

Bateman's Constants Reconsidered and the Distribution of Cubic Residues

By Daniel Shanks and Mohan Lal

Abstract. We analyze the computation of certain slowly convergent infinite products involving cubic characters. A first-order analysis gives a 2D or 3D answer immediately, but extensive computation of cubic residues only improves this to 5D or 6D. To do better, one must examine the distribution of cubic residues or evaluate certain Dedekind Zeta functions. Both are done. The constants thus obtained are used to examine a variant of the Hardy-Littlewood Conjecture K concerning primes of the form $n^3 + a$. Some related mathematics needed and developed includes an answer to this: Which p , satisfying $x^3 \equiv a \pmod{p}$, have two solutions x that differ by $k \pmod{p}$?

1. Introduction. Let

$$(1) \quad A = \prod_p \frac{p - \alpha(p)}{p - 1},$$

where the product is taken over all primes $p = 6m + 1$ (we write $p_1 = 7, p_2 = 13, p_3 = 19, \dots$), and where $\alpha(p)$ is 3, or 0, according as

$$(2) \quad p = u^2 + 27v^2,$$

or not; that is, according as 2 is a cubic residue of p , or not. More generally, let

$$(3) \quad k_a = \prod_{p \nmid a} \frac{p - \alpha_a(p)}{p - 1},$$

taken over all p , not dividing a , and $\alpha_a(p)$ is 3, or 0, according as a is, or is not, a cubic residue of p . Thus, $A = k_2$, and Bateman and Horn [1], [2] also examined $B = k_3$, with $\alpha_3(p) = 3$ if, and only if,

$$(4) \quad p = \frac{1}{4}(u^2 + 243v^2).$$

If a is not a perfect cube, and if $K_a(N)$ is the number of primes of the form

$$(5) \quad n^3 + a$$

for $1 \leq n \leq N$, then Conjecture K of Hardy and Littlewood [3] asserts that

$$(6) \quad K_a(N) \sim \frac{1}{3}k_a \int_2^N \frac{dx}{\log x}.$$

(To eliminate ambiguity, if $a < 0$, and if, for some n , $n^3 + a$ is the negative of a prime, we will count it as a prime.)

Received July 19, 1971.

AMS 1970 subject classifications. Primary 10A20, 10H15, 10H25, 10H35, 12A30.

Key words and phrases. Distribution of cubic residues, distribution of primes, number-theoretic products, Bateman-Horn conjecture, Dedekind Zeta functions.

Copyright © 1972, American Mathematical Society

But these constants k_a offer difficulties in their accurate computation. The product (3) converges, but it does not converge absolutely, and a useful bound on the error for any *partial product* is not available, since there is insufficient knowledge concerning the distribution of the *subsequent* values of $\alpha_a(p)$. Bateman and Horn therefore gave only "tentative" values. They evaluated (3) for $p < 10^8$ using Jacobi's table of indices to decide the question:

$$\alpha_{2,3}(p) = 3, 0.$$

They got

$$(7) \quad A = 1.29, \quad B = 1.38.$$

In a long review [4], one of us discussed this difficulty, and gave an exotic, and interesting, but not very practical method of computing A . The galleys for this review were shown to Andrej Schinzel, and even before it appeared in print, he and Davenport obtained [5] what we shall call a first-order solution, not only for (5), but for all irreducible polynomials, and systems thereof. This was accomplished by using the known behaviour of the corresponding Dedekind Zeta functions $\zeta_K(s)$ as $s \rightarrow 1+$.

Specifically, for (1), they give

$$(8) \quad A = \frac{3\sqrt{3}}{\pi |\log(2^{1/3} - 1)|} \prod_1 \frac{p^2(p-3)}{(p-1)^3} \prod_2 \frac{q^2}{q^2-1} \prod_3 \frac{p^3}{p^3-1}$$

with \prod_1 taken over all p with $\alpha_2(p) = 3$, \prod_3 taken over all p with $\alpha_2(p) = 0$, and \prod_2 taken over all primes $q = 6m + 5$. For B there is a similar formula with $|\log(2^{1/3} - 1)|$ replaced by $\frac{1}{2} |\log(9^{1/3} - 2)|$, and $\alpha_2(p)$ replaced by $\alpha_3(p)$. The three products shown converge absolutely, but very slowly. Davenport and Schinzel confirmed (7).

Our point of departure is this Davenport-Schinzel formula for k_a , but we make several changes. We factor the three products $\prod_1 \prod_2 \prod_3$ in two different ways:

$$(9) \quad L_0 \prod_{4,a} = \prod_1 \prod_2 \prod_3 = U_0 \prod_{5,a}.$$

Here the constants L_0 and U_0 depend only on the quadratic character $(-3/p)$, are "universal" in the sense that they are independent of a , and can be computed very accurately once and for all. In fact, we have

$$(10) \quad \begin{aligned} L_0 &= 0.920038563618492, \\ U_0 &= 1.064378253083636. \end{aligned}$$

The difficult part of the computation, and that dependent on a , is confined to the slowly convergent products, taken over the primes $p = 6m + 1$:

$$(11) \quad \begin{aligned} \prod_{4,a} &= \prod_{a^2 m \not\equiv 1 \pmod{p}} \left(1 - \frac{3(p+1)}{p(p-1)^2}\right)^{-1}, \\ \prod_{5,a} &= \prod_{a^2 m \equiv 1 \pmod{p}} \left(1 - \frac{3(p+1)}{p(p-1)^2}\right). \end{aligned}$$

We note that $\prod_{4,a}$ converges monotonically increasing, and $\prod_{5,a}$ monotonically decreasing, and we therefore have rigorous, (and best possible) lower and upper

bounds. Further, by replacing the individual criteria (2) and (4) with an Euler Criterion

$$(12) \quad a^{2m} = a^{(p-1)/3} \equiv 1 \pmod{p},$$

we not merely obtain instant generalization (which we use in [6]), but we also save time since (12) is quicker to compute. With residue arithmetic, it can be determined in $O(\log m)$ operations, while the simplest programs, for (2), (4), and analogues for other a , require $O(\sqrt{p})$ operations.

With no knowledge of $\alpha_2(p)$, and no computation of (11), one has

$$\frac{3\sqrt[3]{3}}{\pi |\log(2^{1/3} - 1)|} L_0 < A < \frac{3\sqrt[3]{3}}{\pi |\log(2^{1/3} - 1)|} U_0$$

or

$$1.129 < A < 1.307.$$

Similarly,

$$1.205 < B < 1.395.$$

If one evaluates (11) through $p_{35} = 373$, one has

$$(13) \quad \begin{aligned} 1.29805 < A < 1.29878, \\ 1.39001 < B < 1.39080. \end{aligned}$$

Both tentative values (7) are therefore a little low, and, in fact, are low in comparison with Horn's count of the primes [2].

To do better than (13) by the use of (11) one must use a computer since the products (11) converge so slowly. Using a small machine, an IBM 1620, we evaluated (11) for $p \leq p_{10,000} = 225217$, and obtained

$$(14) \quad \begin{aligned} 1.298539124 < A < 1.298539774, \\ 1.390543474 < B < 1.390544171. \end{aligned}$$

Number-theoretically speaking, (14) perhaps suffices, but analytically speaking we are not satisfied. If $p \leq P$ is used in (11), and if the products

$$(14a) \quad L_0 \prod_{4,a} (P), \quad U_0 \prod_{5,a} (P)$$

agree to d decimals, then to obtain $d + 1$ decimals one must go nearly to $p \leq 10P$, that is, one must perform ten times as much arithmetic. This is clearly unsatisfactory, and sets the stage for two extensive mathematical investigations.

