b) \end{pmatrix}
\]

\[
\begin{pmatrix} 1 + (k+1)p'a + p^{2r}(ka^2 + kb^2) & (k+1)p'b + p^{2r}(kab + kb(a+b)) \\ (k+1)p'b + p^{2r}(kba + kb(a+b)) & 1 + (k+1)p'(a+b) + p^{2r}(kb^2 + k(a+b)^2) \end{pmatrix}
\]

\[
\begin{pmatrix} 1 + (k+1)p'a & (k+1)p'b \\ (k+1)p'b & 1 + (k+1)p'(a+b) \end{pmatrix} \mod p'^{r+1} \) because \( r + 1 \leq 2r \)

\[
\therefore (A')^l = \begin{pmatrix} 1 + lp'a & lp'b \\ lp'b & 1 + lp'(a+b) \end{pmatrix} \mod p'^{r+1}.
\]

Letting \( l = p \) in the above claim, we see that
Therefore, \((A')^p = \begin{pmatrix} 1+ pp' a & pp' b \\ pp' b & 1+ pp' (a+b) \end{pmatrix} = \begin{pmatrix} 1+ p^{r+1}a & p^{r+1}b \\ p^{r+1}b & 1+ p^{r+1} (a+b) \end{pmatrix} \mod p^{r+1}.

Therefore, \((A')^p = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p^{r+1}.

Hence, the order of \(A \in GL_2(\mathbb{Z}/p^{r+1}\mathbb{Z})\) divides \(pt\), i.e., \(s | pt\).

Therefore, \(t | s | pt\). In other words, \(T(p^r) | T(p^{r+1}) \mid pT(p^r)\). Because \(p\) is prime, we conclude that \(T(p^{r+1}) = T(p^r)\) or \(T(p^{r+1}) = pT(p^r)\). \(\blacksquare\)

**Corollary 5:** For any prime \(p\) and any \(r > 1\), if \(T(p^r) = pT(p^{r-1})\), then \(T(p^{r+1}) = pT(p^r)\).

**Proof:**

Suppose \(T(p^r) = pT(p^{r-1})\) and let \(T(p^{r-1}) = k\). Then \(T(p^r) = pk\).

Now, \(k = T(p^{r-1})\) implies that the order of \(A \in GL_2(\mathbb{Z}/p^{r-1}\mathbb{Z})\) is \(k\), and so

\[
(A)^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/p^{r-1}\mathbb{Z}).
\]

This means that \(A^k = \begin{pmatrix} 1+ p^{r-1}a & p^{r-1}b \\ p^{r-1}b & 1+ p^{r-1} (a+b) \end{pmatrix}\) for some \(a, b \in \mathbb{Z}\) such that either \(p | a\) or \(p | b\).

For, if \(p | a\) and \(p | b\), then \(A^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p^r\), contradicting the fact that the order of \(A \mod p^r\) is greater than \(k\).
By the claim in the proof of the previous theorem,

\[ A^t = (A^k)^p = \begin{pmatrix} 1 + p^r a & p^r b \\ p^r b & 1 + p^r (a + b) \end{pmatrix} \mod p^r. \]

Because \( p \vert a \) or \( p \vert b \), \( A^t \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p^{r+1}. \)

In other words, \( A^{t+p} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p^{r+1} \), whence \( T(p^{r+1}) \neq T(p^r) \). By Theorem 4, it follows that \( T(p^{r+1}) = pT(p^r) \). 

So our search for the period is once again is narrowed down to the question of when the period jumps to equal \( pT(p^{r-1}) \). It cannot be the case that \( T(p^r) = T(p) \) for all \( r \geq 1 \). If this were the case, then \( A^{t+p} = \begin{pmatrix} 1 + pa & pb \\ pb & 1 + p(a + b) \end{pmatrix} \) would be congruent to \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p^r \) for every \( r \). This would imply that \( p^r \vert a \) and \( p^r \vert b \) for every \( r > 1 \), and this could only happen if \( a = b = 0 \), i.e. \( A^{t+p} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \). But by Lemma 8, this would mean that \( f_{T(p-1)} = 1, f_{T(p)} = 0, f_{T(p+1)} = 1 \), which does not occur in the (non-reduced mod \( n \)) Fibonacci sequence. Therefore, eventually, there will be a \( r_0 \in \mathbb{N} \) such that \( T(p^{r_0}) = pT(p) \), and from then on \( T(p^m) = p^{m-r_0}T(p) \) for all \( m \geq r_0 \). From the data collected (see Appendix C), we believe that \( r_0 = 2 \). In other words, the jump from \( T(p) \) to \( pT(p) \) of the Fibonacci sequence mod \( p \) occurs immediately.
Conjecture 2: For all primes $p$, $T\left( p^2 \right) = pT\left( p \right)$.

We have gathered data on the period of the Fibonacci sequence mod $p$ and mod $p^2$ for all primes up to 16097 and have determined that $T\left( p \right) = pT\left( p^2 \right)$ for every $p$ up to that point (see Appendix B for the code). By the previous lemma, we know that for all prime numbers $p \leq 16097$ this implies $T\left( p^n \right) = pT\left( p^{n-1} \right)$ for all $n > 1$.

The Formula for $T(p)$

If the conjecture is proven correct, our next (and last step!) would be to discover the formula for $T(p)$. Once we would have this formula, our search for the period of the Fibonacci sequence mod $n$ would be complete and hopefully, shed some light on our quest for the period of the decimal representation of $\frac{1}{n}$. From now on, $n$ is assumed to be prime.

Taking powers of the matrix $\overline{A}$ can quickly become tedious because each time you take powers of $A$, you have to do matrix multiplication. However, if we could get $\overline{A}$ in the form of a diagonalized matrix $D = \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix}$, then to take successive powers of the matrix, we would only need to take powers of the entries $a_{11}$ and $a_{22}$. In order to be able to diagonalize matrices, the matrices must be in a field. A field is a ring containing a multiplicative identity, multiplicative inverses for all nonzero elements, and in which multiplication is commutative. If an $n \times n$ matrix with entries in a field has $n$ distinct eigenvalues, then the matrix can be diagonalized (see [4], p.456). So, let us find $\lambda_1$ and $\lambda_2$, the eigenvalues of $\overline{A}$, in order to determine if we can diagonalize it. The eigenvalues of $\overline{A}$ are found by solving the equation
\[
\det(\overline{A} - \lambda \overline{I}) = 0 \text{ where } \overline{I} \text{ is the identity matrix } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p.
\]

\[
\det(\overline{A} - \lambda \overline{I}) = \det\left( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right) = \det\left( \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix} \right) = (-\lambda)(1-\lambda) - 1 = \lambda^2 - \lambda - 1. \text{ By the quadratic formula, } \lambda_1 \text{ and } \lambda_2 \text{ are found to be } \frac{1 \pm \sqrt{5}}{2}.
\]

You might recognize \( \frac{1 + \sqrt{5}}{2} \) as the formula for the golden ratio. (Insert oohs and ahhs here.) Curiously, the golden ratio turns up in a second place in correlation to the Fibonacci sequence. The other time the golden ratio shows up in the Fibonacci sequence is when one takes

\[
\lim_{r \to \infty} \frac{f_{r+1}}{f_r}
\]

where \( f_r \) is the \( r \)th term of the Fibonacci sequence and \( f_{r-1} \) is the previous term. In addition to the two eigenvalues of \( \overline{A} \), this limit is also equal to the golden ratio.

