On the Conjecture of Hardy & Littlewood concerning the Number of Primes of the Form $n^2 + a$

By Daniel Shanks

1. Introduction. In a famous paper, [1], Hardy and Littlewood developed a number of conjectures concerning the twin primes, the Goldbach problem, and other unsettled questions. One of these, Conjecture F, concerned the number of primes of the form $Am^2 + Bm + C$. We reword this conjecture, and at the same time reduce its generality somewhat, as follows:

**Conjecture.** If $a$ is an integer which is not a negative square, $a \neq -k^2$, and if $P_a(N)$ is the number of primes of the form $n^2 + a$ for $1 \leq n \leq N$, then

$$P_a(N) \sim \frac{1}{2} h_a \int_2^N \frac{dn}{\log n}$$

where the constant $h_a$ is the infinite product

$$h_a = \prod_{w \mid a} \left(1 - \left(\frac{-a}{w}\right) \frac{1}{w-1}\right)$$

taken over all odd primes, $w$, which do not divide $a$, and for which $(-a/w)$ is the Legendre symbol.

In the trivial cases, $a = -k^2$, since $(k^2/w) = +1$ for every $w$, we have $h_a = 0$ on the one hand, and on the other there can be at most one prime of the form $n^2 - k^2 = (n - k)(n + k)$. For any other $a$, $h_a > 0$, and the conjecture indicates that there are infinitely many primes. But for no $a$ has this been proven.

In particular, for $a = 1$, since $(-1/w)$ equals $+1$ or $-1$ according as $w = 4m + 1$ or $4m - 1$, we have

$$h_1 = (1 + \frac{1}{2})(1 - \frac{1}{4})(1 + \frac{1}{6})(1 + \frac{1}{10})(1 - \frac{1}{14}) \cdots = 1.37281346 \cdots$$

and therefore (1) implies that

$$P_1(N) \sim 0.68640673 \int_2^N \frac{dn}{\log n}.$$ 

A. E. Western [2] verified that the number of primes of the form $n^2 + 1$ agreed well with the right side of (4) up to $N = 15,000$.

In a recent paper [3] a sieve method was developed for factoring numbers of the form $n^2 + 1$, and more generally of the form $n^2 + a$, and it was shown that the good agreement in (4) continues to hold out to $N = 180,000$; $(N^2 + 1 = 32,400,000,001)$. This verification, however, was not applied to (4) directly but to the related formula, (7), given below.

Let $\pi_a(N)$ be the number of odd primes, $q$, which are $\leq N$, which do not divide

Received April 26, 1960

---

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
It is well known that
\[ \left( \frac{a}{p} \right) = -1. \]
These are the primes which never divide \( n^2 + a \).

It is clear that the \( \pi_a(N) \) in (6) could be replaced by the asymptotically equal
\[ \frac{1}{2} \pi(N) \] or by \( \pi_a(N) \), (for the latter number we count the \( p \)'s such that
\( (-a/p) = +1 \). But (6) as it stands is to be preferred for two reasons. First, \( \pi_a(N) \)
is generally much closer to \( \frac{1}{2} \int_2^N \frac{dn}{\log n} \) than are either of the other two counts.

See [4, sec. 10 and Table 7] for a discussion of the case \( a = 1 \). Second, the ratio
in (6) has a simple geometric interpretation in the algebraic number field \( \mathbb{Q}(\sqrt{-a}) \).
See [3, p. 82] for a discussion of the case \( a = 1 \), the Gauss plane.

In the present paper [5] we first develop an interesting and rapidly converging
formula for computing the \( h_a \) and we tabulate these constants for \( a = -4(1)4 \).
We then present short tables of \( P_a(N) \) and \( \pi_a(N) \) for \( a = \pm 2, \pm 3, \pm 4 \), and for
\( N = 10,000(10,000)180,000 \) which show that (6) also gives good agreement
in these five cases. Finally we present an elementary (sieve) argument which makes
it plausible that the Hardy-Littlewood conjecture is true for every \( a \). Further, an
analysis of this computation enables us to isolate the essential difficulty in obtaining
a proof.

