MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 123–137

Class Groups of Number Fields: Numerical Heuristics

By H. Cohen and J. Martinet

Dedicated to Dan Shanks on his 70th birthday

Abstract. Extending previous work of H. W. Lenstra, Jr. and the first author, we give quantitative conjectures for the statistical behavior of class groups and class numbers for every type of field of degree less than or equal to four (given the signature and the Galois group of the Galois closure). The theoretical justifications for these conjectures will appear elsewhere, but the agreement with the existing tables is quite good.

1. Introduction and Notations. In [3], H. W. Lenstra, Jr., and the first author developed a method for conjecturing quantitative results on class groups of quadratic fields and cyclic extensions of prime degree. In a forthcoming paper [4] we shall show that this technique can be extended to a much wider class of number fields, and also to relative extensions.

The aim of the present paper is to rapidly make available the numerical conjectures obtained, for people not really interested in our heuristic reasoning or not wanting to wait for [4] to appear. Hence, apart from a total lack of justifications for the conjectures that we present, this paper is essentially self-contained. The plan is as follows.

In the rest of this section we present the notations used in the sequel. Some of them being nonstandard (and in general differing from the notations of [3]), we urge the reader to read the notations carefully before applying the conjectures.

In the next section we present templates for the subsequent conjectures, and then the conjectures themselves, illustrated by numerical examples, first for their own sake, and second as a double check for the reader to understand the templates. These conjectures are given for all types of fields of degree less than or equal to four.

In the final section we comment on the consistency of the conjectures with existing tables (which is quite good).

Combinatorial Notations:

★ If X is a set, $|X|$ denotes its cardinality.

★ For an integer $p \geqslant 2$ and α an integer or ∞, we set: $(p)_\alpha = \prod_{1 \leqslant k \leqslant \alpha}(1 - p^{-k})$; in particular $(p)_\infty = \prod_{k \geqslant 1}(1 - p^{-k})$, $(p)_0 = 1$.

Remark. It would have been more consistent with the usual notations of combinatorics to write this as $(1/p)_\alpha$, but the present notation is typographically simpler.

Received June 11, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R29; Secondary 11Y40.
Key words and phases. Class group, class number, number field, zeta function.

0025-5718/87 $1.00 + $.25 per page

Algebraic Notations:

★ The letter K will stand for the generic algebraic number field whose class group we want to study.

★ H_K (resp. $H_{K/k}$ for relative extensions) will denote the subgroup of the class group consisting of elements whose order is not divisible by the given bad prime or primes (resp. and in the kernel of the norm map from K to k).

Warning. H_K does not denote the class group itself, in general.

★ $h_K = |H_K|$, $h_{K/k} = |H_{K/k}|$.

★ The letter M will denote a Galois closure of K over $\mathbf{Q}$, and $\Gamma = \mathrm{Gal}(M/\mathbf{Q})$.

★ A will denote a direct product of Dedekind domains A_i (in fact, in our cases, A will either be a direct product of copies of $\mathbf{Z}$ or a single Dedekind domain).

★ If G is an A-module, $\mathrm{Aut}_A G$ (or simply $\mathrm{Aut}\, G$) will denote the group of A-automorphisms of G, and G_i will denote the component of G on the factor A_i of A (hence $G \simeq \prod G_i$).

★ If $\mathfrak{p}$ is a maximal ideal of a Dedekind domain A, we will write $r_{\mathfrak{p}}^A(G)$ for the $\mathfrak{p}$-rank of G as an A-module, i.e., the dimension of $G/\mathfrak{p}G$ over $A/\mathfrak{p}$. We shall write $r_p^{\mathbf{Z}}(G)$ for the p-rank of G when G is viewed only as a $\mathbf{Z}$-module. Note that when A is the ring of integers of a quadratic field then

(i) if p splits in A, say $pA = \mathfrak{p}\bar{\mathfrak{p}}$,

$$r_p^{\mathbf{Z}}(G) = r_{\mathfrak{p}}^A(G) + r_{\bar{\mathfrak{p}}}^A(G);$$

(ii) if p is inert in A,

$$r_p^{\mathbf{Z}}(G) = 2r_p^A(G).$$

If $A = \mathbf{Z}$ we write simply $r_p(G)$ instead of $r_p^{\mathbf{Z}}(G)$.

Analytic Notations:

★ In the templates, the letter f will stand for a "nice" function (not further specified!) defined on isomorphism classes of finite A-modules.

★ If $A = \prod_{1 \leqslant i \leqslant m} A_i$, where the A_i are Dedekind domains, then the zeta function of A is by definition a function of m complex variables defined by analytic continuation to $\mathbf{C}^m$ of the following function:

$$\zeta^A(\mathbf{s}) = \prod_{1 \leqslant i \leqslant m} \zeta^{A_i}(s_i),$$

where $\mathbf{s} = (s_1, \ldots, s_m)$ and ζ^{A_i} is the Dedekind zeta function of A_i (when it is defined).

Warning. This differs from the usual definition of ζ^A, a function of *one* complex variable s, which one recovers by setting $s_1 = \cdots = s_m = s$.

★ The Z function of A is defined by

$$Z^A(\mathbf{s}) = \prod_{k \geqslant 1} \zeta^A(\mathbf{s} + k \cdot \mathbf{1}),$$

where $\mathbf{1} = (1, \ldots, 1)$ is an m-dimensional vector.