Now, when looking for \( \sqrt{5} \) in any ring \( \mathbb{Z}/n\mathbb{Z} \), keep in mind that we are actually looking for an element of the ring whose square is equal to 5. Then in the ring, that element is equal to \( \sqrt{5} \).

**Example:** In the ring \( \mathbb{Z}/11\mathbb{Z} \), 4 is equal to \( \sqrt{5} \) because \( 4^2 = 16 \equiv 5 \mod 11 \).

Not every group \( \mathbb{Z}/n\mathbb{Z} \) will have \( \sqrt{5} \), but when it does, then the eigenvalues of \( \overline{A} \) are simply elements of the group and the typical group properties will apply. Note that in \( \mathbb{Z}/2\mathbb{Z} \), the eigenvalues do not exist because \( \frac{1 \pm \sqrt{5}}{2} = \frac{1 \pm \sqrt{1}}{0} \mod 2 \), and you cannot divide by zero. Also
note that in $\mathbb{Z}/5\mathbb{Z}$, \( \frac{1 \pm \sqrt{5}}{2} = \frac{1 \pm 0}{2} \mod 5 = \frac{1}{2} \mod 5 \). Therefore, there are not two distinct eigenvalues, and so the matrix $\mathbf{A}$ cannot be diagonalized in this case. However, both of these cases are small enough that they can be calculated by hand either by determining the order of $\mathbf{A} \in GL_2(\mathbb{Z}/n\mathbb{Z})$ or by actually looking at the Fibonacci sequence mod $n$ and figuring out the period. So, we only need to be concerned with whether or not $\sqrt{5}$ exists in the field $\mathbb{Z}/n\mathbb{Z}$. If $\sqrt{5}$ does not exist in the field, then we have to create an extension field that contains $\sqrt{5}$. This concept should be familiar because when you take the set of rational numbers, irrational numbers are obviously excluded. But if you would like to include the irrational numbers, you extend the set of rational numbers to the set of real numbers, and therein $\sqrt{5}$ can be found.

In order to determine those primes for which $\sqrt{5}$ exists in the field $\mathbb{Z}/n\mathbb{Z}$, we use the Legendre symbol, $\left( \frac{a}{n} \right)$, and the Law of Quadratic Reciprocity.

**Definition: (Legendre symbol).** Let $p$ and $q$ be distinct odd prime numbers.

\[
\left( \frac{a}{q} \right) = \begin{cases} 
1, & \text{if } p \text{ is a square mod } q \\
-1, & \text{if } p \text{ is not a square mod } q
\end{cases}
\]

**The Law of Quadratic Reciprocity:** Let $p$ and $q$ be distinct odd prime numbers. Then,

\[
\left( \frac{a}{q} \right) \left( \frac{a}{p} \right) = \begin{cases} 
1, & \text{if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \text{ (or both)} \\
-1, & \text{if } p \equiv q \equiv 3 \mod 4
\end{cases}
\]

The Law of Quadratic Reciprocity allows us to change the difficult question “Is 5 a square mod $p$” into the much easier question to answer “Is $p$ a square mod 5?” This is possible
because \( 5 \mod 4 = 1 \) and so \( \left( \frac{5}{p} \right) = 1 \). Therefore, if \( p \) is a square mod 5, then \( \left( \frac{5}{p} \right) = 1 \) and thus \( \left( \frac{5}{p} \right) = 1 \) as well, which implies that 5 is a square mod \( p \). Below is a chart of \( a \), an element in \( \mathbb{Z}/5\mathbb{Z} \) and \( a^2 \), the square of \( a \) in \( \mathbb{Z}/5\mathbb{Z} \).

<table>
<thead>
<tr>
<th>( a )</th>
<th>( 0 )</th>
<th>( 1 )</th>
<th>( 2 )</th>
<th>( 3 )</th>
<th>( 4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a^2 )</td>
<td>( 0 )</td>
<td>( 1 )</td>
<td>( 4 )</td>
<td>( 4 )</td>
<td>( 1 )</td>
</tr>
</tbody>
</table>

Figure 4: \( a \) and \( a^2 \) in \( \mathbb{Z}/5\mathbb{Z} \).

As you can see, \( p \) is a square mod 5 if and only if \( p \equiv 1 \) or \( 4 \mod 5 \). In other words, \( \sqrt{5} \) will exist in \( \mathbb{Z}/p\mathbb{Z} \) if and only if \( p \equiv 1 \) or \( 4 \mod 5 \).

So, the fact that \( \bar{A} \) has two distinct eigenvalues implies that \( A \) can be diagonalized to \( D \) by finding some invertible matrix \( C \) such that \( CAC^{-1} = D \). Note the entries of \( C \) may not belong to \( \mathbb{Z}/p\mathbb{Z} \), but rather in an extension field of \( \mathbb{Z}/p\mathbb{Z} \). By definition of a diagonalized matrix \( D \), the entries of \( D \) are equal to the eigenvalues of \( A \). So, \( D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \). When we take successive powers of the equation \( CAC^{-1} = D \), we find the conditions that \( A \) must meet in order for \( D \) to equal the identity matrix.

\[
D^n = CAC \cdot A \cdot A \cdot \ldots \cdot A \cdot A^{-1} = C\left(A^n\right)C^{-1}.
\]

\[
D^n = I \Leftrightarrow C\left(A^n\right)C^{-1} = I \Leftrightarrow \left(A^n\right) = I.
\]
Therefore, the order of \( A \mod p \) is the smallest positive \( n \) such that \( (\lambda_1)^n = 1 \) and 
\[(\lambda_2)^n = 1\] in \( \mathbb{Z}/p\mathbb{Z} \). Finding \( n \) such that \( (\lambda_1)^n = 1 \) and \( (\lambda_2)^n = 1 \) will simply be a matter of finding the order of the elements \( \lambda_1 \) and \( \lambda_2 \) in \( (\mathbb{Z}/p\mathbb{Z})^* \). If the orders of the two elements are equal, then \( n \) will equal their common order. Else if the orders are not equal, then the minimal \( n \) will equal the least common multiple of their individual orders. The maximum order \( \lambda_1 \) and \( \lambda_2 \) can have is the order of the group, and the order of \( (\mathbb{Z}/p\mathbb{Z})^* \) is \( p - 1 \). As noted previously, the order of an element always divides the order of the group. Therefore, the orders of \( \lambda_1 \) and \( \lambda_2 \) are factors of \( p - 1 \). This explains why for \( p = 1 \) or \( 4 \mod 5 \), the period of the Fibonacci sequence mod \( p \) always divides \( p - 1 \).

