DISTRIBUTION OF PRIMES
IN CERTAIN CLASSES OF NUMBERS.

by

Helen Rose Garman
A. B., University of Kansas, 1918.

Submitted to the Department of Mathematics and the Faculty of the Graduate School of the University of Kansas in partial fulfillment of the requirements for the degree of Master of Arts.

Approved by:

[Signature]
Instructor in Charge

[Signature]
Head of Department.

May 31, 1924.
CONTENTS.

I INTRODUCTION. 1

II METHOD FOR DETERMINING THE NUMBER
OF PRIMES LESS THAN A GIVEN NUMBER 2

III TO DETERMINE IF THERE ARE TWO PRIMES
p_i, p_j SUCH THAT p_i - p_j = 2, BETWEEN
ANY TWO GIVEN NUMBERS 6

IV NUMBERS OF THE FORM \(2^n \cdot p + 1\) 11

V SPECIAL THEOREMS ON NUMBERS OF
THE FORM \(2^n \cdot p \pm 1\) 22

VI NUMBERS OF THE FORMS \(2^n \cdot q^l \pm 1\) 30
I INTRODUCTION

It is the purpose of this paper to discuss certain problems relating to the distribution of primes using a finite Euclidean modular plane as a basis of suggestion, and, in particular, the distribution of certain primes of form $2^n p + 1$ where $p$ is a prime.

Using modulus 5, the modular Euclidean plane consists of 5$^3$ points, arranged in a square, and, in this plane (see Figure 1) it is noticeable that all primes greater than 3 fall on two lines. Extending these two lines, products of primes appear, the first one being 25. All numbers on these two lines are of the forms $6 n \pm 1$ and consequently all primes greater than 3 are among them.
Figure I
II METHOD FOR DETERMINING THE NUMBER OF PRIMES LESS THAN A GIVEN NUMBER.

In order to find the number of primes which precede any given number \( A \), it is necessary to reject all products of primes from the numbers of the form \( 6n \pm 1 \) which precede \( A \). If \( A \) is not itself of the form \( 6n \pm 1 \) it is possible to find the first \( 6n \pm 1 \) number larger and reckon from it. Call this new number \( N \). There can be no primes between \( A \) and \( N \).

All numbers of the form \( 6n+1 \) lie on the line \( x = 1 \mod 6 \), and numbers of the form \( 6n-1 \) lie on the line \( x = -1 \mod 6 \). If \( N \) is of the form \( 6n+1 \) there will be \( \frac{N-1}{6} \) numbers of that form preceding it and the same number of \( 6n-1 \) numbers, making a total of \( \frac{N-1}{3} \). If \( N \) is of the form \( 6n-1 \) there will be \( \frac{N+1}{6} \) numbers of the form \( 6n+1 \) preceding it, and \( \frac{N+1}{6} - 1 \) or \( \frac{N-5}{6} \) numbers of \( 6n-1 \) form, making a total of \( \frac{N-2}{3} \). In either case represent this number by \( S \).

Next must be taken from \( S \), all numbers in \( S \) which are composite. The numbers will consist of products of primes from 5 to \( \sqrt{N} \). All numbers of \( S \) satisfy the congruences

\[
x \equiv \pm 1, \mod 6.
\]

Multiples of any prime may be found by solving simultaneously the congruences

\[
x \equiv \pm 1, \mod 6
\]
\[
x \equiv 0, \mod p_i \quad (i = 1, 2 \cdots k) \quad p_1 = 5, \quad p_k \leq \sqrt{N}.
\]
The solutions are
\[ x \equiv p_i, 5p_i, \mod 6p_i. \]
They will contain every multiple of every prime from 5 to \( \sqrt{N} \) and will constitute the class \( S_1 \).

In taking out all the multiples of \( p_i \), the numbers divisible by \( p_i \) and \( p_j \) have been removed twice and must be added back. They will satisfy the congruences
\[
\begin{align*}
x &\equiv \pm 1, \mod 6 \\
x &\equiv 0, \mod p_i \quad (i = 1, 2 \ldots \ell - 1) \\
x &\equiv 0, \mod p_j \quad (j = 2, 3 \ldots \ell) .
\end{align*}
\]

Their solutions
\[ x \equiv p_i p_j, 5p_i p_j, \mod 6p_i p_j \]
will make up the class of numbers \( S_2 \).

In the same way \( S_3 \) or numbers that are products of three primes may be found by solving
\[
\begin{align*}
x &\equiv \pm 1, \mod 6 \\
x &\equiv 0, \mod p_i \quad (i = 1, 2 \ldots \ell - 2) \\
x &\equiv 0, \mod p_j \quad (j = 2, 3 \ldots \ell - 1) \\
x &\equiv 0, \mod p_k \quad (k = 3, 4 \ldots \ell)
\end{align*}
\]
The solutions are
\[
\begin{align*}
x &\equiv p_i p_j p_k \mod 6p_i p_j p_k \\
x &\equiv 5p_i p_j p_k
\end{align*}
\]
This process may be continued until the solutions are larger than \( N \). Each solution giving numbers of some class as \( S_n \). This number will be added if \( n \) is even and subtracted if \( n \) is odd. Finally the number of
primes from 2 to \( \sqrt{N} \) must be added in.

The number of primes less than \( N \) and therefore less than \( A \) may be expressed by the formula.

\[
\left[ \frac{s - s_1 + s_2 - s_3 \ldots}{2} \right] - \left( \frac{1}{2} \right)^k \left[ \text{all primes, } 2, 3, \ldots, \sqrt{N} \right]
\]

EXEMPLARY.

To find the number of primes less than 249. 249 is of the form \( 6n-3 \). The first number above it of the form \( 6n+1 \) is 251 which is \( 6n-1 \).

Let \( 251 = N \). \( \sqrt{N} = 13 + \)

\[ S = \frac{N-2}{3} = \frac{251-2}{3} = 83. \]

From \( S \) must be rejected all multiples of 5, 7, 11, 13.

