MATHEMATICS OF COMPUTATION
VOLUME 43, NUMBER 167
JULY 1984, PAGES 313–327

The Expectation of Success Using a Monte Carlo Factoring Method—Some Statistics on Quadratic Class Numbers

By Duncan A. Buell

Abstract. A method has been proposed for factoring an integer N by using the structure of the class groups of quadratic fields of radicand $-kN$ for various small multipliers k. We discuss the method and an implementation of the method, and various theoretical questions which have an impact on the practical use of the method in factoring. Some of the theoretical questions relate to the nature of class numbers and class groups; we present extensive statistical results on the class numbers and class groups of imaginary quadratic fields.

1. The Method. We deal with *binary quadratic forms* (a, b, c) of *discriminant* $b^2 - 4ac = -N$, $N > 0$. The equivalence classes of forms of a fixed discriminant under transformations of the modular group Γ form a finite abelian group, the *class group*. The order of the class group is the *class number* $h = h(N)$.

The crucial fact, used either implicitly or explicitly in several factoring methods, is that for odd N the classes of order 2 in the class group, called *ambiguous* classes, are precisely the classes containing forms $(P, P, (P^2 + N)/4P)$ for the various divisors P of N. Thus finding ambiguous forms leads to finding factors. (For even N there are also ambiguous classes represented by forms $(P, 0, N/P)$ in addition to the classes mentioned above.)

Shanks used the explicit class group structure in his factoring method CLASNO [SHAN]. He estimated h with the product formula, then "fiddled" in the class group until the exact value for h was found. He then found an ambiguous form by finding a form $f = (a, b, c)$ for which $f^{h/2}$ was not the identity.

The new method, which we shall henceforth refer to as the CPS method ((Classgroup/CLASNO)-(Pollard P-1)-(Synthesis)), is somewhat less direct [SCHN]. We let M be the product of all "small" odd primes $p(i)$ raised to "large" exponents $a(i)$. We then compute $f^M = g$ for forms f until we find an f for which f^M is not the identity. Writing $h = 2^m h'$, it is certainly true that *if* $h' \mid M$, then $g^{2^{m-1}}$ is ambiguous.

In short, we exponentiate forms to huge odd powers that we *hope* contain all the odd factors of the class number. If this comes to pass, then we can get ambiguous forms and then factors of N.

Actually, as with many factoring methods, there are several deeper levels of subtlety. First, it is not really necessary that $h' \mid M$. The class groups, being finite

Received March 8, 1983; revised October 11, 1983.
1980 *Mathematics Subject Classification.* Primary 10–04, 10A25, 12A25.

0025-5718/84 $1.00 + $.25 per page

abelian groups, are direct products of their p-Sylow subgroups. If h'' is the maximal order of any form of odd order, then it is only necessary that $h'' \mid M$ in order for an ambiguous form to be generated by this method. We shall return to this question later.

Second, it is not entirely necessary that $h'' \mid M$. A second stage of the algorithm has been suggested in [SCHN] which is based on the gamble that M/h'' is a prime. Rather than continue exponentiating for long periods, one uses a CLASNO-like test to find out whether the form obtained from the previous exponentiation is of order P for larger primes P. More on this later.

Third, it has been suggested that several discriminants $-kN$ be used, for various small k. Since it is not possible to predict exactly the nature of $h(-kN)$, one stands a much better chance of factoring N by trying several different discriminants in hopes that (at least) one has the necessary characteristics to permit an easy factoring of N.

2. The Implementation. The CPS method has been implemented on the IBM 3033N computer at the System Network Computing Center at Louisiana State University. The very-low-level routines of the multiprecise arithmetic have been coded in assembly language. Higher routines have usually first been programmed in PL/1 to allow working programs to be written rapidly, and then translated into IBM VS FORTRAN (the IBM version of FORTRAN 77) for greater speed. It is to be emphasized that the CPS code itself has not been extensively optimized. Since this is a new method, it has been necessary to first find out if it is even possible to consider it as practical. The routines for class group calculation are for the most part general-purpose routines and have not been tailored for this use.

Even considering the fact that faster programs could easily be developed, the method does seem slow. Testing has been done primarily by generating pseudoprimes of 12 to 15 digits and attempting to factor the products of two such pseudoprimes. One attempt was made, and abandoned, to factor a 47-digit composite number from the Cunningham table [BRIL]. The method seems at this point so slow that it would not be possible to attack 50 or 60 digit integers with it. Code optimization could realistically improve the performance by a factor of only three to five, which would not be sufficient.

The routines for composition and reduction of forms came informally from Daniel Shanks via A. O. L. Atkin, neither of whom are responsible for any possible degradation in performance introduced by the author.

Some remarks about languages are in order. Three distinct versions of multiprecise arithmetic have been implemented. All have used assembly-language routines for low-level arithmetic, and all have been compiled with the complete optimizing features of the compilers. One in PL/1 and one in VS FORTRAN have treated multiprecise integers as fixed-length arrays with a pointer to the first nonzero digit. A third, in VS FORTRAN, has used variable-length arrays with an indicator of the length of the array. In heavy arithmetic computation, the PL/1 version ran about 25% faster than the fixed-length FORTRAN, but somewhat slower than the variable-length FORTRAN. The lesson for future programming efforts seems to be that PL/1 is actually much more efficient in array handling than even fully optimized FORTRAN. In all cases of these computations, it seemed that arithmetic on 50-digit

integers could be performed almost 40% faster by working base $2^{30} = 1073741824$ rather than base 10^9. A substantial portion of computing time, it seems, is spent simply in separating doubleword products into component singleword digits in some number base.

3. Theoretical Appeal of the CPS Method. The theoretical appeal of the CPS method comes from the following observations [POMEa]. We let $L(N) = \exp((\log N \log\log N)^{1/2})$. Most factoring algorithms currently in use have a running time measured as $(L(N))^{x+o(1)}$. The new method is the first, if certain assumptions are made about the nature of class numbers and class groups, for which the value of x is as small as 1 [POMEb, POMEc]. These assumptions are essentially that numbers which are class numbers have the same divisibility properties as all numbers of comparable size. Recall that, in order to have this method factor N, it is necessary that $h(N)$ have only "smallish" prime factors. The presence of only one prime factor of h not included in the exponent M will cause the method not to work in the first stage.

4. Implementation Problems. As evidenced by the problems in this first version, substantial work remains if the CPS method is to become practical. We describe some possibilities.

The class group algorithms currently implemented are not only algorithms for general use, they are originally designed for single precision calculation. In the actual implementation, it is entirely probable that some speed could be gained by saving steps in the code. A greater speedup could be obtained by an improved set of algorithms that would take into account the fact that these are multiprecise computations.

Further speedup would be possible if an average-case look at continued exponentiation in the class group revealed ways to predict arithmetic results. By analogy with the GCD algorithm (which is incidentally called extremely often in class group calculation), one can predict, based on a theorem of Levy, that 66% of the quotients are 1, 2, or 3 [KNUT]. Using this, one can avoid division in most instances and use only one to three subtractions. It is conceivable that analogous results hold in class groups.

A final comment concerns reduction. Traditional routines call for reduction after every composition. This is normally done to keep the coefficients within predictable magnitudes. Reduction is certainly not necessary every time, however. Only when the added cost of calculations with longer arguments exceeds the cost of a reduction should that reduction be made.

5. Theoretical Questions. Class Number Characteristics. Implementation questions aside, it is clear that the nature of class numbers and of class groups plays a key role in the question of whether or not this method will be useful. The following results are compiled from a computation of all class numbers for even and odd discriminants from 0 to -16 million, and of all class groups for discriminants from 0 to -4 million. Although there are potential flaws in extrapolating even from this point—the class numbers are still smaller than 8400 and the class groups thus have little opportunity to be very complex—it is nonetheless true that this statistical evidence from about 4.8 million class numbers and one million class groups can be of use in pointing the way for further study.

