A Formula for the Approximation of Definite Integrals of the Normal Distribution Function

A simple expression has been found which may be used to yield approximate numerical values for definite integrals of the normal distribution function. The expression is as follows.

$$\int_x^\infty e^{-t^2/2}dt = \frac{e^{-x^2/2}}{X + .8e^{-.4x}} ; X \geq 0.$$

This approximation is satisfactory for certain applications over a broad range of values for the finite integration limit, as may be judged from the table below.

X	$\int_x^\infty \exp(-t^2/2)dt$	$\frac{\exp(-X^2/2)}{X + .8\exp(-.4X)}$	Difference	% Difference
0	1.253	1.250	−.003	− .2
.2	1.055	1.044	−.011	−1.0
.5	.773	.764	−.009	−1.2
1.0	.398	.395	−.003	− .8
1.5	.1675	.1674	−.0001	0
2.0	.0570	.0573	+.0003	+ .5
2.5	.0156	.0157	.0001	.6
3.0	.00338	.00343	.00005	1.5
3.5	.00058 3	.00059 2	.00000 9	1.5
4.0	.00007 95	.00008 06	.00000 11	1.4
5.0	.00000 0718	.00000 0730	.00000 0012	1.7

Some of the properties of Mill's ratio, the function here approximated by $X + .8\ e^{-.4x}$, have been recently described by Sampford [1].

ROGER G. HART

University of California
Berkeley, California

1. M. R. SAMPFORD, "Some inequalities on Mill's ratio and related functions," *Annals Math. Stat.*, 1953, v. 24, p. 130.

Some Factorizations of Numbers of the Form $2^n \pm 1$

The author has prepared a factorization routine for use on an IBM 701 computer. In this note, we describe the routine briefly, and report on some results obtained during the period February–April 1957 on the computer at the University of California, Berkeley.

In the basic routine, an arithmetic progression is given in which divisors of a number N are to be sought. Only single word divisors, that is, divisors less than 2^{35}, are considered, but the number N may be many words. After deleting those terms of the progression which are multiples of 2, 3, 5, 7, or 11, the remaining terms up to $N^{\frac{1}{2}}$, or up to a prescribed bound, are tried as divisors of N. In order to delete the multiples of 2, 3, 5, 7, and 11 efficiently, use is made of the fact that the differences of the remaining terms of the progression repeat with a period $\phi(2\cdot3\cdot5\cdot7\cdot11) = 480$. The 480 required differences are computed in advance, and used repeatedly.

There are variations of the routine which make it possible to use the fact that ± 2 is a quadratic residue mod N, and which expedite handling very large numbers, several related numbers, or sequences of numbers. For example, using the last of these, it was easy to find that the primes nearest to 2^{35} on either side are $2^{35} - 31$ and $2^{35} + 53$.

The routine can theoretically factor any number $N < 2^{70}$. But if nothing is known about the form of the factors, the maximum possible time (which increases roughly with $N^{\frac{1}{2}}$) would be prohibitive for the larger values of N. However, any number $N < 2^{36}$ can be factored in less than a minute, and any number $N < 2^{48}$ can be factored in less than an hour.

The remainders from the various divisions are summed and the sum is recorded at intervals. If a re-run is made and the remainder sums agree, this indicates that no machine errors have occurred.

The first work undertaken was a search for factors of the early Fermat numbers, supplementing work of a somewhat different character done previously [4], and extending the results of Selfridge [5]. It is known that any prime factor p of the Fermat number $F_m = 2^{2^m} + 1$ must satisfy the congruence $p \equiv 1 \pmod{2^{m+2}}$ if $m > 1$. All possible divisors $p < 2^{32}$ of any Fermat number were tried, and also all possible divisors with $p < 2^{35}$ and $p \equiv 1 \pmod{2^{15}}$. The total running time was about five hours. No new divisors were found. The computation was checked by a re-run. Thus we can say definitely that there are no factors in this range beyond those previously found, all of which have been known for more than thirty years, except the two found by Selfridge [5]. In particular, F_7 has no factor $p < 2^{32}$; since it is composite, it must be the product of either 2 or 3 prime factors. Also, we can say that F_{13}, whose character is unknown, has no factor less than 2^{35}. (After the computation described above was finished, I learned that some unpublished work of Selfridge, extending [5], had covered most of the same range. However, the work had not all been checked, and there were some gaps. Selfridge also tried some divisors between 2^{35} and 2^{36}; I was unable to check this part of his work.)