These are given by the solutions

\[
x \equiv 5, 25 \mod 30 \quad \left[ \frac{251}{30} \right] = 8 \quad \frac{11}{30} \quad 17 \text{ multiples of 5}
\]

\[
x \equiv 7, 35 \mod 42 \quad \left[ \frac{251}{42} \right] = 5 \quad \frac{41}{42} \quad 12 \text{ multiples of 7}
\]

\[
x \equiv 11, 55 \mod 66 \quad \left[ \frac{251}{66} \right] = 3 \quad \frac{53}{66} \quad 7 \text{ multiples of 11}
\]

\[
x \equiv 13, 65 \mod 78 \quad \left[ \frac{251}{78} \right] = 3 \quad \frac{17}{78} \quad 7 \text{ multiples of 13}
\]

\[ S_1 = 17 + 12 + 7 + 7 = 43. \]

Corrections must be made for those numbers which have been taken out twice. They are given by the solutions.

\[
x \equiv 35, 175 \mod 210 \quad \left[ \frac{251}{210} \right] = 1 \quad \frac{41}{210} \quad 3 \text{ rejections}
\]

\[
x \equiv 55, 275 \mod 330 \quad \left[ \frac{251}{330} \right] = 0 \quad \frac{251}{330} \quad 1 \text{ rejection}
\]

\[
x \equiv 65, 325 \mod 390 \quad 1 \text{ rejection}
\]

\[
x \equiv 77, 385 \mod 562 \quad 1 \text{ rejection}
\]

\[
x \equiv 91, 455 \mod 546 \quad 1 \text{ rejection}
\]

\[
x \equiv 143, 715 \mod 858 \quad 1 \text{ rejection}
\]

\[ S_2 = 3 + 1 + 1 + 1 + 1 + 1 = 8. \]
Products of three primes must be added back. They will satisfy the congruence

\[ x \equiv 385, 1925, \mod 2310. \]

Since 385 \( \not\equiv N \), there is no \( S_3 \).

Number of primes \( < N = (83 - 43 + 8) + 6 = 54 \).

Six is the number of primes 2, 3, 5, 7, 11, 13 which have been taken out when their multiples were.
III TO DETERMINE IF THERE ARE TWO PRIMES \( p_x, p_j \), SUCH THAT \( p_x - p_j = 2 \), BETWEEN ANY TWO GIVEN NUMBERS.

If there are two successive primes they are of the forms \( 6n-1 \) and \( 6n+1 \). Let \( a \) represent the number of primes less than the \( 6n-1 \) number and \( b \) represent the number less than the next \( 6n-1 \) number. If \( b - a = 2 \) there are between these two limits two primes, \( p_x, p_j \), such that \( p_x - p_j = 2 \).

All primes below \( \ell \) are in \( a \), all below \( \ell' \) are in \( b \).
The difference between \( b \) and \( a \) will be 0,1,2 depending on whether the two numbers in between are both composite, one prime and one composite or both prime.

Given any two numbers, it is always possible to find all sets of successive numbers of the forms \( 6n-1 \) and \( 6n+1 \). Each of these sets must be tested. Call the \( 6n-1 \) number of a set, \( N \), and the next larger \( 6n-1 \) number \( N' \). \( S \), as before, represents the number of numbers of the forms \( 6n\pm1 \) which precede \( N \) and similarly \( S' \) may be used for the number of such numbers less than \( N' \).

Obviously \( S' - S = 2 \).

\( S \), by the preceding section, contains every multiple of every prime from 5 to \( \sqrt{N} \). \( S' \) has the same meaning for the number \( N' \). If the number of multiples of primes
in $S_i$ is exactly the same as the number in $S_i'$, that is, if $S_i = S_i'$ then the two new numbers in $S'$ must be primes and there will be two primes between $N$ and $N'$.

If $\sqrt{N'} > N$ then $S_i' > S_i$ and it is unnecessary to go on. But if $\sqrt{N'} = N$ i.e. $p_\zeta = p_\zeta'$ then the multiples of each prime must be compared.

The number of multiples of each prime is given by the solutions $x = p_\zeta \pmod{6}$, $5p_\zeta \pmod{6}$ of the congruences

$x = \pm 1 \pmod{6}$

$x = 0 \pmod{p_\zeta}$

This number depends on the quotient obtained by dividing $N$ by the modulus $(6p_\zeta)$ and also on the remainder

\[ \frac{N}{6p_\zeta} = Q + \frac{R}{6p_\zeta} \text{ or } N \equiv R \pmod{6p_\zeta}. \]

If $R \leq p_\zeta$ then there are $Q$ multiples of $p_\zeta$ to be counted, but if $R > p_\zeta$, $Q + 1$ multiples must be counted. The equality of $S_i$ and $S_i'$ may be determined by calculating only $R$ and $R'$ for $p_\zeta$.

**Theorem I**  The necessary and sufficient conditions for $S_i = S_i'$ are:

1. $R < p_\zeta$ and $R' \leq p_\zeta'$
2. $R > p_\zeta$
3. $R < 5p_\zeta$ and $R' \leq 5p_\zeta$
4. $R > 5p_\zeta$

where $N \equiv R \pmod{6p_\zeta}$ and $N' \equiv R' \pmod{6p_\zeta'}$ and $6p_\zeta = 6p_\zeta'$.

**Proof:**

A. The conditions are necessary.

Assume $S_i = S_i'$. 


Then there is the same number of multiples of any prime $p_\alpha$ in $S_\prime$, as in $S_\prime'$. 

$$\frac{N}{6p_\alpha} = Q + \frac{R}{6p_\alpha}$$

or

$$N \equiv R \mod 6p_\alpha$$

If $R < p_\alpha$ there will be $Q$ multiples of $p_\alpha$ in $S_\prime$. Then there must be $Q$ multiples of $p_\alpha'$ in $S_\prime'$ and $R \leq p_\alpha'$. If however $R > p_\alpha$ there will be $Q + 1$ multiples of $p_\alpha$ in $S_\prime$. $R'$ is certainly greater than $p_\alpha$ or it could be $\leq p_\alpha'$, but in that case $Q$ itself would be increased by 1 and there would be $Q + 1$ multiples of $p_\alpha'$ in $S_\prime'$. If $R = p_\alpha$ there will be $Q$ multiples of $p_\alpha$ in $S_\prime$ but $R' > p_\alpha'$ there would be $Q + 1$ multiples of $p_\alpha'$ in $S_\prime'$ which is contrary to the assumption that $S_\prime = S_\prime'$. Therefore $R \neq p_\alpha'$.