TABLE 1

Largest and smallest class numbers and # of forms per genus

ODD DISCRIMINANTS

RUN	SCN	LCN	SFPG	LFPG
0	1	1868	1	1829
1	76	2724	6	2669
2	98	3464	8	3311
3	118	3918	9	3881
4	138	4498	8	4465
5	156	4913	10	4913
6	162	5180	8	5167
7	185	5686	10	5595
8	198	6088	9	6027
9	202	6372	12	6343
10	211	6767	13	6767
11	242	7206	13	7165
12	233	7457	12	7457
13	253	7719	12	7719
14	256	8064	12	7847
15	267	8303	14	8303

EVEN DISCRIMINANTS

RUN	SCN	LCN	SFPG	LFPG
0	1	1044	1	522
1	104	1464	5	704
2	152	1800	7	879
3	176	2082	8	1041
4	210	2352	9	1176
5	222	2580	9	1279
6	260	2870	10	1435
7	270	3040	11	1512
8	282	3286	10	1643
9	304	3392	10	1696
10	323	3600	12	1800
11	352	3730	14	1842
12	376	3896	13	1908
13	378	4132	12	1975
14	388	4344	12	2049
15	392	4392	14	2190

TABLE 2

Percentages of noncyclic p-Sylow subgroups for small p

	EVEN DISCS			ODD DISCS		
RUN	2	3	5	2	3	5
0	2.1	0.8	0.1	1.5	0.8	0.1
1	2.8	1.0	0.1	2.0	1.0	0.1
2	3.0	1.1	0.1	2.4	1.1	0.1
3	3.1	1.1	0.1	2.3	1.2	0.2
4	3.2	1.2	0.1	2.4	1.2	0.1
5	3.3	1.2	0.2	2.5	1.2	0.2
6	3.4	1.2	0.2	2.5	1.2	0.2
7	3.5	1.2	0.1	2.6	1.3	0.1
8	3.4	1.1	0.1	2.5	1.3	0.2
9	3.6	1.2	0.2	2.7	1.3	0.2
10	3.4	1.3	0.2	2.8	1.4	0.2
11	3.4	1.3	0.2	2.6	1.3	0.2
12	3.7	1.3	0.2	2.8	1.4	0.2
13	3.8	1.2	0.2	2.7	1.3	0.2
14	3.7	1.2	0.2	2.8	1.4	0.2
15	3.5	1.3	0.1	2.8	1.3	0.2
16	3.9	1.2	0.2	2.8	1.4	0.2
17	3.8	1.4	0.2	2.8	1.3	0.2
18	3.8	1.3	0.2	2.9	1.3	0.2
19	3.8	1.3	0.2	2.9	1.4	0.2

ADDITIONAL NONCYCLIC SYLOW SUBGROUPS FOR PRIMES > 5:
ODD DISCS: 371/810578 = .04 %
EVEN DISCS: 169/405276 = .04 %

TABLE 3

Percentages of FPG divisible by small integers for odd discriminants of quadratic number fields

	50.0	33.3	25.0	20.0	16.7	14.3	12.5	11.1	10.0	9.1	8.3	7.7	7.1
	2	3	4	5	6	7	8	9	10	11	12	13	14
0	41.9	40.2	21.9	23.0	16.6	15.8	11.0	13.8	9.4	9.5	8.5	7.9	6.4
1	43.7	41.1	23.0	23.4	17.7	15.9	11.8	14.3	10.1	9.6	9.3	8.2	6.9
2	44.2	41.3	23.4	23.3	18.2	16.0	12.0	14.6	10.2	9.7	9.6	8.0	6.9
3	44.6	41.4	23.6	23.2	18.3	16.1	12.0	14.5	10.3	9.6	9.6	8.2	7.2
4	44.6	41.6	23.6	23.7	18.4	16.0	12.0	14.6	10.5	9.7	9.7	8.1	7.1
5	45.0	41.6	23.9	23.6	18.6	16.0	12.2	14.6	10.6	9.7	9.8	8.3	7.2
6	45.0	41.8	24.0	23.7	18.7	16.2	12.4	14.7	10.6	9.8	10.0	8.3	7.2
7	45.3	41.9	24.1	23.7	18.8	16.2	12.3	14.8	10.7	9.7	10.1	8.1	7.3
8	45.4	41.9	24.2	23.4	19.0	16.2	12.4	14.8	10.6	9.8	10.2	8.1	7.3
9	45.3	41.9	24.1	23.6	18.9	16.3	12.4	14.9	10.7	9.7	10.1	8.1	7.3
10	45.4	41.9	24.3	23.4	19.0	16.2	12.5	14.8	10.5	9.9	10.1	8.3	7.3
11	45.7	42.0	24.3	23.6	19.1	16.2	12.4	14.9	10.7	9.8	10.1	8.1	7.3
12	45.6	42.1	24.4	23.7	19.1	16.2	12.6	14.9	10.7	9.8	10.2	8.1	7.4
13	45.7	42.0	24.4	23.8	19.3	16.3	12.6	14.9	10.8	9.8	10.2	8.2	7.4
14	45.7	42.0	24.4	23.6	19.2	16.3	12.5	14.9	10.7	9.8	10.2	8.2	7.4
15	45.9	42.1	24.5	23.7	19.2	16.3	12.6	14.9	10.8	9.9	10.2	8.1	7.5

	6.7	6.3	5.9	5.6	5.3	5.0	4.8	4.5	4.3	4.2	4.0	3.8	3.7
	15	16	17	18	19	20	21	22	23	24	25	26	27
0	9.0	5.4	5.9	5.5	5.2	4.7	6.2	3.7	4.2	4.2	4.5	3.0	4.5
1	9.4	5.8	6.0	6.1	5.4	5.3	6.4	4.1	4.3	4.8	4.6	3.4	4.7
2	9.6	6.0	6.1	6.4	5.4	5.3	6.5	4.1	4.4	4.8	4.8	3.5	4.9
3	9.5	6.0	6.1	6.4	5.3	5.4	6.6	4.2	4.4	4.8	4.7	3.6	4.8
4	9.8	6.0	6.0	6.4	5.4	5.5	6.6	4.3	4.4	4.9	4.8	3.5	4.9
5	9.8	6.2	6.1	6.5	5.4	5.6	6.6	4.3	4.4	5.0	4.8	3.7	4.9
6	9.8	6.3	6.0	6.5	5.5	5.6	6.8	4.3	4.5	5.1	4.7	3.6	4.9
7	9.9	6.2	6.1	6.5	5.4	5.7	6.8	4.3	4.3	5.1	4.8	3.6	5.0
8	9.9	6.2	6.0	6.7	5.5	5.6	6.8	4.4	4.4	5.2	4.7	3.7	5.0
9	10.0	6.2	6.2	6.6	5.4	5.6	6.8	4.4	4.4	5.1	4.8	3.7	5.1
10	9.7	6.3	6.0	6.7	5.4	5.6	6.7	4.5	4.4	5.1	4.7	3.7	5.0
11	9.9	6.2	6.2	6.7	5.5	5.7	6.8	4.5	4.4	5.1	4.8	3.7	4.9
12	10.0	6.3	6.2	6.7	5.5	5.7	6.7	4.5	4.4	5.2	4.8	3.7	5.0
13	10.1	6.3	6.1	6.8	5.4	5.7	6.7	4.4	4.5	5.2	4.9	3.7	4.9
14	10.0	6.3	6.0	6.8	5.4	5.7	6.7	4.5	4.5	5.2	4.8	3.7	5.0
15	10.0	6.3	6.0	6.7	5.4	5.7	6.8	4.5	4.5	5.3	4.9	3.7	5.0

TABLE 4

Percentages of FPG divisible by small integers for odd discriminants of quadratic number fields with 2 genera