(a) In Section 4 we examine a weighted mean of the foregoing upper and lower bounds that gives us approximately $\frac{3}{2}d$ decimals. While it is entirely convincing, it now has no rigorous theory and none can be anticipated soon since, in its stronger form at least, it probably requires the Riemann Hypothesis for the appropriate Dedekind Zeta functions. Arithmetically speaking, though, this mean is very simple, and gives us our own "tentative" values:

$$(15) \quad \begin{aligned} A &= 1.29853956, \\ B &= 1.39054394. \end{aligned}$$

These values are "tentative" (at this point) for essentially the same reason that those in (7) were. One needs detailed and deep knowledge of the fluctuations in the distribution of cubic residues, and the effect of such fluctuations upon the induced oscillations of the sequences (3) or (11). To gain such insight as was possible to us, we proceeded as follows. With our improved values (14) we know with some accuracy the limits of the sequences (3). Thereby, it becomes possible to study quantitatively the oscillations of these sequences around their known limits, and the correlation of these oscillations with the aforementioned fluctuations in the cubic residue distributions.

The three deep and associated problems: the convergence of (3), the distribution of the cubic residues, and the zeros of $\zeta_K(s)$ are surely of greater interest than the special problem that gives rise to their examination here, namely, the justification of the more accurate values (15), but, of necessity, we cannot carry them very far.

(b) While (a) is thus of interest, the real answer to the search for a better analytic method than that which gives (14) is of quite a different character. In Section 6 we show that if we could evaluate $\zeta_K(2)$ we could improve the first-order method (14a) to a second-order one. Likewise, $\zeta_K(3)$ would allow a third-order method, etc. (The values (7) were computed with a zero-order method.) The numbers (10) were not hard to compute since they were based upon the known values of

$$(16) \quad L_3(s) = \sum_{n=0}^{\infty} \left(\frac{-3}{2n+1} \right) (2n+1)^{-s},$$

for $s = 1, 2, 3, \dots$, and, similarly, $\zeta_K(s)$ for $s = 2, 3, \dots$ are what are needed to compute (3) effectively.

In [12], one of us develops a method of computing these $\zeta_K(s)$. With these, and a thorough recasting of the entire problem, we obtain a completely satisfactory solution for this problem of computing k_a . We refer the reader to [12] and merely indicate here that it is (now) fairly easy to compute

$$(15a) \quad \begin{aligned} A &= 1.298539557557843, \\ B &= 1.390543938783812. \end{aligned}$$

These show that the tentative values (15) were correct.

Returning to the present paper, we examine the "twin" primes

$$(n-1)^3 + a, \quad (n+1)^3 + a.$$

Let $T_a(N)$ be the number of such pairs for $1 \leq n+1 \leq N$. The Bateman-Horn conjecture [1] gives

$$(17) \quad T_a(N) \sim \frac{1}{6} t_a \int_2^N \frac{dx}{\log^2 x}$$

for some t_a . We compute t_a from k_a , together with other universal constants, and other upper and lower bound products similar to (10) and (11). But we also need to answer the following question: For which p having a as cubic residue do two cube-roots (mod p) differ by 2? We give a complete answer with this difference 2 replaced by an arbitrary difference Δ .

Finally, using Horn's lists of primes $n^3 \pm 2$, $n^3 \pm 3$, and our computed

$$(18) \quad \begin{aligned} \frac{1}{8} t_2 &= 0.25978891, \\ \frac{1}{8} t_3 &= 0.29427951, \end{aligned}$$

we examine the empirics of (17).

2. The Universal Constants. For any a not equal to a cube the generalization of (8) may be written

$$(19) \quad k_a = \frac{3\sqrt{3} r_a}{\pi H_a \log \epsilon_a} \prod_1 \frac{p^2(p-3)}{(p-1)^3} \prod_2 \frac{q^2}{q^2-1} \prod_3 \frac{p^3}{p^3-1},$$

with \prod_1 taken over those $p = 6m + 1$ satisfying $a^{2m} \equiv 1 \pmod{p}$, \prod_3 over those p satisfying $a^{2m} \not\equiv 1 \pmod{p}$, and \prod_2 over all $q = 6m + 5$. Here ϵ_a is the fundamental unit, H_a is the class number of the cubic field, and r_a is a rational number dependent on a . We note that this is a little different from Davenport-Schinzel. For certain a they have a finite number of factors deleted from \prod_2 and/or \prod_3 , or, again, $2^2/(2^2-1)$ may be included in \prod_2 , but we prefer to standardize as shown, absorbing any of these special factors into our rational factor r_a . We also note that for the two a treated here, (the generalization is in [6]), we have

$$(20) \quad r_2 = 1, \quad r_3 = 2, \quad H_2 = H_3 = 1,$$

and

$$(21) \quad \epsilon_2 = 4^{1/3} + 2^{1/3} + 1, \quad \epsilon_3 = 2 \cdot 9^{1/3} + 3 \cdot 3^{1/3} + 4,$$

consistent with the previous formulas.

We now reduce the two products involving the cubic character to one. We write

$$(22) \quad \prod_1 = \prod_{a \equiv 1 \pmod{p}} \frac{p^2(p-3)}{(p-1)^3} \bigg/ \prod_{a^{2m} \equiv 1 \pmod{p}} \frac{p^2(p-3)}{(p-1)^3},$$

and combining the numerator with \prod_2 , and the denominator with \prod_3 we have

$$(23) \quad \prod_1 \prod_2 \prod_3 = L_0 \prod_{a^{2m} \equiv 1 \pmod{p}} \left(1 - \frac{3(p+1)}{p(p-1)^2} \right)^{-1},$$

with

$$(24) \quad L_0 = \prod_{a \equiv 1 \pmod{p}} \frac{p^2(p-3)}{(p-1)^3} \prod_{a \equiv 1 \pmod{q}} \frac{q^2}{q^2-1}.$$

Also, we write

$$(25) \quad \prod_3 = \prod_{a \equiv 1 \pmod{p}} \frac{p^3}{p^3-1} \bigg/ \prod_{a^{2m} \equiv 1 \pmod{p}} \frac{p^3}{p^3-1},$$

and combining the numerator with \prod_2 , and the denominator with \prod_1 we have

$$(26) \quad \prod_1 \prod_2 \prod_3 = U_0 \prod_{a^{2m} \equiv 1 \pmod{p}} \left(1 - \frac{3(p+1)}{p(p-1)^2} \right)$$

with

$$(27) \quad U_0 = \prod_{a \equiv 1 \pmod{p}} \frac{p^3}{p^3-1} \prod_{a \equiv 1 \pmod{q}} \frac{q^2}{q^2-1}.$$

