Chapter 8

Miscellaneous Facts II

We shall consider in this chapter some basic topics, some of which are clearly interrelated.

First, there are heuristic conjectures by Cohen and Lenstra [COHE84] that, if true, would explain why class numbers and class groups do not appear to be "random" numbers and groups, but have decidedly special properties, among them the strong tendency of the groups to be cyclic.

We shall also present a computational technique for decomposing the finite abelian class groups into their cyclic factors. This technique is successful, in part, because of the observed special nature of class groups.

Also presented will be some results giving conditions under which class numbers possess certain congruence conditions for odd prime moduli, for example, conditions under which there exist elements of order 3 in the group.

In contrast with producing elements of order 2 in class groups, which can be done by choosing highly composite fundamental discriminants, for example, there is no effective way to generate class groups with a large number of elements of a fixed odd order. There has been substan-

tial effort and computation, however, to search for class groups with a large rank in the p-Sylow subgroup for odd primes p. As is evident from the conjectures of the Cohen-Lenstra heuristics, such a search is less likely to succeed the larger the prime p, and most of the effort has gone toward finding class groups of large rank in the 3-Sylow and the 5-Sylow subgroup.

Finally, there is the obvious tantalizing question as to whether there is or should be any connection between the class groups of positive and negative discriminant with similar discriminants. A partial answer has been given by Scholz.

As in the earlier chapter on miscellaneous facts, some of the commentary may involve mathematics which is deeper than the rest of this work. We trust the astute reader can skim the commentary; the statements of the results should be readily comprehensible.

8.2 Decomposing Class Groups

Class groups of forms are finite abelian groups, and we can apply the decomposition theorem for such groups, which we stated in one form in Chapter 4 and which we restate here in a different form.

Theorem. *Let $\mathcal{G}$ be a finite abelian group, written multiplicatively, and let $C(r)$ denote a cyclic group of order r. $\mathcal{G}$ can be written as a direct product of groups of prime power order,*

$$\mathcal{G} = \mathcal{S}_{p_1} \times \mathcal{S}_{p_2} \times \cdots \times \mathcal{S}_{p_k},$$

in which each group $\mathcal{S}_{p_i}$ is of order some power of p_i and is a direct product of cyclic groups each of order some power of p_i:

$$\mathcal{S}_{p_i} = C(p_i^{\alpha_1}) \times C(p_i^{\alpha_2}) \times \cdots \times C(p_i^{\alpha_l}),$$

where we may choose $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_l$.

In any group $\mathcal{G}$ of order $h = p^k h'$ with p prime and not dividing h', the set $\mathcal{S} = \{f^{h'} : f \in \mathcal{G}\}$ is a subgroup of order p^k called the *p-Sylow subgroup*. Our decomposition technique for class groups will actually work for any finite abelian group, but is more effective for class groups than for groups in general because of certain specific characteristics of class groups. The approach outlined here is the one used in both computations by Buell [BUEL76] and [BUEL87a], and is derived from the suggestions about computations in class groups made by Shanks [SHAN69] and conveyed to Buell by A. O. L. Atkin.

We decompose the group one p-Sylow subgroup at a time. An initial step is to determine whether it is possible for the p-Sylow subgroup to be noncyclic. For odd primes p, we must have at least p^2 dividing h.

For the prime 2, we must have at least 4 genera and at least a factor of 16 in the class number (at least a factor of 4 in the number of forms per genus). This is because some basic group structure is inherited from the structure of the genera–a discriminant with k generic characters has exactly $k-1$ cyclic factors of order some power of 2. It is thus customary, in describing "noncyclic" groups, to consider the 2-Sylow subgroup to be noncyclic if and only if the subgroup of squares (that is, the principal genus) is noncyclic. By squaring, any cyclic factors of order 2 disappear. A "minimally noncyclic" 2-Sylow subgroup is thus a subgroup of the form $\mathcal{C}(4) \times \mathcal{C}(4)$.

Having determined that the class number h is sufficiently composite that some p-Sylow subgroup might be noncyclic, we then, for each such prime p, choose a few (perhaps a dozen) forms f at random and compute $f^{h/p}$. If any of these is not the identity, the p-Sylow subgroup is cyclic. If all are the identity, there is reason to suspect that the p-Sylow subgroup is noncyclic. For the 2-Sylow subgroup, we consider the fpg-th power of random forms, where fpg is the number of forms per genus.

Given a class group of order $h = p^k h'$, whose p-Sylow subgroup is thought to be noncyclic, we break down the subgroup into its cyclic factors as follows.

PART I

1. Choose at random a form f_1 of order some power of p.

2. Compute the order p^{ord_1} of f_1. Save, in a list, the penultimate p-power-cycle $f_1^{i(p^{ord_1}-1)}$, for $i = 1, \ldots, p-1$, of f_1.

3. Choose at random a form f_2 of order some power of p.

4. Compute the order p^{ord_2} of f_2. Exchange f_1 and f_2, if necessary, so that $ord_2 \leq ord_1$. If exchange is necessary, compute the penultimate p-power cycle of the new f_1.

