Experiments on the Lattice Problem of Gauss

By H. B. Keller and J. R. Swenson

1. Introduction. One of the classical unsolved problems in analytic number theory is concerned with counting the number of lattice points that lie in a circle. If $A(r)$ is the number of lattice points in $\mathfrak{D}(r) \equiv \{(x, y) \mid x^2 + y^2 \leqq r^2\}$ then the problem is to find the least value of θ such that

$$E(r) \equiv A(r) - \pi r^2 = O(r^\theta). \tag{1}$$

It has been shown by Loo-Keng Hua [1] that (1) holds for $\theta = \frac{13}{20}$ and by G. H. Hardy [2] that it does not hold for $\theta = \frac{1}{2}$. A conjecture, frequently attributed to Hardy, asserts that (1) is valid for all $\theta > \frac{1}{2}$.

The availability of high-speed digital computers suggests actually evaluating the deviation $E(r)$ for "large" values of r in the hope of determining some further evidence of its behavior. At least three independent efforts in this direction have recently been made (as far as we know in the order: [3], [4], and the present paper). It is apparent from our results that the first effort [3] employed insufficiently large radii ($r < 2000$) and that the second effort [4] is incorrect for $r \geqq 3000$. The present calculations, which extend to $r = 259{,}750$, *suggest* that (1) should be valid for some $\theta < \frac{13}{20}$. However, it also seems clear that the computations which would be required to approximate any such lower estimate are impractical on an IBM 7090 or even on any other currently existing computers.

A formula for computing $A(r)$ is presented in Section 2. An efficient algorithm for evaluating this formula on a 7090 or similar machine and the corresponding program are described in Section 3. The numerical results are discussed in Section 4.

2. Formulation. For any positive real number Z, let $[Z]$ denote the integer part of Z. For any radius r, we define the integers

$$K(r) \equiv [r/\sqrt{2}], \qquad L(r) \equiv [r]. \tag{2}$$

For all integers i in $K(r) + 1 \leqq i \leqq L(r)$ we define

$$y_i(r) \equiv \sqrt{r^2 - i^2}, \quad Y_i(r) = [y_i(r)]. \tag{3}$$

If $Q(r)$ is the number of lattice points in $\{(x, y) \mid x > 0, y > 0, x^2 + y^2 \leqq r^2\}$ then (see Figure 1)

$$Q(r) = K^2(r) + 2 \sum_{i=K(r)+1}^{L(r)} Y_i(r). \tag{4}$$

The number of lattice points, $A(r)$, in $\mathfrak{D}(r)$ can now be written as

$$A(r) = 4Q(r) + 4L(r) + 1. \tag{5}$$

The computing problem lies in the evaluation of $\sum Y_i$. It is relatively time

Received September 18, 1962. The work presented in this paper is supported by the AEC Computing and Applied Mathematics Center, Courant Institute of Mathematical Sciences, New York University, under contract with the U. S. Atomic Energy Commission.

