TECHNICAL NOTES AND SHORT PAPERS

Lal's Constant and Generalizations

By Daniel Shanks

1. Introduction. As is known, if $P_1(N)$ is the number of primes of the form $n^2 + 1$ for $1 \leqq n \leqq N$ and, if

$$\mathrm{li}(N) = \int_2^N dn/\log n ,$$

then *empirically* and *heuristically*, one has, cf. [1]:

$$P_1(N) \sim 0.68641\ \mathrm{li}(N) . \tag{1}$$

Thus, while the much weaker proposition

$$P_1(N) \to \infty \tag{2}$$

has still not been proven, the investigation of (1) provides strong evidence that (2) is true.

The case is strengthened when it is realized that even *subsets* of the set of primes $n^2 + 1$ have counts that $\to \infty$ according to well-known laws. For example, if $n = m^2$, we find empirically and heuristically that if $Q_1(N)$ is the number of primes $m^4 + 1$ with $1 \leqq m \leqq N$, then, [2]:

$$Q_1(N) \sim \tfrac{1}{4}\, s_1\, \mathrm{li}(N) = 0.66974\ \mathrm{li}(N) . \tag{3}$$

Or, again, if $(m - 1)^2 + 1$ and $(m + 1)^2 + 1$ are both prime, and if $g(N)$ is the number of such pairs for $m + 1 \leqq N$, then, [3]:

$$g(N) \sim 0.48762\ \mathrm{li}_2(N) \tag{4}$$

where

$$\mathrm{li}_2(N) = \int_2^N dn/\log^2 n .$$

Recently [4], Lal has counted pairs of primes $(m - 1)^4 + 1$ and $(m + 1)^4 + 1$ —the "conceptual intersection" of both previous subsets—and he found that if the number of such pairs with $m + 1 \leqq N$ is $h(N)$, then $h(N)$ is at least roughly proportional to $\mathrm{li}_2(N)$. (The qualification "at least roughly" has reference to the fact that he went to only $N = 4000$, and $h(4000)$ is only equal to 57.) Lal did not evaluate the constant λ in

$$h(N) \sim \lambda\ \mathrm{li}_2(N) ; \tag{5}$$

we do that here.

2. Impossible Congruences. From Bateman's formula [5, Eq. (1)] we find from (3) and (5) that

Received May 18, 1967.

$$\lambda = (s_1/4)^2 \cdot 2 \cdot \prod_{p=8k+1} \frac{p(p-\omega(p))}{(p-4)^2} \tag{6}$$

with the product taken over all primes $p = 8k + 1$, and where $\omega(p)$ is the number of residue classes (mod p) that satisfy

$$[(m-1)^4 + 1]\cdot[(m+1)^4 + 1] \equiv 0 \pmod{p} . \tag{7}$$

Now each factor on the left of (7) has four roots, and therefore $\omega(p) = 8$ for each $p = 8k + 1$, provided that

$$A = (m-1)^4 + 1 \equiv 0 \pmod{p} , \qquad B = (m+1)^4 + 1 \equiv 0 \pmod{p} \tag{8}$$

are not *simultaneously* satisfied for any m. This condition is certainly not obvious; it means that no two of the fourth-roots of -1 (mod p) can differ by 2. But if $A \equiv B \equiv 0$ (mod p) then $32m^2(A + B) - 8m(A - B) - (A - B)^2 = 192m^4 \equiv 0$ (mod p). This implies that $m \equiv 0$ (mod p), which contradicts (8). Therefore

$$\lambda = (s_1/4)^2 \cdot 2 \cdot C \tag{9}$$

with

$$C = \prod_{p=8k+1} \frac{p(p-8)}{(p-4)^2} . \tag{10}$$

3. An Infinite Product. To evaluate (10) we want two cases of the following

LEMMA. *If*

$$1 - 2kx = \prod_{s=1}^{\infty} \left(\frac{1-x^s}{1+x^s}\right)^{b(k,s)} \tag{11}$$

then

$$b(k, s) = \frac{1}{2s} \sum_d \mu(d)(2k)^{s/d} , \tag{12}$$

the sum taken over all odd divisors d of s with $\mu(d)$ the Möbius function. Conversely, the right side of (11) *converges to the left side if* $|2kx| < 1$.

Comments. The lemma for $k = 1$ is proven in [1, p. 322], and the proof of the generalization here is virtually the same. The lemma for $k = 2$ was given without proof in [2, Eq. (5)]. The general lemma is similar to, but not the same as, *Witt's Formula*, cf. [6].