For \( p = 2 \) or \( 3 \mod 5 \), the period of the Fibonacci sequence mod \( p \) always divides \( 2p + 2 \), but this is very difficult to prove and would be out of the scope of this thesis. However, we can verify these periods by graphing the data collected with the program in Appendix B.
Figure 5: primes $\equiv 1 \mod 5$

Figure 6: primes $\equiv 2 \mod 5$
Figure 7: primes $\equiv 3 \mod 5$
Figure 8: primes ≡ 4 mod 5
If you notice, the slope of the top lines for $p \equiv 1$ or $4 \bmod 5$ is $\frac{p-1}{p}$. Also, the slope of the lower lines is equal to $\frac{s}{p}$ where $s$ is some factor of $p-1$.

There is an equivalent relationship to the lines for $p \equiv 2$ or $3 \bmod 5$. In this case, the slope of the top lines is $\frac{2p+2}{p}$ while the slope of the lower lines is $\frac{t}{p}$ where $t$ is some factor of $2p+2$. 
Even though Conjecture 1 regarding the period of \( \frac{1}{n} \) has been proven false by the counterexamples \( p = 487 \) and \( p = 56,598,313 \), our efforts and methods have not been all for naught. Since the counterexamples are so few and far between, perhaps it is the case that

\[ T\left( \frac{1}{p^x} \right) = pT\left( \frac{1}{p} \right) \]

for \( p \) not equal to 487 or 56,598,313. This would imply that

\[
T\left( \frac{1}{n} \right) = T\left( \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}} \right) = \text{lcm}\left( T\left( \frac{1}{p_1^{\alpha_1}} \right), T\left( \frac{1}{p_2^{\alpha_2}} \right), \ldots, T\left( \frac{1}{p_k^{\alpha_k}} \right) \right)
\]

\[
= \text{lcm}\left( p_1^{\alpha_1-1} T\left( \frac{1}{p_1} \right), p_2^{\alpha_2-1} T\left( \frac{1}{p_2} \right), \ldots, p_k^{\alpha_k-1} T\left( \frac{1}{p_k} \right) \right).
\]

Even though computers help us determine the period of the Fibonacci sequence mod \( p \), they will not be able to prove that our conjectures are true because there are infinitely many primes. Therefore, more theoretical work would eventually be needed in order to prove our conjecture that \( T\left( \frac{1}{p^x} \right) = pT\left( \frac{1}{p} \right) \) for all primes \( p \).
Appendix

Definition: If \( \gcd(a, n) = 1 \) and \( a \) is of order \( \phi(n) \mod n \), then \( a \) is a primitive root of \( n \).

It is unknown if there exist an infinite number of primes such that \( T(\frac{1}{p}) = p - 1 \). For the primes that this is true, the order of 10 in \( \left( \mathbb{Z}/p\mathbb{Z} \right) \) is \( p - 1 = \phi(p) \). Therefore, 10 is a primitive root of \( p \). In his *Disquisitiones Arithmeticae*, Gauss conjectured that there are infinitely many primes having 10 as a primitive root. In other words, in relation to what we are studying, his conjecture could be thought of as "there are infinitely many primes such that \( T(\frac{1}{p}) = p - 1 \)". A few such primes that were generated in a program we wrote (see Appendix A) are listed in the chart below.

<table>
<thead>
<tr>
<th>Primes such that ( T(\frac{1}{p}) = p - 1 )</th>
<th>0&lt;p&lt;1000</th>
<th>1000&lt;p&lt;2000</th>
<th>2000&lt;p&lt;3000</th>
<th>3000&lt;p&lt;4000</th>
<th>4000&lt;p&lt;5000</th>
<th>5000&lt;p&lt;6100</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>503</td>
<td>1019</td>
<td>1531</td>
<td>2017</td>
<td>2539</td>
<td>3011</td>
</tr>
<tr>
<td>17</td>
<td>509</td>
<td>1021</td>
<td>1543</td>
<td>2029</td>
<td>2543</td>
<td>3019</td>
</tr>
<tr>
<td>19</td>
<td>541</td>
<td>1033</td>
<td>1549</td>
<td>2063</td>
<td>2549</td>
<td>3023</td>
</tr>
<tr>
<td>23</td>
<td>571</td>
<td>1051</td>
<td>1553</td>
<td>2069</td>
<td>2579</td>
<td>3137</td>
</tr>
<tr>
<td>29</td>
<td>577</td>
<td>1063</td>
<td>1567</td>
<td>2099</td>
<td>2593</td>
<td>3167</td>
</tr>
<tr>
<td>47</td>
<td>593</td>
<td>1093</td>
<td>1603</td>
<td>2113</td>
<td>2617</td>
<td>3221</td>
</tr>
<tr>
<td>59</td>
<td>619</td>
<td>1087</td>
<td>1579</td>
<td>2137</td>
<td>2621</td>
<td>3251</td>
</tr>
<tr>
<td>61</td>
<td>647</td>
<td>1091</td>
<td>1583</td>
<td>2141</td>
<td>2633</td>
<td>3257</td>
</tr>
<tr>
<td>97</td>
<td>659</td>
<td>1097</td>
<td>1607</td>
<td>2143</td>
<td>2657</td>
<td>3259</td>
</tr>
<tr>
<td>109</td>
<td>701</td>
<td>1103</td>
<td>1619</td>
<td>2153</td>
<td>2663</td>
<td>3299</td>
</tr>
<tr>
<td>113</td>
<td>709</td>
<td>1109</td>
<td>1621</td>
<td>2179</td>
<td>2687</td>
<td>3301</td>
</tr>
<tr>
<td>131</td>
<td>727</td>
<td>1153</td>
<td>1663</td>
<td>2207</td>
<td>2699</td>
<td>3313</td>
</tr>
<tr>
<td>149</td>
<td>743</td>
<td>1171</td>
<td>1697</td>
<td>2221</td>
<td>2713</td>
<td>3331</td>
</tr>
<tr>
<td>167</td>
<td>811</td>
<td>1181</td>
<td>1709</td>
<td>2251</td>
<td>2731</td>
<td>3343</td>
</tr>
<tr>
<td>179</td>
<td>821</td>
<td>1193</td>
<td>1741</td>
<td>2269</td>
<td>2741</td>
<td>3371</td>
</tr>
<tr>
<td>181</td>
<td>823</td>
<td>1217</td>
<td>1777</td>
<td>2273</td>
<td>2753</td>
<td>3389</td>
</tr>
<tr>
<td>193</td>
<td>857</td>
<td>1223</td>
<td>1783</td>
<td>2297</td>
<td>2767</td>
<td>3407</td>
</tr>
<tr>
<td>223</td>
<td>863</td>
<td>1229</td>
<td>1789</td>
<td>2309</td>
<td>2777</td>
<td>3433</td>
</tr>
<tr>
<td>229</td>
<td>887</td>
<td>1259</td>
<td>1811</td>
<td>2339</td>
<td>2789</td>
<td>3461</td>
</tr>
<tr>
<td>233</td>
<td>937</td>
<td>1291</td>
<td>1823</td>
<td>2341</td>
<td>2819</td>
<td>3463</td>
</tr>
<tr>
<td>257</td>
<td>941</td>
<td>1297</td>
<td>1847</td>
<td>2371</td>
<td>2833</td>
<td>3469</td>
</tr>
<tr>
<td>263</td>
<td>953</td>
<td>1301</td>
<td>1861</td>
<td>2383</td>
<td>2851</td>
<td>3989</td>
</tr>
<tr>
<td>269</td>
<td>971</td>
<td>1303</td>
<td>1873</td>
<td>2389</td>
<td>2861</td>
<td>4423</td>
</tr>
<tr>
<td>313</td>
<td>977</td>
<td>1327</td>
<td>1913</td>
<td>2411</td>
<td>2887</td>
<td>4447</td>
</tr>
<tr>
<td>337</td>
<td>983</td>
<td>1367</td>
<td>1949</td>
<td>2417</td>
<td>2897</td>
<td>4451</td>
</tr>
<tr>
<td>367</td>
<td>1381</td>
<td>979</td>
<td>1979</td>
<td>2423</td>
<td>2903</td>
<td>4457</td>
</tr>
<tr>
<td>379</td>
<td>1429</td>
<td>1247</td>
<td>2447</td>
<td>2909</td>
<td>4463</td>
<td>5981</td>
</tr>
<tr>
<td>383</td>
<td>1433</td>
<td>1247</td>
<td>2459</td>
<td>2927</td>
<td>6011</td>
<td></td>
</tr>
<tr>
<td>389</td>
<td>1447</td>
<td>1247</td>
<td>2473</td>
<td>2939</td>
<td>6029</td>
<td></td>
</tr>
<tr>
<td>419</td>
<td>1487</td>
<td>2971</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>433</td>
<td>6047</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>461</td>
<td>6113</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>487</td>
<td>6131</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>491</td>
<td>6143</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix A: Mathematica code to determine $T\left(\frac{1}{p}\right)$ and $T\left(\frac{1}{p^2}\right)$ for $1 < p < 6133$