2. The Right Side of (6). To compute the \( h_a \) we will want the following

**Lemma.** For \( |x| < \frac{1}{2} \),
\[ \frac{1}{1 - 2x} = \prod_{n=1}^{\infty} \left( \frac{1 + x^n}{1 - x^n} \right)^{b(n)} \]
where the exponents \( b(s) \) are given by
\( b(1) = b(2) = b(3) = 1, b(4) = 2, b(5) = 3, b(6) = 5 \), and, in general, if \( d \) is an odd
divisor of \( s \) and \( \mu(d) \) is its Möbius function, then
\[ b(s) = \frac{1}{2s} \sum_{d \mid s} \mu(d) 2^{s/d}. \]

Examples of (9): A.) If \( s = p \), an odd prime, \( d = 1 \) or \( d = p \) and [6]
\[ b(p) = \frac{(2^p - 2)}{2p} = \frac{(2^{p-1} - 1)}{p}. \]
B.) If $s = 2^k$, then $d$ can only equal 1 and

$$b(s) = 2^{r-1}/s.$$  

Therefore $b(7) = 9$ and $b(8) = 16$.

**Proof of the Lemma.** After taking the logarithm of both sides of (8),

$$-\ln (1 - 2x) = \sum_{d=1}^{\infty} b(s) \ln [(1 + x^s)/(1 - x^s)],$$

we expand both sides in Maclaurin series and identify the corresponding coefficients. This yields the condition, for $s = 2^k m$, with $m$ odd,

$$2^{r-1} = \sum_{d|m} \frac{s}{d} b\left(\frac{s}{d}\right).$$

Now applying the Möbius inversion formula we obtain (9). Since from (11) we also have $b(s) \leq 2^r/2s$ it follows that (10) converges if $|x| < 1/2$ and the steps may be reversed to yield (8).

Now for any $a \neq -k^2$ let $p_i$ be the odd primes such that $(-a/p) = +1$, let $q_j$ be the odd primes such that $(-a/q) = -1$, and let $r_1 = 2, r_2, r_3, \ldots, r_s$ be the (finite number of) primes which divide $2a$. Further, for $s = 1, 2, 3, \ldots, let$

$$L_a(s) = \left[\prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^s}\right) \left(1 + \frac{1}{q_j^s}\right)\right]^{-1},$$

the product being taken over the $p_i$'s and $q_j$'s in numerical order. Finally for $s = 2, 3, 4, \ldots$, let

$$\zeta_a(s) = \zeta(s) \prod_{i=1}^{s} (1 - r_i^{-s})$$

where $\zeta(s)$ is the Riemann zeta function.

**Theorem.** If

$$f_a^{(0)} = \zeta_a(2)/L_a(1)$$

and $K_a^{(0)}(s) = \zeta_a(2s)/L_a(s)\zeta_a(s)$

for $s = 2, 3, 4, \ldots$, then

$$f_a^{(u)} = f_a^{(0)} \prod_{i=1}^{u} \left(1 - \frac{2}{p_i(p_i - 1)}\right) = f_a^{(0)} \prod_{i=1}^{u} \left(1 - \frac{2}{p_i}\right) \left(p_i + 1\right)/\left(p_i - 1\right),$$

and

$$K_a^{(u)}(s) = K_a^{(0)}(s) \prod_{i=1}^{u} \left(1 + \frac{2}{p_i^s - 1}\right) = K_a^{(0)}(s) \prod_{i=1}^{u} \left(p_i^s + 1\right)/\left(p_i^s - 1\right).$$

