ON THE DETERMINATION OF THE ZEROS OF THE FIBONACCI SEQUENCE

ROBERT P. BACKSTROM, Brighton High School, So. Australia

In his article [1], Brother U. Alfred has given a table of periods and zeros of the Fibonacci Sequence for primes in the range 2,000 < p < 3,000. The range p < 2,000 has been investigated by D. D. Wall [2]. The present author has studied the extended range p < 5,000 by computer, and has found that approximately 68% of the primes have zeros which are maximal or half maximal, i.e., Z(F,p) = p + 1, p - 1, (p + 1)/2 or (p - 1)/2.

It would seem profitable, then, to seek a formula which gives the values of Z(F,p) for some of these "time-consuming" primes. If these can be taken care of this way, the average time per prime would decrease since there are large primes with surprisingly small periods.

We have succeeded in producing a formula for two sets of primes. A table of zeros of the Fibonacci Sequence for primes in the range 3,000 < p < 10,000 discovered by these formulas is included at the end of this paper. It is not known whether these formulae apply to more than a finite set of primes. See [3] for some discussion on this point.

To develop the ideas in a somewhat more general context, we introduce the Primary Numbers F_n defined by the recurrence relation:

\[ F_{n+2} = aF_{n+1} + bF_n ; F_0 = 0, F_1 = 1, \]

where a and b are integral. F_n may be given explicitly in the Binet form;

\[ F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \]

where \( \alpha \) and \( \beta \) are the (assumed distinct) roots of the quadratic equation \( x^2 - ax - b = 0 \). In a like manner, we may define the Secondary Numbers which play the same role as the well known Lucas Numbers do to the Fibonacci Numbers. Thus the Secondary Numbers L_n are defined by the recurrence relation:
ON THE DETERMINATION OF THE ZEROS

\[ L_{n+2} = aL_{n+1} + bL_n \; ; \; L_0 = 2, \; L_1 = a. \]

\( L_n \) may also be given explicitly in the Binet form as:

\[ L_n = \alpha^n + \beta^n \]

The following three properties of the Primary Sequences may easily be established by induction, or by using formula (1).

1) \( F_r = (-b)^r F_{-r} \)

2) If \((a, b) = 1\), then \((F_n, b) = 1\)

3) If \((a, b) = 1\), then \((F_n, F_{n+1}) = 1\).

Using formula (1), it is a simple algebraic exercise to prove the next result.

**Lemma 1.** \( F_m = F_{i+1} F_{m-i} + b F_i F_{m-i-1} \)

**Proof:** Since \( \alpha \) and \( \beta \) are the roots of \( x^2 - ax - b = 0 \), we have \( \alpha \beta = -b \).

R. H. S. = \( (\alpha^{i+1} - \beta^{i+1})/(\alpha - \beta) \)

\[ = (\alpha^{i+1} - \beta^{i+1})/(\alpha - \beta) \]

\[ = (\alpha^m - \beta^m)/(\alpha - \beta) \]

\[ = F_m \]

Making use of properties 1) and 3) and Lemma 1, we may prove the following Theorem which tells us that the factors of Primary Sequences occur in similar patterns to those encountered in the Fibonacci Sequence itself.

**Theorem 1.** Let \((a, b) = 1\). Chose a prime \( p \) and an integer \( j \) such that \( p^j \) exactly divides \( F_d \) \((d > 0)\), but no Primary Number with smaller subscript. Then \( p^j \) divides \( F_n \) (not necessarily exactly) if and only if \( n = dt \) for some integer \( t \). Or: \( F_d \mid F_n \) iff \( n = dt \) for some integer \( t \).

**Proof.** Suppose that \( n = dt \). We prove by induction on \( t \) that \( p^j \) divides \( F_n \).

Assume true for \( t = t_0 \). \( p^j \) divides \( F_{t_0} \).

\[ *i.e., \; p^j \mid F_d \] but \( p^{j+1} \not\mid F_d \).
Putting \( m = d(t + 1) \) and \( i = d \) in Lemma 1, we have the identity:

\[
F_{dt(t+1)} = F_{dt+1}F_{dt} + bF_d F_{dt-1}
\]

\( p^j \) divides \( F_d \) and \( F_{dt} \) so by (1), divides \( F_{dt(t+1)} \).