(* Jody Radowicz
Thesis, FA 2001
Prime Factorization of $p - 1, 2p + 2; \text{period of } 1/p \]*)

BoundNum = 20000;

ClearAll[EndCount, n, TableRow, p, remainder, PeriodCount, p2Count, p2remainder, a, DataTable];

(* count prime numbers from 2 to the BoundNum *)
EndCount = 0;
For[n = 2, n <= BoundNum, n++, If[PrimeQ[n], EndCount++]];

DataTable = TableForm[Array[a, {EndCount, 7}], TableHeadings ->
{None, {"p", "Factor p-1", "T(p)", "T(p)/(p-1)", "p^2", "T(p^2)", "p * T(p)"}}];

TableRow = 1;

For[n = 2, n <= BoundNum, n++,
If[PrimeQ[n],
  p = n;
  a[TableRow, 1] = p;
  a[TableRow, 2] = FactorInteger[p - 1];
  a[TableRow, 5] = p^2;

  If[n != 2 && n != 5,
    PeriodCount = 0;
    remainder = 10;

    If[Mod[10, n] == 1,
      PeriodCount = 1;
      a[TableRow, 3] = PeriodCount,
      (* else *) PeriodCount++;
    ]

    While[Mod[remainder, n] != 1,
      remainder = Mod[10*remainder, n];
      PeriodCount++ (* end while *);
    
    a[TableRow, 3] = PeriodCount; (* end if: T(p) is calculated. *)
  ]

  a[TableRow, 4] = PeriodCount/(p - 1);
  p2Count = 0;]
p2remainder = 10;

If[Mod[10, n^2] == 1,
    p2Count = 1;
    a[TableRow, 6] = p2Count,
(*else*) p2Count++;

    While[Mod[p2remainder, n^2] != 1,
        p2remainder = Mod[10*p2remainder, n^2];
        p2Count++; (*end while*)
    a[TableRow, 6] = p2Count;]; (*end if: T(p^2) is calculated.*)

a[TableRow, 7] = p*PeriodCount,

(*else p = 2 or 5*)
    PeriodCount = 1;
    a[TableRow, 3] = 1;
    a[TableRow, 4] = PeriodCount/(p - 1);
    a[TableRow, 6] = 1;
    a[TableRow, 7] = p*PeriodCount;
]

(*end if n is prime*);

TableRow++;]

](*end for*)

Print[DataTable];
### Appendix A1: Example Data from code in Appendix A

<table>
<thead>
<tr>
<th>p</th>
<th>Factor p-1</th>
<th>T(p)</th>
<th>T(p) / (p-1)</th>
<th>p(^2)</th>
<th>T(p(^2))</th>
<th>p * T(p)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2 1</td>
<td>1</td>
<td>1/2</td>
<td>9</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>2 2</td>
<td>1</td>
<td>1/4</td>
<td>25</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>2 1</td>
<td>6</td>
<td>1</td>
<td>49</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>11</td>
<td>2 1</td>
<td>2</td>
<td>1/5</td>
<td>121</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>13</td>
<td>2 1</td>
<td>6</td>
<td>1/2</td>
<td>169</td>
<td>78</td>
<td>78</td>
</tr>
<tr>
<td>17</td>
<td>2 4</td>
<td>16</td>
<td>1</td>
<td>289</td>
<td>272</td>
<td>272</td>
</tr>
<tr>
<td>19</td>
<td>2 1</td>
<td>18</td>
<td>1</td>
<td>361</td>
<td>342</td>
<td>342</td>
</tr>
<tr>
<td>23</td>
<td>2 1</td>
<td>22</td>
<td>1</td>
<td>529</td>
<td>506</td>
<td>506</td>
</tr>
<tr>
<td>29</td>
<td>2 2</td>
<td>28</td>
<td>1</td>
<td>841</td>
<td>812</td>
<td>812</td>
</tr>
<tr>
<td>31</td>
<td>2 1</td>
<td>15</td>
<td>1/2</td>
<td>961</td>
<td>465</td>
<td>465</td>
</tr>
<tr>
<td>37</td>
<td>2 2</td>
<td>3</td>
<td>1/12</td>
<td>1369</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>41</td>
<td>2 1</td>
<td>5</td>
<td>1/8</td>
<td>1681</td>
<td>205</td>
<td>205</td>
</tr>
<tr>
<td>43</td>
<td>2 1</td>
<td>21</td>
<td>1/2</td>
<td>1849</td>
<td>903</td>
<td>903</td>
</tr>
<tr>
<td>47</td>
<td>2 1</td>
<td>46</td>
<td>1</td>
<td>2209</td>
<td>2162</td>
<td>2162</td>
</tr>
<tr>
<td>53</td>
<td>2 2</td>
<td>13</td>
<td>1/4</td>
<td>2809</td>
<td>689</td>
<td>689</td>
</tr>
<tr>
<td>59</td>
<td>2 1</td>
<td>58</td>
<td>1</td>
<td>3481</td>
<td>3422</td>
<td>3422</td>
</tr>
<tr>
<td>61</td>
<td>2 1</td>
<td>60</td>
<td>1</td>
<td>3721</td>
<td>3660</td>
<td>3660</td>
</tr>
<tr>
<td>67</td>
<td>2 1</td>
<td>33</td>
<td>1/2</td>
<td>4489</td>
<td>2211</td>
<td>2211</td>
</tr>
<tr>
<td>71</td>
<td>2 1</td>
<td>35</td>
<td>1/2</td>
<td>5041</td>
<td>2485</td>
<td>2485</td>
</tr>
<tr>
<td>73</td>
<td>2 3</td>
<td>8</td>
<td>1/9</td>
<td>5329</td>
<td>584</td>
<td>584</td>
</tr>
<tr>
<td>79</td>
<td>2 1</td>
<td>13</td>
<td>1/6</td>
<td>6241</td>
<td>1027</td>
<td>1027</td>
</tr>
<tr>
<td>83</td>
<td>2 1</td>
<td>41</td>
<td>1/2</td>
<td>6889</td>
<td>3403</td>
<td>3403</td>
</tr>
</tbody>
</table>
Appendix B: Mathematica code to determine the period of the Fibonacci sequence mod $p$