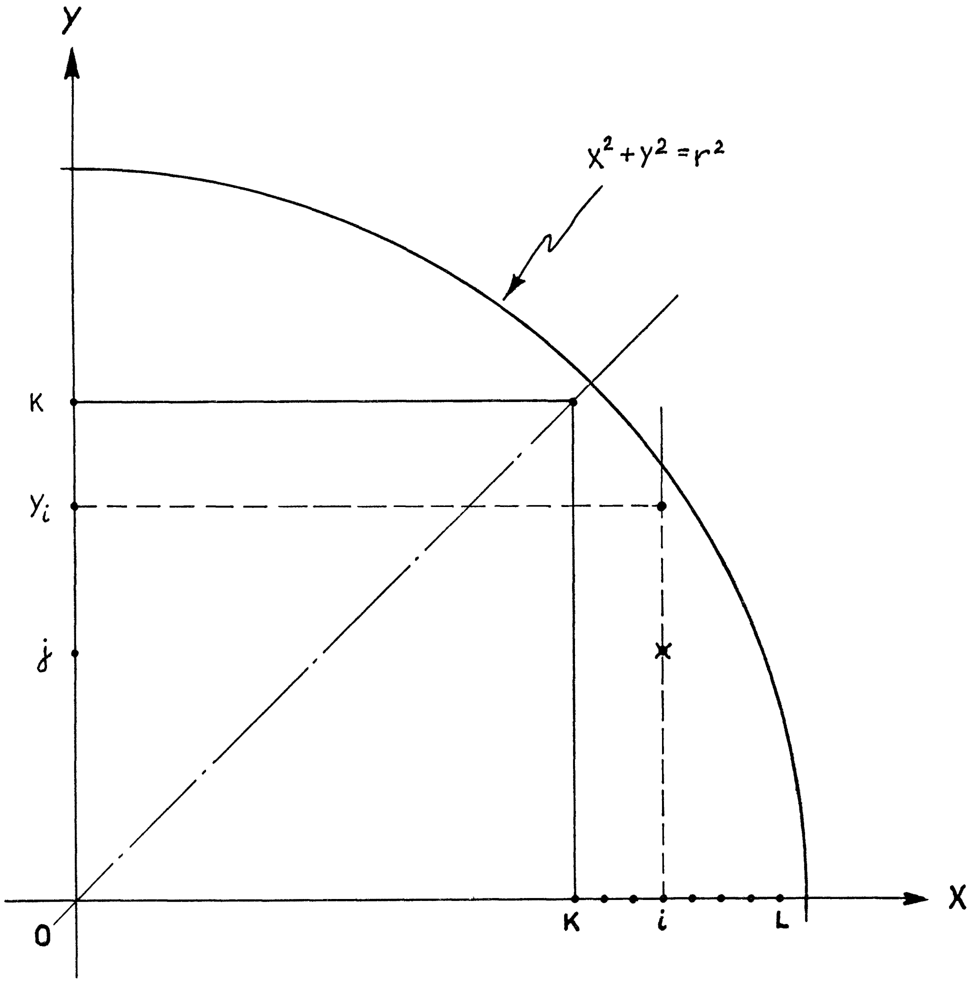

FIG. 1. Diagram to explain the counting algorithm.

consuming to determine square roots on most existing computers and the accuracy required here is to within the integral part of y_i. There is in fact no serious problem for "small" values of r (say, $r < 2^{13} \doteq 8.2 \times 10^3$) either with regard to time or accuracy. However, if, as we desire, r^2 is of the order of magnitude of the machine fixed point word capacity ($2^{36} - 1$ on an IBM 7090) then efficiency and extreme accuracy are crucial. We shall describe a counting procedure to evaluate $\sum Y_i$ which employs no square root computations and is more efficient on a 7090 than any other procedure known to us. This procedure may not be the most efficient on a machine with a very fast fixed point square root instruction.

3. Counting Algorithm and Machine Program. Let $\mathfrak{J}(r)$ denote the set

$$\mathfrak{J}(r) \equiv \{(x, y) \mid y > 0; \quad K + 1 \leqq x \leqq L; \quad (x, y) \in \mathfrak{D}(r)\}.$$

Then $\sum Y_i$ is just the number of lattice points contained in $\mathfrak{J}(r)$. If the lattice point $(i, j) \in \mathfrak{J}(r)$ and the point $(i, j + 1) \notin \mathfrak{J}(r)$ then $Y_i(r) = j$. Furthermore, for such a lattice point (i, j), if $i > K + 1$ then, as a simple geometric or algebraic argument shows, $(i - 1, j + 1) \in \mathfrak{J}(r)$. Thus, roughly speaking, we can count the number of lattice points in $\mathfrak{J}(r)$ by tracing out a piecewise rectangular boundary which is just interior to the circular boundary of $\mathfrak{J}(r)$. This is done by starting at the point $(i, j) = (L, 0)$ and with fixed i increasing j until $R_{i,j}^2 \equiv i^2 + j^2 > r^2$. When the first such j is obtained and $Y_i(r) = (j - 1)$ is accumulated in $\sum Y_i$ then reduce i by unity. Continue this procedure until $i = K + 1$. A great saving in computing time is effected by noting that