We refer to the partial products of (23) and (26) as

$$(28) \quad \begin{aligned} L(a, i) &= L_0 \prod_{a^2 m \not\equiv 1 \pmod{p}; p \leq p_i} \left(1 - \frac{3(p+1)}{p(p-1)^2}\right)^{-1}, \\ U(a, i) &= U_0 \prod_{a^2 m \equiv 1 \pmod{p}; p \leq p_i} \left(1 - \frac{3(p+1)}{p(p-1)^2}\right), \end{aligned}$$

so that

$$(29) \quad L(a, i) < \prod_1 \prod_2 \prod_3 < U(a, i)$$

for any a and all i , and

$$(30) \quad \prod_1 \prod_2 \prod_3 = L(a, \infty) = U(a, \infty)$$

for all a . For example, in evaluating (13) with the p through $p_{35} = 373$, we computed

$$L(2, 35) = 1.057427, \quad U(2, 35) = 1.058020,$$

$$L(3, 35) = 1.060874, \quad U(3, 35) = 1.061470.$$

The computation of U_0 is quite simple, being similar to that of the Landau constants b_n discussed in [7, p. 553]. With $L_3(s)$ as in (16) and

$$(31) \quad \zeta_3(s) = \left(1 - \frac{1}{2^s}\right) \left(1 - \frac{1}{3^s}\right) \zeta(s),$$

one has

$$(32) \quad \prod_q \left(\frac{q^s}{q^s - 1} \right) = \left(\frac{\zeta_3(s)}{L_3(s)} \right)^{1/2} \left(\prod_q \frac{q^{2s}}{q^{2s} - 1} \right)^{1/2}.$$

By iteration of (32) one obtains the very rapidly convergent

$$(33) \quad \prod_q \frac{q^2}{q^2 - 1} = \left(\frac{\zeta_3(2)}{L_3(2)} \right)^{1/2} \left(\frac{\zeta_3(4)}{L_3(4)} \right)^{1/4} \left(\frac{\zeta_3(8)}{L_3(8)} \right)^{1/8} \dots$$

Similarly,

$$(34) \quad \prod_p \frac{p^s}{p^s - 1} = \left(\frac{L_3(s) \zeta_3(s)}{\zeta_3(2s)} \right)^{1/2} \left(\prod_p \frac{p^{2s}}{p^{2s} - 1} \right)^{1/2}$$

and

$$(35) \quad \prod_p \frac{p^3}{p^3 - 1} = \left(\frac{L_3(3) \zeta_3(3)}{\zeta_3(6)} \right)^{1/2} \left(\frac{L_3(6) \zeta_3(6)}{\zeta_3(12)} \right)^{1/4} \dots$$

From tables of $L_3(s)$ and $\zeta_3(s) = L_{-9}(s)$, [8], we easily obtain the U_0 of (10).

The constant L_0 is more difficult. The Hardy-Littlewood C_3 , for prime triples [3], is given by

$$(36) \quad C_3 = \prod_w \frac{w^2(w-3)}{(w-1)^3}$$

taken over all prime $w > 3$. Although it is not necessary to do so, we find it convenient to utilize this number, writing (24) as

$$(37) \quad L_0 = C_3 \prod_q \frac{(q-1)^3}{(q^2-1)(q-3)} = C_3 \prod_q \frac{(q-1)^2}{(q+1)(q-3)}.$$

To compute the slowly convergent product on the right, and at least one other universal constant needed later, we further generalize the Lemma of [9] as follows:

LEMMA. If

$$(38) \quad \frac{1}{1-nx} = \prod_{s=1}^{\infty} \left(\frac{1+x^s}{1-x^s} \right)^{b_n(s)}$$

for even $n (> 1)$, and if

$$(39) \quad \frac{1-x}{1-nx} = \prod_{s=1}^{\infty} \left(\frac{1+x^s}{1-x^s} \right)^{b_n(s)}$$

for odd $n (> 1)$, then

$$(40) \quad b_n(s) = \frac{1}{2s} \sum_{d|s} \mu(d) n^{s/d},$$

the sum taken over all odd divisors d of s with $\mu(d)$ the Möbius function, except for n odd and $s = 2^r$ ($r = 0, 1, \dots$), in which case

$$(41) \quad b_n(s) = \frac{1}{2s} (n^s - 1).$$

Conversely, the right sides of (38), (39) converge to the left sides if $|nx| < 1$.

The proof is, as before, accomplished by taking logarithms of both sides, comparing coefficients, and then utilizing the Möbius Inversion Formula. The needed extension here over the previous version is because (38) is not possible for odd n if the $b_n(s)$ are to remain integers.

As a pertinent example we have

$$(42) \quad \frac{(1-x)(1-x)}{(1-3x)(1+x)} = \left(\frac{1+x^2}{1-x^2} \right)^2 \left(\frac{1+x^3}{1-x^3} \right)^4 \left(\frac{1+x^4}{1-x^4} \right)^{10} \dots$$

with the exponents

$$\begin{aligned} b_3(2) &= 2, & b_3(3) &= 4, & b_3(4) &= 10, & b_3(5) &= 24, \\ b_3(6) &= 60, & b_3(7) &= 156, & b_3(8) &= 410, & b_3(9) &= 1092, \dots \end{aligned}$$

(We note, for future applications, that negative n may also be used in (38) and (39) simply by setting x negative. For example, so doing with $n = -2$ gives

$$\prod_p \frac{p(p-3)}{(p+2)(p-5)} = \prod_{s=2}^{\infty} \left(\frac{p^s+1}{p^s-1} \right)^{a(s)}$$

with $a(2) = 5$, $a(3) = 15$, $a(4) = 70$, $a(5) = 285$, \dots .)

From (42) and (37) we therefore have, by setting $x = 1/q$,

$$(43) \quad L_0 = C_3 \prod_{s=2}^{\infty} \left(\prod_q \frac{q^s+1}{q^s-1} \right)^{b_3(s)}.$$

But, from (32) we have

$$(44) \quad \prod_q \frac{q^s + 1}{q^s - 1} = \frac{\zeta_3(s)}{L_3(s)}.$$

As usual, we get faster convergence by computing several factors in (37) directly, and then compensating in (43). Choosing, say, the first k q 's for such special treatment, (43) and (44) give

$$(45) \quad L_0 = C_3 \prod_{i=1}^k \frac{(q_i - 1)^2}{(q_i + 1)(q_i - 3)} \prod_{s=2}^{\infty} (T_3^{(k)}(s))^{b_s(s)}$$

with

$$T_3^{(k)}(s) = \frac{\zeta_3(s)}{L_3(s)} \prod_{i=1}^k \frac{q_i^s - 1}{q_i^s + 1}.$$

With his kind permission, we used unpublished results of J. W. Wrench, Jr. for C_3 and $T_3^{(5)}(s)$ in (45) to obtain the L_0 of (10).

We digress briefly to indicate that L_0 is, in a way, not a "new" number. The Bateman-Stemmler constant C appropriate for the number of primes p such that $p^2 + p + 1$ is also prime, [10], [11], [2], may be shown by its formula to satisfy

$$(46) \quad C = \frac{3\sqrt{3}}{\pi} L_0 = 1.521731535075706.$$

Previously, C was thought to be applicable to that one problem concerning p and $p^2 + p + 1$, and it was computed only to a few places. Here, we see from (19) and (23), that it enters as a factor for all $n^3 + a$.

3. Cubic Residues and the Bounding Sequences. For each of the first 10,000 primes of the form $6m + 1$, $p_1 = 7$ to $p_{10000} = 225217$, we have determined by the use of Euler's Criterion (12) whether a is a cubic residue of p_i , where a is any positive integer ≤ 20 . The resulting information was punched on IBM cards. These may then be used to easily compute the lower and upper bound sequences defined in (28). They were also used to compute the sequences (3) defined above and the sequences (79) defined below, to examine empirically the questions of distribution alluded to above, and to print out tables of cubic residues [13].

For $a = 2$ and 3 we list in Table 1 the bounding sequences $L(a, i)$ and $U(a, i)$ of (28) for select values of i .