(*Jody Radowicz*

Thesis, FA 2001

Prime Factorization of $p-1$, $2p+2$; period of $1/p$ *)

BoundNum = 2000;

ClearAll[EndCount, n, TableRow, p, remainder, PeriodCount, p2Count, p2remainder, a, DataTable];

(*count prime numbers from 2 to the BoundNum*)

EndCount = 0;
For[n = 2, n <= BoundNum, n++, If[PrimeQ[n], EndCount++]];

DataTable = TableForm[Array[a, {EndCount, 7}], TableHeadings ->

{None, [{"p", "p mod 5", "T(p)", "Factor", "T(p)^2", "p^2", 
"P * T(p)"}]}];

TableRow = 1;
Denom = 0;
MagicMatrix = (0 1;
1 1);

For[n = 2, n <= BoundNum, n++,

If[PrimeQ[n],

 p = n;
 a[TableRow, 1] = p;
 a[TableRow, 2] = Mod[p, 5];
 If[Mod[p, 5] == 2 || Mod[p, 5] == 3, a[TableRow, 4] = FactorInteger[2 + p + 2];
 Denom = 2 + p + 2, a[TableRow, 4] = FactorInteger[p - 1]; Denom = p - 1;]
 a[TableRow, 6] = p^2;

If[n ≠ 2 && n ≠ 5,

 PeriodCount = 0;
 remainder = MagicMatrix;

 If[Mod[MagicMatrix, n] = IdentityMatrix[2],
 PeriodCount = 1;
 a[TableRow, 3] = PeriodCount,

(*else*) PeriodCount++;}
While[Mod[remainder, n] ≠ IdentityMatrix[2],
    remainder = Mod[MatrixPower[MagicMatrix, PeriodCount + 1],
    n];
    PeriodCount++ (*end while*);
]
a[TableRow, 3] = PeriodCount; (*end if: T(p) is calculated.*)
a[TableRow, 5] = PeriodCount / Denom;

p2Count = 0;
p2remainder = MagicMatrix;

If[Mod[MagicMatrix, n^2] == IdentityMatrix[2],
    p2Count = 1,
(*else*) p2Count++;

While[Mod[p2remainder, n^2] ≠ IdentityMatrix[2],
    p2remainder =
    Mod[MatrixPower[MagicMatrix, p2Count + 1], n^2];
    p2Count++ (*end while*);];
(*end if: T(p^2) is calculated.*)

a[TableRow, 7] = p2Count / (p * PeriodCount),

(*else p==2 or 5*)
a[TableRow, 3] = 0;
a[TableRow, 5] = 0;
If[p == 2, a[TableRow, 7] = 1 (*T(4)==6*); a[TableRow, 3] = 3;
a[TableRow, 5] = 3 / 6, a[TableRow, 7] = 1 (*T(25)==100*); a[TableRow, 3] = 20;]

] (*end if n is prime*)

TableRow++;]
(*end for*)

Print[DataTable];
### Appendix B1: Sample data from code in Appendix B

<table>
<thead>
<tr>
<th>$p$</th>
<th>$p \mod 5$</th>
<th>T(p)</th>
<th>Factor (Expected)</th>
<th>$\frac{T(p)}{p^2}$</th>
<th>$p^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2 1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>8</td>
<td>2 3</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>20</td>
<td>2 2</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>16</td>
<td>2 4</td>
<td>1</td>
<td>49</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>10</td>
<td>2 1</td>
<td>1</td>
<td>121</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>28</td>
<td>2 7</td>
<td>1</td>
<td>169</td>
</tr>
<tr>
<td>17</td>
<td>2</td>
<td>36</td>
<td>2 7</td>
<td>1</td>
<td>289</td>
</tr>
<tr>
<td>19</td>
<td>4</td>
<td>18</td>
<td>2 3</td>
<td>1</td>
<td>361</td>
</tr>
<tr>
<td>23</td>
<td>3</td>
<td>48</td>
<td>2 3</td>
<td>1</td>
<td>529</td>
</tr>
<tr>
<td>29</td>
<td>4</td>
<td>14</td>
<td>2 7</td>
<td>1/2</td>
<td>841</td>
</tr>
<tr>
<td>31</td>
<td>1</td>
<td>30</td>
<td>2 5</td>
<td>1</td>
<td>961</td>
</tr>
<tr>
<td>37</td>
<td>2</td>
<td>76</td>
<td>2 19</td>
<td>1</td>
<td>1369</td>
</tr>
<tr>
<td>41</td>
<td>1</td>
<td>40</td>
<td>2 5</td>
<td>1</td>
<td>1681</td>
</tr>
<tr>
<td>43</td>
<td>3</td>
<td>88</td>
<td>2 11</td>
<td>1</td>
<td>1849</td>
</tr>
<tr>
<td>47</td>
<td>2</td>
<td>32</td>
<td>2 3</td>
<td>1/3</td>
<td>2209</td>
</tr>
<tr>
<td>53</td>
<td>3</td>
<td>108</td>
<td>2 3</td>
<td>1</td>
<td>2809</td>
</tr>
<tr>
<td>59</td>
<td>4</td>
<td>58</td>
<td>2 29</td>
<td>1</td>
<td>3481</td>
</tr>
<tr>
<td>61</td>
<td>1</td>
<td>60</td>
<td>2 5</td>
<td>1</td>
<td>3721</td>
</tr>
<tr>
<td>67</td>
<td>2</td>
<td>136</td>
<td>2 17</td>
<td>1</td>
<td>4489</td>
</tr>
</tbody>
</table>
Appendix C: Translation of Mathematica code from Appendix B into (optimized!) C