$$R_{i,j+1}^2 = R_{i,j}^2 + 2j + 1, \qquad R_{i-1,j}^2 = R_{i,j}^2 - 2i + 1.$$

Thus, on a binary machine, given $R_{L,0}^2$, no multiplications are required to evaluate recursively the $R_{i,j}^2$.

The algorithm for computing $A(r)$ based on the above observations is described on the flow diagram, Figure 2. This algorithm was coded in FAP for the 7090. Using fixed-point machine operations the closed loop $1.0 \to 1.1 \to 1.2 \to 1.0$ takes 19 machine cycles while the partial loop $2.0 \to 2.1 \to 2.2 \to 1.2 \to 1.0$ requires 33 cycles. The first loop must be used for each j in $0 < j \leqq K(r)$ or essentially $[r/\sqrt{2}] \doteq 0.7r$ times. The partial loop is used for each i in $K + 1 \leqq i \leqq L$ or essentially $[r] - [r/\sqrt{2}] \doteq 0.3r$ times. Since a 7090 machine cycle is about 2.18 microseconds, this code requires approximately $51r \times 10^{-6}$ seconds in order to compute $A(r)$.

Using the 7090 fixed-point arithmetic operations a code based on the flow diagram of Figure 2 can compute $A(r)$ for all $r < \sqrt{2} \times 2^{17} \doteq 1.8 \times 10^5$. By employing the sign bit to record arithmetic data the range of r is easily extended to $r < 2^{18} \doteq 2.6 \times 10^5$. In order to do this the ordinary arithmetic machine operations must be modified. The closed loop then takes 22 cycles and the partial loop only 32 cycles. The total time to compute $A(r)$ then becomes $55r \times 10^{-6}$ sec. The time estimates given here were found to be extremely accurate.

For values of r such that $r^2 \doteq 2^{35}$ the arithmetic in boxes 0.1 and 3.0 of the flow diagram required special higher precision techniques which do not essentially alter the above time estimates. In fact, by using certain tricks only $(Q + L)$ is required in the 7090 in order to calculate E and a special 1401 output routine can be used to transform $(Q + L)$ in octal to $A(r)$ in decimal.

It is a simple matter to employ the above procedures in order to count the number of lattice points in a sphere, say of radius ρ. We need only compute $A(r_k)$ where $r_k = \sqrt{\rho^2 - k^2}$ for $k = 0, 1, \cdots, [\rho]$. Using the previous estimate this requires at least $55\left(\frac{\pi}{4}\right)\rho^2 \times 10^{-6}$ sec. for the total count.

4. Numerical Results. It is an elementary fact that $A(r)$ is a piecewise constant function with discontinuities only at values of r for which r^2 can be written as the sum of the squares of two integers. Thus, for any integer m there are only a finite number of distinct values of $A(r)$ for all $r \leqq m$. However, it is quite impractical, for large m, to compute all of these values (e.g., for $m = 10^5$ we would require the order of 10^{10} computations). Hence, we content ourselves with some uniform samplings in r, bearing in mind the defects in any such experimental approach.