	50.0	33.3	25.0	20.0	16.7	14.3	12.5	11.1	10.0	9.1	8.3	7.7	7.1
	2	3	4	5	6	7	8	9	10	11	12	13	14
0	49.6	40.7	24.7	23.2	20.1	16.0	12.4	14.2	11.5	9.7	9.9	8.0	7.8
1	49.8	41.3	24.8	23.7	20.4	16.2	12.5	14.5	11.8	9.7	10.2	8.3	7.9
2	50.0	41.5	24.8	23.1	20.7	16.2	12.6	14.7	11.4	9.7	10.2	8.2	8.0
3	49.8	41.8	24.8	23.2	20.9	16.5	12.3	14.7	11.5	9.8	10.3	8.1	8.2
4	49.7	41.8	24.6	23.5	20.7	16.0	12.2	14.8	11.6	9.8	10.3	8.3	7.9
5	50.0	42.1	25.1	23.8	20.9	16.3	12.4	14.8	11.9	9.7	10.5	8.5	8.1
6	49.6	42.3	24.9	23.7	20.9	16.2	12.6	14.8	11.7	10.0	10.5	8.4	8.0
7	49.9	42.1	25.0	23.6	20.9	16.4	12.3	15.1	11.7	9.8	10.5	8.2	8.1
8	50.0	42.1	24.8	23.4	21.1	16.2	12.4	14.8	11.6	10.0	10.4	8.1	8.1
9	49.8	42.1	24.8	23.6	21.0	16.4	12.4	15.0	11.8	9.7	10.5	8.3	8.2
10	49.6	42.0	24.8	23.4	21.0	16.2	12.4	14.9	11.5	9.9	10.4	8.5	7.9
11	50.0	42.2	24.7	23.5	21.1	16.4	12.3	15.0	11.7	10.0	10.4	8.2	8.2
12	49.8	42.3	24.9	23.9	21.0	16.2	12.4	15.0	12.0	9.8	10.4	8.2	8.1
13	49.8	42.7	25.0	24.0	21.4	16.5	12.4	15.1	12.0	9.8	10.7	8.4	8.2
14	49.7	42.3	24.7	23.6	20.9	16.3	12.3	15.1	11.8	9.9	10.3	8.2	8.1
15	50.1	42.3	25.2	23.9	21.2	16.5	12.7	15.0	12.0	9.9	10.6	8.0	8.3

TABLE 4 (*continued*)

	6.7	6.3	5.9	5.6	5.3	5.0	4.8	4.5	4.3	4.2	4.0	3.8	3.7
	15	16	17	18	19	20	21	22	23	24	25	26	27
0	9.3	6.1	6.1	6.9	5.3	5.6	6.4	4.6	4.3	4.8	4.6	3.9	4.7
1	9.7	6.1	6.1	7.2	5.6	5.8	6.6	4.9	4.5	5.1	4.9	4.0	4.8
2	9.8	6.2	6.2	7.3	5.6	5.7	6.7	4.8	4.5	5.1	4.8	4.1	5.0
3	9.6	6.1	6.2	7.4	5.4	5.7	6.9	4.8	4.5	5.1	4.7	4.0	4.9
4	9.9	6.1	5.9	7.3	5.5	5.8	6.7	4.9	4.5	5.1	4.9	4.0	5.0
5	10.0	6.2	6.3	7.4	5.3	6.1	6.9	4.9	4.5	5.2	4.9	4.2	5.1
6	9.9	6.2	6.1	7.4	5.6	5.9	6.9	4.9	4.6	5.3	4.7	4.1	4.9
7	10.0	6.1	6.1	7.4	5.6	5.9	7.0	4.9	4.3	5.2	4.9	4.0	5.2
8	9.9	6.2	6.2	7.4	5.5	5.8	6.9	5.0	4.4	5.2	4.7	4.1	5.1
9	10.0	6.2	6.3	7.4	5.4	5.9	6.8	4.8	4.5	5.2	4.9	4.2	5.2
10	9.9	6.2	6.0	7.4	5.3	5.8	6.7	5.0	4.4	5.2	4.8	4.2	5.1
11	9.9	6.1	6.3	7.5	5.5	5.7	6.9	5.0	4.3	5.1	4.8	4.1	5.0
12	10.2	6.2	6.2	7.4	5.6	5.9	6.9	5.0	4.4	5.1	4.9	4.0	5.0
13	10.3	6.3	6.2	7.6	5.5	6.0	6.9	4.8	4.6	5.3	4.9	4.2	5.1
14	10.1	6.2	6.0	7.5	5.4	5.8	6.8	4.9	4.6	5.1	4.9	4.0	5.1
15	10.2	6.3	6.0	7.4	5.3	5.9	6.8	4.9	4.6	5.3	4.9	4.0	5.0

TABLE 5

Percentages of FPG divisible by small integers for even discriminants of quadratic number fields

	50.0	33.3	25.0	20.0	16.7	14.3	12.5	11.1	10.0	9.1	8.3	7.7	7.1
	2	3	4	5	6	7	8	9	10	11	12	13	14
0	53.7	39.7	28.0	22.9	21.3	15.5	14.0	13.4	12.1	9.0	10.8	7.5	8.0
1	54.7	40.9	28.9	23.3	22.3	16.0	14.7	14.3	12.6	9.6	11.7	7.7	8.5
2	55.1	40.8	29.2	23.2	22.6	15.8	14.9	14.2	12.7	9.5	11.9	8.0	8.5
3	55.3	41.3	29.3	23.3	22.8	16.1	15.1	14.5	12.8	9.8	12.0	8.1	8.7
4	55.4	41.5	29.4	23.5	23.0	16.1	15.2	14.6	12.8	9.7	12.3	8.1	8.8
5	55.5	41.3	29.7	23.6	22.8	16.2	15.2	14.6	13.1	9.6	12.1	8.0	8.8
6	55.8	41.4	29.7	23.4	23.0	16.4	15.2	14.5	13.0	9.6	12.2	8.2	9.0
7	55.8	41.4	29.9	24.0	23.1	16.1	15.6	14.7	13.4	9.8	12.3	8.1	8.9
8	55.9	41.8	29.8	23.6	23.3	16.0	15.2	14.7	13.0	9.7	12.4	8.1	8.8
9	56.0	41.7	29.7	24.1	23.2	15.7	15.4	14.5	13.5	9.8	12.2	7.9	8.7
10	56.0	41.9	29.9	23.4	23.5	16.0	15.5	14.8	13.2	9.6	12.5	8.1	8.8
11	56.0	41.6	30.1	23.9	23.4	15.9	15.5	14.6	13.3	9.7	12.6	8.0	8.8
12	56.1	41.9	29.9	23.5	23.5	16.2	15.3	14.7	13.2	9.6	12.5	8.3	9.1
13	56.1	41.8	30.0	23.4	23.5	16.1	15.5	14.9	13.1	9.7	12.5	8.1	9.1
14	56.1	41.6	30.3	23.5	23.4	16.4	15.5	15.0	13.1	9.6	12.6	8.2	9.2
15	56.1	41.8	30.1	23.5	23.3	16.4	15.4	15.1	13.1	9.7	12.4	8.1	9.2