"thesis.h"
/* This code is released under the GPL or BSD style license. Your choice. However
 * if you use it (read optimize!) please let me know,
 * This program can generate prime numbers itself (assuming you have algomath installed)
 * Just define ALGOMATH when you compile it.
 * However I recommend reading the primes in from an ascii newline terminated file called
 * primes.txt; Your call however.
 * -johncsh@overflow.org
 */

#include <math.h>
#define DEFAULTBOUND 63356
#define PRIMEFACTORS
#define VERSION "1.0"

struct fraction {
    unsigned long num;
    unsigned long den;
    float dec;
};

struct Primefactor {
    int base;
    int exponent;
};

struct node {
    struct Primefactor factor;
    struct node * next;
};

struct DataEntry {
    unsigned long p;
    unsigned long pModFive;
    unsigned long TofP;
    unsigned long Expected;
    struct fraction ExpectedOverTofP;
    struct node * PrimeFactors;
    char * ExpectedPeriodP;
    unsigned long pSquare;
    struct fraction TofPSquareOverStuff;
    char * reserved;
};
unsigned long Prime;
unsigned long *Prime_array;
unsigned long *FullSize_Prime_array;
struct DataEntry * DataTable;
int NUM_PRIMES;
int finished = 0;

unsigned long LowerBound;
unsigned long LowerBoundOffset;
unsigned long UpperBound;

"thesis.c"
#include <stdio.h>
#ifdef ALGOMATH
#include <algomath.h>
#endif

#include "thesis.h"
#include <curses.h>
#include <ncurses.h>
#include <signal.h>

int T(int p); // notorious;
struct node * NewNode();
int PrintNodeList(struct node * n);
void DestroyNodeList(struct node *n);

struct node * PrimeFactorInteger(unsigned long, unsigned long * const);
void printmatrix(const unsigned long[2][2]);
void banner();
int init();
void PrintRecord (struct DataEntry D);
void DisplayOutput();
//struct DataEntry * DataTable;
void InterruptHandler();
void ExitHandler();
void compute(int cnt);
unsigned long * getPrimeWrapper(int lower, int upper);
void parse_arguments(int, char **);
void usage();

int tmp;
int main(int argc, char **argv)
{
    int cnt = 0;
    int i;
    parse_arguments(argc, argv);
    FullSize_Prime_array = (unsigned long *) getPrimeWrapper(2, UpperBound); // we want all the primes in this one
    Prime_array = (unsigned long *) getPrimeWrapper(LowerBound, UpperBound);
    signal(SIGINT, InterruptHandler);
    signal(SIGQUIT, ExitHandler);
    init();
    banner();
    while (cnt < NUM_PRIMES) // bound checking all done elsewhere now..
    {
        compute(cnt);
        cnt++;
    }
    finished = 1;
    free(Prime_array);
    free(FullSize_Prime_array);
    DisplayOutput();
}

void parse_arguments(int argc, char *argv[])
{
    if(argc == 1)
    {
        LowerBound = 2;
        UpperBound = DEFAULTBOUND;
    }
    else if(argc == 3)
    {
        LowerBound = atoi(argv[1]);
        UpperBound = atoi(argv[2]);
    }
    else
    {
        perror("invalid arguments\n");
        usage();
        exit(-1);
    }
}
functions.

```c
void usage()
{
    fprintf(stderr, "/thesis lower-bound upper-bound\n\n```
}

