Heuristics on Class Groups

by

H. Cohen and H.W. Lenstra, Jr.

§1 Experimental facts.

This work was motivated by the desire to understand some experimental observations about class groups of quadratic fields; these observations were made long ago, and confirmed by the most extensive tables known to us, i.e. Buell [1] for imaginary quadratic fields, and Shanks and Williams [5] for real quadratic fields. They are as follows:

(A) If p is a small odd prime, the proportion of imaginary quadratic fields whose class number $h(D)$ is divisible by p is significantly greater than $1/p$. For example for $p = 3$ it is around 43% instead of the expected 33.3%, for $p = 5$ around 23.5% instead of 20% etc.

(B) If one looks only at the odd part of the class group, cyclic groups seem to form the overwhelming majority. In fact, it is quite difficult to find class groups with, say 3-rank greater than or equal to 3, and no examples are known of 3-rank greater than 5.

(C) For real quadratic fields $\mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \bmod 4$ prime, it is conjectured than an infinite number of them have class number 1, and in fact experimental evidence seems to show that there is a definite nonzero proportion ρ of fields $\mathbb{Q}(\sqrt{p})$ of class number 1. A rough extrapolation of known data seems to give $\rho \approx 76\%$.

The work we are about to describe gives quantitative heuristic explana-

/

tions of all these observations and of many more, including for higher degree fields. For example, for imaginary quadratic fields we predict that $p|h(D)$ with approximate probability 43.987% for $p = 3$, 23.967% for $p = 5$. For real quadratic fields the proportion ρ of class number 1 should be approximately 75.446%.

A more detailed version of this paper including complete proofs and extra material will be published elsewhere.

§2 Heuristic assumptions

The basic clue comes from experimental fact (B). Let us consider a specific example: assume that the 3-part of the class group of an imaginary quadratic field has cardinality 9. Then up to isomorphism, only the two groups $\mathbb{Z}/9\mathbb{Z}$ and $(\mathbb{Z}/3\mathbb{Z})^2$ can occur. However, tables show that $(\mathbb{Z}/3\mathbb{Z})^2$ occurs much more rarely. Why?

One answer is that the automorphism group of a cyclic group is smaller than the automorphism group of any other abelian group of the same cardinality. In our example, $\#\mathrm{Aut}\ \mathbb{Z}/9\mathbb{Z} = 6$ while $\#\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})^2 = 48$. The basic heuristic assumption is thus that isomorphism classes of abelian groups G have a "weight" proportional to $1/\#\mathrm{Aut}\ G$. This is similar to many "mass formulas" in other parts of mathematics where the proper weight is indeed the inverse of the number of automorphisms.

For our example this agrees quite well with the tables since the ratio of occurrence of $\mathbb{Z}/9\mathbb{Z}$ versus $(\mathbb{Z}/3\mathbb{Z})^2$ is close to 8 to 1.

Another way of stating our assumption is as follows: let E be an abstract set with n elements. It can easily be shown that the number of abelian group structures on E which are isomorphic to G

is equal to $n!/\#\mathrm{Aut}\ G$. Hence for a given order n, weighting isomorphism classes of abelian groups with weight proportional to $1/\#\mathrm{Aut}\ G$ is equivalent to giving equal weight to each abelian group structure.

We are thus led to the following assumption. Let f be a function defined on the isomorphism classes of finite abelian groups of odd order. We define the average of f by

$$M(f) = \lim_{x\to\infty} \frac{\Sigma_{|D|\le x} f(\mathcal{J}_{odd}(D))}{\Sigma_{|D|\le x} 1} \quad \text{if the limit exists,}$$

where D goes through the sequence of negative fundamental discriminants, $\mathcal{J}(D)$ is the class group of $\mathbb{Q}(\sqrt{D})$, and for every abelian group G, G_{odd} denotes the odd part of G. If f is the characteristic function of a property $\mathcal{P}$, we call $M(f)$ the probability that $\mathcal{P}$ holds. The assumption is then as follows:

Heuristic assumption 1:

$$M(f) = \lim_{x\to\infty} \frac{\Sigma_{\#G\le x} f(G_{odd})/\#\mathrm{Aut}\ G}{\Sigma_{\#G\le x} 1/\#\mathrm{Aut}\ G}$$

where the sums are to be taken over isomorphism classes of abelian groups G of cardinality less than or equal to x.