The same reasoning may be applied to $5p_\alpha$.

B. The conditions are sufficient.

Assume the four conditions hold.

If (1) holds and there are $Q$ multiples of $p_\alpha$ there will be $Q$ multiples of $p_\alpha'$. The same is true for (2), (3), (4). If there are the same number of products of primes in $S_\prime$ as in $S_\prime'$ then $S_\prime = S_\prime'$ and the conditions are sufficient.

EXAMPLES.

(1) To test if there are two primes two apart between 386 and 395.
386 = 6n - 4
389 = 6n - 1 = N
395 = 6n' - 1 = N'

\[ \sqrt{389} = 19 + p_e \quad \sqrt{395} = 19 + p'_e. \]

\[ p_1 = 5, \quad 5p_1 = 25 \]
\[ 389 \equiv 29 \mod 30 \]
\[ 395 \equiv 5 \mod 30 \]

\[ p_2 = 7, \quad 5p_2 = 35 \]
\[ 389 \equiv 11 \mod 42 \]
\[ 395 \equiv 17 \mod 42 \]

\[ p_3 = 11, \quad 5p_3 = 55 \]
\[ 389 \equiv 59 \mod 66 \]
\[ 395 \equiv 65 \mod 66 \]

\[ p_4 = 13, \quad 5p_4 = 65 \]
\[ 389 \equiv 77 \mod 78 \]
\[ 395 \equiv 5 \mod 78 \]

\[ p_5 = 17, \quad 5p_5 = 85 \]
\[ 389 \equiv 89 \mod 102 \quad 83 < 85 \text{ but } 87 > 85 \]

\[ [(3) \text{ does not hold}] \]

\( S \neq S' \quad \text{There cannot be two primes whose difference is 2 between 386 and 395.} \)
(2) Between 1056 and 1065.

\[ N = 1061 \quad N' = 1067 \]

\[ \sqrt{N} = 31 + \quad \sqrt{N'} = 31 + \]

<table>
<thead>
<tr>
<th>( p )</th>
<th>( 5p )</th>
<th>( R )</th>
<th>( R' )</th>
<th>mod ( 6p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>25</td>
<td>1061 ≡ 11</td>
<td>1067 ≡ 17</td>
<td>mod 30</td>
</tr>
<tr>
<td>7</td>
<td>35</td>
<td>1061 ≡ 11</td>
<td>1067 ≡ 17</td>
<td>mod 42</td>
</tr>
<tr>
<td>11</td>
<td>55</td>
<td>1061 ≡ 5</td>
<td>1067 ≡ 11</td>
<td>mod 66</td>
</tr>
<tr>
<td>13</td>
<td>65</td>
<td>1061 ≡ 47</td>
<td>1067 ≡ 53</td>
<td>mod 73</td>
</tr>
<tr>
<td>17</td>
<td>85</td>
<td>1061 ≡ 41</td>
<td>1067 ≡ 47</td>
<td>mod 102</td>
</tr>
<tr>
<td>19</td>
<td>95</td>
<td>1061 ≡ 35</td>
<td>1067 ≡ 41</td>
<td>mod 114</td>
</tr>
<tr>
<td>23</td>
<td>115</td>
<td>1061 ≡ 95</td>
<td>1067 ≡ 101</td>
<td>mod 138</td>
</tr>
<tr>
<td>29</td>
<td>145</td>
<td>1061 ≡ 17</td>
<td>1067 ≡ 23</td>
<td>mod 174</td>
</tr>
<tr>
<td>31</td>
<td>155</td>
<td>1061 ≡ 131</td>
<td>1067 ≡ 137</td>
<td>mod 187</td>
</tr>
</tbody>
</table>

The conditions (1), (2), (3), (4) hold in every case. Hence \( S = S' \) and there are two primes, 1061 and 1063, between 1056 and 1065.
One very interesting section of the theory of numbers is that pertaining to Fermat numbers: #

\[ F_n = 2^n + 1. \]

Fermat believed that numbers in this series were all prime, although he admitted he had no proof. The numbers \( F_0, F_1, F_2, F_3, F_4 \) are all prime, but \( F_5 \), as first shown by Euler, has the factor 641. In fact, no primes except the first five have been found in this series, although the only ones which have been shown to be composite are those for \( n = 5, 6, 7, 8, 9, 11, 12, 13, 23, 36, 38, 73. \)

The numbers \( F_n \) have a very important geometric connection. Gauss proved that a regular polygon of \( m \) sides can be inscribed in a circle if \( m \) is the product of a power of 2 and distinct odd primes each of the form \( F_n \) and that the construction is impossible if \( m \) is not such a product.

The first general theorem about Fermat numbers was proved by Euler, who stated that all factors of an \( F_n \) are of the form \( 2^{n+1} \cdot K + 1 \). This was extended by Lucas, who showed that \( K \) must be even in the above and that all factors of an \( F_n \) are of the form \( 2^{n+2} \cdot K + 1 \) where \( K \) may contain 2 as a factor but is not a power of 2.

An investigation of numbers of the form \(2^n p + 1\) might aid in the factorization of Fermat numbers. Numbers of the form \(2^{n+2}K + 1\), \(K \equiv 9 \cdot 2^{n+2}\), will not be factors of an \(F_n\) if they are composite. Hence one method of attack is to examine numbers of the forms \(2^n 3 + 1\), \(2^n 5 + 1\), \(2^n 7 + 1\), etc., to see which are primes.

A great many numbers in the series \(2^n p + 1\) will be found to be composite by testing the series for multiples of small prime numbers, up to 200 or 300. This may be done by congruences in the following way.

