lines are shown on each page, with spaces between successive sets of five lines, as before; thus, a total of 3200 octal digits are accommodated on each sheet.

In a related paper [1] the authors have presented similar statistical information concerning these square roots. While this statistical information is believed correct, the unpublished printed-out values of the roots computed at that time contained several erroneous digits because of a programming error. Discrepancies between those decimal approximations obtained for $\sqrt{2}$ and $\sqrt{3}$ and the values previously published by Uhler [2, 3] were erroneously attributed by the authors to purported errors in Uhler's calculations. The corrected values appearing in the present manuscript are believed by the authors to be free from error. In partial confirmation of this, the reviewer has found complete agreement of the value of $\sqrt{2}$ herein with the unpublished approximation [4] of Lal, which extends to 19600D.

J. W. W.

1. Kōki Takahashi & Masaaki Sibuya, "Statistics of the digits of $\sqrt{n}$," *Jōhō Shori (Information Processing)*, v. 6, 1965, pp. 221–223. (Japanese)
2. H. S. Uhler, "Many-figure approximations to $\sqrt{2}$, and distribution of digits in $\sqrt{2}$ and $1/\sqrt{2}$," *Proc. Nat. Acad. Sci. U. S. A.*, v. 37, 1951, pp. 63–67.
3. H. S. Uhler, "Approximations exceeding 1300 decimals for $\sqrt{3}$, $1/\sqrt{3}$, $\sin(\pi/3)$ and distribution of digits in them," *ibid.*, pp. 443–447.
4. M. Lal, *Expansion of $\sqrt{2}$ to 19600 Decimals*, ms. deposited in the UMT file. (See *Math. Comp.*, v. 21, 1967, pp. 258–259, RMT 17.)

19[F].—L. G. Diehl & J. H. Jordan, *A Table of Gaussian Primes*, Washington State University, Pullman, Washington, a strip of computer paper deposited in the UMT file.

If p, a prime, is of the form $4m + 1$ then $p = A^2 + B^2$. As is known

$$\pm A \pm Bi \quad \text{and} \quad \pm B \pm Ai$$

are then Gaussian primes. This table lists A and B for each $p = 4m + 1 \leqq 90997$.

Whereas such a table is not readily available, a somewhat larger table for $p < 10^5$ was published by A. J. C. Cunningham long ago [1].

The present table was computed in 15 minutes on an IBM 709 at Washington State University. No details are given as to how this was done. It may be of interest to survey briefly known methods that have been used for these and related problems.

Four methods of theoretical interest are reviewed by Davenport [2]. The simplest conceptually is that of Gauss. If $p = 4m + 1$, set

$$A \equiv (2m)!/2(m!)^2, \qquad B \equiv (2m)!\, A \pmod{p}.$$

It is clear that this is quite inefficient arithmetically speaking. Related to this is Jacobsthal's method. Let

$$S(a) = \sum_{n=1}^{p-1} \left(\frac{n(n^2 - a)}{p} \right)$$

where the quantity summed is the Legendre symbol. Then if R is any quadratic residue, say $R = 1$, and N is any nonresidue, set

$$A = \tfrac{1}{2} \mid S(R) \mid, \qquad B = \tfrac{1}{2} \mid S(N) \mid.$$

Recently Chowla [3] has given an attractive proof of Jacobsthal's method, a consequent simple proof of Gauss's method, and the relation of these Jacobsthal sums to the Riemann Hypothesis.

More practical are the other two methods. That of Legendre is based on the regular continued fraction of $\sqrt{p}$. This would require a number of operations $O(p^{1/2+\epsilon})$, since this is the bound on the period of the continued fraction. This contrasts favorably with the $O(p)$ operations needed for Gauss's method.

But better still is Serret's method. This is based on the finite continued fraction for p/s, where $0 < s < \frac{1}{2}p$ and $p \mid s^2 + 1$. This fraction has only $O(\log p)$ terms. Now, if we were to compute $\sqrt{-1} = s \pmod{p}$ by Wilson's Theorem:

$$s \equiv \pm[(p-1)/2]!$$

we would be back to an $O(p)$ algorithm, but we can do better. We need any nonresidue N of p. If $p = 8m + 5$, then 2 will do. If not, but if $p = 24m + 17$, then 3 will do. In $O(\log p)$ attempts we can find an N. Then

$$s \equiv \pm N^{(p-1)/4} \pmod{p}.$$

The power shown can also be computed in $O(\log p)$ operations by expressing $(p-1)/4$ in binary, and then successively squaring powers of N. For example, if $p = 1429$,

$$(2/1429) = -1,$$

and

$$\pm 2^{357} \equiv s,$$

or

$$-2^{1+4+32+64+256} \equiv 620 = s.$$

Thus, the Serret algorithm, with s found as above is $O(\log p)$. This is perhaps the best one can do for large p. For further discussion of the Legendre and Serret methods see [4, Exercises 145–149, pp. 187–188].