Remarks 1) We restrict to the odd part of the class groups since the even part is certainly not random because of genus theory and the theory of ambiguous classes.

2) It could very well be argued that one could replace the weighting factor $1/\#\mathrm{Aut}\ G$ by a factor of the form $\psi(\#G)/\#\mathrm{Aut}\ G$, where ψ is a smooth function. However it can be shown that for a very wide

class of functions ψ including for instance the nonzero polynomials, the limit of

$$(\Sigma_{\#G\leq x} f(G_{odd})\psi(\#G)/\#\mathrm{Aut}\ G)/(\Sigma_{\#G\leq x}\psi(\#G)/\#\mathrm{Aut}\ G)$$

is independent of ψ, so there is not much loss in generality in assuming $\psi = 1$.

§3 Some algebraic and analytic results

To be able to use our heuristic assumption 1 above, we need to have a number of algebraic and analytic results.

The key algebraic result which we need is the following:

Theorem 3.1: Let K and C be finite abelian groups. Then

$$\Sigma_{G \text{ up to isomorphism}} \#[G_1 \text{ subgroup of } G: G_1 \cong K \text{ and } G/G_1 \cong C]/\#\mathrm{Aut}\ G = 1/(\#\mathrm{Aut}\ K\ \#\mathrm{Aut}\ C)$$

We now set

$$w(n) = \Sigma_{\substack{G \text{ up to isomorphism} \\ \#G=n}} 1/\#\mathrm{Aut}\ G$$

We can obtain from theorem 3.1 the following properties of the function $w(n)$:

Theorem 3.2:

(i) $\Sigma_{d|n} w(d) = nw(n)$

(ii) $\Sigma_{n\geq 1} w(n)n^{-s} = \zeta(s+1)\zeta(s+2)\ldots$

(iii) $w(n) = \prod_{p^\alpha \| n} (p^\alpha(1-\frac{1}{p})(1-\frac{1}{p^2})\ldots(1-\frac{1}{p^\alpha}))^{-1}$

(This last formula is due to Hall, 1938.)

(iv) $\Sigma_{n\leq x} w(n) = C_\infty \log x + D_\infty + O(\frac{\log x}{x})$

where $C_\infty = \zeta(2)\zeta(3)\ldots = 2.294856589\ldots$ and D_∞ is an explicit constant.

It follows from this theorem that there exist positive constants A and B such that

$$A/\varphi(n) \leq w(n) \leq B/\varphi(n).$$

Remark: The constant C_∞ is well known to be the average number of abelian groups of a given order. However it occurs in that context as the residue at $s = 1$ of the function $\zeta(s)\zeta(2s)\zeta(3s)\ldots$, which is quite a different function from the function $\zeta(s+1)\zeta(s+2)\ldots$.

§4 Sample averages for imaginary quadratic fields

It is now a fairly straightforward matter to obtain averages of interesting functions for imaginary quadratic fields. We give here a few sample results (holding of course only with our heuristic assumption 1).

a) The probability that the odd part of the class group is cyclic is

$$\zeta(2)\zeta(3)/(\zeta(6)\, C_\infty\, 3\, (1-\tfrac{1}{2})(1-\tfrac{1}{2^2})\ldots) = 97.757\%$$

approximately. This seems very large, but agrees with table counts.

b) If p is an odd prime, the probability that p divides the class number is

$$1 - (1-\tfrac{1}{p})(1-\tfrac{1}{p^2})\ldots = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^5} - \frac{1}{p^7} + \frac{1}{p^{12}} + \frac{1}{p^{15}} - \ldots .$$

This gives 43.987% for $p = 3$, 23.967% for $p = 5$ etc.

c) If e is a fixed odd integer, the average number of elements of order exactly e in the class group is 1.

d) Write $r_p(G)$ for the p-rank of an abelian group G. Then if p is an odd prime, the probability that the p-rank of the class group be equal to a given integer r is

$$p^{-r^2}(1-\tfrac{1}{p})(1-\tfrac{1}{p^2})\ldots/(1-\tfrac{1}{p})^2(1-\tfrac{1}{p^2})^2\ldots(1-\tfrac{1}{p^r})^2.$$

This decreases very rapidly as r increases, and helps to explain why no examples of p-rank greater than 5 have been found.

e) The average of $p^{r_p(\mathcal{H}(D))}$ is 2. The average of $p^{2r_p(\mathcal{H}(D))}$ is $p + 3$.

