Orders in Quadratic Fields. V

By R. A. MOLLIN

Department of Mathematics and Statistics, The University of Calgary, Canada

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1995)

Abstract: We provide a simple proof of a necessary and sufficient condition for the class group of a complex quadratic field to have exponent at most 2. This criterion is given in terms of the form of the discriminant arising from the number of split primes less than the Minkowski bound. We also prove a conjecture related to it which we left in earlier work.

1. Introduction. This continues work in [1]-[5] to which we refer for notation and background. In particular, a conjecture was made in [1, p.48] which gave a criterion for an arbitrary order (of positive or negative discriminant) to have class group generated by ambiguous ideals, i.e. to have $e_\Delta \leq 2$. However, in [2] we were able to provide counterexamples to the conjecture for both positive and negative discriminants. It turns out that the conjecture in [1] was overly ambitious, in that it included ramified primes, and it was precisely the use of such primes which led to the counterexamples in [2]. What we show herein is that we do in fact have a criterion for $\Delta = \Delta_0 < 0$, and it is even stronger than that suggested by the conjecture in [1], provided that we do not include the ramified primes. Effectively, what the conjecture in [1] claims, for $\Delta < 0$, is that $e_\Delta \leq 2$ if and only if there exists a squarefree divisor $q \geq 1$ of Δ such that, for any prime $p < M_\Delta$ relatively prime to q, there exists an integer x such that $|F_{\Delta,q}(x)| = p$. If we modify this to say "any *split* prime $p < M_\Delta$", rather than primes p "relatively prime to q", then the conjecture holds. Furthermore, it is always true for $x = 0$! We proved this in [4] using the results of [3]. Herein, we improve upon this by providing a two line proof of this criterion. Furthermore, we are able to prove a conjecture left in [4], which is related to the criterion.

2. The criterion. Before giving our simple proof of the criterion discussed above and the conjecture related to it, we need a technical result which holds for arbitrary quadratic orders. What the following essentially says is that representation of integers by binary quadratic forms is tantamount to equivalence of the related ideals in the underlying quadratic order.

Lemma 2.1 *Let Δ be a discriminant with $q \geq 1$, a squarefree divisor of $|\Delta|$. If $a > 0$ is an integer with $F_{\Delta,q}(x) = a$, where x is any non-negative rational integer, then $\mathcal{Q} \sim \mathcal{A}$, where $\mathcal{Q}$ is the unique $\mathcal{O}_\Delta$-prime above q and $\mathcal{A}$ is an $\mathcal{O}_\Delta$-ideal of norm a.*

Proof. Form the ideal $\mathcal{A}\mathcal{Q} = [aq, (b+\sqrt{\Delta})/2]$, where $b = (2x + \alpha - 1)q$, then $N((b+\sqrt{\Delta})/2) = qF_{\Delta,q}(x) = aq$. Therefore, $\mathcal{A}\mathcal{Q} = ((b+\sqrt{\Delta})/2)$; i.e. $\mathcal{Q} \sim \mathcal{A}$. □

Now we may state the criterion.

Theorem 2.1 *If $\Delta < 0$ is a fundamental discriminant, then the following are equivalent.*

(1) $e_\Delta \leq 2$.

(2) *For every split prime $p < M_\Delta$, there exists a squarefree divisor $q > p$ of $|\Delta|$ such that $\Delta = q^2 - 4pq$.*

Proof. If (2) holds, then (1) follows from [1, Theorem 1.2, p.46] and Lemma 2.1, since $F_{\Delta,q}(0) = p$ when $\Delta \not\equiv 0 (mod\ 8)$, which we may assume, given that such a split prime p does not otherwise exist. Conversely, if (1) holds and $p < M_\Delta$ is any split prime, then there exists an $\mathcal{O}_\Delta$ ideal $I = [p, (b+\sqrt{\Delta})/2]$ for some $b \in \mathbf{Z}$ with $|b| < p$; and the result now follows from [3, Corollary 2.1]. □

Theorem 2.1 provides a simple proof of the modified conjecture discussed at the outset, and which we proved in [4] as a simple criterion for the class group of a complex quadratic field to have exponent $e_\Delta \leq 2$. Moreover, we now prove a conjecture related to it, namely [4, Conjecture 3.1].

Corollary 2.1 *If $\Delta < 0$ is a fundamental discriminant, $p < M_\Delta$ is a split prime, and $e_\Delta \leq 2$, then the $\mathcal{O}_\Delta$-primes above p are reduced, i.e. there do*

not exist any non-reduced $\mathcal{O}_\Delta$-ideals of norm $p < M_\Delta$.

Proof. Suppose that $p < M_\Delta$ is a split prime such that the ideal $I = [p, (b+\sqrt{\Delta})/2]$, with $|b| < p$, is not reduced. By [3, Theorem 2.1(b)], $p > (b^2 - \Delta)/(4p) = c$.

Claim. $|b| < c$.

We assume that $b > 0$ since the other case is similar. If $p > b > c$, then $p = c + l$ and $b = c + k$ with $0 < k < l$. Thus, $3p^2 + b^2 = 3(c+l)^2 + (c+k)^2 > 4c^2 + 4cl = 4cp$. Hence, $p > \sqrt{(4cp - b^2)/3} = \sqrt{-\Delta/3}$, a contradiction.

By the Claim, and [3, Theorem 2.1(b)] the ideal $(c, (-b+\sqrt{\Delta})/2]$ is reduced. By the Claim c cannot divide $|\Delta|$. Thus, by [3,Theorem 2.1(e)], $b^2 - \Delta = 4c^2$, forcing $c = p$, a contradiction. □

This now completes the simple proof of the criterion, as well as the proof of the related conjecture and so our task is accomplished.

References

[1] Mollin, R. A.: Orders in quadratic fields. I. Proc. Japan Acad., **69A**, 45–48 (1993).

[2] Mollin, R. A.: Orders in quadratic fields. III. Proc. Japan Acad., **70A**, 176–181 (1994).

[3] Mollin, R. A.: Orders in quadratic fields. IV. Proc. Japan Acad., **71A**, 131–133 (1995).

[4] Mollin, R. A.: Quadratic polynomials producing consecutive distinct primes and class groups of complex quadratic fields (to appear: Acta Arith.).

[5] Mollin, R. A., and Zhang, L. -C.: Orders in quadratic fields. II. Proc. Japan Acad., **69A**, 368–371 (1993).