TABLE 1

| i | $L(2, i)$ | $U(2, i)$ | $L(3, i)$ | $U(3, i)$ |
|-------|---------------|---------------|---------------|---------------|
| 0 | 0.92003 85636 | 1.06437 82531 | 0.92003 85636 | 1.06437 82531 |
| 1 | 1.01688 47282 | 1.06437 82531 | 1.01688 47282 | 1.06437 82531 |
| 3 | 1.05046 14822 | 1.06437 82531 | 1.05046 14822 | 1.06437 82531 |
| 10 | 1.05574 07265 | 1.05886 99857 | 1.05897 11102 | 1.06210 99444 |
| 30 | 1.05729 67073 | 1.05802 02971 | 1.06076 74209 | 1.06149 33860 |
| 100 | 1.05772 30757 | 1.05787 40421 | 1.06117 63182 | 1.06132 77776 |
| 300 | 1.05779 66974 | 1.05783 40491 | 1.06125 27987 | 1.06129 02724 |
| 1000 | 1.05781 59782 | 1.05782 43888 | 1.06127 27480 | 1.06128 11862 |
| 3000 | 1.05782 00846 | 1.05782 23030 | 1.06127 68315 | 1.06127 90571 |
| 10000 | 1.05782 12119 | 1.05782 17420 | 1.06127 79658 | 1.06127 84977 |

These sequences converge monotonically and very slowly to limits that were subsequently determined to be

$$(47) \quad \begin{aligned} L(2, \infty) &= 1.057821565488936 = U(2, \infty), \\ L(3, \infty) &= 1.061278320384041 = U(3, \infty). \end{aligned}$$

We note that increase in the index i by a factor of 10 only gives us about one more decimal agreement between the bounds $L(a, i)$ and $U(a, i)$. With the values listed above for $i = 10,000$, and the coefficients

$$(48) \quad \begin{aligned} \frac{3\sqrt{3} r_2}{\pi H_2 \log \epsilon_2} &= 1.227560110251339, \\ \frac{3\sqrt{3} r_3}{\pi H_3 \log \epsilon_3} &= 1.310253787414239, \end{aligned}$$

given by (19)–(21), we obtain our first-order values (14).

It is clear that this Davenport-Schinzel first-order method, together with the improvements made here, leads rather easily to 2D or 3D values such as (13), and, with considerable computation, yields 5D or 6D values such as (14), but if one wishes a better analysis of the numbers k_a the method is not really satisfactory. It is also clear that the location of the limits $L(a, \infty) = U(a, \infty)$ between the universal bounds L_0 and U_0 depends mostly on whether or not a is a cubic residue for the small primes 7, 13, 19, 31, \dots . Since the smallest prime having 2 as a residue is $p_4 = 31$, while that for 3 is $p_7 = 61$, we expect, and find, that both limits lean toward U_0 , and that for 3 is the larger.

Defining the *Ratio*, $R(i)$, by

$$(49) \quad R(i) = \frac{U(a, i)}{L(a, i)} = \frac{U_0}{L_0} \prod_{p \leq p_i} \left(1 - \frac{3(p+1)}{p(p-1)^2}\right) = \prod_{p > p_i} \left(1 - \frac{3(p+1)}{p(p-1)^2}\right)^{-1},$$

we note that it is *independent* of a . It thus provides an excellent check on the arithmetic, and specifically on whether a large value of i leads to excessive round-off error. Further, its deviation from 1 shows at once the extent to which the upper and lower bounds agree. We have

$$(50) \quad R(10,000) = 1.0000005012,$$

in line with the previously noted accuracy. In the Appendix we derive the approximate equation:

$$(51) \quad R(i) \approx 1 + \frac{3/2}{p_{i+1}(\log p_{i+1} + 1)}.$$

Since $p_{10001} = 225223$, this gives the reasonably accurate value $R(10,000) \approx 1.0000004998$. Equation (51) supports our previous observation that to obtain even one more correct decimal we must increase i nearly by a factor of 10.

4. The Weighted Mean and the Distribution of Residues. We seek to circumvent the slow convergence of (28) by introducing a weighted *geometric* mean:

$$(52) \quad G(a, i) = [L(a, i) \cdot U^2(a, i)]^{1/3}$$

as an estimate of the sought limit

$$(53) \quad G(a, i) \approx L(a, \infty) = U(a, \infty).$$

For i large, say, for our present $i = 10^4$, $G(a, i)$ is nearly equal to a weighted *arithmetic* mean:

$$(54) \quad A(a, i) = \frac{1}{3}[L(a, i) + 2U(a, i)],$$

and since the difference $A(a, i) - G(a, i)$ is of a lower order than the error in (53), $A(a, i)$ can be used instead.

The motivation for (52) is simple. Suppose the index i is increased by a Δi which is large, but small in relation to i . Then

$$(55) \quad \begin{aligned} L(a, i + \Delta i) &= L(a, i) \prod_{\text{some } p} \left(1 - \frac{3(p+1)}{p(p-1)^2}\right)^{-1}, \\ U(a, i + \Delta i) &= U(a, i) \prod_{\text{some } p} \left(1 - \frac{3(p+1)}{p(p-1)^2}\right). \end{aligned}$$

The individual factors in the products on the right are nearly equal, since Δi is small in relation to i . On the other hand, since Δi is large, we expect (nearly) $\frac{2}{3}\Delta i$ factors in the upper product, and $\frac{1}{3}\Delta i$ factors in the lower. It follows that we have an approximation

$$(56) \quad L(a, i + \Delta i)U^2(a, i + \Delta i) \approx L(a, i)U^2(a, i),$$

the error of which is presently unknown. To the extent that (56) is accurate, however, we extrapolate:

$$(57) \quad (L(a, i)U^2(a, i))^{1/3} \approx (L(a, \infty)U^2(a, \infty))^{1/3} = L(a, \infty) = U(a, \infty).$$

Similarly, by the foregoing, we may approximate

$$(58) \quad A(a, i) \approx L(a, \infty) = U(a, \infty).$$

But how accurate is this approximation?

In Table 2 we show the behaviour of $G(3, i)$ for $i = 6200(200)10000$. (Actually, we computed the simpler $A(3, i)$ here, but they agree to 12 decimals for these i .)

TABLE 2

| i | $G(3, i)$ | i | $G(3, i)$ |
|------|---------------|-------|---------------|
| 6200 | 1.06127832170 | 8200 | 1.06127831971 |
| 6400 | 1.06127832148 | 8400 | 1.06127831939 |
| 6600 | 1.06127832092 | 8600 | 1.06127831980 |
| 6800 | 1.06127831985 | 8800 | 1.06127832062 |
| 7000 | 1.06127832080 | 9000 | 1.06127832076 |
| 7200 | 1.06127831914 | 9200 | 1.06127832081 |
| 7400 | 1.06127831922 | 9400 | 1.06127832063 |
| 7600 | 1.06127831957 | 9600 | 1.06127832004 |
| 7800 | 1.06127831947 | 9800 | 1.06127832028 |
| 8000 | 1.06127831965 | 10000 | 1.06127832038 |

Now, we note that while $L(3, i)$ and $U(3, i)$ are converging monotonically towards each other

$$U(3, 6200) = 1.06127863370 \quad \downarrow \quad U(3, 10000) = 1.06127849768,$$

$$L(3, 6200) = 1.06127769769 \quad \uparrow \quad L(3, 10000) = 1.06127796580,$$

but agree to only five (and a fraction) digits, the mean oscillates randomly around a value of 1.06127832. But *to the extent* that $G(3, i)$ remains unchanged, we may say that the approximation (53) is valid. And since the changes in $G(3, i)$ here are in the ninth digit, we heuristically expect that

$$L(3, \infty) = U(3, \infty) = 1.06127832$$

is correct—or, at worst, nearly correct—to eight decimals. (In fact, by (47) it is correct.)