Then for every $u = 0, 1, 2, \ldots,

$$h_a = f_a^{(u)} \prod_{i=1}^{u} [K_a^{(u)}(s)]^{b^{(s)}}.$$
Proof. For every \( s = 2, 3, 4, \ldots \),
\[
\xi(s) = \left[ \prod_{p \leq x} \left( 1 - \frac{1}{p^s} \right) \left( 1 - \frac{1}{q^s} \right) \left( 1 - \frac{1}{r^s} \right) \right]^{-1}
\]
and we easily verify that
\[
1 = K^{(0)}_s(s) \prod_p \left( \frac{p^s + 1}{p^s - 1} \right).
\]
We likewise find that
\[
h_a = f^{(0)}_a \prod_p \left( 1 - \frac{2}{p} \right) \left( \frac{p + 1}{p - 1} \right)
\]
so for any positive integer \( m \), we have from (19) and (20)
\[
h_a = f^{(u)}_a \prod_{i=2}^{m} [K^{(u)}_a(s)]^{b(s)} \cdot \prod_{i=m+1}^{\infty} \left( 1 - \frac{2}{p_i} \right) \left( \frac{p_i + 1}{p_i - 1} \right) \cdot \prod_{i=2}^{m} \prod_{i=m+1}^{\infty} \left( \frac{p_i^s + 1}{p_i^s - 1} \right)^{b(s)}.
\]
Since \( m \) is finite the order of the products may be changed to give
\[
h_a = f^{(u)}_a \prod_{i=2}^{m} [K^{(u)}_a(s)]^{b(s)} \cdot \prod_{i=m+1}^{\infty} \left( 1 - \frac{2}{p_i} \right) \cdot \prod_{i=2}^{m} \prod_{i=m+1}^{\infty} \left( \frac{p_i^s + 1}{p_i^s - 1} \right)^{b(s)}.
\]
Now every \( p > 2 \), and we may therefore use (8) with \( x = 1/p_i \) to obtain
\[
h_a = f^{(u)}_a \prod_{i=2}^{m} [K^{(u)}_a(s)]^{b(s)} \cdot \prod_{i=m+1}^{\infty} \prod_{i=m+1}^{\infty} \left( \frac{p_i^s - 1}{p_i^s + 1} \right)^{b(s)}.
\]
But it may be readily seen that the double infinite product on the right converges (monotonically increasing) to 1 as \( m \to \infty \), and it thus follows that the right side of (18) converges (monotonically decreasing) to \( h_a \) as \( m \to \infty \).

The computation of the \( h_a \) from (18) requires knowledge of the \( L_a(s) \). Now every \( L_a(s) \) has a Dirichlet series
\[
L_a(s) = \sum_{n=1}^{\infty} d_n(a)n^{-s}
\]
with real periodic coefficients. Specifically we have
\[
L_1(s) = 1 - 3^{-s} + 5^{-s} - 7^{-s} + \cdots,
\]
\[
L_2(s) = 1 + 3^{-s} - 5^{-s} - 7^{-s} + \cdots,
\]
\[
L_{-2}(s) = 1 - 3^{-s} - 5^{-s} + 7^{-s} + \cdots,
\]
\[
L_3(s) = 1 - 5^{-s} + 7^{-s} - 11^{-s} + \cdots,
\]
\[
L_{-3}(s) = 1 - 5^{-s} - 7^{-s} + 11^{-s} + \cdots,
\]
\[
L_4(s) = 1 - 3^{-s} + 5^{-s} - 7^{-s} + \cdots.
\]

The \( L_a(1) \), which enter into \( f^{(0)}_a \) as defined by eq. (14), may be obtained in closed form by use of Gauss sums and Fourier series, [7]. Specifically, for \( a > 0 \) we have the simple
\[
L_a(1) = \frac{\pi}{2\sqrt{a}} q_a
\]
where the \( q_a \) for \( 1 \leq a \leq 100 \) are listed in Table 1.
The $L_\alpha(1)$ for negative $\alpha$ are a little more complicated and will not be listed here. As regards $L_\alpha(s)$ for other values of $s$, $L_\alpha(s)$ is a well known function, but except for a few scattered results, [8], values of the other $L$'s do not seem to have been published. J. W. Wrench, Jr. has computed unpublished tables of $L_\alpha(s)$ for $\alpha = \pm 2$ and $\pm 3$. With his permission the author used these tables, together with (18), to compute the four corresponding values of $h_\alpha$ in Table 2. The remaining entries, $a_i = f_\alpha = 0$ and $h_i = h_i$, are trivial.

