ON THE LOCATION OF GAUSS SUMS

Thus we have half of seven $8 \times 8$ squares. In projective terms we have a total of 45 lines with 9 points on a line which are consistent with themselves but which cannot be completed to the 73 lines of a projective plane.

Marshall Hall, Jr.

J. Dean Swift

Robert J. Walker

Ohio State University
Columbus, Ohio

University of California
Los Angeles, California

Cornell University
Ithaca, New York

This research was supported by the National Science Foundation and the Office of Naval Research.


On the Location of Gauss Sums

We shall understand by a generalized Gauss sum of order $k$ the sum

$$S_k = \sum_{m=0}^{p-1} \exp \left( \frac{2\pi im^k}{p} \right), \quad (p = kf + 1, \text{ a prime}).$$

This sum can be thought of as the principal root $z_0$ of the reduced period equation of degree $k$ for the so-called $f$-nomial periods, $z_i = k\eta_i + 1$, where, as usual,

$$\eta_i = \sum_{j=0}^{k-1} \exp \left( \frac{2\pi ig^{b+i}}{p} \right) \quad (i = 0, 1, \ldots, k - 1).$$

Since the remaining $k - 1$ roots of the period equation depend on the primitive root $g$, the singling out of one root $z_0$ as the principal root is justifiable.

For $k = 2$, it is well known that $[1]

$$S_2 = \begin{cases} \sqrt{p} & \text{if } p = 4n + 1 \\ i\sqrt{p} & \text{if } p = 4n - 1. \end{cases}$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
In general it is known that

\[ - (k - 1)\sqrt{p} \leq S_k \leq (k - 1)\sqrt{p}. \]

For \( k = 3 \), and \( 4p = L^2 + 27M^2 \), the three roots of the reduced trinomial cubic

\[ F(z) = z^3 - 3pz - pL = 0 \quad (L \equiv 1 \pmod{3}) \]

lie in the intervals

\[ (-2\sqrt{p}, -\sqrt{p}), \quad (-\sqrt{p}, \sqrt{p}), \quad (\sqrt{p}, 2\sqrt{p}). \]

Kummer [2] noticed that the principal root \( z_0 \) lies in these intervals with frequencies approximately of 1 to 2 to 3 for primes less than 500 and conjectured that these ratios hold in general. Further calculations by Goldstine and von Neumann [3] for primes up to 10,000 exhibited ratios of the order of 2 to 3 to 4. They conclude that “these results would seem to indicate a significant departure from the conjectured densities and a trend toward randomness.” On the other hand a case has been made by G. Beyer [4] that these are indeed the true ratios since \( 2 + 3 + 4 = 3^2 \), and since these densities hold for composite as well as prime moduli. It therefore seemed of interest to continue this investigation on the SWAC at the Numerical Analysis Research of the University of California at Los Angeles. The results of Goldstine and von Neumann covering the first 611 primes were extended to the first 1000 primes of the form \( 6n + 1 \), with the result that the ratios have now become of the order of 3 to 4 to 5, thus continuing the trend away from the conjecture and towards equal distribution noted by Goldstine and von Neumann. The actual figures will be given below.

Before doing this we would like to suggest another division of the primes of the form \( 6n + 1 \) into three classes with respect to the absolute value of \( S_3 \). Since

\[ F_3(-\sqrt{3p}) = F_3(\sqrt{3p}) = -pL, \]

there is always one root of \( F_3 = 0 \) which is greater than \( \sqrt{3p} \) in absolute value, and we already know that there is a root of \( F_3 = 0 \) which is less than \( \sqrt{p} \) in absolute value. Therefore the absolute value of \( S_3 \) lies in one of the three intervals

\[ (0, \sqrt{p}), \quad (\sqrt{p}, 2\sqrt{p}). \]

