

Review

Reviewed Work(s): Class Number of Primes of the Form  $4n + 1$  by K. E. Kloss, M. Newman and E. Ordman

Review by: D. S.

Source: *Mathematics of Computation*, Vol. 23, No. 105 (Jan., 1969), pp. 213-214

Published by: American Mathematical Society

Stable URL: <http://www.jstor.org/stable/2005084>

Accessed: 28-02-2018 16:47 UTC

---

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at <http://about.jstor.org/terms>



JSTOR

*American Mathematical Society* is collaborating with JSTOR to digitize, preserve and extend access to *Mathematics of Computation*

Of these, the first table is a special table giving the complete factorization of  $5U_n^2 \pm 5U_n + 1$  for odd  $n \leq 77$ , the two trinomials being the algebraic factors in

$$V_{5n}/V_n = (5U_n^2 - 5U_n + 1)(5U_n^2 + 5U_n + 1),$$

$n$  odd.

The second table is the general factor table for  $U_n$  and  $V_n$  with  $n \leq 385$ . The overall bound for prime factors is  $2^{35}$  for  $n < 300$  and  $2^{30}$  for  $300 \leq n \leq 385$ . It also shows that  $U_n$  and  $V_n$  are completely factored up to  $n = 172$  and  $n = 151$  respectively. The table gives as well an indication for the incomplete factorizations whether their cofactors are composite or pseudoprime. The introduction to this table provides the further information that  $U_n$  is prime for  $n \leq 1000$  iff  $n = 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571$ , while  $V_n$  is prime for  $n \leq 500$  iff  $n = 0, 2, 4, 5, 7, 8, 11, 13, 16, 17, 19, 31, 37, 41, 47, 53, 61, 71, 79, 113, 313, 353$ . The number  $U_{353}$ , which was only known to be a pseudoprime at the time of publication of the tables, has since been shown to be a prime by the reviewer.

JOHN BRILLHART

University of Arizona  
Tucson, Arizona 85721

10[9].—K. E. KLOSS, M. NEWMAN & E. ORDMAN, *Class Number of Primes of the Form  $4n + 1$* , National Bureau of Standards, 1965, 15 Xeroxed computer sheets deposited in the UMT file.

This interesting table lists the first 5000 primes of the form  $4n + 1$ —from  $p = 5$  to  $p = 105269$ . For each such prime  $p$  is listed the class number  $h(p)$  of the real algebraic quadratic field  $R(\sqrt{p})$ . Alternatively, this is also the number of classes of binary quadratic forms of discriminant  $p$ . The table is similar to that announced in [1], and was computed about five years ago on an experimental machine, the NBS PILOT. The method used was the classical one of listing all reduced forms and counting the “periods” into which they fall. Appended are short extensions: the class numbers for the first 100 primes  $4n + 1 > 10^6$  and for the first  $35 > 10^7$ .

In [1], Kloss reports that about 80% of these primes have class number 1. We have tallied the following more detailed statistics: the number of examples with class number 1, 3, 5, etc. that occur among the first 1000, 2000, etc. primes.

TABLE

	$h = 1$	3	5	7	9	11	13	15	17	19	21	23	25	27	29	>30
1000	816	101	35	22	9	6	5	2	1	—	1	—	—	1	—	1
2000	1622	213	70	36	19	10	8	7	2	2	1	2	1	3	—	4
3000	2420	306	111	58	34	13	14	13	7	5	2	2	4	3	1	7
4000	3198	422	145	79	50	19	20	16	9	8	5	3	7	4	2	13
5000	3987	522	183	98	66	29	28	20	11	11	7	4	10	4	4	16

It will be noted that Kloss’s 80% is remarkably steady. Similarly, a little over 10% have class number 3, 3.6% have class number 5, 2% have class number 7, 1.2% have class number 9, etc. *Queries*: What is this 80%? More generally, what is

this distribution? Can it be deduced now from some heuristically reasonable postulates, if not yet more rigorously? Gauss, in §304 of his *Disquisitiones*, raises the question whether the number of examples of one class/genus does not tend to some *fixed fraction* of the total number of examples as the *determinant* goes to infinity. There are two differences between his population and the present one. Gauss is concerned with all (nonsquare) positive *determinants*, and here we have the  $4n + 1$  prime *discriminants*. This latter implies that we have one genus only here, and an odd class number. Nonetheless, the similarity of the two propositions is obvious.

It may be helpful to add that for primes  $p = 8n + 1$  the class number is the same whether  $p$  is regarded as the discriminant or the determinant. And the same is true for those primes  $8n + 5$  where there is a solution of

$$x^2 - py^2 = 4, \quad x \equiv y \equiv 1 \pmod{2}.$$

But if there is no solution, as for  $p = 37, 101, \text{etc.}$ , then Gauss's class number (for determinants) is 3 times that listed here (for discriminants). The distribution for determinants would therefore differ somewhat from that shown above, but it should also be studied, particularly as its analysis may be easier. There are then simpler relations among the class number, the solution of the Pell equation, and the corresponding Dirichlet series. It would also be of interest to study the distribution for the primes  $8n + 1$  taken alone. Here, the prime 2 must be represented by one of the quadratic forms, and that should have a heavy influence on the outcome.

Turning our attention to a different aspect of this data, we list the sequence of primes  $p = 4n + 1$  for which a larger class number occurs than for any smaller prime.

$p$	$h$	$p$	$h$	$p$	$h$
229	3	401	5	577	7
1129	9	1297	11	7057	21
8761	27	14401	43	32401	45
41617	57	57601	63	90001	87

It will be noted that most of these  $p$  are of the form  $(4m)^2 + 1$ . This guarantees a relatively small solution for the Pell equation, and, therefore, a relatively large class number. In fact, one has

$$\frac{\log(4m + \sqrt{p})}{\sqrt{p}} h = \sum_{k=0}^{\infty} \left( \frac{p}{2k+1} \right) (2k+1)^{-1},$$

and since the Dirichlet series on the right can grow as  $O(\log m)$ , and since it does so grow if  $p$  has numerous small prime quadratic residues: 3, 5, 7, etc., the class numbers shown are therefore roughly proportional to  $m$ . In a case such as  $p = 14401 = 120^2 + 1$ , where the Dirichlet series,  $L = 1.964$ , is fortuitously large, the class number,  $h = 43$ , is also fortuitously large—ahead of its time, so to speak.

D. S.

1. K. E. KLOSS, "Some number-theoretic calculations," *J. Res. Nat. Bur. Standards Sect. B*, v. 69B, 1965, pp. 335-336.