	6.7	6.3	5.9	5.6	5.3	5.0	4.8	4.5	4.3	4.2	4.0	3.8	3.7
	15	16	17	18	19	20	21	22	23	24	25	26	27
0	8.8	6.6	5.4	6.9	4.7	6.0	5.7	4.4	3.7	5.1	3.9	3.6	4.0
1	9.4	7.4	5.8	7.7	5.0	6.5	6.3	5.1	4.2	5.9	4.4	4.0	4.7
2	9.3	7.4	5.9	7.8	5.2	6.6	6.4	5.2	4.1	6.0	4.6	4.2	4.6
3	9.6	7.5	6.0	7.9	5.1	6.7	6.5	5.3	4.2	6.1	4.4	4.3	4.7
4	9.7	7.4	5.9	8.0	5.3	6.7	6.5	5.3	4.3	6.3	4.7	4.4	4.7
5	9.7	7.5	6.0	7.9	5.2	7.0	6.6	5.2	4.4	6.0	4.6	4.3	4.9
6	9.5	7.7	6.1	7.9	5.3	6.9	6.7	5.2	4.4	6.2	4.6	4.4	4.7
7	9.8	7.7	5.9	8.2	5.3	7.1	6.6	5.4	4.3	6.4	4.7	4.3	4.8
8	9.8	7.5	6.0	8.1	5.4	6.8	6.6	5.4	4.2	6.2	4.7	4.5	4.8
9	10.2	7.7	6.1	8.0	5.3	7.1	6.5	5.5	4.4	6.2	4.9	4.3	4.9
10	9.7	7.8	6.0	8.2	5.4	7.0	6.6	5.4	4.3	6.4	4.7	4.5	5.0
11	9.9	7.9	6.1	8.2	5.3	7.1	6.6	5.4	4.3	6.5	4.8	4.4	4.9
12	9.9	7.7	6.0	8.2	5.3	7.0	6.7	5.3	4.6	6.3	4.7	4.6	4.9
13	9.7	7.8	6.1	8.4	5.3	7.0	6.6	5.5	4.3	6.4	4.7	4.5	4.9
14	9.8	7.8	6.1	8.4	5.3	7.1	6.7	5.3	4.3	6.4	4.7	4.5	5.0
15	9.8	7.7	6.0	8.4	5.4	6.9	6.7	5.4	4.4	6.3	4.8	4.4	5.0

TABLE 6

Percentages of FPG divisible by small integers for even discriminants of quadratic number fields with 4 genera

	50.0	33.3	25.0	20.0	16.7	14.3	12.5	11.1	10.0	9.1	8.3	7.7	7.1
	2	3	4	5	6	7	8	9	10	11	12	13	14
0	53.1	39.8	28.2	22.8	21.2	15.6	14.3	13.6	11.9	9.3	10.9	7.5	8.2
1	53.6	41.3	28.8	23.5	22.4	16.2	14.8	14.6	12.5	9.7	12.1	7.9	8.5
2	54.2	41.4	29.5	23.3	22.7	16.0	15.2	14.6	12.5	9.5	12.3	8.1	8.5
3	54.0	41.4	29.2	23.4	22.4	16.0	15.3	14.5	12.5	10.1	12.1	8.4	8.5
4	54.1	41.6	29.1	23.8	22.6	16.3	15.1	14.5	12.8	9.9	12.3	8.2	8.7
5	54.1	41.7	29.4	23.6	22.5	16.3	15.1	15.0	12.6	9.6	12.1	8.1	8.8
6	54.4	41.7	29.6	23.4	22.6	16.8	15.4	14.8	12.7	9.6	12.3	8.1	9.0
7	54.4	41.7	29.5	23.9	22.7	16.2	15.5	14.9	12.9	9.9	12.1	8.3	8.7
8	54.3	42.1	29.1	23.7	22.8	16.1	15.0	15.0	12.5	9.7	12.0	8.2	8.6
9	54.4	41.6	29.4	24.1	22.6	15.8	15.3	14.6	13.1	10.0	12.1	8.2	8.4
10	54.5	42.3	29.5	23.4	23.0	15.9	15.5	15.1	12.8	9.7	12.4	8.2	8.6
11	54.1	42.1	29.3	24.0	23.0	16.0	15.1	14.9	13.0	9.7	12.5	8.2	8.7
12	54.5	42.1	29.6	23.6	23.0	16.1	15.4	14.9	12.9	9.7	12.5	8.5	8.7
13	54.4	41.7	29.5	23.6	22.8	16.2	15.5	15.1	12.9	9.9	12.3	8.2	8.9
14	54.5	42.2	29.9	23.4	23.1	16.7	15.6	15.4	12.9	9.8	12.7	8.3	9.0
15	54.4	42.1	29.6	23.7	22.9	16.3	15.1	15.7	12.8	9.8	12.4	8.0	9.0

	6.7	6.3	5.9	5.6	5.3	5.0	4.8	4.5	4.3	4.2	4.0	3.8	3.7
	15	16	17	18	19	20	21	22	23	24	25	26	27
0	8.8	6.9	5.6	6.9	4.8	6.1	5.9	4.6	3.8	5.3	4.1	3.7	4.1
1	9.6	7.6	6.0	7.8	5.1	6.6	6.5	5.0	4.4	6.1	4.6	4.1	4.8
2	9.5	7.6	6.1	8.0	5.4	6.7	6.6	5.1	4.2	6.2	4.8	4.3	4.7
3	9.7	7.6	5.9	7.9	5.3	6.7	6.6	5.4	4.4	6.2	4.4	4.4	4.6
4	10.0	7.5	5.9	7.9	5.4	6.8	6.7	5.4	4.4	6.2	4.8	4.4	4.7
5	9.9	7.5	6.0	8.0	5.3	6.8	6.7	5.1	4.6	6.1	4.6	4.4	5.2
6	9.8	7.8	6.1	7.9	5.3	6.8	6.9	5.2	4.6	6.3	4.8	4.5	5.0
7	9.8	7.7	6.0	8.0	5.4	7.1	6.8	5.4	4.4	6.3	4.9	4.4	4.9
8	10.0	7.5	6.1	8.3	5.4	6.6	6.5	5.2	4.2	6.2	4.9	4.4	5.1
9	10.3	7.8	6.1	8.0	5.3	7.1	6.5	5.4	4.4	6.3	4.8	4.4	4.9
10	9.7	7.9	6.1	8.2	5.3	6.9	6.8	5.3	4.4	6.5	4.8	4.4	5.1
11	10.2	7.8	6.2	8.2	5.5	7.0	6.6	5.2	4.3	6.5	4.9	4.5	5.1
12	10.1	8.0	6.0	8.1	5.3	7.1	6.7	5.2	4.7	6.5	4.7	4.6	5.0
13	9.6	7.9	6.3	8.4	5.4	7.0	6.6	5.4	4.3	6.4	4.8	4.5	5.0
14	9.8	7.9	6.2	8.5	5.7	7.0	7.0	5.4	4.3	6.6	4.7	4.5	5.1
15	9.9	7.7	5.9	8.7	5.4	6.8	6.8	5.4	4.4	6.2	4.8	4.3	5.3

TABLE 7

Percentages of occurrence of the ratio $100p/h'$ *where* p *is the largest odd prime dividing* h, *and* h' *is the odd portion of* h

(*column X is for class numbers* $h = 2^k$ *for some* k)

FOR ODD DISCRIMINANTS

	100	33	20	14	11	9	7	6	5	4	3	2	1	X
0	40.3	21.0	9.7	4.8	7.8	1.8	1.0	3.3	0.6	2.5	2.5	1.2	1.0	2.4
1	35.4	19.4	9.9	5.5	8.1	2.4	1.5	4.2	1.2	3.6	3.3	2.2	2.2	1.2
2	33.8	18.6	9.5	5.7	8.0	2.6	1.7	4.3	1.5	4.1	3.6	2.7	3.0	1.0
3	32.7	18.2	9.5	5.8	7.8	2.7	1.8	4.4	1.6	4.3	3.8	3.0	3.4	0.9
4	32.0	17.9	9.4	5.7	7.7	2.8	1.9	4.5	1.7	4.5	4.0	3.2	4.0	0.7
5	31.4	17.6	9.3	5.6	7.6	2.8	2.0	4.5	1.8	4.6	4.0	3.5	4.5	0.7
6	30.9	17.3	9.4	5.7	7.6	2.9	2.0	4.5	2.0	4.7	4.1	3.6	4.7	0.6
7	30.5	17.1	9.2	5.8	7.5	2.9	2.0	4.6	2.0	4.8	4.2	3.8	5.1	0.6
8	30.4	17.1	9.0	5.7	7.5	3.0	2.0	4.5	2.0	4.8	4.3	3.8	5.3	0.5
9	30.0	16.8	9.0	5.8	7.4	2.9	2.1	4.6	2.2	4.9	4.3	3.9	5.6	0.5
10	29.7	16.8	8.8	5.8	7.4	3.0	2.1	4.5	2.1	5.0	4.4	4.0	5.8	0.5
11	29.3	16.6	9.0	5.7	7.4	3.0	2.1	4.5	2.2	5.0	4.3	4.1	6.1	0.5
12	29.2	16.5	8.8	5.7	7.3	3.0	2.1	4.6	2.2	5.0	4.4	4.2	6.3	0.5
13	28.9	16.4	8.8	5.7	7.2	3.0	2.2	4.6	2.3	5.1	4.4	4.3	6.6	0.5
14	28.9	16.3	8.7	5.7	7.2	3.1	2.2	4.6	2.4	5.0	4.5	4.3	6.6	0.4
15	28.7	16.2	8.7	5.7	7.2	3.1	2.1	4.6	2.3	5.2	4.5	4.4	6.8	0.4