We have actually counted the number of times that the principal root lies in these intervals using the tables of Goldstine and von Neumann and our own tabulation from the SWAC for primes above 10,000. We find that the number of primes in these three categories is approximately the same over the whole range covered. It is hoped that these figures will encourage some characterization of these classes of primes, which escapes the writer. The actual figures follow, where the primes are divided into 10 groups of 100 primes each.
Table 1. Number of primes $p \equiv 1 \pmod{6}$ such that

| Group | $S_1 < -\sqrt{p}$ | $-\sqrt{p} < S_1 < \sqrt{p}$ | $S_2 > \sqrt{p}$ | $|S_1| < \sqrt{p}$ | $\sqrt{p} < |S_1| < \sqrt{3p}$ | $|S_1| > \sqrt{3p}$ |
|-------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| I     | 18              | 28              | 54              | 28              | 36              | 36              |
| II    | 21              | 38              | 41              | 38              | 35              | 27              |
| III   | 21              | 33              | 46              | 33              | 34              | 33              |
| IV    | 29              | 32              | 39              | 32              | 32              | 36              |
| V     | 28              | 29              | 43              | 29              | 35              | 36              |
| VI    | 18              | 38              | 44              | 38              | 26              | 36              |
| VII   | 34              | 26              | 40              | 26              | 31              | 43              |
| VIII  | 24              | 32              | 44              | 32              | 41              | 27              |
| IX    | 29              | 37              | 37              | 34              | 35              | 31              |
| X     | 19              | 31              | 50              | 31              | 38              | 31              |
| Total | 241             | 321             | 438             | 321             | 343             | 336             |

A similar problem has been raised in the quartic case for the sum

$$S_4 = \sum_{m=0}^{p-1} \exp\left(2\pi im^4/p\right)$$

by Hasse [5] in the closing pages of his book on the theory of numbers. The discussion of the problem, as given there, depends on much of what is in the book and an elementary treatment of it might be in order together with additional numerical evidence.

It was already known to Lebesgue [6] that $S_4$, as well as the companion sum

$$S_4' = \sum_{m=0}^{p-1} \exp\left(2\pi irm^4/p\right),$$

where $r$ is any quadratic, but not quartic, residue of $p$, satisfies the quartic equation

$$[z^2 + (1 + (-1)^{(p-1)/4})p]z^2 - 4p(z - a)^2 = 0,$$

where $p = a^2 + 4b^2$ and $p = a \equiv 1 \pmod{4}$.

We can write (2) in factored form as follows

$$[z^2 - 2\sqrt{p}z + (1 - (-1)^{(p-1)/4})p + 2\sqrt{pa}]$$
$$\times [z^2 + 2\sqrt{p}z + (1 - (-1)^{(p-1)/4})p - 2\sqrt{pa}] = 0.$$

Since by definition of $S_2$, $S_4$ and $S_4'$ and by (1)

$$S_4 + S_4' = 2S_2 = 2\sqrt{p},$$

it follows that $S_4$ and $S_4'$ are roots of the first factor of (3) and hence

$$S_4, S_4' = p \pm \sqrt{2}\sqrt{(-1)^{(p-1)/4}p - \sqrt{pa}}.$$
Besides the obvious ambiguity in the sign of $\varepsilon$, the sign of $a$ is "known" only by reference to a table of quadratic partitions [7].

Hasse divides all primes of the form $4n + 1$ into four categories as follows:

$$p_1 = \begin{cases} 
8n + 1 & \sqrt{2p}/2 < \Delta < \sqrt{p} \\
8n + 5 & 0 < \Delta < \sqrt{2p}/2
\end{cases} \quad (\varepsilon = +1, |a| \equiv -1 \pmod{4})$$

$$p_3 = \begin{cases} 
8n + 1 & -\sqrt{2p}/2 < \Delta < 0 \\
8n + 5 & \sqrt{2p}/2 < \Delta < \sqrt{p}
\end{cases} \quad (\varepsilon = -1, |a| \equiv +1 \pmod{4})$$

$$p_5 = \begin{cases} 
8n + 1 & -\sqrt{p} < \Delta < -\sqrt{2p}/2 \\
8n + 5 & -\sqrt{2p}/2 < \Delta < 0
\end{cases} \quad (\varepsilon = -1, |a| \equiv -1 \pmod{4})$$

$$p_7 = \begin{cases} 
8n + 1 & 0 < \Delta < \sqrt{2p}/2 \\
8n + 5 & -\sqrt{p} < \Delta < -\sqrt{2p}/2
\end{cases} \quad (\varepsilon = +1, |a| \equiv +1 \pmod{4})$$