To test \(2^n 3 + 1\) for multiples of 13.

\[
2^n 3 + 1 \equiv 0, \mod 13 \\
2^n \equiv -\frac{1}{3} \equiv -9 \equiv 4, \mod 13 \\
2^n \equiv 2^2, \mod 13
\]

\(n \equiv 2, \mod 12\) (2 appertains to 12, \(\mod 13\))

Then all \(2^n 3 + 1\) numbers, such that \(n \equiv 2, \mod 12\), are divisible by 13 and are not prime.

A large number of numbers in the list \(2^n p + 1\) \((n=1, 2, 3, \ldots)\) can be eliminated in this way. In order to determine by this method whether or not a number \(2^n p + 1\) is a prime it would be necessary to test out all primes \(\leq \sqrt{2^n p + 1}\). If \(2^n p + 1\) is a very large number that would be impossible.

However this process will eliminate a great many of the numbers of any series \(2^n p + 1\), for \(n\) less than a fixed limit and the remaining ones may be tested by different schemes.
One of these is setting up a sequence of factors such that if the given number divides any one of the factors, or perhaps a certain factor, it is a prime.

The converse of Fermat's theorem may be used to suggest the type of factors a prime of the form \(2^p + 1\) might divide. However it can be used as an absolute test only with certain restrictions.

Fermat's theorem states that if \(p\) is a prime and \(x\) is prime to \(p\), then
\[
x^{p-1} \equiv 1, \mod p.
\]
The converse of this is not in general true. It may however be stated with an added condition, thus:

If \(m\) is prime to \(x\) and
\[
x^{m-1} \equiv 1, \mod m.
\]
\(m\) is a prime if \(x\) appertains to \(m - 1\), \mod \(m\).

In testing numbers of the form \(2^p \cdot 3 + 1\) for prime factors less than 200, \(2^p \cdot 3 + 1\) still remained in the list so the following test was used.

Assuming that \(2^3 + 1\) is a prime
\[
x^{2^3} - 1 \equiv 0, \mod 2^3 + 1.
\]
Since 2 is prime to \(2^3 + 1\)
\[
2^{2^3} - 1 \equiv 0, \mod 2^3 + 1,
\]
\[
\left(2^2\right)^3 - 1 \equiv 0, \mod 2^3 + 1,
\]
\[
\left(2^3\right)^{3^1} - 1 \equiv 0, \mod 2^3 + 1,
\]
\[
(2^2 - 1)(2 + 2 + 1) \equiv 0, \mod 2^3 + 1
\]
\[ (2^9 + 1)(2^9 + 1) \quad \text{and} \quad (2^9 - 2^9 + 1) \quad \text{mod} \quad 2^3 \cdot 3 + 1. \]

The test to determine if \( 2^3 \cdot 3 + 1 \) divides any one of these factors is made by means of congruences.

\[
\begin{array}{ccc}
2^4 & 2^{16} & \equiv 65,536, \\
2^5 & 2^{32} & \equiv 1,073,741,823, \\
2^6 & 2^{64} & \equiv 1,789,569,709, \\
2^7 & 2^{128} & \equiv 2,823,543,319, \\
2^8 & 2^{256} & \equiv 2,680,181,363, \\
2^9 & 2^{512} & \equiv 2,619,512,439, \\
2^{10} & 2^{1024} & \equiv 2,568,188,054, \\
2^{11} & 2^{2048} & \equiv 968,661,660, \\
2^{12} & 2^{4096} & \equiv 284,107,013, \\
2^{13} & 2^{8192} & \equiv 169,472,026, \\
2^{14} & 2^{16384} & \equiv 2,377,954,849, \\
2^{15} & 2^{32768} & \equiv 1,936,264,007, \\
2^{16} & 2^{65536} & \equiv 2,237,516,130,
\end{array}
\]
### Table of Residues

<table>
<thead>
<tr>
<th>$2^k$</th>
<th>$131,072$</th>
<th>$1,727,764,320$, mod $2^{30} \cdot 3 + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^2$</td>
<td>$2$</td>
<td>$1$</td>
</tr>
<tr>
<td>$2^3$</td>
<td>$2$</td>
<td>$2$</td>
</tr>
<tr>
<td>$2^4$</td>
<td>$2$</td>
<td>$2$</td>
</tr>
<tr>
<td>$2^5$</td>
<td>$529,288$</td>
<td>$2,580,793,757$, mod $2$</td>
</tr>
<tr>
<td>$2^6$</td>
<td>$2,048,576$</td>
<td>$2,790,750,043$, mod $2$</td>
</tr>
<tr>
<td>$2^7$</td>
<td>$2,097,152$</td>
<td>$2,338,520,778$, mod $2$</td>
</tr>
<tr>
<td>$2^8$</td>
<td>$2,144,309$</td>
<td>$2,265,749,702$, mod $2$</td>
</tr>
<tr>
<td>$2^9$</td>
<td>$2,388,608$</td>
<td>$2,656,619,387$, mod $2$</td>
</tr>
<tr>
<td>$2^{10}$</td>
<td>$14,777,216$</td>
<td>$1,808,672,996$, mod $2$</td>
</tr>
<tr>
<td>$2^{11}$</td>
<td>$33,584,432$</td>
<td>$821,039,136$, mod $2$</td>
</tr>
<tr>
<td>$2^{12}$</td>
<td>$47,108,864$</td>
<td>$814,403,528$, mod $2$</td>
</tr>
<tr>
<td>$2^{13}$</td>
<td>$134,217,728$</td>
<td>$1,610,563,585$, mod $2$</td>
</tr>
<tr>
<td>$2^{14}$</td>
<td>$268,435,456$</td>
<td>$1,610,563,584$, mod $2$</td>
</tr>
</tbody>
</table>