Conversely, suppose that \( p^j \) divides \( F_n \), where \( n = dt + r \) for some \( r \) satisfying \( 0 < r < d \). We seek a contradiction, forcing \( r \) to equal 0.

Putting \( m = dt \) and \( i = -r \) in Lemma 1, we have the identity:

\[
F_{dt} = F_{-r+1}F_{dt+r} + bF_{-r}F_{dt+r-1}
\]

Multiplying through by \((-b)^{-r-1}\) and using the fact that \( F_r = (-b)^r F_{-r} \), we have:

\[
-b^r F_{dt} = F_{r-1}F_{dt+r} - F_r F_{dt+r-1}
\]

Since \( p^j \) divides both \( F_{dt} \) and \( F_{dt+r} \), it divides \( F_r F_{dt+r-r} \). However, if \( (a, b) = 1 \), consecutive Primary Numbers are co-prime, and so \( p \) does not divide \( F_{dt+r-r} \). Thus \( p^j \) divides \( F_r \), which is a contradiction.

Another result which we will need is contained in the next Theorem. This result is a direct generalization of the well-known result applied to Fibonacci Numbers. The proof follows precisely the one given by Hardy and Wright in [4], and so need not be repeated here.

**Theorem 2.** Let \( k = a^2 + 4b \neq 0 \) and \( p \) be a prime such that \( p \not| 2b \), then \( p \) divides \( F_{p^{-1}}F_p \) or \( F_{p+1} \) according as the Legendre Symbol \((k/p)\) is +1, 0 or -1.

**Proof.** Let the roots of the quadratic equation \( x^2 - ax - b = 0 \) be:

\[
\alpha = \frac{(a + \sqrt{a^2 + 4b})/2}{2} \quad \text{and} \quad \beta = \frac{(a - \sqrt{a^2 + 4b})/2}{2}
\]

Hence

\[
F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{(a + \sqrt{b})^n - (a - \sqrt{b})^n}{2^n \sqrt{k}}
\]
ON THE DETERMINATION OF THE ZEROS

Case 1. \((k/p) = +1\)

\[
2^{p-2} F_{p-1} = \left( (a + \sqrt{k})^{p-1} - (a - \sqrt{k})^{p-1} \right) / (2\sqrt{k})
\]

\[
= \left( \sum_{r=0}^{p-1} \binom{p-1}{r} a^{p-r} (\sqrt{k})^r - \sum_{r=0}^{p-1} \binom{p-1}{r} a^{p-r} (-\sqrt{k})^r \right) / (2\sqrt{k})
\]

\[
= \left( \sum_{\text{odd } r \leq p-2} \binom{p-1}{r} a^{p-r} (\sqrt{k})^r \right) / (\sqrt{k})
\]

\[
= \frac{(p-1)/2}{\sum_{s=0}^{(p-3)/2} \left( \binom{p-1}{2s+1} a^{p-2s-2} k^s \right)}
\]

since \((p-1)/2 \equiv -1 \pmod{p}\) for \(s = 0, 1, \ldots, (p-3)/2\), we find that

\[
2^{p-2} F_{p-1} \equiv - \sum_{s=0}^{(p-3)/2} a^{p-2s-2} k^s \pmod{p}.
\]

Summing this geometric progression, we have:

\[
2^{p-1} F_{p-1} \equiv a^p - a k^{(p-1)/2} \pmod{p}.
\]

Making use of Euler's Criterion \(k^{(p-1)/2} \equiv (k/p) \pmod{p}\) for the quadratic character of \(k \pmod{p}\), assuming that \(p \mid 2b\), \((k/p) = +1\) and knowing that \(a^p \equiv a \pmod{p}\), we have:

\[
F_{p-1} \equiv 0 \pmod{p}.
\]

Case 2. \((k/p) = 0\)

\[
2^{p-1} F_p = \left( (a + \sqrt{k})^p - (a - \sqrt{k})^p \right) / (2\sqrt{k})
\]

\[
= \left( \sum_{r=0}^{p} \binom{p}{r} a^{p-r} (\sqrt{k})^r - \sum_{r=0}^{p} \binom{p}{r} a^{p-r} (-\sqrt{k})^r \right) / (2\sqrt{k})
\]

\[
= \left( \sum_{\text{odd } r \leq p} \binom{p}{r} a^{p-r} (\sqrt{k})^r \right) / (\sqrt{k}) = \sum_{s=0}^{(p-1)/2} \left( \binom{p}{2s+1} a^{p-2s-2} k^s \right).
\]
p divides each Binomial Coefficient except the last and so:

\[ 2^{p-1} F_p \equiv k^{(p-1)/2} \pmod{p}, \]