The variation of the $h_\alpha$ in Table 2 is notable. For example, there should be

## Table 1

<table>
<thead>
<tr>
<th>$a$</th>
<th>$q\alpha$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>3</td>
</tr>
<tr>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>21</td>
<td>4</td>
</tr>
<tr>
<td>22</td>
<td>2</td>
</tr>
<tr>
<td>23</td>
<td>3</td>
</tr>
<tr>
<td>24</td>
<td>4</td>
</tr>
<tr>
<td>25</td>
<td>2</td>
</tr>
</tbody>
</table>

## Table 2

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>$h_\alpha$</th>
</tr>
</thead>
<tbody>
<tr>
<td>-4</td>
<td>0</td>
</tr>
<tr>
<td>-3</td>
<td>1.38342429</td>
</tr>
<tr>
<td>-2</td>
<td>1.85005441</td>
</tr>
<tr>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1.37281346</td>
</tr>
<tr>
<td>2</td>
<td>0.71306310</td>
</tr>
<tr>
<td>3</td>
<td>1.12073275</td>
</tr>
<tr>
<td>4</td>
<td>1.37281346</td>
</tr>
</tbody>
</table>
more than two and one-half times as many primes of the form \( n^2 - 2 \) as of the form \( n^2 + 2 \). As a side remark, we note from (15) that \( J_a^{(6)} = 2\sqrt{a}/\pi q_a \) is the leading factor of \( h_a \). Thus for \( a > 0 \), \( n^2 + a \) will therefore have few or many primes according as \( q_a \) is large or small (relative to \( 2\sqrt{a}/\pi \)). From Table 1 we see that there will be few primes for \( a = 2, 5, 11, 14, 26, 41, 89, \) and 194, \((q_{194} = 20)\), and there will be many primes for \( a = 7, 37, 58, \) and 163, \((q_{163} = 3)\). The famous function of Euler, \( n^2 + n + 41 \), equals \( \frac{1}{4}[(2n + 1)^2 + 163] \) and its well-known richness in primes is thus closely related to the small value of \( q_{41} \). This, in turn, is related in class number theory to the unique factorization of the integers in the algebraic number field \( R(\sqrt{−163}) \).

3. The Left Side of (6). Tables of \( P_a(N) \) and \( \pi_a(N) \) for \( a = ±2, ±3, ±4, \) and \( N = 100k \ (k = 1, 2, \cdots, 1800) \) were computed with an IBM 704 program based on the sieve method and the \( p \)-adic square roots of \(-a, \) \([3, \sec. 9]\). At the same time the prime divisors of \( n^2 + a \) which do not exceed \( N \) were counted, and from these counts the values of \( \pi_a(N) \) are easily obtained. Summaries of these results are given in Tables 3, 4, and 5. In the last of these, the results for \( a = 4 \) are compared with the previous results \([3]\) for \( a = 1 \).

4. Both Sides of (6). In Figure 1 we plot \( P_a(N)/\pi_a(N) \) versus \( N \) together with the conjectured limits, \( h_a \), for \( a = ±2 \) and ±3. The cases \( a = 1 \) and \( a = 4 \), (which should be asymptotically equal since \( h_1 = h_4 \)), are not included in this figure for clarity. If included, these two graphs would intertwine that for the case \( a = -3 \).

5. An Elementary Interpretation. The over-all impression of the foregoing results is that (6) and its equivalent (1) are almost surely true for \( a = 1, ±2, ±3, 4. \)