These intervals become meaningful if one thinks of them as the projections on the $x$ and $y$ axis respectively of the first, third, fifth and seventh octants of the circle of radius $\sqrt{p}$. Hasse (there are two errors in Hasse's table, which he attributes to Kaluza. The primes 677 and 877 belong to class $p_7$ and not $p_5$, giving ratios 21:21:12:26 instead of 21:23:12:24) found that for primes less than 1000 the four types of primes appear with frequencies which are approximately 2:2:1:2 for the primes of the form $8n + 1$ as well as for primes of the form $8n + 5$. He conjectured that there are infinitely many primes in each class and that the frequencies for primes of the forms $8n + 1$ are the same as for the primes of the form $8n + 5$.

Another, possibly more simple-minded, way of dividing these primes into four categories would be by grouping together all primes, irrespective of their form modulo 8 for which $\Delta$ lies in a given interval as follows:

$$p_0 \quad \text{for which} \quad -\sqrt{p} < \Delta < -\sqrt{2p}/2 \quad (\varepsilon = -1, |a| = -(-1)^{(p-1)/4} \pmod{4})$$

$$p_2 \quad \text{for which} \quad -\sqrt{2p}/2 < \Delta < 0 \quad (\varepsilon = -1, |a| = (-1)^{(p-1)/4} \pmod{4})$$

$$p_4 \quad \text{for which} \quad 0 < \Delta < \sqrt{2p}/2 \quad (\varepsilon = +1, |a| = (-1)^{(p-1)/4} \pmod{4})$$

$$p_6 \quad \text{for which} \quad \sqrt{2p}/2 < \Delta < \sqrt{p} \quad (\varepsilon = +1, |a| = -(-1)^{(p-1)/4} \pmod{4}).$$

If we now denote by $\pi_k(x)$ the number of primes in the class $p_k$ not exceeding $x$, then obviously

$$\pi_1(x) + \pi_6(x) = \alpha_1(x), \text{ the number of primes } < x \text{ for which } |a| = -1 \pmod{4}$$

$$\pi_3(x) + \pi_7(x) = \alpha_3(x), \text{ the number of primes } < x \text{ for which } |a| = +1 \pmod{4}$$

$$\pi_0(x) + \pi_6(x) = \alpha_0(x), \text{ the number of primes } < x \text{ for which } |a| = -(-1)^{(p-1)/4} \pmod{4}$$

$$\pi_2(x) + \pi_4(x) = \alpha_2(x), \text{ the number of primes } < x \text{ for which } |a| = (-1)^{(p-1)/4} \pmod{4}.$$
It has been shown by Lindau [8] that the Gaussian primes of the form \( a + bi \), when divided into residue classes with respect to any modulus are asymptotically equally distributed. The Gaussian primes can be divided into two classes modulo 4, according as \( |a| \equiv +1 \), or \( -1 \) (mod 4), \( a \equiv 1 \) (mod 4), or according as \( |a| \equiv \pm (-1)^{(p-1)/4} \) (mod 4). It therefore follows that

\[
\lim_{x \to \infty} \alpha_3(x) / \alpha_1(x) = \lim_{a \to \infty} \alpha_2(x) / \alpha_0(x) = 1.
\]

Since the ratios observed by Hasse at \( x = 1000 \) give

\[
\alpha_1(1000) / \alpha_3(1000) = 3/4,
\]

they cannot be the limiting ratios.