From which,

$$2^2 - 2^{17} + 1 \equiv 0, \text{ mod } 2^{30} \cdot 3 + 1.$$  

In order to be certain this work was accurate every second residue was checked with the following list of congruences.
<table>
<thead>
<tr>
<th>$2^n$</th>
<th>$\equiv$</th>
<th>$\text{mod } 2 \cdot 3 + 1.$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{20}$</td>
<td>$1,048,576,$</td>
<td></td>
</tr>
<tr>
<td>$2^{40}$</td>
<td>$1,073,741,483,$</td>
<td></td>
</tr>
<tr>
<td>$2^{60}$</td>
<td>$2,863,428,040,$</td>
<td></td>
</tr>
<tr>
<td>$2^{160}$</td>
<td>$530,242,372,$</td>
<td></td>
</tr>
<tr>
<td>$2^{320}$</td>
<td>$1,901,455,336,$</td>
<td></td>
</tr>
<tr>
<td>$2^{640}$</td>
<td>$524,150,829,$</td>
<td></td>
</tr>
<tr>
<td>$2^{1280}$</td>
<td>$418,263,290,$</td>
<td></td>
</tr>
<tr>
<td>$2^{2560}$</td>
<td>$922,353,767,$</td>
<td></td>
</tr>
<tr>
<td>$2^{5120}$</td>
<td>$762,201,009,$</td>
<td></td>
</tr>
<tr>
<td>$2^{10,240}$</td>
<td>$2,906,796,372,$</td>
<td></td>
</tr>
<tr>
<td>$2^{20,480}$</td>
<td>$611,880,581,$</td>
<td></td>
</tr>
<tr>
<td>$2^{40,960}$</td>
<td>$1,293,570,037,$</td>
<td></td>
</tr>
<tr>
<td>$2^{81,920}$</td>
<td>$2,579,934,397,$</td>
<td></td>
</tr>
<tr>
<td>$2^{163,840}$</td>
<td>$1,472,271,016,$</td>
<td></td>
</tr>
<tr>
<td>$2^{327,680}$</td>
<td>$2,861,585,202,$</td>
<td></td>
</tr>
<tr>
<td>$2^{655,360}$</td>
<td>$2,210,668,708,$</td>
<td></td>
</tr>
<tr>
<td>$2^{1,310,720}$</td>
<td>$515,548,281,$</td>
<td></td>
</tr>
<tr>
<td>$2^{2,621,440}$</td>
<td>$9,713,756,$</td>
<td></td>
</tr>
</tbody>
</table>
\[
\begin{align*}
2 & \quad 5,242,880 \quad \equiv \quad 919,072,420, \quad \mod 2 \cdot 3 + 1. \\
2 & \quad 10,485,760 \quad \equiv \quad 1,103,893,155, \quad " \quad " \\
2 & \quad 20,971,520 \quad \equiv \quad 613,873,902, \quad " \quad " \\
2 & \quad 41,943,040 \quad \equiv \quad 1,375,529,269, \quad " \quad " \\
2 & \quad 83,886,080 \quad \equiv \quad 2,613,498,640, \quad " \quad " \\
2 & \quad 167,772,160 \quad \equiv \quad 207,632,640, \quad " \quad " \\
2 & \quad 335,544,320 \quad \equiv \quad 199,542,951, \quad " \quad " \\
2 & \quad 671,088,640 \quad \equiv \quad 1,610,661,889, \quad " \quad " \\
\end{align*}
\]

If the test of a number \( m \) by this method shows that \( 2^{m-1} \equiv 1 \pmod{m} \), then \( m \) is a prime if also \( 2 \) appertains to \( m - 1 \), \( \mod m \), where \( 2 \) is prime to \( m \).

But numbers of the form \( 2^{n} p + 1 \) are also of the form \( 81 + 1 \) and have \( 2 \) for a quadratic residue, so \( 2^{m-1} \equiv 1 \pmod{m} \) or \( 2^{\frac{n-1}{p}} \equiv 1 \pmod{2^p + 1} \). If \( 2 \) appertains then to \( 2^{\frac{n-1}{p}} \), modulus \( 2^p + 1 \) it follows at once that \( 2^p + 1 \) is a prime. If, however \( 2^a \cdot p - 1 \equiv \alpha \pmod{2^p + 1} \) \( (a < n - 1) \), it does not follow that \( 2^p + 1 \) is composite because for the prime \( 2^3 \cdot 3 + 1 \), \( 2^3 \cdot 3 - 1 \equiv 0 \pmod{2^4 \cdot 3 + 1} \) \( 39 = n - 2 \).
In the test given for the number $2 \cdot 3 + 1$ it was discovered that

$$2^8 - 2^7 + 1 \equiv 0, \mod 2 \cdot 3 + 1$$

which means that

$$2^2 \cdot 3 - 1 \equiv 0, \mod 2 \cdot 3 + 1.$$ 

Since $2^8 = n - 2$, no definite conclusion can be made about the primality of $2 \cdot 3 + 1$.

Numbers of the form $2^n \cdot 3 + 1$ cannot be factors of Fermat numbers, so this test is of interest mainly to show the power of residues in dealing with very large numbers, $2^8 - 2^7 + 1$ being a number of more than three hundred million places. It will be noticed also that if the $2^n \cdot p + 1$ number in question is a divisor of an $F_n$ that will appear in the test since all $F_n$'s of which it might be a factor are included in the factors of $2^2 - 1$. In fact the proof for the largest number definitely known to be a prime, $2 \cdot 5 + 1$, is based on the fact that it is a divisor of $F_{73}$.

An investigation of the numbers $2^n \cdot 5 + 1$ soon reveals the fact that for $n$ an even number $2^n \cdot 5 + 1$ is composite since it contains the factor 3. For, 

$$2^n \cdot 5 + 1 \equiv 0, \mod 3.$$ 

$$2^n \equiv -\frac{1}{5} \equiv -2 \equiv 1 \equiv 2, \mod 3.$$ 

$n = 0, \mod 2$ (2 appertains to 2, $\mod 3$)

Odd values of \( n \leq 79 \) for which \( 2^n + 5 + 1 \) is prime have been computed to be \( n = 1, 3, 7, 13, 15, 25, 39, 55, 75 \). Of these four are factors of \( F_n \), namely, \( n = 7, 25, 39, 75 \).