As we have indicated, we do not believe any presently obtainable bound on the error in (57) will be sufficiently useful; it would surely be grossly too large. On the other hand, a useful bound will not be rigorous. Nonetheless, we continue this heuristic and empirical treatment in the next section for any insight that it may give into the convergence of (3), and the closely related distribution of cubic residues. We return to an exact treatment in the rest of the paper.

5. Observations and their Heuristic Implications. It is clear that $G(a, i)$ converges to $L(a, \infty)$. The question is: How large are its oscillations around this limit? These oscillations are a damped-down reflection of the much larger oscillations in (3). If, locally, there are many p satisfying (12), the sequences will fall; if there are few such p , the sequences will rise. We wish to gain insight into the (delicate) oscillations in the $G(a, i)$ by examining the grosser behaviour in the partial products of (3).

For $a = 2$ and 3, Bateman and Horn computed (3) for $p < 1000$. We have examined all $a \leq 20$ and computed these products for

$$(59) \quad p < P = n \cdot 1000 \quad (n = 1, 2, 3, \dots, 100).$$

By comparing these with the reasonably accurate limits (14), and their analogues for $a > 3$, we may state, first, the unexpected

Observation 1. The convergence of (3) is mostly from below. In all cases up to $a = 20$, the partial products of (3) exceed k_a for certain limits P , but usually the partial product is smaller. For example, of the 100 values (59), 84 partial products $< k_a$ for $a = 2$, 79 for $a = 3$, 92 for $a = 5$, etc. While these “fractions” vary greatly with both a and P , the overall phenomena is unmistakable. That both estimates (7) would be low was the most probable case.

This Observation 1 has the following implication: Usually, that is, for most ranges of primes

$$(60) \quad P < p < P + \Delta P,$$

with ΔP large but small compared to P , we expect somewhat less than $\frac{1}{3}$ of these p to have a as a cubic residue, and somewhat more than $\frac{2}{3}$ to have a as a cubic nonresidue.

For, suppose there are $3k$ primes p in (60), and that they split as k residues and

$2k$ nonresidues uniformly distributed. The corresponding factors in (3) will yield a product

$$(61) \quad \left[\left(\frac{p-3}{p-1} \right) \left(\frac{p}{p-1} \right) \left(\frac{p}{p-1} \right) \right]^k = \left[1 - \frac{3p-1}{(p-1)^3} \right]^k < 1.$$

But this shows that in such circumstances, (3) would converge *from above*, not *mostly from below*. Since this contradicts Observation 1 we must conclude that usually there will be $< k$ residues and $> 2k$ nonresidues.

In our tables [13], mentioned at the beginning of Section 3, we include data for $a \leq 20$ on the distribution of residues and nonresidues. These counts were both for the primes p_i with

$$i < I = n \cdot 100 \quad (n = 1, 2, 3, \dots, 100),$$

and for those with

$$p_i < P = n \cdot 1000 \quad (n = 1, 2, 3, \dots, 100).$$

While these counts are *cumulative*, and not local as in (60), these results are consistent with the foregoing. We have

Observation 2. For $a \leq 20$, and for most limits I and P above, the fraction of residues is less than $\frac{1}{3}$. Again, while these fractions vary greatly with a and I (or P), the overall phenomena is unmistakable. On the average, for about 85% of the examined limits I (or P), the number of nonresidues exceeds twice the number of residues.*

Let a be fixed, say $a = 3$, and consider

$$(62) \quad S(P) = \frac{D\sqrt{P}}{4I}$$

where $N(P)$ is the number of $p_i \leq P$ for which a is a cubic nonresidue, $R(P)$ is the corresponding number of residues, and

$$(63) \quad \begin{aligned} D &= N(P) - 2R(P), \\ I &= N(P) + R(P). \end{aligned}$$

From Observation 2 we know that $S(P)$ is usually positive. Explicitly, for $a = 3$, and the $P = 1000n$, ($n = 1, 2, \dots, 100$) mentioned above, one finds a local maximum at $n = 7-10$:

$$\begin{aligned} S(7000) &= 1.56, & S(8000) &= 1.22, \\ S(9000) &= 1.29, & S(10000) &= 1.56, \end{aligned}$$

a local minimum at $n = 29-32$:

$$\begin{aligned} S(29000) &= -0.44, & S(30000) &= -0.84, \\ S(31000) &= -0.45, & S(32000) &= -0.42, \end{aligned}$$

and an average S over the 100 values of n :

* Of course, as I (or P) $\rightarrow \infty$, the limiting fraction of residues is exactly $\frac{1}{3}$. That is a special case of Landau's Prime Ideal Theorem.

$$\bar{S} = 0.79.$$

For $a = 2$, one similarly finds

$$S(100000) = 1.77, \quad S(45000) = -0.27, \quad \bar{S} = 0.69,$$

and though we do not wish to give more elaborate statistics here we will merely state that for other a , and other ranges of P , the behaviour is similar.

Now there are two points that should be made about this ratio $S(P)$. First, consider the corresponding partial products of (3):

$$(64) \quad k_a(P) = \prod_{p \nmid a}^P \frac{p - \alpha_a(p)}{p - 1}.$$

We cannot expect an exact correlation between $S(P)$ and $k_a(P)$ since the former merely reflects the *total* counts $N(P)$ and $R(P)$, while the latter depends on the *details* of this distribution. But we do expect a rough correlation and a rough coincidence of their extrema. In fact, for $a = 3$, we find high values at

$$\begin{aligned} k_3(7000) &= 1.39179, & k_3(8000) &= 1.39065, \\ k_3(9000) &= 1.39110, & k_3(10000) &= 1.39229, \end{aligned}$$

low values at

$$\begin{aligned} k_3(29000) &= 1.38799, & k_3(30000) &= 1.38729, \\ k_3(31000) &= 1.38793, & k_3(32000) &= 1.38797, \end{aligned}$$

and, with less precision, that $k_3(P)$ is closest to k_3 when

$$0.7 < S < 1.3.$$

Secondly, this behaviour of $S(P)$ is that which is intuitively expected from analogy with quadratic residues. If we write [14]

$$(65) \quad \tau(P) = -\frac{\sqrt{P}}{\pi(P)} \sum_{p \nmid a}^P \left(\frac{a}{p} \right)$$

for a fixed $a \neq k^2$ with (a/p) the Legendre symbol, we know that $\tau(P)$ is usually positive and has a mean value close to 1. If we replace $\pi(P)$ by $2I$, and (a/p) by the cubic character χ :

$$\begin{aligned} \chi &= 1 && \text{for cubic residues,} \\ \chi &= (-1 \pm \sqrt{3}i)/2 && \text{for cubic nonresidues,} \end{aligned}$$

then $S(P)$ is the real part of the resulting ratio.

This described behaviour of $\tau(P)$ is associated with the complex zeros of the corresponding Dirichlet L functions, and will persist as $P \rightarrow \infty$ if and only if none of these zeros have a real part $> \frac{1}{2}$. One expects that $S(P)$ depends similarly on the corresponding Dedekind Zeta function of the cubic field $\mathbb{Q}(a^{1/3})$.