TABLE 7 (*continued*)

FOR EVEN DISCRIMINANTS

	100	33	20	14	11	9	7	6	5	4	3	2	1	X
0	48.5	23.5	8.6	3.1	7.2	0.6	0.2	1.7	0.0	0.6	1.2	0.1	0.1	4.6
1	41.9	22.5	10.3	4.7	8.8	1.3	0.5	3.1	0.2	1.6	2.1	0.5	0.2	2.4
2	40.3	21.9	10.3	5.1	8.8	1.6	0.8	3.5	0.3	2.1	2.3	0.8	0.4	1.8
3	38.4	21.4	10.3	5.4	9.0	1.9	1.0	3.9	0.4	2.4	2.5	1.0	0.6	1.7
4	37.5	21.2	10.3	5.5	8.7	2.0	1.0	4.0	0.6	2.7	2.8	1.3	0.8	1.4
5	37.1	20.6	10.3	5.6	8.7	2.1	1.2	4.1	0.6	3.0	3.1	1.4	0.9	1.3
6	36.4	20.5	10.3	5.8	8.7	2.2	1.2	4.1	0.7	3.2	3.0	1.6	1.1	1.2
7	35.8	20.0	10.5	5.7	8.7	2.3	1.3	4.3	0.8	3.4	3.2	1.7	1.2	1.2
8	35.5	20.1	10.2	5.7	8.6	2.4	1.3	4.4	0.9	3.4	3.3	1.9	1.3	1.0
9	35.2	19.9	10.3	5.6	8.3	2.5	1.4	4.6	0.9	3.5	3.4	2.0	1.5	1.0
10	34.8	19.9	10.1	5.7	8.6	2.4	1.5	4.4	1.0	3.7	3.5	2.0	1.5	0.9
11	34.8	19.5	10.1	5.7	8.4	2.5	1.5	4.6	1.0	3.8	3.4	2.1	1.7	1.0
12	34.3	19.4	9.9	6.0	8.5	2.5	1.6	4.6	1.0	3.8	3.5	2.2	1.7	0.9
13	34.1	19.1	10.1	6.0	8.8	2.5	1.6	4.5	1.1	3.9	3.5	2.2	1.8	0.8
14	34.0	18.8	10.0	6.0	8.6	2.6	1.7	4.5	1.1	4.0	3.6	2.4	1.9	0.9
15	33.5	18.9	9.8	6.0	8.5	2.6	1.7	4.6	1.2	4.0	3.7	2.5	2.1	0.9

TABLE 8

Percentages of occurrence of the ratio $100p/h'$, *where* p *is the largest odd prime dividing* h, *and* h' *is the odd portion of* h

(*column X is for class numbers* $h = 2^k$ *for some* k)

FOR ODD DISCRIMINANTS WITH 2 GENERA

	100	33	20	14	11	9	7	6	5	4	3	2	1	X
0	38.4	21.1	10.5	5.5	8.8	1.9	1.0	3.8	0.5	2.6	2.7	1.1	0.6	1.6
1	32.8	18.5	10.2	6.4	8.2	2.9	1.8	5.0	1.2	4.3	3.8	2.5	1.8	0.6
2	31.4	17.7	9.4	6.4	7.9	3.1	2.1	4.9	1.7	5.0	4.1	3.0	2.7	0.5
3	30.2	17.2	9.4	6.3	7.7	3.3	2.2	4.9	1.9	5.3	4.4	3.5	3.3	0.4
4	29.8	16.7	9.1	5.9	7.7	3.4	2.3	4.9	2.1	5.4	4.4	3.8	4.1	0.3
5	28.9	16.4	9.1	6.0	7.3	3.3	2.5	5.0	2.2	5.6	4.4	4.1	4.7	0.3
6	28.2	16.3	9.1	6.0	7.3	3.4	2.6	5.0	2.4	5.5	4.5	4.4	5.0	0.3
7	28.1	15.8	8.8	6.1	7.2	3.4	2.5	5.0	2.5	5.6	4.7	4.5	5.6	0.3
8	28.1	15.9	8.7	5.8	7.0	3.5	2.5	4.8	2.5	5.7	4.8	4.6	5.8	0.3
9	27.4	15.6	8.6	6.1	7.1	3.4	2.6	4.8	2.7	5.7	4.9	4.9	6.1	0.2
10	27.4	15.6	8.4	6.0	6.9	3.5	2.6	4.7	2.7	5.7	4.9	4.8	6.5	0.2
11	27.1	15.4	8.5	5.9	7.1	3.3	2.6	4.6	2.9	5.8	4.7	5.0	6.9	0.2
12	26.9	15.2	8.5	5.8	6.8	3.3	2.5	4.9	2.9	5.8	4.8	5.2	7.2	0.2
13	26.3	15.3	8.3	5.8	6.9	3.4	2.6	4.9	2.8	5.8	4.9	5.3	7.4	0.2
14	26.3	15.1	8.3	5.8	6.8	3.5	2.6	4.8	3.0	5.7	5.1	5.2	7.4	0.2
15	26.5	15.0	8.3	5.8	6.7	3.3	2.5	4.8	2.8	6.0	4.9	5.4	7.8	0.2

FOR EVEN DISCRIMINANTS WITH 4 GENERA

	100	33	20	14	11	9	7	6	5	4	3	2	1	X
0	47.2	23.9	9.7	3.6	8.2	0.4	0.0	1.8	0.0	0.3	1.2	0.0	0.0	3.6
1	39.2	21.9	11.1	5.9	9.6	1.5	0.5	4.1	0.0	1.7	2.7	0.2	0.1	1.6
2	37.6	21.2	10.7	6.1	9.3	2.0	0.8	4.6	0.2	2.5	2.9	0.6	0.2	1.2
3	36.2	20.5	10.6	6.3	9.1	2.6	1.2	4.9	0.3	3.0	3.1	1.0	0.4	0.9
4	34.8	20.1	10.4	6.4	8.8	2.7	1.4	4.9	0.5	3.7	3.3	1.4	0.6	0.8
5	34.6	19.4	10.4	6.3	8.9	2.9	1.6	4.8	0.5	3.9	3.7	1.6	0.8	0.6
6	33.7	19.2	10.1	6.6	8.7	2.9	1.6	5.0	0.6	4.3	3.6	1.9	1.0	0.8
7	33.0	19.1	10.5	6.2	8.6	3.0	1.8	5.0	0.9	4.4	3.6	2.2	1.1	0.7
8	32.7	18.8	10.1	6.4	8.5	3.0	1.8	5.1	1.0	4.5	3.9	2.4	1.2	0.6
9	32.8	18.5	10.2	6.2	8.2	3.2	2.0	5.3	1.1	4.5	3.7	2.5	1.4	0.6
10	32.2	18.8	9.8	6.0	8.4	3.1	2.0	5.0	1.2	4.7	3.9	2.5	1.6	0.6
11	31.8	18.4	9.8	6.1	8.3	3.2	2.0	5.3	1.3	4.9	3.9	2.8	1.6	0.5
12	31.9	18.1	9.6	6.3	8.2	3.2	2.2	5.2	1.3	4.9	4.0	3.0	1.8	0.5
13	31.5	17.6	10.0	6.4	8.5	3.1	2.3	5.0	1.4	5.0	3.9	2.9	1.8	0.5
14	31.1	17.6	9.6	6.5	8.4	3.2	2.2	5.1	1.5	5.1	4.1	3.2	2.0	0.4
15	31.1	17.4	9.7	6.3	8.3	3.2	2.2	5.0	1.6	5.0	4.3	3.4	2.1	0.4