Since \( p \not\mid 2b \) and \( (k/p) = 0 \), we have

\[ F_p \equiv 0 \pmod{p}. \]

**Case 3.** \( (k/p) = -1 \)

\[
2^{p}_{p+1} = \frac{(a + \sqrt{k})^{p+1} - (a - \sqrt{k})^{p+1}}{(2\sqrt{k})} \]

\[
= \left( \sum_{r=0}^{p} \binom{p+1}{r} a^{p-r+1} (\sqrt{k})^r \right) - \sum_{r=0}^{p+1} \binom{p+1}{r} a^{p-r+1} (-\sqrt{k})^r \right) \pmod{2\sqrt{k}}

\[
= \left( \sum_{r \text{ odd \population{1}}}^{p} \binom{p+1}{r} a^{p-r+1} (\sqrt{k})^r \right) \pmod{\sqrt{k}}

\[
= \sum_{s=0}^{(p-1)/2} \binom{p+1}{2s+1} a^{p-2s} k^s.
\]

All the Binomial Coefficients except the first and last are divisible by \( p \) and so:

\[
2^{p}_{p+1} \equiv a^p + ak^{(p-1)/2} \pmod{p}.
\]

Since \( p \not\mid 2b \), \( (k/p) = -1 \) and \( a^p \equiv a \pmod{p} \), we have:

\[ F_{p+1} \equiv 0 \pmod{p}. \]

Yet another well-known result which can be extended to the Primary Sequences is given in Lemma 2. A proof may be constructed on the model provided by Glenn Michael in [5], and is a simple exercise for the reader.
Lemma 2. If \((a, b) = 1\) and \(c, d\) are positive integers, then \(\left( F_e, F_d \right) = \left| F(c, d) \right| \).

Proof. Let \(e = (c, d)\) and \(D = (F_e, F_d)\). \(e\) and \(d\) hence by Theorem 1, \(F_e \mid F_c\) and \(F_e \mid F_d\). Thus \(F_e \mid D\).

There exist integers \(x\) and \(y\) (given by the Euclidean Algorithm) such that \(e = xc + yd\). Suppose without loss of generality that \(x > 0\) and \(y \leq 0\). Using Lemma 1 with \(m = xc\) and \(i = e\) we have:

\[
F_{xc} = F_{e-1}F_{-y} = bF_{e-y-1}.
\]

Thus \(D \mid F_c\) and \(D \mid F_d\) and so by Theorem 1, \(D \mid F_{xc}\) and \(F \mid F_{yd}\). Thus \(D \mid bF_{e-y-1}\), but by property 2, \((D, b) = 1\), and by property 3, \((D, F_{yd}) = 1\). Thus \(D \mid F_e\). This, together with \(F_e \mid D\) gives the result.

Lemma 3.

\[
F_{2n-1} - F_{n-1}L_n = (-b)^{n-1}
\]

Proof.

\[
\text{L.H.S.} = \left( \alpha^{2n-1} - \beta^{2n-1} - (\alpha^{n-1} - \beta^{n-1})(\alpha^n + \beta^n) / (\alpha - \beta) \right)
\]

\[
= \left( \alpha^{2n-1} - \beta^{2n-1} - \alpha^{2n-1} - \alpha^{n-1} \beta^n + \beta^{n-1} \alpha^n + \beta^{2n-1} / (\alpha - \beta) \right)
\]

\[
= (-\alpha^{n-1} \beta^n + \beta^{n-1} \alpha^n / (\alpha - \beta)
\]

\[
= (\alpha - \beta)(\alpha \beta)^{n-1} / (\alpha - \beta) = (\alpha \beta)^{n-1} = (-b)^{n-1} = \text{R.H.S.}
\]

MAIN RESULTS

We shall divide the main results of this paper into 6 parts — four Lemmas in which the essential ideas are proven, a Theorem utilizing these ideas and a Corollary applying them in particular to the Fibonacci Numbers. It will be implicitly understood that from now on, \((a, b) = 1\) and \(p \nmid 2abk\).