If our observations concerning $S(P)$ would persist as $P \rightarrow \infty$ we would expect

$$(66) \quad k_a(P) = k_a + O(P^{-1/2+\epsilon}).$$

We referred to the Bateman-Horn estimate as a "zero-order" method, and, in fact,

that is all that can be proven. But, probably it really is a "half-order" method in agreement with (66). At $P = 10^5$, and therefore $i = 4784$, one has

$$R(4784) = 1.0000012$$

from (49). The upper and lower bounds in the first-order method therefore differ in the sixth decimal here. But $k_3(P)$ is oscillating in the third decimal at $P \approx 10^5$.

Applying the same assumption on the distribution of residues and nonresidues to (55) instead of (3), would therefore lead us to expect, for $p_i = P$,

$$(67) \quad G(a, i) = G(a, \infty) + O(P^{-3/2+\epsilon}).$$

We did see that $G(a, i)$ was oscillating in the ninth decimal at comparable P . Apparently, then, (52) is a $1\frac{1}{2}$ -order method.

Clearly, all of this section is merely heuristic. We have not proven that (52) has the accuracy suggested above. Nonetheless, the intuitive picture presented may be of interest.

In (15) we gave a quite conservative estimate; we made no serious attempt to squeeze out one extra decimal by careful correlation of $G(a, i)$ with $S(P)$ as suggested above. The real method for computing a more accurate k_a is in [12], as we mentioned, but these studies in the distribution of cubic residues nonetheless induced us to compute some quite elaborate tables [13]. These may find other use.

6. Utilizing $\zeta_K(s)$ for $s = 2, 3, \dots$, if Available. From (19), (20), (23) and (46) we may write

$$(68) \quad A = k_2 = \frac{C}{\ln \epsilon_2} \prod_{4^m \nmid 1 \pmod{p}} \frac{(1 - 1/p)^3}{(1 - 3/p)(1 - 1/p^3)}.$$

Now just as [5] introduced $\text{Lim}_{s \rightarrow 1} \zeta(s)/\zeta_K(s)$ into the slowly convergent product (3), we may similarly remove the most slowly convergent "factor" from the product (68).

Consider $\zeta(s)$ and the $L_3(s)$ and $\zeta_3(s)$ of (16) and (31). Each has an Euler product as does also the Dedekind Zeta function $\zeta_K(s)$ for $K = Q(2^{1/3})$. If we combine the four products we find

$$(69) \quad f(s) = \frac{\zeta(s)\zeta_3(s)L_3(s)}{\zeta_K(s)} = \prod_{4^m \nmid 1 \pmod{p}} \frac{1 - 1/p^{3s}}{(1 - 1/p^s)^3}$$

taken over the same primes. Let us write $x = 1/p$ and note the factor in (68) is a rational function $R_2(x)$ satisfying

$$R_2(x) = 1 + 3x^2 + O(x^3)$$

as $x \rightarrow 0$. But the factor in (69) for $s = 2$ is also $1 + 3x^2 + O(x^3)$ and so we write

$$k_2 = \frac{C}{\ln \epsilon_2} f(2) \prod R_3(x)$$

with a new rational function

$$R_3(x) = 1 + 9x^3 + O(x^4).$$

Iterating, we next obtain

$$k_2 = \frac{C}{\ln \epsilon_2} f(2)[f(3)]^3 \prod R_4(x)$$

with

$$R_4(x) = 1 + 18x^4 + O(x^5),$$

etc.

Since $\zeta(s)$, $\zeta_3(s)$ and $L_3(s)$ have well known values for $s = 2, 3, \dots$, [8] it is clear that we can obtain a sequence that converges to k_2 with arbitrary rapidity provided we can compute $\zeta_\pi(s)$ for $s = 2, 3, \dots$. We need not continue this point since a complete (and more elegant) treatment is given in [12].

7. The Twin Constants. Let us evaluate (more briefly) the constants (18). The Bateman-Horn formula [1] gives, for $a = \pm 2$ and ± 3 ,

$$(70) \quad \frac{1}{9} t_a = \frac{1}{9} \frac{2}{(2-1)^2} \frac{3}{(3-1)^2} \prod_q \frac{q(q-2)}{(q-1)^2} \prod_p \frac{p(p-\omega(p))}{(p-1)^2}$$

where $\omega(p)$ is the number of solutions of

$$(71) \quad [(n-1)^3 + a][(n+1)^3 + a] \equiv 0 \pmod{p}$$

for $p = 6m + 1$. We need

$$(72) \quad T = \frac{1}{6} \prod_q q(q-2)/(q-1)^2$$

and could compute it as in Section 2 using the lemma there with $n = 2$. However, T may be expressed in terms of known constants. The twin-prime constant [15]:

$$c_2 = \prod_{\text{odd primes } r} r(r-2)/(r-1)^2,$$

the Hardy-Littlewood constant [16]:

$$h_3 = \prod_p \frac{p-2}{p-1} \prod_q \frac{q}{q-1},$$

and the Landau constant [7]:

$$b_3 = \left[\frac{2}{27^{1/2}} \prod_q q^2/(q^2-1) \right]^{1/2}$$

may be combined into

$$(73) \quad T = \frac{2c_2 b_3^2}{\pi h_3}.$$

(In its universality, (73) reminds us a bit of Euler's useful $e^{\pi i} = -1$ and Eddington's unfortunate $hc/2\pi e^2 = 137$.)

If, for $1 \leq n \leq N$, $B_3(N)$ is the number of $n = a^2 + 3b^2$, $Z(N)$ is the number of (usual) twin-prime pairs, and $P_3(N)$ is the number of primes n^2+3 , then, by two conjectures and two theorems, we have

$$(73a) \quad T = \lim_{N \rightarrow \infty} \frac{1}{2\pi} \frac{Z(N)}{P_3(N)} \left[\frac{B_3(N)}{\pi(N)} \right]^2.$$

But we prefer to obtain

$$(74) \quad T = 0.153075970785714$$

from the known values

$$c_2 = 0.6601618158468696,$$

$$h_3 = 1.1207327535492914,$$

$$b_3 = 0.6389094054453439.$$

Now we examine the last product in (70). If $a^{2^m} \not\equiv 1 \pmod{p}$, $\omega(p) = 0$, whereas if $a^{2^m} \equiv 1 \pmod{p}$ usually $\omega(p) = 6$. But note that if $a = 2$, $p = 43$, (71) has only five solutions:

$$n \equiv 8, 10, 12, 22, 24 \pmod{43}.$$

And for $a = 3$, there are only five solutions for $p = 307$:

$$n \equiv 78, 80, 112, 114, 116 \pmod{307}.$$

This *degeneracy* comes about if two solutions m of $m^3 + a = 0 \pmod{p}$ differ by 2 \pmod{p} . Let us write

$$(75) \quad O_a = \prod_{p^*} (p^* - \omega(p^*)) / (p^* - 6) \quad (a = \pm 2, \pm 3)$$

for all such exceptional primes p^* . For other a [6], (70) may have other exceptional factors since some q and/or some p may divide a . We could then absorb these exceptional rational factors into O_a just as we did in the r_a of (19). We return to (75) below.