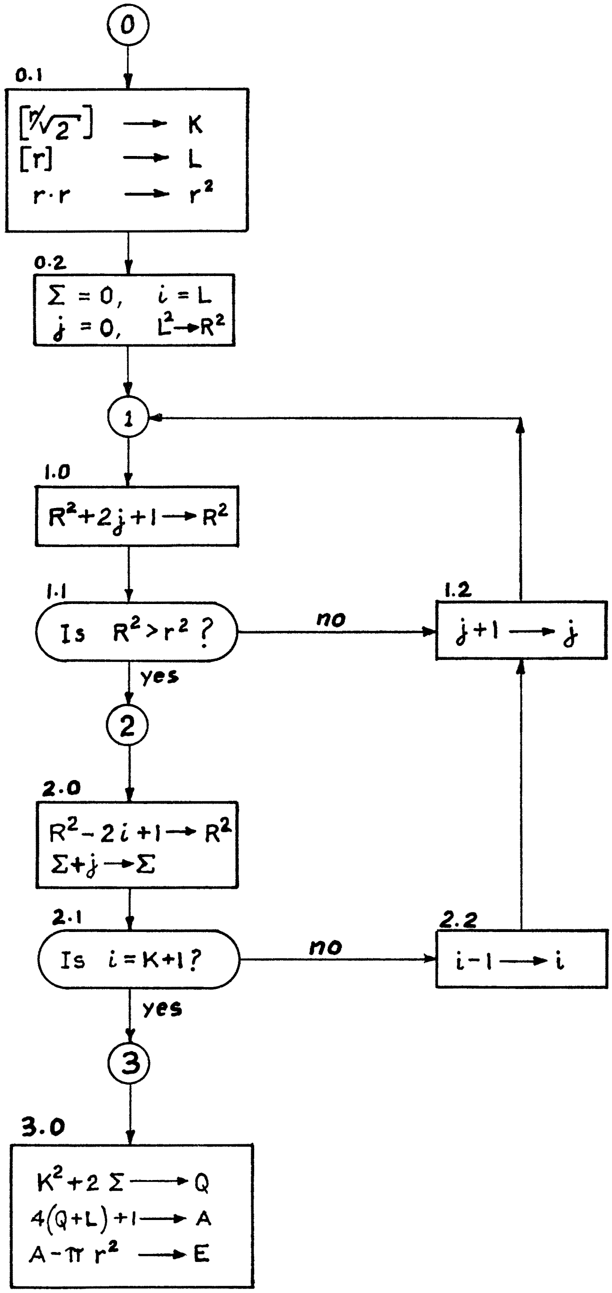

FIG. 2. Flow diagram for lattice point counting algorithm.

TABLE 1

r	$A(r)$	$E(r)$	$\ln \mid E(r) \mid / \ln r$	$E(r)/r^{1/2}$
250000	196349539105	−.174436 04	.600532	−.348872 01
250250	196742432789	−.349160 04	.656313	−.697971 01
250500	197135722817	−.159392 04	.593180	−.318466 01
250750	197529403589	−.165132 04	.595978	−.329770 01
251000	197923477597	−.117181 04	.568341	−.233894 01
251250	198317943985	−.101137 04	.556454	−.201771 01
251500	198712801597	−.232602 04	.623385	−.463815 01
251750	199108054785	−.763754 03	.533784	−.152219 01
252000	199503696777	−.309656 04	.646291	−.616850 01
252250	199899736189	−.708459 03	.527657	−.141058 01
252500	200296165009	−.161143 04	.593679	−.320687 01
252750	200692987501	−.154149 04	.590065	−.306616 01
253000	201090202865	−.129862 04	.576238	−.258181 01
253250	201487810273	−.171084 04	.598349	−.339967 01
253500	201885812629	.125849 03	.388575	.249955 00
253750	202284203409	−.231253 04	.622471	−.459076 01
254000	202682990469	−.116999 04	.567674	−.232149 01
254250	203082168909	−.134654 04	.578921	−.267048 01
254500	203481740881	−.690174 03	.525179	−.136809 01
254750	203881703117	−.246888 04	.627530	−.489151 01
255000	204282060473	−.182667 04	.603280	−.361735 01
255250	204682810189	−.152354 04	.588658	−.301560 01
255500	205083952957	−.867505 03	.543380	−.171623 01
255750	205485487441	−.119454 04	.569028	−.236207 01
256000	205887414661	−.148466 04	.586443	−.293431 01
256250	206289735777	−.577861 03	.510629	−.114154 01
256500	206692447577	−.168614 04	.596569	−.332928 01
256750	207095553973	−.897506 03	.545897	−.177126 01
257000	207499050769	−.240795 04	.625081	−.474986 01
250000.000000	196349539105	−.174436 04	.600532	−.348872 01
.015625	196349565329	−.640554 02	.334675	−.128110 00
.031250	196349589697	−.239750 03	.440864	−.479500 00
.046875	196349614641	.160553 03	.408603	.321106 00
.062500	196349639409	.384855 03	.478941	.769710 00
.078125	196349664377	.809155 03	.538729	.161831 01
.093750	196349688785	.673454 03	.523960	.134690 01
.109375	196349713721	.106575 04	.560891	.213150 01
.125000	196349737825	.626047 03	.518087	.125209 01
.140625	196349761401	−.341657 03	.469362	−.683315 00
.156250	196349787081	.794635 03	.537273	.158926 01
.171875	196349810921	.909264 02	.362858	.181852 00
.187500	196349835377	.321620 01	.093988	.643239−02
.203125	196349860537	.619504 03	.517242	.123900 01
.218750	196349885521	.105979 04	.560439	.211958 01
.234375	196349910209	.120407 04	.570709	.240815 01
.250000	196349934809	.126035 04	.574384	.252071 01
.265625	196349959225	.113264 04	.565788	.226528 01
.281250	196349983153	.516922 03	.502677	.103384 01
.296875	196350007041	−.138798 03	.396889	−.277596 00
.312500	196350031185	−.538520 03	.505971	−.107704 01