Another project was the study of the Mersenne numbers $2^n - 1$, where n itself is a Mersenne prime, that is, $n = 2^m - 1$, where m and n are prime. According to a well-known conjecture, any such number is prime. An extremely long computation of D. J. Wheeler (see [3], page 844) indicated that $2^{8191} - 1$ (corresponding to $m = 13$) is composite, and the conjecture therefore false. However, no factor of this number was found. It was decided to make a search for factors $p < 2^{35}$ of such numbers. The factors must satisfy $p \equiv 1 \pmod{2n}$ and $p \equiv 1, 7 \pmod 8$. The only values of m in question are $m = 13, 17, 19, 31$. Two factors were found, namely

$$1768(2^{17} - 1) + 1 \mid 2^{2^{17}-1} - 1$$

and

$$120(2^{19} - 1) + 1 \mid 2^{2^{19}-1} - 1.$$

These results can easily be verified using a desk calculator. Thus the conjecture is certainly false. The time required for the test was about an hour and a half. The computation was checked by a re-run. Thus we are sure that there are no other factors in the range considered. In particular, $2^{8191} - 1$ has no factor less than 2^{35}.

Finally, factorization of various numbers of the forms $2^n - 1$ and $2^n + 1$, which had not previously been factored, was attempted. (A table of the factors, known in 1925, of numbers of these forms with $n < 500$ appears in Cunningham and Woodall [1], and a number of additions to this table were given by Lehmer [2]. A few other factorizations have appeared elsewhere.) A somewhat arbitrary selection of cases was made, consisting of the following:

(a) $2^n - 1$ with n odd. The primitive factors satisfy $p \equiv 1 \pmod{2n}$ and $p \equiv 1, 7 \pmod 8$. The cases tried were $n = 95, 97, 101, 103, 109, 119, 121, 125, 129, 131, 133, 137, 139, 149, 157$.

(b) $2^n + 1$ with n odd. The primitive factors satisfy $p \equiv 1 \pmod{2n}$ and $p \equiv 1, 3 \pmod 8$. The cases tried were $n = 71, 101, 103, 107, 109, 113, 115$.

(c) $2^n + 1$ with $n \equiv 0 \pmod 4$. The primitive factors satisfy $p \equiv 1 \pmod{4n}$. The cases tried were $n = 104, 112, 116, 124$. (For the cases $n = 128, 256$, etc., see the discussion of Fermat numbers above.)

(d) $2^n + 1$ with $n \equiv 2 \pmod 4$. The primitive factors satisfy $p \equiv 1 \pmod{2n}$. The identity

$$2^{4i+2} + 1 = (2^{2i+1} - 2^{i+1} + 1)(2^{2i+1} + 2^{i+1} + 1)$$

shows that in this case the factorization of $2^n + 1$ is reduced to factorization of numbers of the form $2^{2i+1} \pm 2^{i+1} + 1$. Four numbers of this type were tried, namely $2^{67} - 2^{34} + 1$, $2^{67} + 2^{34} + 1$, $2^{71} - 2^{36} + 1$, and $2^{73} - 2^{37} + 1$, of which the first two are the factors of $2^{134} + 1$, and the others are factors of $2^{142} + 1$ and $2^{146} + 1$.

In each of the thirty cases, all possible divisors less than 2^{30} were tried. The time for each run was about half an hour, except that when factors were found, this was reduced, in some cases very sharply. The following factorizations were found:

$$2^{67} - 2^{34} + 1 = 5 \cdot 269 \cdot 42\,875\,177 \cdot 2\,559\,066\,073,$$
$$2^{67} + 2^{34} + 1 = 15\,152\,453 \cdot 9\,739\,278\,030\,221,$$
$$2^{71} + 1 = 3 \cdot 56\,409\,643 \cdot 13\,952\,598\,148\,481,$$
$$2^{95} - 1 = 31 \cdot 191 \cdot 524\,287 \cdot 420\,778\,751 \cdot 30\,327\,152\,671,$$
$$2^{109} - 1 = 745\,988\,807 \cdot X,$$
$$2^{109} + 1 = 3 \cdot 104\,124\,649 \cdot Y,$$
$$2^{112} + 1 = 449 \cdot 2689 \cdot 65\,537 \cdot 183\,076\,097 \cdot 358\,429\,848\,460\,993,$$
$$2^{113} + 1 = 3 \cdot 227 \cdot 48\,817 \cdot 636\,190\,001 \cdot 491\,003\,369\,344\,660\,409,$$
$$2^{157} - 1 = 852\,133\,201 \cdot Z.$$

All the factors written out are less than 2^{60}, and hence are shown to be prime by the routine. This fact was checked by an additional run. The three factors X, Y, Z exceed 2^{60}, and are of an unknown character.