<table>
<thead>
<tr>
<th>( N )</th>
<th>( P_a(N) )</th>
<th>( \pi_a(N) )</th>
<th>( P_a(N)/\pi_a(N) )</th>
<th>( P_a(N) )</th>
<th>( \pi_a(N) )</th>
<th>( P_a(N)/\pi_a(N) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000</td>
<td>446</td>
<td>622</td>
<td>0.7137</td>
<td>1153</td>
<td>625</td>
<td>1.8448</td>
</tr>
<tr>
<td>20000</td>
<td>817</td>
<td>1134</td>
<td>0.7205</td>
<td>2140</td>
<td>1140</td>
<td>1.8772</td>
</tr>
<tr>
<td>30000</td>
<td>1180</td>
<td>1632</td>
<td>0.7230</td>
<td>3087</td>
<td>1631</td>
<td>1.8927</td>
</tr>
<tr>
<td>40000</td>
<td>1494</td>
<td>2117</td>
<td>0.7057</td>
<td>3977</td>
<td>2112</td>
<td>1.8830</td>
</tr>
<tr>
<td>50000</td>
<td>1821</td>
<td>2580</td>
<td>0.7058</td>
<td>4824</td>
<td>2587</td>
<td>1.8647</td>
</tr>
<tr>
<td>60000</td>
<td>2160</td>
<td>3051</td>
<td>0.7080</td>
<td>5643</td>
<td>3041</td>
<td>1.8556</td>
</tr>
<tr>
<td>70000</td>
<td>2489</td>
<td>3478</td>
<td>0.7156</td>
<td>6464</td>
<td>3481</td>
<td>1.8569</td>
</tr>
<tr>
<td>80000</td>
<td>2823</td>
<td>3942</td>
<td>0.7161</td>
<td>7296</td>
<td>3927</td>
<td>1.8579</td>
</tr>
<tr>
<td>90000</td>
<td>3139</td>
<td>4378</td>
<td>0.7170</td>
<td>8083</td>
<td>4374</td>
<td>1.8480</td>
</tr>
<tr>
<td>100000</td>
<td>3422</td>
<td>4798</td>
<td>0.7132</td>
<td>8888</td>
<td>4808</td>
<td>1.8486</td>
</tr>
<tr>
<td>110000</td>
<td>3721</td>
<td>5229</td>
<td>0.7116</td>
<td>9681</td>
<td>5242</td>
<td>1.8468</td>
</tr>
<tr>
<td>120000</td>
<td>4027</td>
<td>5649</td>
<td>0.7129</td>
<td>10500</td>
<td>5682</td>
<td>1.8479</td>
</tr>
<tr>
<td>130000</td>
<td>4347</td>
<td>6090</td>
<td>0.7138</td>
<td>11304</td>
<td>6117</td>
<td>1.8480</td>
</tr>
<tr>
<td>140000</td>
<td>4652</td>
<td>6516</td>
<td>0.7139</td>
<td>12086</td>
<td>6533</td>
<td>1.8500</td>
</tr>
<tr>
<td>150000</td>
<td>4966</td>
<td>6945</td>
<td>0.7150</td>
<td>12828</td>
<td>6956</td>
<td>1.8442</td>
</tr>
<tr>
<td>160000</td>
<td>5250</td>
<td>7347</td>
<td>0.7146</td>
<td>13628</td>
<td>7362</td>
<td>1.8511</td>
</tr>
<tr>
<td>170000</td>
<td>5522</td>
<td>7767</td>
<td>0.7110</td>
<td>14397</td>
<td>7763</td>
<td>1.8546</td>
</tr>
<tr>
<td>180000</td>
<td>5847</td>
<td>8192</td>
<td>0.7138</td>
<td>15134</td>
<td>8184</td>
<td>1.8492</td>
</tr>
</tbody>
</table>
We now offer a theoretical argument in favour of these asymptotic equations for all \( a \). We will specifically carry it through for \( a = 1 \), but the argument is easily generalized. The case \( a = 1 \) is the only one which Hardy and Littlewood treated in detail. Their computation, however, was deep and function-theoretic. In contrast, the present argument is elementary, [9]. It will be assumed that the reader is acquainted with the \( n^2 + 1 \) sieve which is described in detail in [3].
Consider the infinite product (3) for \( h_1 \), not in the form in which it was given by Hardy and Littlewood, (2),

\[
h_1 = \left(1 + \frac{1}{3} - 1\right) \left(1 - \frac{1}{5} - 1\right) \left(1 + \frac{1}{7} - 1\right) \left(1 + \frac{1}{11} - 1\right) \left(1 - \frac{1}{13} - 1\right) \ldots,
\]

since this masks its true nature; but in the equivalent form

\[
h_1 = \frac{1}{(1 - \frac{1}{3}) \left(1 - \frac{2}{5}\right) \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{13}\right) \ldots}
\]
or, even better, as

\[
(23) \quad h_1 = \frac{1}{(1 - \frac{1}{2}) \left(1 - \frac{1}{3}\right) \left(1 - \frac{2}{5}\right) \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{13}\right) \ldots}.
\]

Now for a suitably large \( N \) let \( w^* \) be the greatest prime satisfying \( w \leq N \) and let \( p^* \) be the greatest prime of the form \( 4m + 1 \) which satisfies \( p \leq N \). We write the corresponding partial product of (23), which approximates \( h_1 \), as follows:

\[
(24) \quad h_1 \approx N \cdot \frac{N \left(1 - \frac{1}{2}\right) \left(1 - \frac{2}{5}\right) \left(1 - \frac{1}{11}\right) \ldots \left(1 - \frac{2}{p^*}\right)}{N^2 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \ldots \left(1 - \frac{1}{w^*}\right)}.
\]