TABLE 1—*Continued*

r	$A(r)$	$E(r)$	$\ln \| E(r) \| / \ln r$	$E(r)/r^{1/2}$
250000.328125	196350055801	−.466245 03	.494376	−.932489 00
.343750	196350080809	−.197063 01	.054578	−.394127−02
.359375	196350105305	−.496977 02	.314256	−.993954−01
.375000	196350129513	−.385426 03	.479060	−.770852 00
.390625	196350153921	−.521156 03	.503334	−.104231 01
.406250	196350178761	−.224888 03	.435715	−.449776 00
.421875	196350202577	−.952621 03	.551862	−.190524 01
.437500	196350227629	−.444356 03	.490507	−.888711 00
.453125	196350252989	.371907 03	.476188	.743813 00
.468750	196350277597	.436169 03	.489011	.872338 00
.484375	196350302053	.348430 03	.470941	.696859 00
.500000	196350326845	.596689 03	.514223	.119337 01

TABLE 2

r	$A(r)$	$E(r)$	$\ln \| E(r) \| / \ln r$	$E(r)/r^{1/2}$
1000	3141549	−.436535 02	.546673	−.138044 01
2000	12566345	−.256143 02	.426680	−.572754 00
3000	28274197	−.136882 03	.614401	−.249911 01
4000	50265329	−.153457 03	.606871	−.242637 01
5000	78539677	−.139339 03	.579641	−.197056 01
6000	113097185	−.150529 03	.576372	−.194332 01
7000	153937805	−.235025 03	.616659	−.280909 01
8000	201061681	−.248829 03	.613847	−.278200 01
9000	254468477	−.527940 03	.688522	−.556498 01
10000	314159053	−.212358 03	.581767	−.212358 01
20000	1256636857	−.204435 03	.537210	−.144558 01
30000	2827432965	−.423230 03	.586666	−.244352 01
40000	5026547529	−.716743 03	.620453	−.358371 01
50000	7853981045	−.588974 03	.589511	−.263397 01
60000	11309732881	−.671923 03	.591718	−.274311 01
70000	15393802989	−.101358 04	.620392	−.383100 01
80000	20106192121	−.861974 03	.598702	−.304754 01
90000	25446899381	−.111307 04	.614932	−.371025 01
100000	31415925457	−.107889 04	.606596	−.341177 01
125000	49087384401	−.811340 03	.570777	−.229481 01
150000	70685833345	−.136077 04	.605434	−.351349 01
175000	96211274253	−.763187 03	.549801	−.182436 01
200000	125663704421	−.172259 04	.610481	−.385183 01
225000	159043126541	−.154698 04	.595922	−.326132 01
250000	196349539105	−.174436 04	.600532	−.348872 01