The first of these results is particularly significant, because by a theorem of Davenport and Heilbronn [2], it is known that the average of $3^{r_3(\mathcal{H}(D))}$ is 2.

f) If one is interested in results concerning nonfundamental discriminants, one can use the well known formula

$$h(Df^2) = h(D)f\prod_{p|f}(1 - (\tfrac{D}{p})/p)$$

where D is a negative fundamental discriminant, to obtain heuristic results about class numbers. For example the probability that p divides the class number is approximately 52.4664% for $p = 3$; 24.130% for $p = 5$.

§5 Real quadratic fields.

Since the class groups of real quadratic fields behave quite differently from the class groups of imaginary quadratic fields, it is

clear that a new heuristic assumption is necessary. In plain English, it is as follows: if we assume isomorphism classes of groups G weighted by $1/\#\mathrm{Aut}\ G$, our first heuristic assumption was that the odd part of the class group of imaginary quadratic fields was "random". For real quadratic fields, we will assume that the odd part of the class group is of the form $G/\langle g\rangle$ where G is "random" as above, and g is a "random" element in G ($\langle g\rangle$ is the cyclic subgroup generated by g). With a similar definition of $M(f)$, the assumption is as follows:

Heuristic assumption 2:

$$M(f) = \lim_{x\to\infty} \frac{\sum_{\#G\le x} \frac{1}{\#G} \sum_{g\in G} f((G/\langle g\rangle)_{\mathrm{odd}})/\#\mathrm{Aut}\ G}{\sum_{\#G\le x} 1/\#\mathrm{Aut}\ G}.$$

It is not very easy to give good justifications for this assumption. We will give two. The first one has been suggested to us by B. Gross. Let O_D be the ring of integers of $\mathbb{Q}(\sqrt{D})$, where D is a negative fundamental discriminant, and let p be a fixed prime which splits in O_D $(p) = \beta\cdot\bar{\beta}$. Then the class group of $O_D[1/p]$ is easily seen to be equal to $\mathcal{H}(D)/\langle\beta\rangle$. Now, as for real quadratic fields the unit rank of $O_D[1/p]$ is equal to 1, and a table of such class groups reveals a striking resemblance to tables of class groups of real quadratic fields.

The second justification can be considered essentially as due to Gauss, but with deeper insight by D. Shanks [4]. It is well known that there is a multiplication on quadratic forms of equal discriminant called composition. This law is not quite a group law on the set of reduced forms since first of all the product of two reduced forms is not reduced, and second the law is not associative. However in a certain sense which we cannot make precise here it is "almost" a group law

/

[3] [4]. On the other hand the set of reduced forms divides itself under the reduction operation into cycles, and the number of such cycles is the class number. Furthermore these cycles can have different number of forms, but they have the same "length" (essentially the regulator) if an appropriate notion of distance is defined [3], [4]. Finally, in [4] Shanks shows that the principal cycle, although not a group, displays a cyclic-group-like structure. Thus, although it does not quite make much sense, it is tempting to interpret the equation $h = hR/R$ by saying that the class group of a real quadratic field is the quotient of the "group" of reduced forms by the "cyclic subgroup" formed by the principal cycle.

Anyway, if we assume heuristic assumption 2, essentially all the necessary algebraic and analytic results have already been obtained in the imaginary quadratic case. This allows us to obtain the following sample results:

a) The probability that the odd part of the class group is isomorphic to L (where L is a given group of odd order) is

$$(\#L\#\mathrm{Aut}\ L\ C_\infty(1-\frac{1}{2^2})(1-\frac{1}{2^3}\ldots)^{-1}$$

In particular the probability that it is of order ℓ (ℓ odd) is

$$w(\ell)/(\ell\ C_\infty(1-\frac{1}{2^2})(1-\frac{1}{2^3})\ldots).$$

This gives approximately 75.446% for $\ell = 1$, 12.574% for $\ell = 3$, 3.772% for $\ell = 5$ etc.