Now this approximation to \( h_1 \) is in turn seen to be approximated (and we will inquire later as to the degree of the approximation) by \( N \) times the ratio of the primes which remain in two sieves, the Eratosthenes sieve (for all primes) from \( n = 1 \) to \( n = N^2 \) in the denominator and the \( n^2 + 1 \) sieve from \( n^2 + 1 = 2 \) to \( n^2 + 1 = N^2 + 1 \) in the numerator.
Without attempting precision at this point—that is, without bounding the error—we note that in the Eratosthenes sieve one first strikes out the multiples of 2. This leaves $N^2(1 - \frac{1}{2})$ numbers (with an error of 0 or $\frac{1}{2}$). One then strikes out the remaining multiples of 3 leaving $N^2(1 - \frac{1}{2})(1 - \frac{1}{3})$ numbers (again except for a possible end-effect correction.) Continuing with the primes 5, 7, $\cdots$, $w^*$ creates the denominator of (24). The latter therefore equals

$$\pi(N^2) - \pi(N) + E(N),$$

the number of primes up to $N^2$ minus the number of primes up to $N$, with an end-effects error, $E(N)$, which is not yet bounded. We note that

$$\pi(N^2) - \pi(N) \sim \frac{N}{2} \pi(N) \sim N\pi_1(N)$$

by the prime number theorem.

In the $n^2 + 1$ sieve we first factor a 2 from all numbers where $n = 2m + 1$ leaving $N(1 - \frac{1}{2})$ of the numbers (except for an end-effect error). We then factor a 5 where $n = 5m + 2$ and where $n = 5m + 3$. This leaves $N(1 - \frac{1}{2})(1 - \frac{1}{3})$ numbers (except for the end-effect error). Continuing with all primes of the form $4m + 1; 13, 17, \cdots, p^*$ generates the numerator. The latter therefore equals

$$P(N) - P(\sqrt{N} - 1) + e(N),$$

the number of primes of the form $n^2 + 1$ up to $N^2 + 1$ minus the number of such primes up to $N$ with an end effect $e(N)$.

Therefore, we may write

$$h_1 = \lim_{N \to \infty} \frac{P(N) - P(\sqrt{N} - 1) + e(N)}{\pi_1(N) + E(N)/N},$$

while what we would like to write is

$$h_1 = \lim_{N \to \infty} \frac{P(N)}{\pi_1(N)}.$$  

Now by Merten’s Theorem the denominator of (24) is asymptotic to $N^2 e^{-\gamma}/\log N$ where $\gamma$ is Euler’s constant [10]. Therefore the end effect, $E(N)/N$, is not negligible compared with $\pi_1(N)$. Instead we have

$$\frac{E(N)/N}{\pi_1(N)} \sim 0.1229 = 2e^{-\gamma} - 1.$$  

If we could show

$$\frac{e(N)}{P(N) - P(\sqrt{N} - 1)} \sim 2e^{-\gamma} - 1$$

all would be well, but the difficulty of the problem is such that we cannot even prove that the left side of (27) is bounded from above. If we could do that, we would at least have $P(N) \to \infty$ but even this “weak” result eludes us.

It is of interest to analyze this difficulty. Let

$$D(N) = P(N) - P(\sqrt{N} - 1)$$
and

\begin{equation}
S(N) = N \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{2}{5} \right) \cdots \left( 1 - \frac{2}{p^*} \right).
\end{equation}

Then the conjectured relation (27) is equivalent to the conjecture

\begin{equation}
\frac{S(N)}{D(N)} \sim 2e^{-\gamma} = 1.1229.
\end{equation}

Now from the sieve for \( n^2 + 1 \), [3], we can obtain an exact formula for \( D(N) \) by using the "integer part of \( x \)" function, \([x]\). Consider the set of numbers obtained from

\[ d = 2^a \cdot 5^b \cdot 13^c \cdots p^{*}\]

by assigning (in all possible ways) 0 and 1 to the exponents \( a, b, c, \cdots \). For each such \( d \), let \( A_i \) be the solutions of

\[ A^2 \equiv -1 \pmod{d} \]

which satisfy

\[ 0 \leq A < d. \]