Numbers in the list \( 2^n + 1 \) are always composite if \( n \) is odd, for 3 is a factor.

\[ 2^n \cdot 7 + 1 \equiv 0 \pmod{3} \]

\[ 2^n \equiv -1 \equiv 2 \pmod{3} \]

\[ n \equiv 1 \pmod{2} \]

The following results were obtained when the series \( 2^n \cdot 7 + 1 \) was tested for multiples of other small primes

\[ P = 5 \quad n \equiv 1 \pmod{4} \]
\[ 11 \quad n \equiv 3 \pmod{10} \]
\[ 13 \quad n \equiv 7 \pmod{12} \]
\[ 17 \quad \text{none} \]
\[ 19 \quad n \equiv 3 \pmod{18} \]
\[ 23 \quad n \equiv 7 \pmod{11} \]
\[ 29 \quad n \equiv 2 \pmod{28} \]
\[ 31 \quad \text{none} \]
\[ 37 \quad n \equiv 22 \pmod{36} \]
\[ 41 \quad \text{none} \]
\[ 43 \quad \text{none} \]
\[ 47 \quad \text{none} \]
\[ 53 \quad n \equiv 12 \pmod{52} \]
\[ 59 \quad n \equiv 11 \pmod{58} \]
\[ 61 \quad n \equiv 41 \pmod{60} \]
<table>
<thead>
<tr>
<th>n</th>
<th>mod</th>
</tr>
</thead>
<tbody>
<tr>
<td>67</td>
<td>10 mod 66</td>
</tr>
<tr>
<td>71</td>
<td>29 mod 35</td>
</tr>
<tr>
<td>73</td>
<td>none</td>
</tr>
<tr>
<td>79</td>
<td>16 mod 39</td>
</tr>
<tr>
<td>83</td>
<td>33 mod 82</td>
</tr>
<tr>
<td>89</td>
<td>none</td>
</tr>
<tr>
<td>97</td>
<td>none</td>
</tr>
<tr>
<td>101</td>
<td>41 mod 100</td>
</tr>
<tr>
<td>103</td>
<td>none</td>
</tr>
<tr>
<td>107</td>
<td>10 mod 106</td>
</tr>
<tr>
<td>109</td>
<td>none</td>
</tr>
<tr>
<td>113</td>
<td>4 mod 28</td>
</tr>
<tr>
<td>127</td>
<td>none</td>
</tr>
<tr>
<td>131</td>
<td>99 mod 130</td>
</tr>
<tr>
<td>137</td>
<td>57 mod 64</td>
</tr>
<tr>
<td>139</td>
<td>19 mod 138</td>
</tr>
<tr>
<td>149</td>
<td>80 mod 148</td>
</tr>
<tr>
<td>151</td>
<td>none</td>
</tr>
<tr>
<td>157</td>
<td>15 mod 52</td>
</tr>
<tr>
<td>163</td>
<td>8 mod 81</td>
</tr>
<tr>
<td>167</td>
<td>none</td>
</tr>
<tr>
<td>173</td>
<td>163 mod 173</td>
</tr>
<tr>
<td>179</td>
<td>96 mod 173</td>
</tr>
<tr>
<td>181</td>
<td>75 mod 180</td>
</tr>
<tr>
<td>191</td>
<td>76 mod 190</td>
</tr>
<tr>
<td>193</td>
<td>55 mod 192</td>
</tr>
</tbody>
</table>
197 \( n \equiv 148 \mod 196 \)

199 \( n \equiv 107 \mod 198 \)

Accordingly in the series of numbers 2 \( 7 - 1 \) the only values for \( n \) 100 which remain untested are for

\( n = 24, 26, 34, 36, 42, 44, 46, 50, 52, 54, 56, 66, 70, 72, 74, 82, 90, 92. \)
V SPECIAL THEOREMS ON NUMBERS OF THE FORM $2^n p \pm 1$.

THEOREM II For any given number $N$ it is always possible to find two successive numbers of the forms $6n - l$ and $6n + l > N$, such that both of the numbers are composite.

PROOF: Consider the numbers $6^K \pm l$. For any given $N$ it is always possible to select a $K$ such that $6^K - l > N$. $6^K - l$ and $6^K + l$ are two successive numbers of the forms $6n - l$ and $6n + l$. $6^K - l$ is always divisible by 5 and $6^K + l$ is divisible by 7 for every odd value of $K$.

THEOREM III The necessary and sufficient condition that $2^n 3 - 1$ shall be composite is that for some prime $p$, where $5 \leq p < \sqrt{2^n 3 - 1}$ there exists a $K$ and an $\epsilon$ such that

$$3K \equiv 1 \mod p$$

$$K \equiv \epsilon \mod p$$

$$\epsilon \equiv n \mod t_2$$

where $2$ appertains to $t_2$, mod $p$.

A. The condition is necessary. Assume $2^n 3 - 1$ to be composite; then $2^n 3 - 1 \equiv 0 \mod p$, $5 \leq p < \sqrt{2^n 3 - 1}$. Since $3 < p$ and prime to $p$ there exists in the reduced residue system, modulus $p$, a $K$ such that $3K \equiv 1$, mod $p$. Then

$$2^n \equiv K, \mod p$$

$K$ is therefore a power residue of 2, mod $p$, say of $2^\epsilon$.

Hence $2^n \equiv 2^\epsilon \equiv K, \mod p$

where $n \equiv \epsilon, \mod t_2$. 
B. The condition is sufficient

If \(3K = 1, \mod p\) \hspace{1cm} (1)
\[K = 2^e, \mod p\] \hspace{1cm} (2)
and \(e = n, \mod t_2\) \hspace{1cm} (3)

From (1) and (2) \(3 \cdot 2^e = 1, \mod p\).

and from (3) \(n = rt_2 + e\),

then \(3 \cdot 2^{rt_2 + e} = 1, \mod p\). Since \(2^{rt_2} = 1, \mod p\).

Therefore \(2^n - 3 - 1 = 0, \mod p\).

COROLLARY: \(2^n - 3 - 1\) is a prime number if no \(K\) exists which satisfies the conditions \(\begin{cases} 3K = 1 \\ K = 2^e \end{cases}\) \mod p

for all values of \(p\) from 5 to \(\sqrt{2^n \cdot 3 - 1}\).