It should also be noted that by (6), \( \alpha_0 \) gives the number of primes \( x \), for which \( |\Delta| > \sqrt{2p}/2 \), while \( \alpha_2(x) \) counts those for which \( |\Delta| < \sqrt{2p}/2 \); therefore \( |\Delta| \) is in the limit equally likely to be in the two intervals \( (0, \sqrt{2p}/2) \) and \( (\sqrt{2p}/2, \sqrt{p}) \). This could possibly be used to support the conjecture that the absolute value of \( S_3 \) is also equally divided between three intervals in the limit. However, the consideration of the Eisenstein primes of the form \( a + b\omega \) modulo three does not seem to shed any light on the cubic problem any more than the consideration of the Gaussian primes modulo four helps us to find the limiting densities over the four intervals as taken by Hasse or as given in (6). We have therefore turned to the SWAC once more in order to calculate \( \Delta \) for all primes of the form \( 4n + 1 \) less than 10,000.

The time required by the SWAC for all 2549 primes for which \( \Delta \) was calculated was about eight hours. Towards the end of the run, for primes in the neighborhood of 10,000 it took almost a minute per prime, but considering that there were about 5000 sines or cosines to compute and add, not to speak of the calculation of the appropriate arguments, the time does not seem excessive. Also the accuracy of about 6 decimal places in cases which were computed by hand by (4) seemed very gratifying.

The results are as follows:

<table>
<thead>
<tr>
<th>( x )</th>
<th>( \pi_1(x) )</th>
<th>( \pi_2(x) )</th>
<th>( \pi_3(x) )</th>
<th>( \pi_4(x) )</th>
<th>( \pi_5(x) )</th>
<th>( \pi_6(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>21</td>
<td>21</td>
<td>12</td>
<td>26</td>
<td>17</td>
<td>15</td>
</tr>
<tr>
<td>2000</td>
<td>42</td>
<td>34</td>
<td>27</td>
<td>44</td>
<td>23</td>
<td>26</td>
</tr>
<tr>
<td>3000</td>
<td>54</td>
<td>55</td>
<td>43</td>
<td>59</td>
<td>46</td>
<td>46</td>
</tr>
<tr>
<td>4000</td>
<td>77</td>
<td>68</td>
<td>49</td>
<td>75</td>
<td>54</td>
<td>55</td>
</tr>
<tr>
<td>5000</td>
<td>87</td>
<td>86</td>
<td>60</td>
<td>96</td>
<td>67</td>
<td>74</td>
</tr>
<tr>
<td>6000</td>
<td>105</td>
<td>99</td>
<td>71</td>
<td>108</td>
<td>78</td>
<td>84</td>
</tr>
<tr>
<td>7000</td>
<td>125</td>
<td>116</td>
<td>79</td>
<td>122</td>
<td>86</td>
<td>94</td>
</tr>
<tr>
<td>8000</td>
<td>145</td>
<td>126</td>
<td>93</td>
<td>135</td>
<td>101</td>
<td>106</td>
</tr>
<tr>
<td>9000</td>
<td>163</td>
<td>136</td>
<td>102</td>
<td>153</td>
<td>116</td>
<td>114</td>
</tr>
<tr>
<td>10000</td>
<td>179</td>
<td>151</td>
<td>113</td>
<td>166</td>
<td>125</td>
<td>131</td>
</tr>
</tbody>
</table>

These results do not change appreciably the picture obtained for primes less than one thousand. The frequency \( \pi_6 \) is still consistently low, but Hasse's ratios of
2:2:1:2 now look more like 3:3:2:3, giving the ratio of $5/6$ for $a_1(x)/a_3(x)$ for $x = 10,000$, instead of $3/4$ at $x = 1000$, which is in line with the fact that this ratio tends to unity. The figures also seem to indicate that $\pi_0(x)$ and $\pi_2(x)$ are very close. The same can be said of $\pi_4(x)$ and $\pi_6(x)$ giving $a_6/a_2$ very close to one all along the line.