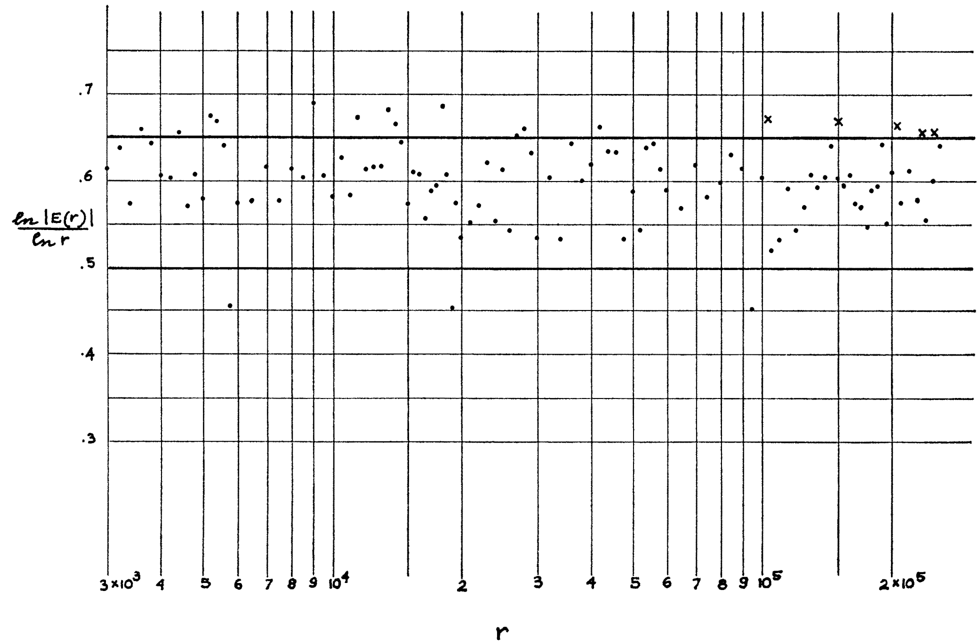

FIG. 3. Distribution of some computed values of $\ln \mid E(r) \mid / \ln r$.

Computations were made for each value of r in the following sets:

a) $r = 1(1)10{,}000$
b) $r = 10{,}000(250)100{,}000$
c) $r = 100{,}000(10{,}000)150{,}000$
d) $r = 150{,}000(250)259{,}750$
e) $r = 100{,}000(1)100{,}099$
f) $r = 150{,}000(1)150{,}099$
g) $r = 200{,}000(1)200{,}099$
h) $r = 250{,}000(1)250{,}099$
i) $r = 100{,}000(\frac{1}{64})100{,}002$
j) $r = 150{,}000(\frac{1}{64})150{,}002$
k) $r = 200{,}000(\frac{1}{64})200{,}002$
l) $r = 250{,}000(\frac{1}{64})250{,}002$.

The quantities computed were: $E(r)$, $E(r)/r^{1/2}$, $\ln \mid E(r) \mid / \ln r$, $\ln \mid E(r)/r^{1/2} \mid / \ln r$, and $E(r)/(r \ln r)^{1/2}$. The values of $A(r)$ and $E(r)$ were compared with all the values reported in [4]. Exact agreement for $A(r)$ and agreement to at least five digits for $E(r)$ was observed for $r = 1(1)1{,}000$ and $r = 2{,}000$. However, the remaining 27 values of $A(r)$ for r in $3{,}000 \leqq r \leqq 200{,}000$ reported in [4] did not agree with our values. Independent check calculations were made for $r = 3000, = 4000, = 5000$ by using equations (2)–(5). The square roots were evaluated by means of a Newton-Raphson subroutine and exact agreement for $A(r)$ with those computed by the method of Section 3 was obtained. Thus, we conclude that the results in [4] are incorrect for $r \geqq 3000$. We also believe that our calculations are correct for all reported values of r. Since our method depends upon r only through the quantities r^2, $K(r)$, and $L(r)$ and then only integer arithmetic is performed on numbers which fit into a machine word, it seems quite likely that our claim is justified.