Lemma 4. If \((-b/p) = (k/p) = +1\) (Legendre Symbols), then \(p \mid F_{(p-1)/2}\).

Proof. Using Lemma 3 with \(n = (p + 1)/2\) gives

\[
F_p - \frac{F_{p-1}}{2} \frac{L_{p+1}}{2} = (-b)^{(p-1)/2}.
\]
In the proof of Theorem 2 we find that
\[ 2^{p-1} F_p \equiv F_p \equiv (k/p) \pmod{p}. \]

Thus:
\[ (k/p) - \frac{F_{p-1}}{2} \frac{L_{p+1}}{2} \equiv (-b/p) \pmod{p}. \]

Putting \((-b/p) = (k/p) = +1\) we have:
\[ \frac{F_{p-1}}{2} \frac{L_{p+1}}{2} \equiv 0 \pmod{p}. \]

Suppose, now, that \(p\) divides \(L_{(p+1)/2}\). Since \(L_{(p+1)/2} = F_{p+1} / F_{(p+1)/2}\), \(p\) divides \(F_{p+1}\). Theorem 2 tells us that \(p\) divides \(F_{p+1}\) since \((k/p) = +1\).

Applying Lemma 2, we see that \(p\) divides \(F_{(p-1),p+1}\) which is \(F_2\).

But \(F_2 = a\) and so we have a contradiction.

**Lemma 5.** If \((-b/p) = (k/p) = -1\), then \(p \nmid F_{(p+1)/2}\).

**Proof.** Using (3) with \((-b/p) = (k/p) = -1\) we have:
\[ \frac{F_{p-1}}{2} \frac{L_{p+1}}{2} \equiv 0 \pmod{p}. \]

Suppose that \(p \nmid F_{(p-1)/2}\). Therefore \(p \nmid F_{p-1}\). By Theorem 2, \(p \nmid F_{p+1}\), and so as before, we find that \(p \nmid F_2 = a\) a contradiction. Hence \(p \nmid L_{(p+1)/2}\).

Since \(L_n = a F_n + 2b F_{n-1}\) any prime divisor common to \(F_n\) and \(L_n\) must divide \(2b\) by property 3). These primes are excluded, and so \(p \nmid F_{(p+1)/2}\) as asserted.

**Lemma 6.** If \((-b/p) = +1, (k/p) = -1\), then \(p \nmid F_{(p+1)/2}\).

**Proof.** Putting \((-b/p) = +1\) and \((k/p) = -1\) in (3) we have:
\[ \frac{F_{p-1}}{2} \frac{L_{p+1}}{2} \equiv -2 \pmod{p}. \]
Thus $p | (p+1)/2$ since $p \neq 2$. Suppose, to the contrary, that $p | F_{(p+1)/2}$. By Theorem 2, $p | F_{p+1}$, and so $p | F_{p+1}/F_{(p+1)/2} = L_{(p+1)/2}$ a contradiction.

Lemma 7. If $(-b/p) = -1$ and $(k/p) = +1$, then $p | F_{(p-1)/2}$.

Proof. Similarly we have:

$$\frac{F_{p-1}}{2} \cdot \frac{L_{p+1}}{2} \equiv +2 \pmod{p}.$$ 

Clearly

$$p | F_{(p-1)/2}.$$ 

To distinguish from the Fibonacci case, we shall employ the terminology $Z(F; a, b; p)$ for the first non-trivial zero $(\pmod{p})$ of the Primary Sequence with parameters $a$ and $b$. Thus $Z(F; 1, 1; p) = Z(F, p)$ following the notation used by Brother U. Alfred in [1]. Similar remarks apply to $Z(L; a, b; p)$.

Main Theorem.

1) If $r$ is a prime and $p = 2r + 1$ is a prime such that $(-b/p) = (k/p) = +1$, then $Z(F; a, b; p) = r$.

2) If $s$ is a prime and $p = 2s - 1$ is a prime such that $(-b/p) = (k/p) = -1$, then $Z(F; a, b; p) = p + 1$.

3) If $s$ is a prime and $p = 2s - 1$ is a prime such that $(-b/p) = +1$, and $(k/p) = -1$, then $Z(F; a, b; p) = s$.