The next case, $S_8$, has not been studied in detail before, although the quintic period equation which it satisfies is known $[9]$ (There is a misprint in equation (10) of $[9]$. A correct expression is (8) of the present paper.) in terms of the following quadratic partitions:

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2$$

$$xw = u^2 - v^2 - 4uv, \quad p \equiv x \equiv 1 \pmod{5}$$

and is as follows:

$$F_6(z) = z^6 - 10px^2 - 5p+x^4 + 5[x - (x^2 - 125w^2)/4]z$$

$$+ p^3x - p[x^3 + 625(u^2 - v^2)w]/8 = 0.$$  

The roots of this equation lie between $-4\sqrt{p}$ and $4\sqrt{p}$, but when divided by $\sqrt{p}$ they no longer lie one each in any five fixed intervals. However, we can show by straightforward algebra that there always is a root $z$ such that $|z| > \sqrt{5}p$, and that there are one, two, or three roots in the middle interval $|z| < \sqrt{p}$. Figures obtained for the five roots of (8) for primes less than 10,000 on the SWAC show that all of these cases do arise and that for approximately half the primes there are two roots in the middle interval, while for about a quarter of the primes there are one or three roots in the middle interval. The majority of cases with one root in the middle has one root in each interval, but there are exceptions. Nevertheless, the frequency of $|S_8|$ in these three intervals is surprisingly uniform, namely

| $p$  | $|S_8| < \sqrt{p}$ | $\sqrt{p} < |S_8| < \sqrt{5}p$ | $\sqrt{5}p < |S_8| < 4\sqrt{p}$ | Total |
|------|--------------------|--------------------------------|-----------------------------|-------|
| 1000 | 15                 | 10                            | 15                          | 40    |
| 2000 | 30                 | 19                            | 24                          | 73    |
| 3000 | 37                 | 33                            | 33                          | 103   |
| 4000 | 46                 | 43                            | 45                          | 134   |
| 5000 | 55                 | 50                            | 58                          | 163   |
| 6000 | 67                 | 60                            | 67                          | 194   |
| 7000 | 76                 | 71                            | 79                          | 226   |
| 8000 | 84                 | 76                            | 86                          | 246   |
| 9000 | 91                 | 88                            | 94                          | 273   |
| 10000| 108                | 97                            | 101                         | 306   |

These figures seem to be in line with the conjecture that $|S_8|$ is equally likely to lie in any one of the three intervals

$$(0, \sqrt{p}), \quad (\sqrt{p}, \sqrt{5}p), \quad (\sqrt{5}p, 4\sqrt{p}).$$
The distribution of $S_5$ itself over the corresponding 5 intervals gives at 10,000 the following numbers from left to right

$$33, 34, 108, 63, 68$$

with ratios of the order of $1:1:3:2:2$.

Another possible division into intervals is provided by the scaled projections of the fifth roots of unity on the x-axis. This gives $\pm (1 \pm \sqrt{5})$ for division points. For $p = 10,000$ the distribution from left to right over the five intervals is

$$12, 51, 122, 97, 24$$

or ratios of the order of $1:4:10:8:2$. Although the sum of these figures is temptingly 25, our experience with the cubic and quartic cases does not permit us to indulge in the hypothesis that these are indeed the limiting ratios. It is also hard to see how to interpret these figures as a generalization of Kummer's conjecture.

We have pursued a step further the conjecture about the equal distribution of $|S_k|$ for odd $k$ in the intervals

$$(0, \sqrt{p}), \quad (\sqrt{p}, \sqrt{kp}), \quad (\sqrt{kp}, (k - 1)\sqrt{p})$$

by calculating on the SWAC the values of $S_7$ for $p = 7n + 1 < 5000$ with the following results:

| $p$  | $|S_7| < \sqrt{p}$ | $\sqrt{p} < |S_7| < \sqrt{7p}$ | $\sqrt{7p} < |S_7| < 6\sqrt{p}$ | Total |
|------|-------------------|--------------------------------|-------------------------------|-------|
| 1000 | 6                 | 11                             | 10                            | 27    |
| 2000 | 10                | 21                             | 13                            | 44    |
| 3000 | 16                | 32                             | 21                            | 69    |
| 4000 | 23                | 38                             | 27                            | 88    |
| 5000 | 33                | 43                             | 32                            | 108   |

These figures are not quite as convincing as those for the quintic, but since nothing is known about the distribution of the roots of the seventh degree period equation or about the form of the equation itself it is hoped that the actual tabulation of the roots as given by the SWAC will be of some use.