We write the last product in (70) as

$$O_a(k_a)^2 u(a, \infty)$$

with

$$(76) \quad u(a, \infty) = \prod_{a^{2^m} \equiv 1 \pmod{p}} p(p-6)/(p-3)^2.$$

Then

$$(77) \quad \frac{1}{2}t_a = T(k_a)^2 O_a u(a, \infty).$$

We compute (76) as we did $U(a, \infty)$. With

$$(78) \quad l_0 = \prod_{\text{all } p} p(p-6)/(p-3)^2$$

we have bounding sequences

$$(79) \quad \begin{aligned} l(a, i) &= l_0 \prod_{a^{2^m} \not\equiv 1 \pmod{p}; p \leq p_i} (p-3)^2/p(p-6), \\ u(a, i) &= \prod_{a^{2^m} \equiv 1 \pmod{p}; p \leq p_i} p(p-6)/(p-3)^2. \end{aligned}$$

We obtained

$$(78a) \quad l_0 = 0.368209383803918$$

from the lemma with $n = 6$ and 3, and evaluated the bounds (79) and their weighted

mean from our IBM data, as before. That gives

$$\begin{aligned} l(2, 10000) &= 0.9799883425, & u(2, 10000) &= 0.9799898160, \\ l(3, 10000) &= 0.9909293369, & u(3, 10000) &= 0.9909308268. \end{aligned}$$

Then

$$\begin{aligned} (80) \quad u(2, \infty) &= 0.97998932(4), \\ u(3, \infty) &= 0.99093033(0) \end{aligned}$$

are obtained by the weighted mean, or, more simply (and nearly equal), by

$$(81) \quad u(a, \infty) \approx u(a, i)/R(i).$$

Thus, $l(a, i)$ and l_0 are really redundant.

There remains O_a . We have the

THEOREM. *If a prime p has a as a cubic residue, and if two cube-roots of $a \pmod{p}$ differ by Δ , with $p \nmid \Delta$, then*

$$(82) \quad p \mid \Delta^6 + 27a^2.$$

Proof. Let

$$A = (n + \Delta)^3 - a, \quad B = n^3 - a.$$

Then

$$\begin{aligned} (\Delta^4 - 3n\Delta^3 + 6n^2\Delta^2 + 9an - 9a\Delta)A \\ - (10\Delta^4 + 15n\Delta^3 + 6n^2\Delta^2 + 9an + 18a\Delta)B = \Delta(\Delta^6 + 27a^2). \end{aligned}$$

Thus, if $A \equiv B \equiv 0 \pmod{p}$ we obtain (82).

(The proof is efficient but brutal. A more charming proof is given in the Appendix.)

Now for $\Delta = 2$, $a = \pm 2$, $p \mid 172$ and can only be 43. For $\Delta = 2$, $a = \pm 3$, $p \mid 307$ and can only be 307. Therefore,

$$(83) \quad O_{\pm 2} = \frac{38}{37}, \quad O_{\pm 3} = \frac{302}{301},$$

and so, from (74), (80), and (77) we obtain (18).

We have not previously stated that

$$\begin{aligned} (84) \quad k_2 &= k_{-2} = k_4 = k_{-4}, \\ k_3 &= k_{-3} = k_9 = k_{-9}, \end{aligned}$$

but of course that follows from (12). Not so with the $t_{\pm a}$ and $t_{\pm a^*}$. We have

$$(85) \quad O_{\pm 4} = \frac{26}{25}, \quad O_{\pm 9} = \frac{2246}{2245}$$

and so $T_{\pm 4}(N)$ should be a little larger than $T_{\pm 2}(N)$ while $T_{\pm 9}(N)$ should be a bit smaller than $T_{\pm 3}(N)$.

8. Comparison with Horn's Data. In Table 3 we list values of $T_a(N)$ for $N = 2000(2000)14000$ and $a = \mp 2, \mp 3$. These counts were obtained from Horn's

TABLE 3

| $10^{-3}N$ | $T_{-2}(N)$ | $T_2(N)$ | <i>Theory</i> | $T_{-3}(N)$ | $T_3(N)$ | <i>Theory</i> |
|------------|-------------|----------|---------------|-------------|----------|---------------|
| 2 | 15 | 14 | 13.9 | 17 | 23 | 15.7 |
| 4 | 26 | 25 | 22.1 | 24 | 38 | 25.0 |
| 6 | 36 | 34 | 29.2 | 32 | 49 | 33.1 |
| 8 | 43 | 36 | 35.9 | 40 | 58 | 40.6 |
| 10 | 46 | 46 | 42.1 | 43 | 66 | 47.7 |
| 12 | 52 | 56 | 48.2 | 52 | 71 | 54.5 |
| 14 | 58 | 60 | 53.9 | 54 | 82 | 61.1 |

lists of primes up to 14000 [2] that he kindly made available to us. We also give the right side of (17) with the t_a taken from (18).

Considering the small counts $T_a(N)$ and limits N here, we would not expect better agreement than that recorded for $a = \mp 2$ and $a = -3$. These are acceptable. But $T_3(N)$ is surprisingly, consistently and disturbingly large. In view of the usual good standing of conjectures of this type, one is inclined to surmise that this is merely a (rather large) fluctuation which will dissipate as N increases. But that could well be wishful thinking rather than scientific and we felt obliged to investigate this discrepancy.

9. Our Own Data. We wish to check the counts $T_3(N)$ listed above, and, if they prove accurate, to extend the data to larger values of N . Since the $T_3(N)$ in Table 3 are too large in comparison with the theory, we can greatly abbreviate the computation, as we shall see.

We determined all n such that

$$(86) \quad m_1 = (n-1)^3 + 3, \quad m_2 = (n+1)^3 + 3$$

both satisfy Euler's Criterion:

$$(87) \quad 2^{(m-1)/2} \equiv -1 \pmod{m},$$

and also, for $n > 3$, satisfy

$$(88) \quad m \not\equiv 0 \pmod{2, 3, 5, 11, 17, 23, 61, 67, 73}.$$

The number of such n in $1 \leq n+1 \leq N$ we call $T_3^*(N)$. This $T_3^*(N)$ is much faster to compute than $T_3(N)$.

The two values: $n = 1, (m_1 = 3, m_2 = 11)$ and $n = 3, (m_1 = 11, m_2 = 67)$ do not satisfy (88)—that is why we stipulated $n > 3$ for that condition. But all other prime-pairs (86) satisfy both (87) and (88) and so

$$(89) \quad T_3^*(N) \geq T_3(N).$$

Since almost all m satisfying

$$2^{m-1} \equiv 1 \pmod{m}$$

are prime, [17], and since we have added strong further conditions in (87) and (88), we can expect that $T_3^*(N) - T_3(N)$ will be relatively very small, or even zero.

We find, in fact, that

$$T_3^*(14000) = T_3(14000) = 82,$$

and precisely the same 82 values of n are contained in each list. This shows that Horn's data is sound and that the phenomenon (of large $T_3(N)$) is a real one. We therefore extended $T_3^*(N)$ to $N = 50000$ and obtained

TABLE 4

| $10^{-3}N$ | $T_3^*(N)$ | Theory | $10^{-3}N$ | $T_3^*(N)$ | Theory |
|------------|------------|--------|------------|------------|--------|
| 16 | 92 | 67.5 | 30 | 127 | 108.5 |
| 18 | 97 | 73.7 | 40 | 146 | 135.4 |
| 20 | 100 | 79.7 | 50 | 166 | 161.0 |

The increment $T_3^*(50000) - T_3^*(20000) = 66$ is less than the theoretical $161.0 - 79.7 = 81.3$ and the previous excess is now essentially liquidated. But, by (89), $T_3(50000)$ can only be smaller than $T_3^*(50000) = 166$, if it differs at all. Therefore, the surmise was correct and we now have no reason to believe that (17) is false for $a = 3$.