b) The probability that p divides the class number (p odd prime) is

$$1 - (1-\frac{1}{p^2})(1-\frac{1}{p^3})\ldots = \frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} - \frac{1}{p^7} - \frac{1}{p^8} - \ldots .$$

c) If e is a fixed odd integer the average number of elements of order exactly e in the class group is $1/e$.

d) If p is an odd prime, the probability that the p-rank of the class group is equal to a given integer r is

$$p^{-r(r+1)}(1-\frac{1}{p})(1-\frac{1}{p^2})\ldots/(1-\frac{1}{p})^2(1-\frac{1}{p^2})^2\ldots(1-\frac{1}{p^r})^2(1-\frac{1}{p^{r+1}}).$$

e) The average of $p^{r_p(\mathcal{H}(D))}$ is $1 + 1/p$. The average of $p^{2r_p(\mathcal{H}(D))}$ is $2 + 1/p + 1/p^2$.

As in the imaginary case, the first of these results is particularly significant because by a theorem of Davenport and Heilbronn [2], it is known that the average of $3^{r_3(\mathcal{H}(D))}$ is $4/3$.

§6 Higher degree fields.

We consider only the case of cyclic extensions of $\mathbb{Q}$ of prime degree p. Let $\Gamma = \langle\sigma\rangle$ be the Galois group. It is clear that the class group is a $\mathbb{Z}[\Gamma]$-module, and even a $\mathbb{Z}[\Gamma]/(1+\sigma+\ldots+\sigma^{p-1})$-module, since the norm of an ideal is principal. But this last ring is isomorphic to $\mathbb{Z}[\zeta_p]$ where ζ_p is a primitive p-th root of unity, and this is a Dedekind domain, and even a principal ideal domain if $p \leq 19$. It can then be shown that all the theory above can be generalized to this case, the Riemann zeta function being simply replaced by the Dedekind zeta function of the field $\mathbb{Q}(\zeta_p)$.

The heuristic assumption is that the prime to p part of the class group behaves like $G/\langle g\rangle$, where G is a "random" finite $\mathbb{Z}[\zeta_p]$-module (weighted with $1/\#\mathrm{Aut}_\Gamma G$) and $\langle g\rangle$ is the cyclic $\mathbb{Z}[\zeta_p]$-module

/

generated by a random element in G. Note that although the unit rank of a typical field is $p - 1$ if $p \geq 3$, as a $\mathbb{Z}[\zeta_p]$-module the unit rank is still equal to 1. (If the unit rank is equal to u it seems reasonable to consider $G/\langle g_1, \ldots, g_u \rangle$).

We give two examples for cyclic cubic fields:

a) The probability that the prime to 3 part of the class group is equal to 1 is approximately 85.0%.

b) The probability that 4 divides the class number is approximately 8.195%. (Remark: it is easy to show that if 2 divides the class number, then 4 also divides it.)

§7 Concluding remarks.

All the above heuristics agree very closely with available tables, and furthermore they agree exactly with the theorems of Davenport and Heilbronn. This seems to give strong support for the validity of our heuristic assumptions.

Extensions of this work in several different directions are under way. Also it would be interesting to know if similar heuristic estimates can be made in different contexts, for example for Tate-Shafarevitch groups of a given elliptic curve twisted by quadratic characters.

Finally it is a pleasure to thank our friends and colleagues B. Gross, D. Shanks and L. Washington for interesting discussions on this subject.

Bibliography

[1] D. Buell, Class groups of quadratic fields, Math. Comp. v. 30, 1976, pp. 610-623.

[2] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, Proc. Royal. Soc., A, 322 (1971), 405-420.

[3] H.W. Lenstra, Jr., On the calculation of regulators and class numbers of quadratic fields, pp. 123-150 in J.V. Armitage (ed.), Journees Arithmetiques 1980, London Math. Soc. Lecture Notes Series 56, Cambridge University Press, 1982.

[4] D. Shanks, The infrastructure of a real quadratic field and its applications, Proc. 1972 number theory conference, Boulder, 1972.

[5] D. Shanks, H. Williams, in preparation.

H. Cohen, L.A. au C.N.R.S. n°226,
UER de Mathematiques et Informatique
Universite de Bordeaux I
351, Cours de la Liberation
33405 Talence, FRANCE

H.W. Lenstra, Jr.
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam
the NETHERLANDS