The actual values of these roots together with those of the quintic and the principal root of the cubic equation will be deposited in the UMT File of $MTAC$.

We wish to express our thanks to the Numerical Analysis Research Group of the University of California at Los Angeles for the use of the SWAC and in particular to Ruth Horgan and John Selfridge for checking out the various codes and operating the machine.

The code itself is diagrammed below. It presented no special difficulties and was put together from a standard cosine subroutine (a five term approximation of the 9th degree), which is used on the SWAC and fundamental number-theoretic subroutines, which will be described elsewhere.
ON THE LOCATION OF GAUSS SUMS

Program for the calculation of $S_k = \sum_{m=1}^{p-1} \exp(2\pi i m^k)/p$

1. Input last prime $p = kn + 1$

2. $p + n \rightarrow p$

3. Is $p$ a prime?
   Yes
   No

4. Find $1/p$

5. Find $m^k \equiv \theta_m \pmod{p}$

6. Find $\cos 2\pi \theta_m/p$

7. Accumulate $\sum_{m=1}^{p-1} \cos 2\pi \theta_m/p$

8. $m + 1 \rightarrow m$

9. Is $m < p$?
   Yes
   No

10. Is $s^2 < p$?
    Yes
     No

11. $-p \rightarrow p$

12. Does $S_n$ check?
    Yes
    No
    Stop

13. Output $\pm p, S_n$

Box 3 uses the trial divisor test for primality.
Box 5 uses a standard reduction modulo $p$.
Box 6 uses the cosine subroutine.
Box 11 provides an indication on the size of the sum for output.
Box 12 consisted of either substituting the principal root into the equation, or adding all the roots to zero, in case all were computed. In a few cases, where the check failed, the calculation was repeated.
A Method for Computing Certain Inverse Functions

A method will be demonstrated for computing the inverse of certain functions. The method is applicable to the computation of logarithms and inverse trigonometric functions. It makes use of the binary expansion of real numbers and is, therefore, particularly suitable for use in automatic digital computing machines which use the binary number system. It is not recommended for hand computing.

1. The Method. Let \( f(x) \) be a function which satisfies the following conditions,

(i) \( f(x) \) is continuous and monotone on an interval \((0, a]\)
    (including \( a \), but not including 0),

(ii) \( f(a/2) \) is known,

(iii) \( f(2x) \) and \( f(2x - a) \) can be computed when \( f(x) \) is known.

\((0, a]\) is taken to mean \([a, 0)\) if \( a \) is negative. Also, the symbol \((f(0), f(a)]\) will be taken to mean \((f(0, +), f(a)]\) \((f(0, -), f(a)]\) \([f(a), f(0, +)]\) or \([f(a), f(0, -)]\), whichever is appropriate.

Examples are:

\[
\begin{align*}
\text{(a)} & \quad f(x) = 2^x \quad a = -1 \\
& \quad f(2x) = (f(x))^2 \quad f(2x + 1) = 2(f(x))^2 \\
\text{(b)} & \quad f(x) = \cos x \quad a = \pi \\
& \quad f(2x) = 2(f(x))^2 - 1 \quad f(2x - \pi) = 1 - 2(f(x))^2
\end{align*}
\]

Let \( y \in (f(0), f(a)] \), and let it be required to compute \( f^{-1}(y) \), that is, to find \( x \) such that \( f(x) = y \). The existence and uniqueness of such an \( x \) in \((0, a]\) are guaranteed by condition (i). Let \( w = x/a \). Then \( w \) is in the interval \((0, 1]\). It