10. On Class Numbers of Quadratic Extensions of Algebraic Number Fields

By Richard A. MOLLIN
Mathematics Department, University of Calgary,
Calgary, Alberta, Canada, T2N 1N4

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 13, 1986)

In [14] Nagell showed that there are infinitely many imaginary quadratic extensions of the rational number field $\boldsymbol{Q}$, each of which has class number divisible by a given integer. Subsequently several authors have proved this result (see [1], [4], [5] and [17] as well as the most recent proof by Uehara [16]). In this paper we generalize this well-known result by explicit construction of infinitely many imaginary quadratic extensions of a given number field K (subject only to having a totally ramified rational prime) each with class number divisible by a given integer. The proof and construction given is simpler than that given in previous proofs cited above for the trivial case $K=\boldsymbol{Q}$, and applications are given. The next result is a sufficient condition for an arbitrary quadratic extension of $\boldsymbol{Q}$ to have an element of given order in its class group. Finally for a certain class of real quadratic extensions of $\boldsymbol{Q}$ we give a sufficient condition for its class number to be divisible by a given prime, and we provide applications.

Before presenting the first result some comments on notation and a lemma are required. For a given number field K, $h(K)$ denotes the class number of K, $\mathcal{C}_K$ denotes the class group of K, $\mathcal{O}_K$ denotes the ring of integers of K, (α) for $\alpha \in \mathcal{O}_K$ denotes the principal ideal generated by α, and $N(\cdot)$ denotes the norm from K to $\boldsymbol{Q}$.

In the proof of Theorem 1 we will need the following result whose proof (mutatis mutandis) is the same as that of [1, Lemma 1, p. 321] of which the following lemma is a generalization.

Lemma 1. *Let ε be any positive real number and let p be any odd prime. Denote by N the number of square-free integers of the form p^g-x^2 where x is an even integer such that $0<x<\varepsilon p^{g/2}$. Then for g sufficiently large, $N \geq c_p \varepsilon p^{g/2}$ where c_p is a positive constant depending only on p.*

Theorem 1. *Let $t>1$ be any integer. If K is any algebraic number field in which there is a totally ramified rational odd prime p, then there are infinitely many imaginary quadratic extensions L of K such that $t \mid h(L)$. Moreover L may be chosen of the form $K(\sqrt{n})$ where n is any square-free rational integer of the form $n=r^2-m^t$ where p does not divide n and r is an even integer subject to $r^2 \leq m^{t-1}(m-1)$.*

Proof. Let r be an arbitrarily chosen but fixed even integer. Let n