TABLE 9

Actual and Random ratios for FPG values for odd discriminants with 2 genera and even discriminants with 4 genera between -15800000 *and* -16000000

ALL ODD	100	33	20	14	11	9
ACTUAL	26.8	15.0	8.2	5.7	6.6	3.1
RANDOM	30.1	11.8	7.6	5.5	4.6	3.7
SUBSET ODD						
ACTUAL	27.4	15.3	8.1	5.8	6.6	3.1
RANDOM	32.4	12.6	8.2	6.0	5.1	3.8
ALL EVEN						
ACTUAL	31.2	17.2	9.5	6.6	9.1	3.1
RANDOM	35.6	14.3	9.0	6.3	5.8	3.9
SUBSET EVEN						
ACTUAL	31.2	17.5	9.6	6.5	8.6	3.1
RANDOM	37.0	15.2	9.6	6.9	6.0	3.9

The computation of class numbers and of class groups was performed in a manner similar to that of [BUEL76], working with discriminants $-N$ in a range of 200000 at a time. All the graphs use these data for blocks of 200000 at a time. To make the tables more concise, however, we have collected these original data for blocks of one million integers at a time. Except in Table 2, each line in the tables is data on class numbers for discriminants in the interval $-1000000n$ to $-1000000(n+1)$. This is the "run count" n in the various tables. (In Table 2, each "run count" covers discriminants in the interval $-200000n$ to $-200000(n+1)$.) In Table 1, we present the largest and smallest values of h and of FPG (the number of forms per genus) in each block of one million integers. In each such block there were about 10100 even and 20200 odd fundamental discriminants, that is, discriminants of quadratic forms which are also discriminants of imaginary quadratic number fields.

5.1. *Noncyclic Class Groups.* In Table 2 we present the percentages of noncyclic p-Sylow subgroups for small p, remarking as in [BUEL76] that "noncyclic" has a special meaning. For odd p, a class group is considered noncyclic if it is indeed noncyclic. Some of the structure of the 2-SSG is dictated by the factoring of the discriminant into primes, however. The 2-SSG was considered noncyclic if the 2-SSG of the subgroup of squares in the class group was noncyclic. As can be seen from the table, most of the class groups are as cyclic as they can be, although there is a small growth in the percentage of noncyclic groups. From the point of view of the CPS factoring method, this is not a particularly good sign.

5.2. *Divisibility of h by Small Primes.* In this and the next subsection, we shall consider the empirical evidence to support the assumption of Section 3, that class numbers "look like" ordinary integers of corresponding size. One key consideration in this assumption and in the practical implementation of the CPS method is the

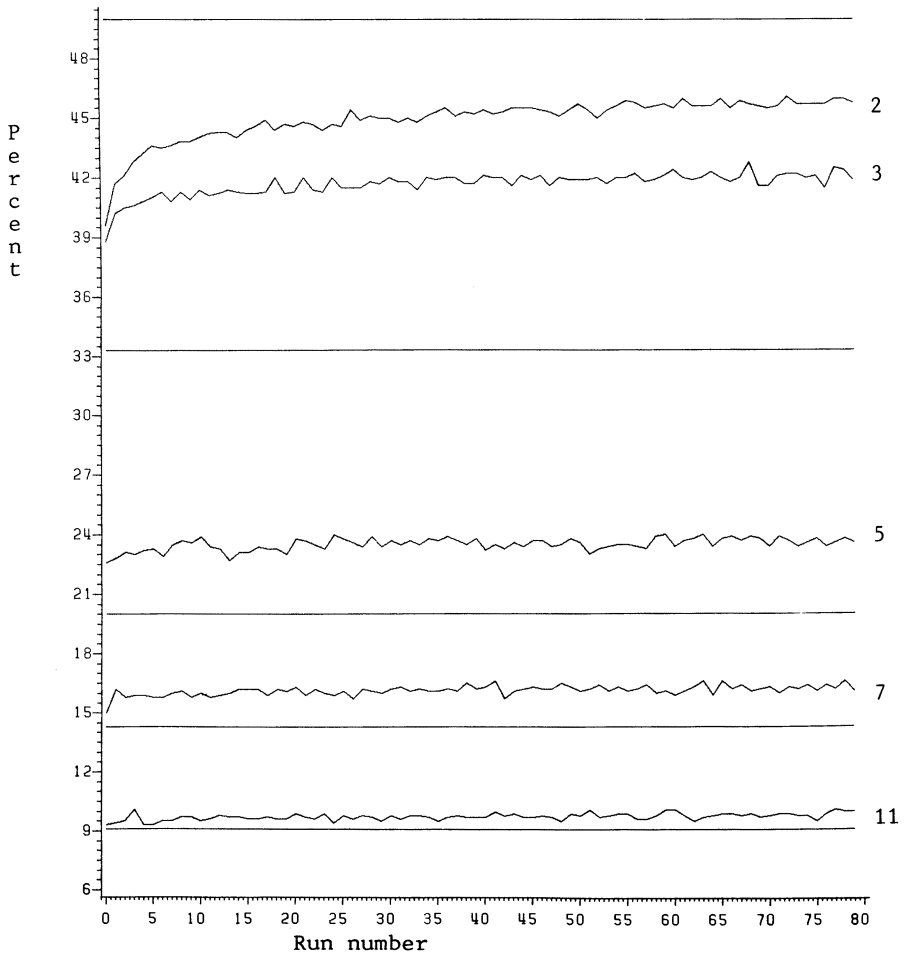

FIGURE 1: *Div. of FPG by* 2, 3, 5, 7, 11 (*all odd discs.*)

divisibility of h by small primes. Leopold observed (cited in [ZIMM72]) that class numbers were divisible by small primes p more often than $1/p$ of the time. Canfield, Erdös, and Pomerance proved the following [POMEb]:

Let $P(n, v) = \#\{x \leqslant n: x \text{ is free of primes} > v\}$. Then $P(n, n^{1/r})/n = r^{-r+o(r)}$, provided $n^{1/r} \geqslant (\log n)^{1+e}$, $e > 0$ fixed.

We present, in Tables 3 through 6, our results on the divisibility of class numbers by "small" integers. We table the statistics for all discriminants and for odd discriminants $-N$ and even discriminants $-4N$ for N a product of two primes. To illustrate these tables, we present Figures 1 and 2 as sample graphs. We graph the expected (straight line) and actual (broken line) values, and observe:

1. For an odd prime p, p^n divides h with a frequency of about

$$((p+1)/p^2)(1/p^{n-1}).$$

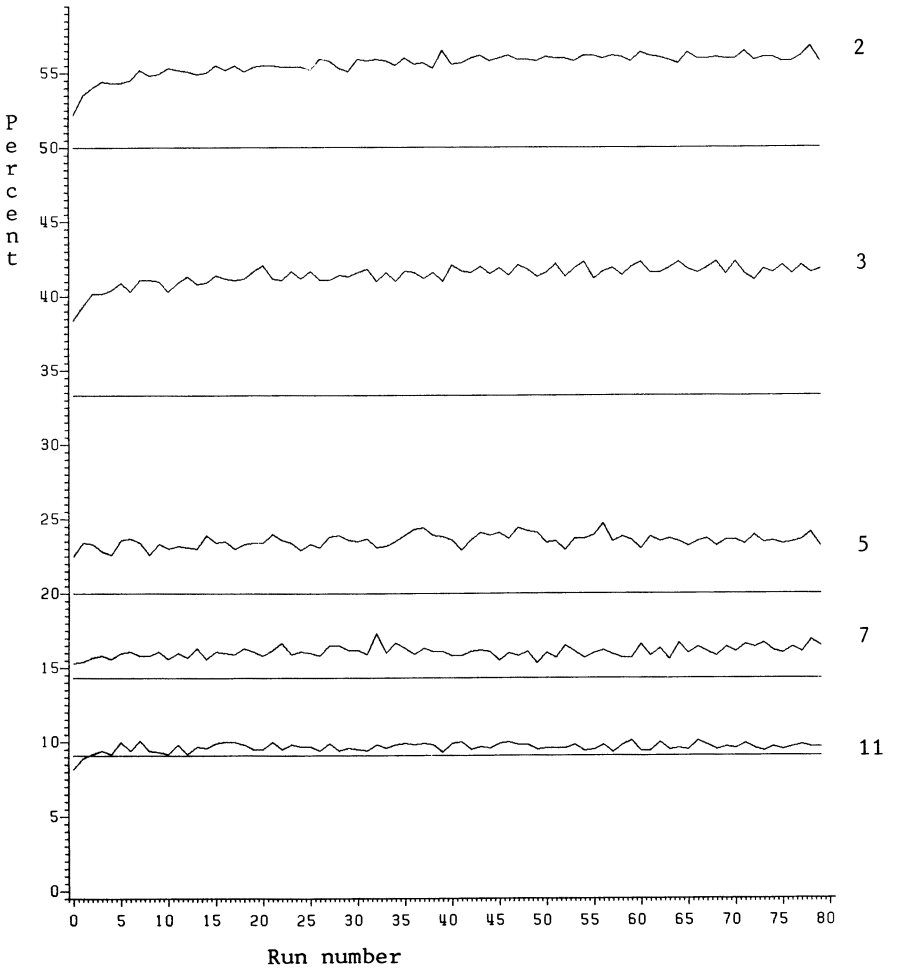

FIGURE 2: *Div. of FPG by* 2, 3, 5, 7, 11 (*all even discs.*)

2. Some sort of loose multiplicativity exists. If primes p and q divide h with frequencies Fp and Fq, respectively, then pq divides h with frequency about $FpFq$.

3. We offer at least the conjecture that an odd prime p divides class numbers with a frequency whose main term resembles $(p + 1)/p^2$.

4. With regard to the difference between even and odd discriminants, it appears that class numbers for even discriminants have decidedly more twos in them than do class numbers for odd discriminants. This holds for discriminants of comparable size, for radicands $-N$ of comparable size (so that the discriminants are $-N$ and $-4N$), and for class numbers of comparable size.

5.3. *The Size of the Largest Prime Factor Dividing h.* In the previous subsection we saw that class numbers are more often divisible by small primes than are random integers. In this subsection we carry this sort of question one step further. If the CPS method is to work in the first stage, the largest prime dividing the class number must

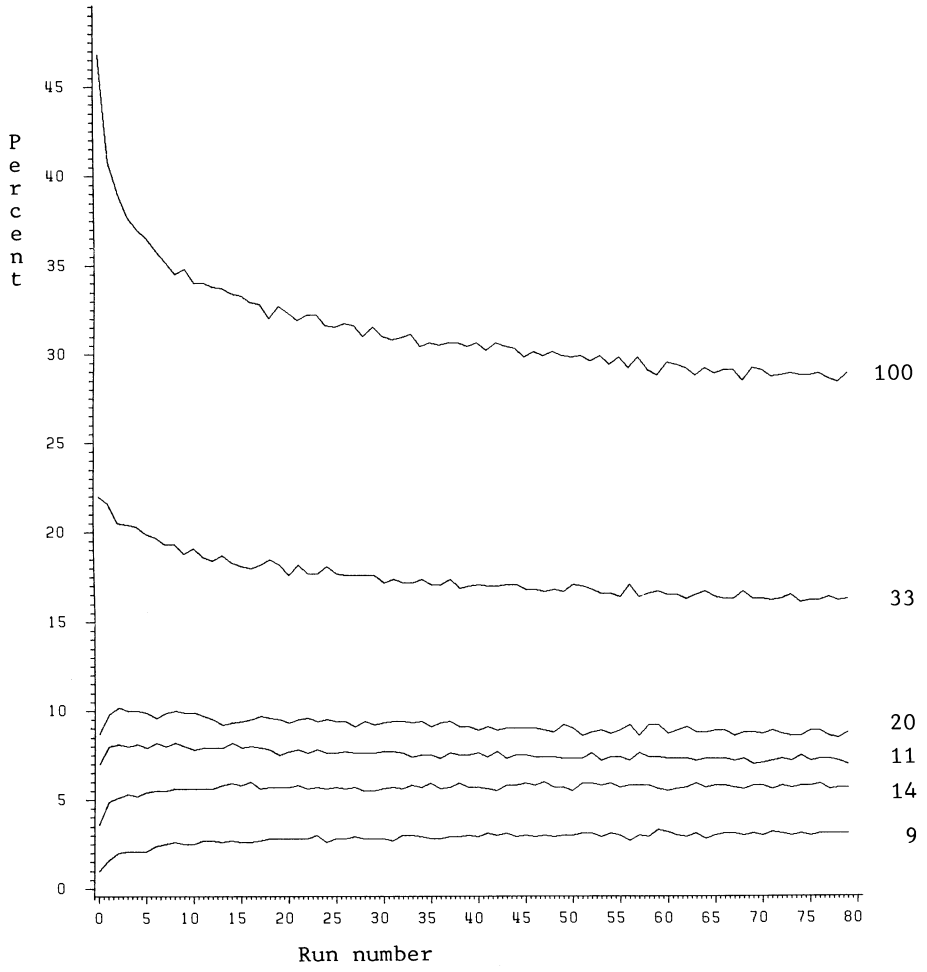

FIGURE 3: *Ratios* 100, 33, 20, 14, 11, 9 (*all odd discs.*)

be "small" relative to the size of the class number itself. In Tables 7 and 8 and Figures 3 and 4 we display the values of 100 times the ratio of the largest odd prime dividing the class number to the odd part of the class number. That is, if the class number $h = 2^k h'$, with h' odd, this ratio would be 100 if h' were a prime, 33 if it were three times a prime, and so forth. (These values were computed as $100p/h'$ in VS FORTRAN integer arithmetic.) At first glance, it seems that the largest prime dividing the class number is normally quite large by comparison with the class number. This is somewhat deceptive, however, since class numbers are small in this range and primes are fairly dense. For example, in the interval 1 to 100, there are 9 integers such that the ratio of the largest odd prime to the odd portion of the integer is 1/5. (These are 25, 35, 55, 65, 85, 95, 50, 70, and 100.) One would then expect 9% of "random" integers between 1 and 100 to have ratio 20 in this sort of table.