   (We now have f_1 of order ord_1 and f_2 of order ord_2, with $ord_2 \leq ord_1$.)

5. If $f_2^{p^{ord_2-1}}$ is equal to $f_1^{i(p^{ord_1-1})}$ for any i, replace f_2 by $f_2 f_1^{-i(p^{ord_1-1})}$ and go to Step 4.

At the end of Part I we have two forms which generate independent cycles. If the sum of ord_1 and ord_2 is equal to k, then we have generated the p-Sylow subgroup, and its structure is $\mathcal{C}(p^{ord_2}) \times \mathcal{C}(p^{ord_1})$. If not, we must compute further.

PART II

6. Save, in a list, the penultimate p-power-cycle $f_2^{j(p^{ord_2-1})}$, for $j = 1, \ldots, p-1$, of f_2, and all cross products $f_1^{i(p^{ord_1-1})} f_2^{j(p^{ord_2-1})}$.

7. Choose at random a form f_3 of order some power of p.

8. Compute the order p^{ord_3} of f_3. If $ord_3 > ord_1$, we replace f_1 with f_3 and return to Step 3. If $ord_3 > ord_2$, we replace f_2 with f_3 and return to Step 5.

   (We now have forms f_1 of order ord_1, f_2 of order ord_2, and f_3 of order ord_3, with $ord_3 \leq ord_2 \leq ord_1$ and with f_1 and f_2 generating independent cycles.)

9. If $f_3^{p^{ord_3-1}}$ is equal to $f_1^{i(p^{ord_1-1})} f_2^{j(p^{ord_2-1})}$ for any i, j, $0 \leq i, j \leq p-1$, replace f_3 by $f_3 f_1^{-i(p^{ord_1-1})} f_2^{-j(p^{ord_2-1})}$ and go to Step 8.

Some comments are appropriate. In Steps 1, 3, and 7, we choose a form of order some power of p by choosing a form f and computing $f^{h'}$. In theory, we have no guarantee that any given "random" technique for generating forms will not produce elements for which $f^{h'}$ is not always the identity. In practice, we have found that choosing forms whose first coefficients are simply the primes q, in order, such that $b^2 \equiv \Delta \pmod{4q}$ is solvable, provides a perfectly adequate list of "random" forms for the purposes of this algorithm.

We also have ignored the obvious exit conditions if we find, in fact, that the group is cyclic. Since the class groups tend to be cyclic about 96% of the time, it is certainly worthwhile to do the test above to determine if a given group is probably noncyclic before beginning the more elaborate decomposition computation. If we ever discover a form f such that $f^{h/p}$ is not the identity, however, then we know that the p-Sylow subgroup is cyclic, and we stop.

The heart of this technique is the observation that underlies Steps 5 and 9: If f_1 is of order p^{ord_1} and f_2 is of order p^{ord_2} with $ord_1 \leq ord_2$, and if $f_2^{p^{ord_2-1}}$ is equal to $f_1^{i(p^{ord_1-1})}$ for some i, then $f_2 f_1^{-i(p^{ord_1-1})}$ is of strictly smaller order and is less "dependent" on f_1. For example, if we have a group of order 81,

$$\{1, a, a^2\} \times \{1, b, b^2, \ldots, b^{26}\}$$

and we choose elements b and ab^5, both of order 27, these two elements generate the full group, but not in a way which can be recognized without generating nearly the entire group, a process wasteful both in time and space. By saving the penultimate cycle of b, that is, b^9 and b^{18}, we can determine that the penultimate p-power of ab^5, which is $(ab^5)^9 = b^{18}$, matches one of our saved elements, and $(ab^5)b^{-2} = ab^3$

or properties. Weinberger has done this in an alternate proof of the existence of infinitely many positive fundamental discriminants with class number divisible by a given integer n [WEIN73]. Weinberger shows that if we let the discriminant Δ be the fundamental part of $\Delta(x) = x^{2n}+4$, then the class number of Δ is infinitely often divisible by n. Honda earlier showed [HOND68] that if we let Δ be the fundamental part of discriminants $4x^3 - 27y^2$ for an appropriate choice of x and y, then for infinitely many positive Δ we have class numbers divisible by 3. Similarly, Chowla and Hartung [CHOW74] showed that for discriminants of the form $\Delta = -(27n^2 + 4)$ for which $-\Delta$ is prime, the class number is divisible by 3. The opposite question has also been studied by Hartung, who showed [HART74] that there exist infinitely many negative fundamental discriminants whose class numbers are *not* divisible by 3.

Unfortunately, as a moment's thought will show, (8.2) is not entirely practical as a means of generating classes of order n in class groups. The problem is twofold. First, the equation itself is open-ended, as there are no conditions of magnitude on any of the variables. Second, the equation is of degree n, so that the computational question of handling the arithmetic in searching for solutions is significant. For these reasons, solving (8.2) has usually been used as a heuristic in finding forms of some order n rather than a method for exhaustively enumerating them.