4) If $r$ is a prime and $p = 2r + 1$ is a prime such that $(-b/p) = -1$, and $(k/p) = +1$, then $Z(F; a, b; p) = p - 1$.

Proof of the Main Theorem.

1) Since $(k/p) = +1$, we see from Theorems 1 and 2 that $p | F_d$, where $d$ is a divisor of $p - 1 = 2r$. The only divisors of $2r$ are $1, 2, r$ and $2r$ since $r$ is prime. Clearly $p | F_1 = 1$ and by assumption $p | F_2 = a$. Lemma 4 tells us that $p | F_r$ and so $Z(F; a, b; p) = r$.

2) Since $(k/p) = -1$, $p | F_d$, where $d | p + 1 = 2s$. The divisors of $2s$ are $1, 2, s$ and $2s$. $p | F_1$ and $p | F_2$. Lemma 5 then tells us that $p | F_s$ and so $p$ must divide $F_{2s} = F_{p+1}$, i.e., $Z(F; a, b; p) = p + 1$.

3) Since $(k/p) = -1$, $p | F_d$, where $d | p + 1 = 2s$. Thus $d$ must be $1, 2, s$ or $2s$ because of the primality of $s$. $p | F_1$ and $p | F_2$. Lemma 6 tells us that $p | F_s$ and so $Z(F; a, b; p) = s$. 


4) Since \((k/p) = +1\), \(p|F_d\) where \(d|p - 1 = 2r\). Again \(d\) must be one of: \(1, 2, r\) or \(2r\) since \(r\) is prime, \(p|F_1\) and \(p|F_2\). Lemma 7 tells us that \(p|F_r\) and so \(p\) must divide \(F_{2r} = F_{p-1}\). Hence \(Z(F,a,b,p) = p - 1\).

Specializing the above results to the case of the Fibonacci Sequence \((F_{n+2} = F_{n+1} + F_n; F_0 = 0, F_1 = 1)\) by choosing \(a = b = 1\) and hence \(k = 5\), we find that parts 1) and 2) of the Main Theorem are now vacuous. Indeed, 1) requires \(p\) to be of the form \(20k + 1\) or \(9\), and thus \(r\) to be of the form \(10k + 0\) or \(4\) which cannot be prime; 2) requires \(p\) to be of the form \(20k + 3\) or \(7\), and thus \(s\) to be of the form \(10k + 2\) or \(4\) giving only the prime 2; 3) requires \(p\) to be of the form \(20k + 13\) or 17 requiring \(s\) to be of the form \(10k + 7\) or \(9\) which may now be prime and 4) requires \(p\) to be of the form \(20k + 11\) or 19 and thus \(r\) to be of the form \(10k + 5\) or 9 giving primes 5 and 10k + 9.

Thus we have established the following result:

**Corollary.** Employing the symbol \(Z(F,p)\) to denote the first non-trivial zero \((\mod p)\) among the Fibonacci Sequence \((F_{n+2} = F_{n+1} + F_n; F_0 = 0, F_1 = 1)\) we have:

1) \(s = 2\) and \(p = 2s - 1 = 3\) are both prime, and so \(Z(F,3) = 4\).

2) If \(s \equiv 7\) or 9 \((\mod 10)\) and \(p = 2s - 1\) are both prime, then \(Z(F,p) = s\).

3) \(r = 5\) and \(p = 2r + 1 = 11\) are both prime, and so \(Z(F,11) = 10\).

4) If \(r \equiv 9\) \((\mod 10)\) and \(p = 2r + 1\) are both prime, then \(Z(F,p) = p - 1\).

It would be interesting to discover other sets of primes which have determinable periods and zeros. One such set is the set of Mersenne primes \(M_p = 2^p - 1\), where \(p\) is a prime of the form \(4t + 3\). Since \((-1/M_p) = 6/M_p = -1\), Lemma 5 tells us that \(M_p|F_{2t} + 2\) and so \(M_p|F_{2g}\) for \(0 \leq g < 4t + 2\), otherwise we could obtain a contradiction from Theorem 1. However, Theorem 2 tells us that \(M_p|F_{2p}\), and so \(Z(F,M_p) = 2^p\).