THEOREM IV The necessary and sufficient condition that \(2^n - 3 + 1\) shall be composite is that for some prime \(p\), where \(5 \leq p < \sqrt{2^n \cdot 3 + 1}\) there exists a \(K\) and an \(e\) such that

\[
\begin{cases} 3K = 1, \mod p. \\ -K = 2^e, \mod p. \\ e = n, \mod t_2. \end{cases}
\]

where \(2\) appertains to \(t_2, \mod p\).

A. The condition is necessary.

Assume \(2^n - 3 + 1\) to be composite; then

\(2^n - 3 + 1 = 0, \mod p\). \(5 \leq p < \sqrt{2^n \cdot 3 + 1}\). Since 3 is prime to \(p\) and \(p\), there will be a \(K\) in the reduced residue system, modulus \(p\), such that \(3K = 1, \mod p\).

\(-K = -K, \mod p\).

\(-K\) is therefore a power residue of 2, \mod p say \(2^e\).

Hence \(2^n = -K = 2^e, \mod p\), where \(n = e, \mod t_2\).
B. The condition is sufficient.

Assume

\[
\begin{align*}
3K &= 1, \quad \text{mod } p \quad (1) \\
-K &= 2^e, \quad \text{mod } p \quad (2) \\
n &= e, \quad \text{mod } t_2 \quad (3)
\end{align*}
\]

From (1) and (2) it follows that

\[3 \cdot 2^e \equiv -1, \quad \text{mod } p\]

but from (3) \(n = e + rt_2\),

hence \(3 \cdot 2^{e+rt_2} \equiv -1, \quad \text{mod } p\), since \(2^t_2 \equiv 1, \quad \text{mod } p\).

Therefore \(3 \cdot 2^n \equiv -1, \quad \text{mod } p\).

**COROLLARY:** \(2^n3 + 1\) is a prime number if no \(K\) exists which satisfies the conditions

\[
\begin{align*}
3K &= 1, \quad \text{mod } p \\
-K &= 2^e, \quad \text{mod } p
\end{align*}
\]

for all values of \(p^t_2, 5 \leq p < \sqrt{2^n3 + 1}\).

**THEOREM V** The necessary and sufficient condition that numbers of the form \(2^n5 - 1\) shall be composite is that for some prime \(p\), where \(3 \leq p < \sqrt{2^n5 - 1}\) there exists a \(K\) such that

\[
\begin{align*}
3K &= 1, \quad \text{mod } p \\
K &= 2^e, \quad \text{mod } p \\
n &= e, \quad \text{mod } t_2 \quad \text{where } 2 \text{ appertains to } t_2, \quad \text{mod } p.
\end{align*}
\]

A. The condition is necessary.

Assume \(2^n5 - 1\) to be composite; then for some \(p\), \(2^n5 - 1 \equiv 0, \quad \text{mod } p\).
Since $5 \leq p$ there is a $K$ such that $2^K = K \mod p$.

Therefore $K$ is a power residue of $2$, mod $p$, say $2^e$.

Then $2^n = 2^e = K \mod p$, where $n = e \mod t_2$.

**B. The condition is sufficient.**

Assume:

\[
\begin{cases}
5K \equiv 1 \quad \text{mod } p \quad (1) \\
K \equiv 2^e \quad \text{mod } p \quad (2) \\
e \equiv n \mod t_2 \quad (3)
\end{cases}
\]

From (1) and (2) it follows that $2^e - 5 \equiv 1 \mod p$.

From (3) $n = e \mod t_2$.

Then $2^e + 5 \equiv 1 \mod p$.

Therefore $5 \cdot 2^n \equiv 1 \mod p$.

**EXAMPLE:**

\[
2^e \cdot 5 - 1
\]

\[
2^e \cdot 5 - 1 = 0 \mod 11 \quad 5K \equiv 1 \mod 11 \\
K \equiv 9 \mod 11
\]

\[
2^e = 9 \mod 11
\]

\[
2^e = 9 = 2^e \mod 11
\]

\[
16 \equiv 6 \mod 10
\]

\[
2^e \cdot 5 - 1 \text{ is composite.}
\]

**COROLLARY:** $2^n - 5 - 1$ is a prime number if no $K$ exists which satisfies the conditions

\[
\begin{cases}
5K \equiv 1 \mod p \\
K \equiv 2^e \mod p
\end{cases}
\]

for all values of $p$, $p \leq 3$ and $< \frac{2^n - 5 - 1}{2^e}$. 
THEOREM VI The necessary and sufficient condition that \(2^n \cdot 5 + 1\) is composite is that for some prime \(p\), where \(3 \leq p < \sqrt{2^n \cdot 5 + 1}\) there exists a \(K\) and an \(e\) such that \(5K \equiv 1, \mod p\)

\(-K \equiv 2^e, \mod p\)

\[n \equiv e, \mod t_2,\] where \(2\) appertains to \(t_2, \mod p\).

A. The condition is necessary.

Assume \(2^n \cdot 5 + 1\) to be composite; then

\(2^n \cdot 5 + 1 \equiv 0, \mod p\) \(3 \leq p < \sqrt{2^n \cdot 5 + 1}\).

Since \(5 < p\) and prime to \(p\) there is a \(K\)

\(2^n \equiv -K, \mod p\).

\(-K\) is therefore a power residue of \(2, \mod p\), say \(2^e\). Then

\(2^n \equiv -K \cdot 2^e, \mod p\).

where \(n \equiv e, \mod t\).

B. The condition is sufficient.

Assume

\[
\begin{cases}
5K \equiv 1, \mod p \\
-K \equiv 2^e, \mod p \\
\quad \quad \quad n \equiv e, \mod t_2
\end{cases}
\]

From (1) and (2) it follows that \(5 \cdot 2^e \equiv 1, \mod p\).

From (3) \(n \equiv e + rt_2\)

then \(5 \cdot 2^{e + rt_2} \equiv -1, \mod p\). Since \(2^{rt_2} \equiv 1, \mod p\)

Therefore \(5 \cdot 2^n \equiv -1, \mod p\).

\(5 \cdot 2^n + 1 \equiv 0, \mod p\).