8.3.2 Exact and Exotic Groups

Having guaranteed by various means that noncyclic p-Sylow subgroups exist for all p, at least for negative discriminants, it is not necessarily trivial to find examples even for all small primes p. In the following table we list for the small primes p the first occurrence, for even and odd negative discriminants, of a noncyclic p-Sylow subgroup (the notation

in the third column 3×9, for example, indicates a group $\mathcal{C}(3) \times \mathcal{C}(9)$) [BUEL76, BUEL87a].

Prime	Discriminant	Complete Class Group
3	−3299	3×9
	−3896	3×12
5	−11199	5×20
	−17944	5×10
7	−63499	7×7
	−159592	7×14
11	−65591	11×22
	−580424	22×22
13	−228679	13×26
	−703636	13×26
17	−1997799	34×34
	−4034356	17×34
19	−373391	19×38
	−3419828	19×38
23	−7472983	23×46
	−11137012	23×46
29	−20113607	29×116
	−16706324	58×58
31	−11597903	31×62
41	−6112511	41×82

The discussion of this section has centered on subgroups of the class group; there is also some small interest in knowing which finite abelian groups actually occur as the exact class group, not just a subgroup. Chowla proved that not all elementary 2-groups can occur as class groups of quadratic fields [CHOW34]. In our computation of class groups of negative discriminant, we found that all abelian groups of rank two and order less than 1000 occurred as class groups except $\mathcal{C}(11) \times \mathcal{C}(11)$, $\mathcal{C}(19) \times \mathcal{C}(19)$, $\mathcal{C}(29) \times \mathcal{C}(29)$, and $\mathcal{C}(31) \times \mathcal{C}(31)$ [BUEL87a]. It is therefore almost certain that $\mathcal{C}(11) \times \mathcal{C}(11)$ occurs as

$b^2 - 4a^3$ in a number of different ways, usually by finding polynomials $b_1(x)$, $b_2(x)$, $a_1(x)$, $a_2(x)$, such that

$$\Delta(x) = b_1(x)^2 - 4a_1(x)^3 = b_2(x)^2 - 4a_2(x)^3$$

With appropriate conditions on the sizes of terms, one can guarantee in this way that for negative discriminants we have at least rank two in the 3-Sylow subgroup. Shanks generally took the approach of finding a few very select polynomials, often choosing them so as to be able to apply Scholz's theorem, mentioned at the end of this section. Buell and Diaz y Diaz by contrast used a large number of polynomials. Diaz y Diaz, who was most successful, generated at one point hundreds of discriminants of 3-rank at least two from a large number of polynomials, and then sorted the discriminants in order to find matches. If a discriminant had been generated by different polynomials, with different 3-cycles, it would have rank three or four. More recently Schoof [SCHO83] has found groups with large 3-rank and 5-rank by using the theory of elliptic curves.

We summarize the first occurrences of large rank. The first four lines represent discriminants known to be the first occurrence of 3-rank or of 5-rank three, as all previous class groups have been computed. The remaining examples are merely the first known occurrences.

Discriminant	Complete Class Group
−3321607	$3 \times 3 \times 63$
−4447704	$6 \times 6 \times 24$
−18397407	$5 \times 10 \times 40$
−11203620	$10 \times 10 \times 10$
−653329427	$3 \times 3 \times 3 \times 210$
−2520963512	$3 \times 3 \times 6 \times 276$
−258559351511807	$5 \times 5 \times 10 \times 59140$

In computing 3-Sylow subgroups, a significant theorem of Arnold Scholz has been extensively used, especially by Shanks. The theorem relates the class groups of the quadratic fields of radicands $+\Delta$ and -3Δ [SCHO32].

Theorem 8.6. *Let $+\Delta$ and -3Δ be the radicands of the quadratic fields $\mathbf{Q}\sqrt{\Delta}$ and $\mathbf{Q}\sqrt{-3\Delta}$, where Δ may or may not be divisible by 3. If r is the rank of the 3-Sylow subgroup of the field with negative discriminant, and s is the rank of the 3-Sylow subgroup of the field with positive discriminant, then*

$$s \leq r \leq s + 1.$$

Duncan A. Buell

Binary Quadratic Forms

Classical Theory and Modern Computations

Springer-Verlag
New York Berlin Heidelberg
London Paris Tokyo Hong Kong

Duncan A. Buell
Supercomputing Research Center
Bowie, MD 20715-4300, USA

Mathematical Subject Classification Codes: 11-02, 11R11, 11R29

Library of Congress Cataloging-in-Publication Data

Buell, Duncan A.
Binary quadratic forms : classical theory and modern computations
/ Duncan A. Buell.
p. cm.
Bibliography: p.
1. Forms, Binary. 2. Forms, Quadratic. I. Title.
QA201.B84 1989
512'.5—dc20 89-11314

Printed on acid-free paper.

Camera-ready copy prepared by the author using TEX.
Printed and bound by Edwards Brothers, Incorporated, Ann Arbor, Michigan.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-97037-1 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-97037-1 Springer-Verlag Berlin Heidelberg New York