If we now take $x = 1/p$ and $k = 4$ and 2, (10), (11) and (12) give us

$$C = \prod_{p=8k+1} \left(\frac{p^2-1}{p^2+1}\right)^8 \left(\frac{p^3-1}{p^3+1}\right)^{64} \left(\frac{p^4-1}{p^4+1}\right)^{448} \left(\frac{p^5-1}{p^5+1}\right)^{3072} \cdots . \tag{13}$$

4. Lal's Constant and Generalizations. But for $s > 1$ we have [2, Eq. (6)]:

$$\prod_{p=8k+1} \left(\frac{p^s-1}{p^s+1}\right)^2 = \frac{L_{-1}^2(2s)}{L_{-1}(s)L_1(s)L_{-2}(s)L_2(s)} \tag{14}$$

so the factors on the right of (13) are given in terms of the known [7] Dirichlet series $L_a(s)$. As is usual in such calculations we may obtain much faster convergence by computing the first f factors in (10) *directly*—that is, by computing

$$p(p-8)/(p-4)^2 \text{ for } p = 17, 41, 73, 89, \cdots,$$

and then compensating by utilizing instead of (14) the modified

$$(15) \qquad \prod_{p>p_f} \left(\frac{p^s-1}{p^s+1}\right)^2 = \frac{L_{-1}^2(2s)}{L_{-1}(s)L_1(s)L_{-2}(s)L_2(s)} \prod_{p \leqq p_f} \left(\frac{p^s+1}{p^s-1}\right)^2 .$$

We therefore obtain

$$(16) \qquad C = 0.88307$$

and, from (3) and (9),

$$(17) \qquad \lambda = 0.79220.^*$$

It is clear that the same techniques may be used in evaluating a large class of constants. Let

$$(18) \qquad c = \prod_{p=Ak+B} \prod_{i=1}^{r} \frac{p-2k_i}{p-2t_i}$$

with $A = 2, 4, 6, 8, 12$, or 24, with B prime to A, and with

$$(19) \qquad \sum_{i=1}^{r} (k_i - t_i) = 0 .$$

This generalizes our (10), in which $A = 8$, $B = 1$, $k_1 = 0$, $k_2 = 4$, $t_1 = t_2 = 2$. By use of the Lemma, and products analogous to (14) for other A and B, all such constants (18) are computable without undue difficulty. The needed products

$$\prod_{p=Ak+B} \left(\frac{p^s-1}{p^s+1}\right)$$

can all be evaluated in terms of $L_a(s)$, where the subscripts a are some, or all, of the twelve divisors of 18: ± 1, ± 2, ± 3, ± 6, ± 9, and ± 18. All these $L_a(s)$ are known [7]. If one or more primes $p = Ak + B$ in (18) are less than one or more $2k_i$ or $2t_i$, then clearly one must choose the p_f above to be greater than all such p, otherwise the sequence analogous to (13) will diverge. By increasing p_f, one first eliminates any divergence, and then obtains more rapid convergence.

Applied Mathematics Laboratory
Naval Ship Research and Development Center
Washington, D. C. 20007

1. Daniel Shanks, "On the conjecture of Hardy and Littlewood concerning the number of primes of the form $n^2 + a$," *Math. Comp.*, v. 14, 1960, pp. 321–332. MR **22** #10960.

2. Daniel Shanks, "On numbers of the form $n^4 + 1$," *Math. Comp.*, v. 15, 1961, pp. 186–189; Corrigendum, *ibid.*, v. 16, 1962, p. 513. MR **22** #10941.

3. Daniel Shanks, "A note on Gaussian twin primes," *Math. Comp.*, v. 14, 1960, pp. 201–203. MR **22** #2586.

4. M. Lal, "Primes of the form $n^4 + 1$," *Math. Comp.*, v. 21, 1967, pp. 245–247.

5. 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.

6. Marshall Hall, Jr., *The Theory of Groups*, Macmillan, New York, 1959, p. 169. MR **21** #1996.

7. Daniel Shanks & J. W. Wrench, Jr., "The calculation of certain Dirichlet series," *Math. Comp.*, v. 17, 1963, pp. 136–154; Corrigenda, *ibid.*, p. 488. MR **28** #3012.

* One has $\lambda\, \mathrm{li}_2(4000) = 67.3$, which is high, but not disturbingly so.