COROLLARY: \(2^n \cdot 5 + 1\) is prime if no \(K\) exists which satisfies the conditions \(5K \equiv 1\), \(-K \equiv 2^e\) \mod \(p_i\) for all values of \(p_i \equiv 3\) and \(\leq \sqrt{2^n \cdot 5 + 1}\).
THEOREM VII The necessary and sufficient condition that $2^n \cdot q - 1$ is composite is that for some prime $p$, where $3 \leq p < \sqrt{2^n \cdot q - 1}$ there exists a $K$ and an $e$ such that

\[
\begin{align*}
qK &= 1, \mod p \\
K &= 2^e, \mod p \\
n &= e, \mod t, \text{ where } 2 \text{ appertains to } t
\end{align*}
\]

mod $p$.

A. The condition is necessary.

Assume $2^n \cdot q - 1$ to be composite; then for some $p$, $2^n \cdot q - 1 \equiv 0, \mod p$, $3 \leq p < \sqrt{2^n \cdot q - 1}$.

Since is prime to $p$ there is a $K$ such that $qK \equiv 1, \mod p$.

$2^n \equiv K, \mod p$.

$K$ is therefore a power residue of $2, \mod p$, say $2^e$.

$2^n \equiv K \equiv 2^e, \mod p$.

$n \equiv e, \mod t$.

B. The condition is sufficient.

Assume

\[
\begin{align*}
qK &= 1, \mod p \\
+K &= 2^e, \mod p \\
n &= e, \mod t
\end{align*}
\]

From (1) and (2) it follows that $2^e \cdot q \equiv 1, \mod p$.

From (3) $n = e + rt$.

then $2^{e+rt} \equiv q \equiv 1, \mod p$. Since $2^t \equiv 1, \mod p$.

Therefore $2^n \cdot q \equiv 1, \mod p$. 

COROLLARY: $2^n \cdot q - 1$ is prime if no $K$ exists which satisfies the conditions

$$\begin{align*}
qK = 1 \\
K = 2^e
\end{align*} \mod p$$

for all values of $p_n \geq 3$ and $< \sqrt{2^n \cdot q - 1}$.  

THEOREM VIII The necessary and sufficient condition that $2^n \cdot q + 1$ is composite is that for some prime $p$, where $3 \leq p < \sqrt{2^n \cdot q + 1}$ there exists a $K$ and an $e$ such that

$$\begin{align*}
\{ qK = 1, \mod p, \\
K = 2^e, \mod p.
\end{align*}$$

A. The condition is necessary.  
Assume $2^n \cdot q + 1$ to be composite; then for some $p$,

$$2^n \cdot q + 1 = 0, \mod p. \quad 3 \leq p < \sqrt{2^n \cdot q + 1}.$$  
Since $q$ is prime to $p$ there is a $K$, $qK = 1, \mod p$.

$$2^n \equiv K, \mod p.$$  
K is therefore a power residue of 2, $mod p$, say $2^e$.

$$2^n = K = 2^e, \mod p.$$  
$n = e, \mod t_2$.

B. The condition is sufficient.  
Assume

$$\begin{align*}
\{ qK = 1, \mod p. \\
-K = 2^e, \mod p. \\
n = e, \mod t_2.
\end{align*}$$

From (1) and (2) it follows that $2^e \cdot q \equiv -1, \mod p$.  


From (3) \( n = e + r t_2 \),

then \( 2^{x_1} q \equiv -1 \mod p \). Since \( 2^{x_1} \equiv 1 \mod p \).

Therefore \( 2^n \cdot q \equiv -1 \mod p \).

\[ 2^n \cdot q + 1 \equiv 0 \mod p. \]

**COROLLARY:** \( 2^n \cdot q + 1 \) is prime if no \( K \) exists which satisfies the conditions

\[
\begin{align*}
qK &= 1 \\
-K &= 2
\end{align*}
\mod p.
\]

for all values of \( p_c \), \( 5 \leq p_c < \sqrt{2^n \cdot q + 1} \).
VI NUMBERS OF THE FORMS $2^n \cdot q^\ell \pm 1$.

The discussion of numbers of the forms $2^n \cdot q^\ell \pm 1$ may be divided into two cases, namely:

(1) $n$ and $\ell$ have a common factor,

(2) $n$ and $\ell$ are relatively prime numbers.

CASE (1)

If $n$ and $\ell$ have an odd common factor, $2^n \cdot q^\ell + 1$ is composite.

Let $d$ = any odd factor common to $n$ and $\ell$, then

$n = cd$ \hspace{1em} $\ell = bd$

and $2^n \cdot q^\ell + 1 = 2^{cd} \cdot q^{\ell d} + 1$

\[ = (2^c \cdot q^d)^\ell + 1 \]

\[ = [2^c \cdot q + 1] \left[ (2^c \cdot q^d)^{\ell - 1} - (2^c \cdot q^d)^{\ell - 2} \cdots - 1 \right]. \]

CASE (2)

If $n$ and $\ell$ do not have an odd common factor $q^\ell$ may be reduced by the modulus and $2^n \cdot q^\ell + 1$ will be composite or prime according as the conditions of THEOREM IV do or do not exist.

CASE (1)

If $n$ and $\ell$ have a common factor, $2^n \cdot q^\ell - 1$ is com-
positive. Let \( e \) = a factor common to \( n \) and \( \ell \) then

\[
n = ce \quad \ell = be
\]

and \( 2^n \cdot q^\ell - 1 = 2^{ce} \cdot q^{\ell e} - 1 \)

\[
= (2^{ce} \cdot q^{\ell e}) - 1
\]

\[
= [2^{ce} \cdot q^{\ell e} - 1] \left[ (2^{ce} \cdot q^{\ell e})^{\ell e} + (2^{ce} \cdot q^{\ell e})^{\ell e^2} + \cdots + 1 \right]
\]

CASE (2)

If \( n \) and \( \ell \) are relatively prime numbers \( q^\ell \) may be reduced by the modulus and \( 2^n \cdot q^\ell - 1 \) will be composite or prime according as the conditions of THEOREM III do or do not exist.
BIBLIOGRAPHY.


Arnoux - Essai de Geometrie Analytique Modulaire Gauthier-Villars, 1911.


Carmichael - "Fermat Numbers \( F_n = 2^{2^n} + 1 \)"