Table 1 lists a small sample of the numerical results from sets d) and l) and Table 2 lists sample results from sets a)–d). The numbers in the columns headed $E(r)$ and $E(r)/r^{1/2}$ are in floating decimal notation with signed exponents and those in the $A(r)$ column are integers. Positive values of $E(r)$ were observed to be extremely rare for integer values of r. For example, in the approximately 890 cases contained in sets c)–h) only one such value was found, namely, $r = 253{,}500$. However, in the sets i)–l) the sign distribution of $E(r)$ was about uniform or perhaps even slightly biased in favor of positive values.

In Figure 3 values of $\ln | E(r) |/\ln r$ vs. r are plotted on a semi-log scale. The dots have the abscissae: $r = 3000(200)6000(500)2 \times 10^4(10^3)3 \times 10^4(2 \times 10^3)6 \times 10^4(5 \times 10^3)2 \times 10^5(10^4)2.6 \times 10^5$. The horizontal lines in Figure 3 of ordinate 0.5 and 0.65 represent respectively Hardy's lower bound and Hua's upper bound on the order θ in equation (1). The points marked with an X in Figure 3 were plotted to indicate that not all values computed for $r > 10^5$ were below Hua's bound. Many such values of $\ln | E(r) |/\ln r > 0.65$ were obtained in the sets i)–l) at non-integral values of r. The largest such value observed in $10^5 \leqq r \leqq 259{,}750$ was 0.672 at $r = 103{,}000$.

The results summarized in Figure 3 clearly suggest that (1) is valid for $\theta = 0.70$ or even perhaps for $\theta = 0.68$. But since it is known to be valid for all $\theta \geqq 0.65$ no useful quantitative estimates are obtained. However, an extrapolation of these data does suggest that a smaller order should suffice and that computations for larger values of r could indicate this. For example, to obtain a significant improvement, say $\theta \leqq 0.60$, a crude extrapolation implies a radius of about 10^8. Unfortunately, calculations for such radii, employing a partial-double-precision version of our present method on a 7090, would require at least two hours per case. Hence, they are impractical for the number of cases required to show a reasonable trend in the data. Furthermore, serious problems arise in attempting to insure the accuracy of such computations.

It was also observed that for all of our calculations $| E(r) |/r^{1/2} < 7$. Since by Hardy's result this ratio is unbounded we must conclude that either our sampling is too crudely spaced or more likely that our range in r is relatively small.

A.E.C. Computing and Applied Mathematics Center
Courant Institute of Mathematical Sciences
New York University

1. L. K. Hua, "The lattice-points in a circle," *Quart. J. Math., Oxford Ser.*, v. 13, 1942, p. 18–29.
2. G. H. Hardy, "On the expression of a number as the sum of two squares," *Quart. J. Math.* v. 46, 1915, p. 263–283, and "On Dirichlet's divisor problem," *Proc. London Math. Soc.*, Ser. 2, v. 15, 1916, p. 1–25.
3. W. Fraser & C. C. Gotlieb, "A calculation of the number of lattice points in the circle and sphere," *Math. Comp.*, v. 16, 1962, p. 282–290.
4. H. L. Mitchell, III, *Numerical Experiments on the Number of Lattice Points in the Circle*, Technical Report No. 17, Appl. Math. and Stat. Labs., Stanford University, Stanford, California.