In all of the foregoing the expansion $p = A^2 + B^2$ is being carried out for a single p at a time. There also exists a sieve method based upon the p-adic square roots of -1 which can carry out such computations *en masse*, with the p's and their corresponding s's arising automatically [5].

Still other techniques, less interesting mathematically, but quite feasible programming-wise, have been used. These mostly involved trial-and-error subtractions, or additions combined with a sorting process of some type.

Finally, we might note, for some of the largest known $p = 4m + 1$, such as Brillhart's $p = 2^{457} - 2^{229} + 1$, one has at once, by inspection,

$$p = (2^{228})^2 + (2^{228} - 1)^2.$$

With a bit more effort one can deduce from the third-largest known prime of the form $4m + 1$ (which was found recently by Brillhart and Selfridge):

$$\tfrac{1}{5}(2^{691} - 2^{346} + 1),$$

the *largest* known complex Gaussian prime:

$$\tfrac{1}{5}(3 \cdot 2^{345} - 1) + \tfrac{1}{5}(2^{345} - 2)i.$$

The two largest known primes of the form $4m + 1$:

$$5 \cdot 2^{1947} + 1 \quad \text{and} \quad 7 \cdot 2^{830} + 1,$$

are due to Robinson, but I know of no easy way of finding their Gaussian factors.

Perhaps the best algorithm for the first would again be Serret's, starting from the fact that this prime divides a specific Fermat number.

D. S.

1. A. J. C. CUNNINGHAM, *Quadratic Partitions*, Hodgson, London, 1904.
2. H. DAVENPORT, *The Higher Arithmetic*, Harper, New York, 1960, pp. 120–123.
3. S. CHOWLA, *The Riemann Hypothesis and Hilbert's Tenth Problem*, Gordon and Breach, New York, 1965, Chapters IV, V.
4. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, Spartan, Washington, 1962.
5. D. SHANKS, "A sieve method for factoring numbers of the form $n^2 + 1$," *MTAC*, v. 13, 1959, pp. 78–86.

20[F].—M. F. JONES, M. LAL & W. J. BLUNDON, *Table of Primes*, Memorial University of Newfoundland, St. John's, Newfoundland, Canada, June 1966, ms. of 100 computer sheets, 28 cm. Copy deposited in the UMT file.

This table lists all 47273 primes in the eight ranges:

$$10^n(1)10^n + 150{,}000; \qquad n = 8(1)15.$$

It, and its statistics, have been discussed earlier in this journal [1]. As indicated in [1], the primes were computed on an IBM 1620. They are very nicely printed, in an elegant format, 500 to the page. Anyone familiar with programming would note at once the great care that must have been taken here to produce such a format.

The range $10^{12}(1)10^{12} + 10^4$ was checked against Kraitchik's 335 primes in [2], with perfect agreement. (Kraitchik's tables are seldom *that* accurate.) For $n = 9$, a successful spot check was made against Beeger's manuscript table [3].

D. S.

1. M. F. JONES, M. LAL & W. J. BLUNDON, "Statistics on certain large primes," *Math. Comp.*, v. 21, 1967, pp. 103–107.
2. M. KRAITCHIK, "Les grand nombres premiers," *Sphinx*, v. 8, 1938, pp. 82–86.
3. N. G. W. H. BEEGER, *Tafel van den kleinsten factor de getallen van* 999 999 000-1 000 119 120, *etc.*, deposited in the UMT file and reviewed in UMT 68, *Math. Comp.*, v. 20, 1966, p. 456.

21[F, G].—L. D. BAUMERT & H. FREDRICKSEN, *The Cyclotomic Numbers of Order Eighteen*, Jet Propulsion Laboratory, California Institute of Technology, 18 computer sheets deposited in the UMT file.

This table presents the cyclotomic numbers of order eighteen. The derivation and computation of these formulas are described adequately in Section 4 of the authors' paper which appears elsewhere in this journal [1].

The identities (2.2) in the paper enable one to group the 324 cyclotomic constants (h,k), $0 \leqq h, k \leqq 17$, into 64 sets. There is a formula for each set, depending on ind 2 (mod 9) and ind 3 (mod 6). Thus there are 54 cases, each with 64 formulas. The table consists of the formulas for sixteen cases; the other formulas can be derived from these formulas. Table 5 of the paper is one of the cases given in the table.

It is interesting to note that not all the formulas in a given case are different. For example, in Table 5, (0,3) = (0,6), (1,2) = (1,8) = (2,7) = (2,16), (1,5) = (1,17) = (2,1) = (5,1), and (1,14) = (2,4) = (4,2) = (4,5).

JOSEPH B. MUSKAT

University of Pittsburgh
Pittsburgh, Pennsylvania

1. L. D. BAUMERT & H. FREDRICKSEN, "Cyclotomic numbers of order eighteen with applications to difference sets," *Math. Comp.*, v. 21, 1967, pp. 204–219.