10. Appendix. Derivation of (51). We have

$$R(i) = \prod_{n=i+1}^{\infty} \left(1 - \frac{3(p_n + 1)}{p_n(p_n - 1)^2}\right)^{-1}$$

and so

$$\log R(i) = \sum_{n=i+1}^{\infty} \left[\frac{3}{p_n^2} + O\left(\frac{1}{p_n^3}\right) \right].$$

We write

$$\log R(i) \approx \int_{i+1}^{\infty} 3 \, dn/p_n^2,$$

and from the Prime Number Theorem:

$$2n \approx p_n/(\log p_n - 1)$$

we obtain

$$\log R(i) \approx \frac{3}{2} \int_{p_{i+1}}^{\infty} \frac{dp_n(\log p_n - 2)}{p_n^2(\log p_n - 1)^2}.$$

Let

$$x = \log p_n - 1, \quad x_0 = \log p_{i+1} - 1.$$

Then

$$\log R(i) \approx \frac{3}{2e} \int_{x_0}^{\infty} \frac{e^{-x}(x-1)}{x^2} dx.$$

The integral, call it I , may be evaluated by Exponential Integrals which in turn, have known continued fractions:

$$\begin{aligned} I &= E_1(x_0) - \frac{1}{x_0} E_2(x_0) \\ &= \frac{e^{-x_0}}{x_0 + \frac{1}{1 + \frac{1}{x_0 + \frac{2}{1 + \dots}}}} - \frac{1}{x_0} \frac{e^{-x_0}}{x_0 + \frac{2}{1 + \frac{1}{x_0 + \frac{3}{1 + \dots}}}}. \end{aligned}$$

Or,

$$\begin{aligned} I &= \frac{e^{-x_0}}{(x_0 + 1) - \frac{1}{(x_0 + 1)} + \dots} - \frac{e^{-x_0}}{(x_0 + 1)^2 - 3 + \dots} \\ &= \frac{e^{-x_0}}{x_0 + 1} \left(1 - \frac{1}{(x_0 + 1)} + \frac{1}{(x_0 + 1)^2} + \dots \right) \approx \frac{e^{-x_0}}{x_0 + 2}. \end{aligned}$$

Thus,

$$\log R(i) \approx \frac{3}{2p_{i+1}[\log p_{i+1} + 1]}$$

which leads to (51).

Geometric Interpretation of (82). Consider two equilateral triangles, of side S , displaced with respect to each other a distance D . See Fig. 1.

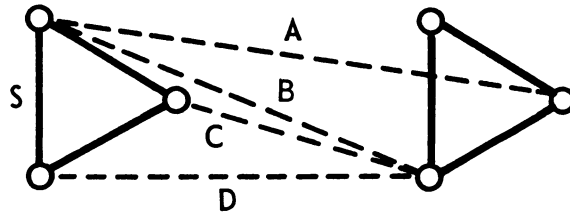


FIGURE 1

The fifteen lines joining the six vertices comprise: 6 of length S , 3 of length D , and 2 each of length A , B , and C .

We have

$$A^2 = \left(\frac{S}{2}\right)^2 + \left(D + \frac{\sqrt{3}}{2} S\right)^2,$$

$$B^2 = S^2 + D^2,$$

$$C^2 = \left(\frac{S}{2}\right)^2 + \left(D - \frac{\sqrt{3}}{2} S\right)^2.$$

Then

$$A^2 C^2 = (S^2 + D^2 + SD\sqrt{3})(S^2 + D^2 - SD\sqrt{3})$$

and so

$$A^2 B^2 C^2 = S^6 + D^6.$$

The product P of all 15 lines is

$$(90) \quad P = S^6 D^3 (S^6 + D^6).$$

Now consider the congruence

$$f(z) = [(z + \Delta)^3 - a][z^3 - a] \equiv 0 \pmod{p}.$$

It will have a double root only if p divides the discriminant. This equals the product of the squares of the 15 differences among the 6 roots of $f(z) = 0$. The 6 roots are disposed in the complex plane as in Fig. 1 if

$$(91) \quad S = \sqrt[3]{3} a^{1/3}, \quad D = \Delta.$$

Then (90) becomes

$$P = 27a^2 \Delta^3 (\Delta^6 + 27a^2),$$

and if p divides neither a nor Δ it must divide $\Delta^6 + 27a^2$.

Computation & Mathematics Department
Naval Ship Research & Development Center
Bethesda, Maryland 20034

Department of Mathematics
Memorial University of Newfoundland
St. John's, Newfoundland, Canada

1. P. T. BATEMAN & R. A. HORN, "A heuristic asymptotic formula concerning the distribution of prime numbers," *Math. Comp.*, v. 16, 1962, pp. 363–367. MR 26 #6139.
2. P. T. BATEMAN & R. A. HORN, "Primes represented by irreducible polynomials in one variable," *Proc. Sympos. Pure Math.*, vol. 8, Amer. Math. Soc., Providence, R. I., 1965, pp. 119–132. MR 31 #1234.
3. G. H. HARDY & J. E. LITTLEWOOD, "On the expression of a number as a sum of primes," *Acta Math.*, v. 44, 1923, pp. 1–70.
4. DANIEL SHANKS, "Review of [2]," RMT 112, *Math. Comp.*, v. 19, 1965, pp. 684–686.
5. H. DAVENPORT & A. SCHINZEL, "A note on certain arithmetical constants," *Illinois J. Math.*, v. 10, 1966, pp. 181–185. MR 32 #5632.
6. MOHAN LAL & DANIEL SHANKS, "Distribution of primality in the neighborhood of cubes." (To appear.)
7. DANIEL SHANKS & LARRY P. SCHMID, "Variations on a theorem of Landau," *Math. Comp.*, v. 20, 1966, pp. 551–569. MR 35 #1564.
8. DANIEL SHANKS & JOHN W. WRENCH, JR., "The calculation of certain Dirichlet series," *Math. Comp.*, v. 17, 1963, pp. 136–154. MR 28 #3012.
9. DANIEL SHANKS, "Lal's constant and generalizations," *Math. Comp.*, v. 21, 1967, pp. 705–707. MR 36 #6363.
10. P. T. BATEMAN & R. STEMMLER, "Waring's problem for algebraic number fields and primes of the form $(p^* - 1)/(p^4 - 1)$," *Illinois J. Math.*, v. 6, 1962, pp. 142–156. MR 25 #2059.
11. DANIEL SHANKS, "Corrigendum to [8]," *Math. Comp.*, v. 22, 1968, p. 246.
12. DANIEL SHANKS, "Calculation and applications of Epstein zeta functions." (To appear.)
13. MOHAN LAI & DANIEL SHANKS, *Tables of Cubic Residues*. (To appear.)
14. DANIEL SHANKS, "Quadratic residues and the distribution of primes," *MTAC*, v. 13, 1959, pp. 272–284. MR 21 #7186.
15. JOHN W. WRENCH, JR., "Evaluation of Artin's constant and the twin-prime constant," *Math. Comp.*, v. 15, 1961, pp. 396–398. MR 23 #A1619.
16. DANIEL SHANKS, "On the conjecture of Hardy & Littlewood concerning the number of primes of the form $n^2 + a$," *Math. Comp.*, v. 14, 1960, pp. 321–332. MR 22 #10960.
17. P. ERDŐS, "On almost primes," *Amer. Math. Monthly*, v. 57, 1950, pp. 404–407. MR 12, 80.