Then if \( d \) is a product of \( \alpha \) primes, we have

\begin{equation}
D(N) = \sum_d (-1)^\alpha \sum_i \left[ \frac{N + A_i}{d} \right].
\end{equation}

It may be seen that if there are \( M \) primes of the form \( 4m + 1 \) which are \( \leq N \), then there will be \( 2 \cdot 3^M \) terms in this sum. Even for a very modest \( N \), say 15, we have \( p^* = 13, M = 2 \), and there are already 18 terms. Specifically,

\[ D(15) = [N] - \left[ \frac{N + 1}{2} \right] - \left[ \frac{N + 3}{5} \right] - \left[ \frac{N + 2}{10} \right] + \left[ \frac{N + 7}{10} \right] + \left[ \frac{N + 3}{10} \right] - \left[ \frac{N + 8}{13} \right] - \left[ \frac{N + 5}{13} \right] + \left[ \frac{N + 21}{26} \right] + \left[ \frac{N + 5}{26} \right] + \left[ \frac{N + 57}{65} \right] + \left[ \frac{N + 47}{65} \right] + \left[ \frac{N + 18}{65} \right] + \left[ \frac{N + 8}{130} \right] - \left[ \frac{N + 83}{130} \right] - \left[ \frac{N + 73}{130} \right] - \left[ \frac{N + 57}{130} \right] - \left[ \frac{N + 47}{130} \right]. \]

In general, it is easily seen, the formula for \( S(N) \) may be obtained from that for \( D(N) \) by deleting the \( A_i \) and the square brackets. Thus for \( N = 15 \) in the example, we have

\[ S(N) = N - \frac{N}{2} - \frac{2N}{5} + \frac{2N}{10} - \frac{2N}{13} + \frac{2N}{26} + \frac{4N}{65} - \frac{4N}{130} = N \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{2}{5} \right) \left( 1 - \frac{2}{13} \right). \]
For $N$ small, $S(N)$ and $D(N)$ are nearly equal; e.g., $S(15) = 3.81$, $D(15) = 4$. As $N$ increases, $S(N)$ gradually pulls ahead of $D(N)$, as is seen in Table 6.

The end effect

$$e(N) = S(N) - D(N)$$

is given by

$$e(N) = \sum_{d} (-1)^{a} \sum_{i} \left\{ \frac{N}{d} - \left\lfloor \frac{N + A_i}{d} \right\rfloor \right\}. \quad (32)$$

Since the quantity in each brace is smaller in magnitude than unity, it is easy enough to bound $e(N)$. What is difficult to obtain is a sufficiently good bound—that is, to prove in general, the extensive cancellation of terms of opposite sign which occurs in the sum of (32). The essential difficulty stems from the very rapid increase in the number of terms, $2^{3^N}$.

Techniques of deleting or combining terms, in sieve formulations of related problems, have been devised by Brun and others [11] but to date nothing sufficiently sharp has been developed. A general assessment of sieve techniques given by Selberg [12] is not encouraging.

Applied Mathematics Laboratory
David Taylor Model Basin
Washington 7, District of Columbia

6. The numbers \( b(s) \) also arise in an entirely different connection—they are related to the number of distinct circular parity switches of order \( s \). See Daniel Shanks, “A circular parity switch and applications to number theory,” Notices, Amer. Math. Soc., v. 5, 1958, p. 96. Abstract 543-7. It was in this connection that the author first noted the unusual proof of a special case of the Fermat “little” theorem—see (9a) above. Likewise it was in this connection that Bernard Elpsas, in a private communication to the author (Sept. 3, 1958), developed the formula (9).


8. Fletcher, Miller & Rosenhead, *Index of Mathematical Tables*, McGraw-Hill, 1946, p. 42, 43, p. 63. The correspondence between our notation and theirs is as follows: \( L_1(s) = u_n \), \( L_2(s) = p_n \), \( L_3(s) = q_n \), \( L_4(s) = h_n \), and \( L_5(s) = t_n \).