Thus we have completely factored the numbers $2^{71} + 1$, $2^{95} - 1$, $2^{112} + 1$, $2^{113} + 1$, and $2^{134} + 1$, the last factorization being obtained by multiplying together the first two of the above equations. (The entry for $2^{134} + 1$ in Cunningham and Woodall [1] erroneously gives the product of the two largest prime factors of $2^{67} - 2^{34} + 1$ as a prime.) We have also found factors of two Mersenne numbers, $2^{109} - 1$ and $2^{157} - 1$, for which no factor was previously known, and a factor of $(2^{109} + 1)/3$.

No factors other than those shown above were found in any of the cases tried, except for the algebraic factors and the factors less than 300,000 which appear in Cunningham and Woodall [1]. Check runs were not made, but it appears to be quite unlikely that any factor less than 2^{30} was missed.

Appendix. At the suggestion of the referee, two lists are included which show the progress which has been made in factoring numbers of the form $2^n \pm 1$. These lists have been prepared with the help of D. H. Lehmer and J. L. Selfridge. First we have a list of all the cases we could find in which complete factorizations have been claimed, where for $2^n - 1$ only odd values of n are considered.

$2^n - 1$: n = 1–99, 105, 107, 111, 113, 115, 117, 123, 127, 129, 135, 151, 521, 607, 1279, 2203, 2281

$2^n + 1$: n = 0–102, 105, 106, 108, 110, 111, 112, 113, 114, 118, 120, 122, 123, 126, 130, 134, 135, 138, 146*, 148, 150, 154, 162, 170, 174, 182, 186*, 190*, 198, 210, 234*, 270

Some of these were not known to the author at the time the work described above was carried out. It should be mentioned that in several cases there is doubt that the factorizations are in fact complete; this is true, in particular, in the cases marked with an asterisk. Notice that M. Kraitchik [6] had already given a supposedly complete factorization of $2^{95} - 1$, but that we found above that a further decomposition of one of his factors is possible.

The second list concerns the "original Mersenne numbers" (that is, numbers of the form $2^p - 1$ where p is prime and $p \leq 257$), and brings up to date a similar list by R. C. Archibald in *MTAC* [7].

p	Character of $2^p - 1$
2,3,5,7,13,17,19,31,61,89,107,127	Prime
(All other $p < 100$),113,151	Composite and completely factored
163,173,179,181,223,233,239,251	Two or more prime factors known
109,131,157,167,191,197,211,229	Only one prime factor known
101,103,137,139,149,193,199,227,241,257	Composite but no factor known

RAPHAEL M. ROBINSON

University of California
Berkeley, California

The operation of this computer is supported in part by the National Science Foundation.

1. A. J. C. CUNNINGHAM & H. J. WOODALL, *Factorisation of* $y^n \mp 1$, $y = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers* (n), Francis Hodgson, London, 1925.
2. D. H. LEHMER, "On the factors of $2^n \pm 1$," Amer. Math. Soc., *Bull.*, v. 53, 1947, p. 164–167.
3. RAPHAEL M. ROBINSON, "Mersenne and Fermat numbers," Amer. Math. Soc., *Proc.*, v. 5, 1954, p. 842–846.
4. RAPHAEL M. ROBINSON, "Factors of Fermat numbers," *MTAC*, v. 11, 1957, p. 21–22.
5. J. L. SELFRIDGE, "Factors of Fermat numbers," *MTAC*, v. 7, 1953, p. 274–275.
6. M. KRAITCHIK, *Introduction à la Théorie des Nombres*, Gauthier-Villars, Paris, 1952. p. 39.
7. R. C. ARCHIBALD, "Mersenne numbers," *MTAC*, v. 3, Note **98**, 1949, p. 398.

On the Solution of "Jury" Problems with Many Degrees of Freedom

1. Introduction. In a recent numerical investigation using the Differential Analyser, it was found necessary to solve differential equations of up to the eighth order with two-point boundary conditions, the so-called "Jury" problem. Now,