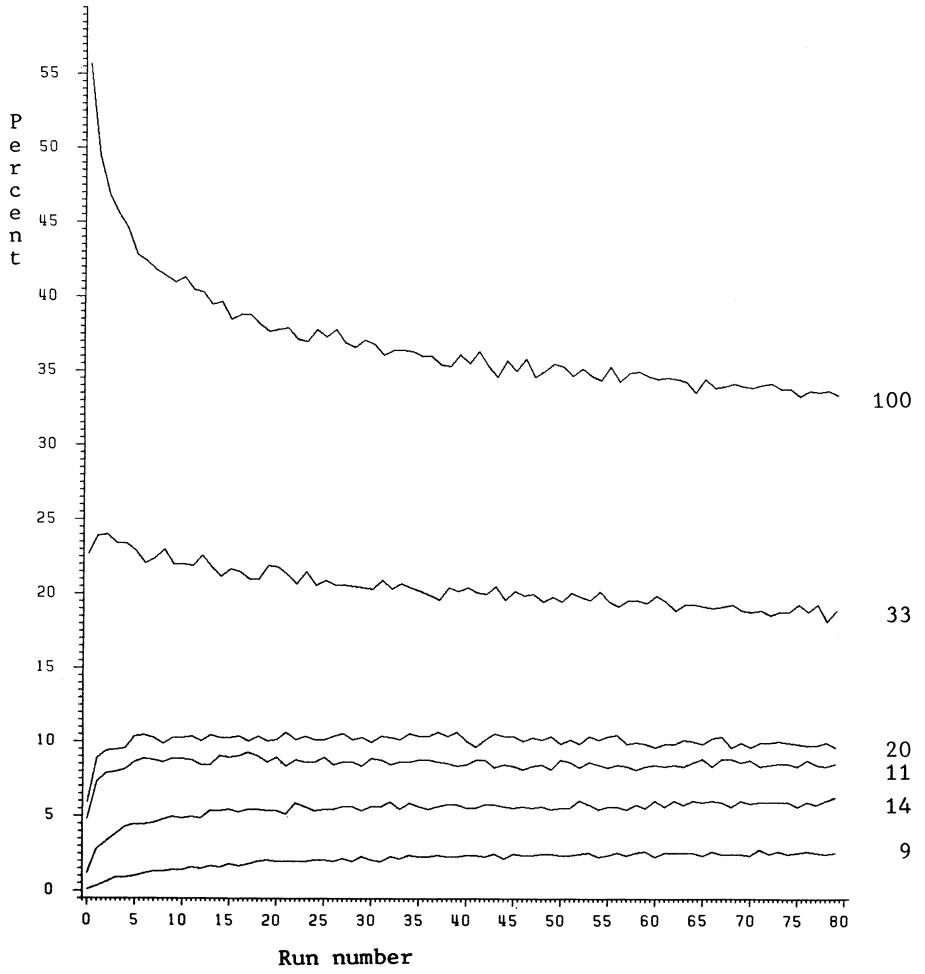

FIGURE 4: *Ratios* 100, 33, 20, 14, 11, 9 (*all even discs.*)

For the discriminants in the range -15800000 to -16000000, then, we present a closer analysis of these ratios. This is Table 9. We first present the observed and expected frequencies of occurrence of the various ratios. Then, based on the examination of the distribution of the class numbers, we have taken a subset of these data. A graph of the distribution of class numbers for odd discriminants in this interval appears as Figure 5. It shows that class numbers are not evenly distributed, but obey some sort of gamma-distribution [MOOD]. We have, therefore, taken as a subset those class numbers which lie within one standard deviation of the mean, and presented the observed and expected frequencies of occurrence of the ratios. The data in the table are inconclusive. Although ratios are more often 100 in the subset than random, no other patterns seem marked enough to allow for inferences to be made. The evidence about divisibility seems convincing; this is not the case for the data on ratios.

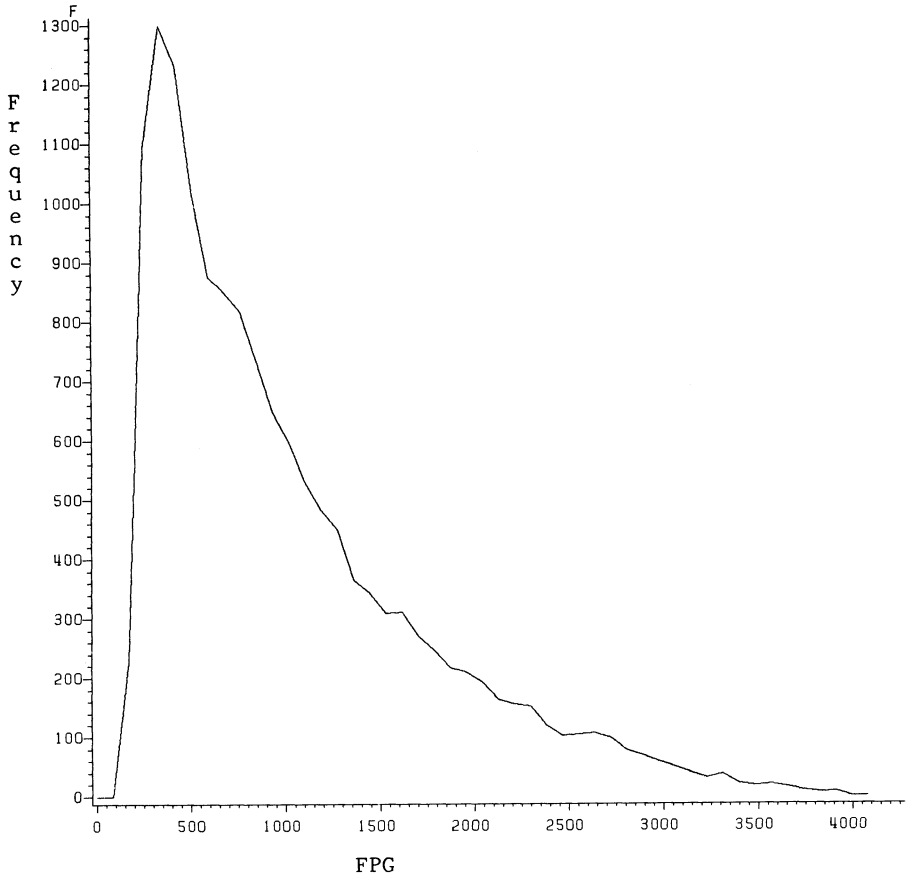

FIGURE 5: *FPG frequencies, odd discs. with* 2 *genera*

6. Summary / Conclusions. An appealing new factoring method has been proposed that relies for its effectiveness on the expectation that class numbers of imaginary quadratic fields are at least as composite as random integers of comparable size. A study of actual class numbers seems to indicate that they may actually be *more* composite than random. The data indicate that efforts should be made to overcome some serious implementation problems with this new method.

7. Acknowledgement. All computing mentioned in this paper was done on the IBM 3033N computer at the System Network Computing Center, Louisiana State University, Baton Rouge, Louisiana.

Computer Science Department
Louisiana State University
Baton Rouge, Louisiana 70803

[BRIL] JOHN BRILLHART, D. H. LEHMER, J. L. SELFRIDGE, B. TUCKERMAN & S. S. WAGSTAFF, JR., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$, *up to High Powers*, Contemporary Math., Vol. 22, Amer. Math. Soc., Providence, R. I., 1983.

[BUEL76] DUNCAN A. BUELL, "Class groups of quadratic fields," *Math. Comp.*, v. 30, 1976, pp. 610–623.

[KNUT] DONALD KNUTH, *The Art of Computer Programming*, 2nd ed., Vol. 2, Addison-Wesley, Reading, Mass., 1981, p. 323.

[MOOD] ALEXANDER M. MOOD & FRANKLIN A. GRAYBILL, *Introduction to the Theory of Statistics*, 2nd ed., McGraw-Hill, New York, 1963, pp. 126–129.

[POMEa] CARL POMERANCE, private communication.

[POMEb] CARL POMERANCE, "Analysis and comparison of some integer factoring methods," *Computational Methods in Number Theory* (H. W. Lenstra, Jr., R. Tijdeman, eds.), Math. Centrum, Amsterdam, 1982.

[POMEc] CARL POMERANCE & SAMUEL S. WAGSTAFF, JR., "Implementation of the continued fraction integer factoring algorithm." (To appear.)

[SCHN] C. P. SCHNORR & H. W. LENSTRA, JR., "A Monte Carlo factoring algorithm with finite storage." (To appear.) (Extended abstract appears in *Lecture Notes in Comput. Sci.*, Vol. 145, Springer-Verlag, New York, pp. 19–34.)

[SHAN] DANIEL SHANKS, *Class Number, A Theory of Factorization, and Genera*, Proc. Sympos. Pure Math., Vol. 20, Amer. Math. Soc., Providence, R. I., 1971, pp. 415–440.

[ZIMM72] H. G. ZIMMER, *Computational Problems, Methods, and Results in Algebraic Number Theory*, Lecture Notes in Math., Vol. 262, Springer-Verlag, New York, 1972.