A definite formula for \(Z(F,p)\) is not to be expected for the same reason that one would not expect to find a formula for the exponent to which a given integer \(c\) belongs modulo \(p\). However, some problems, such as that of classifying the set of primes for which \(Z(F,p)\) is even (the set of divisors of the Lucas Numbers \((p \neq 2)\)) may have partial or complete solutions, and so we leave the reader to investigate them.

TABLE OF ZEROS

<table>
<thead>
<tr>
<th>p</th>
<th>Z(F,p)</th>
<th>p</th>
<th>Z(F,p)</th>
<th>p</th>
<th>Z(F,p)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3119</td>
<td>3118</td>
<td>5399</td>
<td>5398</td>
<td>7393</td>
<td>3697</td>
</tr>
<tr>
<td>3217</td>
<td>1609</td>
<td>5413</td>
<td>2707</td>
<td>7417</td>
<td>3709</td>
</tr>
<tr>
<td>3251</td>
<td>1627</td>
<td>5437</td>
<td>2719</td>
<td>7477</td>
<td>3739</td>
</tr>
<tr>
<td>3313</td>
<td>1657</td>
<td>5659</td>
<td>5658</td>
<td>7537</td>
<td>3769</td>
</tr>
<tr>
<td>3517</td>
<td>1759</td>
<td>5879</td>
<td>5878</td>
<td>7559</td>
<td>7558</td>
</tr>
<tr>
<td>3733</td>
<td>1867</td>
<td>5939</td>
<td>5938</td>
<td>7753</td>
<td>3877</td>
</tr>
<tr>
<td>3779</td>
<td>3778</td>
<td>6037</td>
<td>3019</td>
<td>7933</td>
<td>3967</td>
</tr>
<tr>
<td>4057</td>
<td>2029</td>
<td>6073</td>
<td>3037</td>
<td>8039</td>
<td>8038</td>
</tr>
<tr>
<td>4079</td>
<td>4078</td>
<td>6133</td>
<td>3067</td>
<td>8053</td>
<td>4027</td>
</tr>
<tr>
<td>4139</td>
<td>4138</td>
<td>6217</td>
<td>3109</td>
<td>8317</td>
<td>4159</td>
</tr>
<tr>
<td>4177</td>
<td>2089</td>
<td>6337</td>
<td>3169</td>
<td>8353</td>
<td>4177</td>
</tr>
<tr>
<td>4259</td>
<td>4258</td>
<td>6373</td>
<td>3187</td>
<td>8677</td>
<td>4339</td>
</tr>
<tr>
<td>4273</td>
<td>2137</td>
<td>6599</td>
<td>6598</td>
<td>8699</td>
<td>8698</td>
</tr>
<tr>
<td>4357</td>
<td>2179</td>
<td>6637</td>
<td>3319</td>
<td>8713</td>
<td>4357</td>
</tr>
<tr>
<td>4679</td>
<td>4678</td>
<td>6659</td>
<td>6658</td>
<td>8819</td>
<td>8818</td>
</tr>
<tr>
<td>4799</td>
<td>4798</td>
<td>6719</td>
<td>6718</td>
<td>8893</td>
<td>4447</td>
</tr>
<tr>
<td>4919</td>
<td>4918</td>
<td>6779</td>
<td>6778</td>
<td>9013</td>
<td>4507</td>
</tr>
<tr>
<td>4933</td>
<td>2467</td>
<td>6899</td>
<td>6898</td>
<td>9133</td>
<td>4567</td>
</tr>
<tr>
<td>5077</td>
<td>2539</td>
<td>6997</td>
<td>3499</td>
<td>9277</td>
<td>4639</td>
</tr>
<tr>
<td>5099</td>
<td>5098</td>
<td>7057</td>
<td>3529</td>
<td>9817</td>
<td>4909</td>
</tr>
<tr>
<td>5113</td>
<td>2557</td>
<td>7079</td>
<td>7078</td>
<td>9839</td>
<td>9838</td>
</tr>
<tr>
<td>5233</td>
<td>2617</td>
<td>7213</td>
<td>3607</td>
<td>9973</td>
<td>4987</td>
</tr>
</tbody>
</table>

REFERENCES


3. Daniel Shanks, Solved and Unsolved Problems in Number Theory.

4. Hardy and Wright, An Introduction to the Theory of Numbers.


Continued from p. 306


*****