```c
void compute( int cnt)
{
    int p;
    int i;
    p = Prime_array[cnt];
    if (p == 0)
    {
        perror("fuck!!\n");
        exit(-1);
    }
    Prime = p; //prime is a global accessed by signal handler..
    DataTable[cnt].p = Prime_array[cnt];
    DataTable[cnt].pModFive = p % 5;
    DataTable[cnt].pSquare = p * p;
    #ifdef PRIMEFACTORS
    if (DataTable[cnt].pModFive == 2 || DataTable[cnt].pModFive == 3)
    {
        DataTable[cnt].Expected = (2*p+2);
        DataTable[cnt].PrimeFactors = PrimeFactorInteger((2*p+2),FullSize_Prime_array);
    }
    else
    {
        DataTable[cnt].Expected = (p-1);
        DataTable[cnt].PrimeFactors = PrimeFactorInteger(p-1, FullSize_Prime_array);
    }
    #endif
    // compute T(P)
    DataTable[cnt].TofP = T(p);
    DataTable[cnt].TofPSquareOverStuff.num = T(p*p);
    DataTable[cnt].TofPSquareOverStuff.den = p * DataTable[cnt].TofP;
    DataTable[cnt].TofPSquareOverStuff.dec = DataTable[cnt].TofPSquareOverStuff.num /
    DataTable[cnt].TofPSquareOverStuff.den;
```
void DisplayOutput()
{
    int i;

    printf("P p\%5 T(p) Factor\tT(p)/Expected / T(P)\tT(P^2)\tP*\tT(P)\n\n");
    if (finished)
        for (i = 0; i < NUM_PRIMES; i++)
            {
                PrintRecord(DataTable[i]);
            }
    else // terminating prematurely
        while (Prime_array[i] != Prime)
            {
                PrintRecord(DataTable[i]);
                i++;
            }
}

void printMatrix(const unsigned long m[2][2])
{
    printf("[%d][%d]\n", m[0][0], m[0][1]);
    printf("[%d][%d]\n", m[1][0], m[1][1]);
}

void banner()
{
    fprintf(stderr,"Number Crunching stuff by Jon and Jody.\n");
    fprintf(stderr,"This run were crunching upto %lu\n", UpperBound);
    fprintf(stderr,"Version : %s\n", VERSION);
}
int init() /* mise */
{
    fprintf(stderr, "INIT: NUM_PRIMES= %d\n", NUM_PRIMES);
    DataTable = NULL;
    DataTable = (struct DataEntry *) malloc (sizeof(struct DataEntry) * NUM_PRIMES);
    if (DataTable == NULL)
    {
        perror("malloc");
        exit(-1);
    }

    #ifdef ALGOMATH
    printf("AM-INIT: %d", am_init());
    #endif
}

void PrintRecord(struct DataEntry d)
{
    printf("%u\t", d.p);
    printf("%u\t", d.pModFive);
    printf("%u\t", d.TofP);
    #ifdef PRIMEFACTORS
    PrintNodeList(d.PrimeFactors);
    DestroyNodeList(d.PrimeFactors);
    #endif
    printf("(%u)/(%u) = (%d)", d(ExpectedOverToP).num, d(ExpectedOverToP).den, (int)
    d(ExpectedOverToP).dec);
    printf("%u\t", d.pSquare);
    printf("(%u)/(%u) = (%.2f)\n", d.TofPSquareOverStuff.num, d.TofPSquareOverStuff.den,
    d.TofPSquareOverStuff.dec);
}

struct node * NewNode()
{
    struct node * n;
    n = (struct node *) malloc(sizeof(struct node));
    if (n == NULL)
    {
        perror("malloc:");
        exit(-1);
    }

    n->factor.base=0;
n->factor.exponent=0;
n->next = NULL;
}

void DestroyNodeList(struct node *head)
{
    struct node *last;
    struct node *t;
t = head;
    while (t != NULL)
    {
        last = t;
        t = t->next;
        free(last);
    }
}

struct node *PrimeFactorInteger(unsigned long n, unsigned long *const Primes)
{
    int i = 0;
    int k;
    int t;
    struct node *head;
    struct node *tmp;

    head = NewNode();
tmp = head;

    i = 0;
    while (n != 1)
    {
        k = Primes[i];
        while (n == k*(n / k)) // while k divides n evenly;
        {
            tmp->factor.base = k;
            tmp->factor.exponent++;
            n = n / k;
        }
        tmp->next = NewNode();
tmp = tmp->next;
i++;
    }

    return head;
int PrintNodeList(struct node * n)
{
    while (n->factor.base != 0) {
        printf(" [%d %d] : ", n->factor.base, n->factor.exponent);
        n = n->next;
    }
}

int mats_twoxtwo_mod(unsigned long m[2][2], unsigned long p)
{
    m[0][0] = m[0][0] % p;
    m[0][1] = m[0][1] % p;
    m[1][0] = m[1][0] % p;
    m[1][1] = m[1][1] % p;
}

int simd_mats_2x2_mul(unsigned long a[2][2], unsigned long b[2][2], unsigned long c[2][2])
{
    c[0][0] = a[0][0]*b[0][0]+a[0][1]*b[1][0];
    c[0][1] = a[0][0]*b[0][1]+a[0][1]*b[1][1];
    c[1][0] = a[1][0]*b[0][0]+a[1][1]*b[1][0];
    c[1][1] = a[1][0]*b[0][1]+a[1][1]*b[1][1];
}

void InterruptHandler()
{
    fprintf(stderr, "Currently Crunching %d\n", Prime);
}

void ExitHandler()
{
    fprintf(stderr,"Exiting..\n");
    finished = 0;
    DisplayOutput();
    exit(-1);
}

int T(int p)
{
int i = 0;
unsigned long answer[2][2];
unsigned long temp[2][2];
unsigned long MagicMatrix[2][2];
MagicMatrix[0][0] = 0;
MagicMatrix[0][1] = 1;
MagicMatrix[1][0] = 1;
MagicMatrix[1][1] = 1;

memcpy(answer, MagicMatrix, sizeof(answer));
do {
    simd_mats_2x2_mul(MagicMatrix, answer, temp);
mats_twoxtwo_mod(temp, p);
    memcpy(answer, temp, sizeof(temp));
i = i + 1;
} while (memcmp(MagicMatrix, answer, sizeof(answer)) != 0);
return i;

unsigned long * getPrimeWrapper(int lower, int upper)
{
    unsigned long *ret;
    FILE *fp;
    char currentp[1024]; // if we ever have prime numbers > 1000 digits we'll be in trouble... >:
    int p;
    int cnt = 0;
    int tmp;
    int i;
#ifdef ALGOMATH
    if (lower != 2)
    {
        printf("algomath and ranges dont mix. setting lower bound to 2.\n");
        LowerBound = 2;
    }
    ret = _getPrimes(upper);
    while (ret[NUM_PRIMES] != 0)
        NUM_PRIMES++;
    return(ret);
#else
    fp = fopen("primes.txt","r");
    if (fp == NULL)
perror("cant open primes.txt, and you havent defined algomath. exiting. fopen():");

exit(-1);

/* first we need to know how many primes to allocate space for.
   this is inefficient but is it worse than constantly calling
   realloc on every prime? probably not. anyway it doesn't matter
   in the long run
*/
cnt = 0;
do {
    fgets(currentp, sizeof(currentp),fp);
    tmp = atoi(currentp);
    if ((tmp <= upper) && (tmp >= lower))
        cnt ++;
} while (tmp != 0);

// inefficient to go all the way. sue me.
NUM_PRIMES = cnt;
ret = (unsigned long *) malloc(sizeof(unsigned long) * (NUM_PRIMES));
if (ret == NULL)
{
    perror("malloc:");
    exit(-1);
}
rewind(fp);
cnt = 0;

do
{
    p = atoi(fgets(currentp, sizeof(currentp),fp));
    if ( (p >= lower) && (p <= upper))
    {
        ret[cnt] = p;
        cnt ++;
    }
} while (p != 0);

return ret;

#endif
### Appendix C1: Example of Data Generated by Code in Appendix C

AM-INIT: I Number Crunching stuff by Jon and Jody.
This run were crunching upto 65535
Version : 0.4
Exiting..

<table>
<thead>
<tr>
<th>P</th>
<th>P%5</th>
<th>T(p)</th>
<th>T(p)/Expected / T(P)</th>
<th>p^2</th>
<th>T(P^2)/p^2T(p)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>[2 1] : [3 1] : (6)/(3) = (2)</td>
<td>4</td>
<td>(6)/(6) = (1.00)</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>8</td>
<td>[2 3] : (8)/(8) = (1)</td>
<td>9</td>
<td>(24)/(24) = (1.00)</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>20</td>
<td>[2 2] : (4)/(20) = (0)</td>
<td>25</td>
<td>(100)/(100) = (1.00)</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>16</td>
<td>[2 4] : (16)/(16) = (1)</td>
<td>49</td>
<td>(112)/(112) = (1.00)</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>10</td>
<td>[2 1] : (10)/(10) = (1)</td>
<td>121</td>
<td>(110)/(110) = (1.00)</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>28</td>
<td>[2 2] : (28)/(28) = (1)</td>
<td>169</td>
<td>(364)/(364) = (1.00)</td>
</tr>
<tr>
<td>17</td>
<td>2</td>
<td>36</td>
<td>[2 2] : [3 2] : (36)/(36) = (1)</td>
<td>289</td>
<td>(612)/(612) = (1.00)</td>
</tr>
<tr>
<td>19</td>
<td>4</td>
<td>18</td>
<td>[2 1] : [3 2] : (18)/(18) = (1)</td>
<td>361</td>
<td>(342)/(342) = (1.00)</td>
</tr>
<tr>
<td>23</td>
<td>3</td>
<td>48</td>
<td>[2 2] : [2 1] : (48)/(48) = (1)</td>
<td>529</td>
<td>(1104)/(1104) = (1.00)</td>
</tr>
<tr>
<td>29</td>
<td>4</td>
<td>14</td>
<td>[2 2] : (28)/(14) = (2)</td>
<td>841</td>
<td>(406)/(406) = (1.00)</td>
</tr>
<tr>
<td>31</td>
<td>1</td>
<td>30</td>
<td>[2 1] : [3 1] : (5 1) : (30)/(30) = (1)</td>
<td>961</td>
<td>(930)/(930) = (1.00)</td>
</tr>
<tr>
<td>37</td>
<td>2</td>
<td>76</td>
<td>[2 2] : (76)/(76) = (1)</td>
<td>1369</td>
<td>(2812)/(2812) = (1.00)</td>
</tr>
<tr>
<td>41</td>
<td>1</td>
<td>40</td>
<td>[2 3] : (40)/(40) = (1)</td>
<td>1681</td>
<td>(1640)/(1640) = (1.00)</td>
</tr>
<tr>
<td>43</td>
<td>3</td>
<td>88</td>
<td>[2 3] : (88)/(88) = (1)</td>
<td>1849</td>
<td>(3784)/(3784) = (1.00)</td>
</tr>
<tr>
<td>47</td>
<td>2</td>
<td>32</td>
<td>[2 5] : [3 1] : (96)/(32) = (3)</td>
<td>2209</td>
<td>(1504)/(1504) = (1.00)</td>
</tr>
<tr>
<td>53</td>
<td>3</td>
<td>108</td>
<td>[2 2] : [3 3] : (108)/(108) = (1)</td>
<td>2809</td>
<td>(5724)/(5724) = (1.00)</td>
</tr>
<tr>
<td>59</td>
<td>4</td>
<td>58</td>
<td>[2 1] : (58)/(58) = (1)</td>
<td>3481</td>
<td>(3422)/(3422) = (1.00)</td>
</tr>
<tr>
<td>61</td>
<td>1</td>
<td>60</td>
<td>[2 2] : [3 1] : (5 1) : (60)/(60) = (1)</td>
<td>3721</td>
<td>(3660)/(3660) = (1.00)</td>
</tr>
<tr>
<td>67</td>
<td>2</td>
<td>136</td>
<td>[2 3] : (136)/(136) = (1)</td>
<td>4489</td>
<td>(9112)/(9112) = (1.00)</td>
</tr>
<tr>
<td>71</td>
<td>1</td>
<td>70</td>
<td>[2 2] : (70)/(70) = (1)</td>
<td>5041</td>
<td>(4970)/(4970) = (1.00)</td>
</tr>
<tr>
<td>73</td>
<td>3</td>
<td>148</td>
<td>[2 2] : (148)/(148) = (1)</td>
<td>5329</td>
<td>(10804)/(10804) = (1.00)</td>
</tr>
<tr>
<td>79</td>
<td>4</td>
<td>78</td>
<td>[2 1] : [3 1] : (78)/(78) = (1)</td>
<td>6241</td>
<td>(6162)/(6162) = (1.00)</td>
</tr>
<tr>
<td>83</td>
<td>3</td>
<td>168</td>
<td>[2 3] : [3 1] : (168)/(168) = (1)</td>
<td>6889</td>
<td>(13944)/(13944) = (1.00)</td>
</tr>
<tr>
<td>89</td>
<td>4</td>
<td>44</td>
<td>[2 3] : (88)/(44) = (2)</td>
<td>7921</td>
<td>(3916)/(3916) = (1.00)</td>
</tr>
<tr>
<td>97</td>
<td>2</td>
<td>196</td>
<td>[2 2] : (196)/(196) = (1)</td>
<td>9409</td>
<td>(19012)/(19012) = (1.00)</td>
</tr>
<tr>
<td>101</td>
<td>1</td>
<td>50</td>
<td>[2 2] : (100)/(50) = (2)</td>
<td>10201</td>
<td>(5050)/(5050) = (1.00)</td>
</tr>
<tr>
<td>103</td>
<td>3</td>
<td>208</td>
<td>[2 4] : (208)/(208) = (1)</td>
<td>10609</td>
<td>(21424)/(21424) = (1.00)</td>
</tr>
<tr>
<td>107</td>
<td>2</td>
<td>72</td>
<td>[2 3] : [3 3] : (216)/(72) = (3)</td>
<td>11449</td>
<td>(7704)/(7704) = (1.00)</td>
</tr>
<tr>
<td>113</td>
<td>3</td>
<td>76</td>
<td>[2 2] : [3 1] : (228)/(76) = (3)</td>
<td>12769</td>
<td>(8588)/(8588) = (1.00)</td>
</tr>
<tr>
<td>127</td>
<td>2</td>
<td>256</td>
<td>[2 8] : (256)/(256) = (1)</td>
<td>16129</td>
<td>(32512)/(32512) = (1.00)</td>
</tr>
<tr>
<td>131</td>
<td>1</td>
<td>130</td>
<td>[2 1] : (130)/(130) = (1)</td>
<td>17161</td>
<td>(17030)/(17030) = (1.00)</td>
</tr>
<tr>
<td>137</td>
<td>2</td>
<td>276</td>
<td>[2 2] : [3 1] : (276)/(276) = (1)</td>
<td>18769</td>
<td>(37812)/(37812) = (1.00)</td>
</tr>
<tr>
<td>139</td>
<td>4</td>
<td>46</td>
<td>[2 1] : [3 1] : (138)/(46) = (3)</td>
<td>19321</td>
<td>(6394)/(6394) = (1.00)</td>
</tr>
<tr>
<td>149</td>
<td>4</td>
<td>148</td>
<td>[2 2] : (148)/(148) = (1)</td>
<td>22201</td>
<td>(22052)/(22052) = (1.00)</td>
</tr>
<tr>
<td>151</td>
<td>1</td>
<td>50</td>
<td>[2 1] : [3 1] : [5 2] : (150)/(50) = (3)</td>
<td>22801</td>
<td>(7550)/(7550) = (1.00)</td>
</tr>
<tr>
<td>157</td>
<td>2</td>
<td>316</td>
<td>[2 2] : (316)/(316) = (1)</td>
<td>24649</td>
<td>(49612)/(49612) = (1.00)</td>
</tr>
<tr>
<td>163</td>
<td>3</td>
<td>328</td>
<td>[2 3] : (328)/(328) = (1)</td>
<td>26569</td>
<td>(53464)/(53464) = (1.00)</td>
</tr>
</tbody>
</table>
Bibliography


   <http://www.lrz-muenchen.de/~hr/numb/fact486.htm>.

   <http://2357.a-tu.net/include/pages/software/algomath.zip>.