★ The Z function of A relative to the function f is obtained by analytic continuation of

$$Z^A(f; \mathbf{s}) = \sum_G f(G) |\mathrm{Aut}_A G|^{-1} |G_1|^{-s_1} \cdots |G_m|^{-s_m},$$

where the summation is over all A-isomorphism classes of finite A-modules G.

★ If $\mathbf{1}$ is the constant function equal to 1 everywhere, then it is a theorem (*not* a conjecture!) that

$$Z^A(\mathbf{1}, \mathbf{s}) = Z^A(\mathbf{s})$$

(see [3, Corollary 3.7] or [4]), whence the notation.

★ $C(A) = \mathrm{Res}_{s=0} Z^A(s) = \mathrm{Res}_{s=1} \zeta^A(s) \prod_{k \geqslant 2} \zeta^A(k)$ (used only when A is a Dedekind domain).

★ If ℓ is a prime number which we want to exclude (a "bad" prime), we use $\zeta^A_{\neq \ell}(\mathbf{s})$ and $Z^A_{\neq \ell}(\mathbf{s})$ to mean that we omit the Euler factors corresponding to prime ideals dividing ℓ, and more generally $Z^A_{\neq \ell}(f; \mathbf{s})$ to mean that in the sum defining $Z^A(f; \mathbf{s})$ we take only finite A-modules of order not divisible by ℓ.

★ Finally, we set

$$M^A(f; \mathbf{s}) = Z^A_{\neq \ell}(f; \mathbf{s}) / Z^A_{\neq \ell}(\mathbf{s}),$$

where it is understood that the limit is taken if both the numerator and denominator vanish.

2. The Conjectures. Let K be a generic algebraic number field, M a Galois closure of K, and $\Gamma = \mathrm{Gal}(M/\mathbf{Q})$ as usual.

For a given Γ we first give a diagram indicating interesting subfields of M and their interrelations (although usually not the conjugates of K), then the "bad" prime ℓ (when $[K : \mathbf{Q}] \leqslant 4$ there is only one such), the ring A, and in the non-Galois case, relations between class groups *outside the bad prime* as always (these relations being theorems, not conjectures!). We indicate the degrees of the field extensions, except when they are equal to two.

We then consider the set $\mathscr{C}$ of isomorphism classes of fields K having given Γ, r_1, r_2 (number of real and complex embeddings of K). If f is a function (see notations), we define the *average* of f as the following limit, if it exists:

$$\mathscr{M}(f) = \lim_{X \to \infty} \sum_{\substack{K \in \mathscr{C} \\ |D_K| \leqslant X}} f(H_K) / \sum_{\substack{K \in \mathscr{C} \\ |D_K| \leqslant X}} 1,$$

where D_K is the discriminant of K. (If we work with relative extensions, replace H_K by $H_{K/k}$ in this definition.)

We then give a general heuristic prediction linking $\mathscr{M}(f)$ to the function $M^A_{\neq \ell}(f; \mathbf{s})$ defined above, and we specialize this prediction to a number of interesting functions f. In many cases, f will be the characteristic function of a property P of H_K (i.e., 1 if P is true, 0 if not), and in this case we shall speak of the "probability" that P holds (written $\mathrm{pr}(P)$), although evidently $\mathscr{M}(f)$ is only finitely additive.

For each of the functions f we give a few numerical examples, the numbers being rounded to six decimals.

In what follows:

★ ℓ will be the bad prime.

★ H will be a finite A-module of cardinality h.

★ h and m will denote integers not divisible by ℓ.

★ p will denote a good prime, and $\mathfrak{p}$ a prime ideal of A dividing p.

We shall give in turn:

(a) $\Pr(H_K \simeq_A H)$, $\Pr(h_K = h)$.

(b) $\Pr(m \mid h_K)$.

(c) $\Pr(r_{\mathfrak{p}}^A(H_K) = r)$ and similar quantities.

(d) The average of $(N\mathfrak{p})^{nr_{\mathfrak{p}}^A(H_K)}$ (n a positive integer).

(e) The average of h_K.

(f) In a few cases, some additional conjectures.

For relative extensions, we of course replace H_K and h_K above by $H_{K/k}$ and $h_{K/k}$.

Recall once more that H_K denotes the class group with its ℓ-component removed.

(1) *Quadratic Fields.*

$$\begin{array}{cc} K & \Gamma = \mathbf{Z}/2\mathbf{Z} \\ | & \text{bad prime: } \ell = 2 \\ \mathbf{Q} & A = \mathbf{Z} \end{array}$$

(1.1) *Complex quadratic fields.*

$$(r_1 = 0,\ r_2 = 1),$$
$$\mathscr{M}(f) = M_{\neq 2}^{\mathbf{Z}}(f; 0).$$

(a) $\operatorname{pr}(H_K \simeq H) = 0$, $\operatorname{pr}(h_K = h) = 0$.

(b) $\operatorname{pr}(m \mid h_K) = \prod_{p^\alpha \| m}(1 - (p)_\infty/(p)_{\alpha-1})$.

Examples.

$$m = 3\colon 0.439874; \quad m = 5\colon 0.239667;$$
$$m = 7\colon 0.163204; \quad m = 9\colon 0.159811.$$

(c) $\operatorname{pr}(r_p(H_K) = r) = p^{-r^2}(p)_\infty/(p)_r^2$.

Examples.

$$p=3\colon\ r = 0\colon 0.560126; \quad r = 1\colon 0.420095;$$
$$r = 2\colon 0.019692; \quad r \geqslant 3\colon 0.000087;$$
$$p=5\colon\ r = 0\colon 0.760333; \quad r = 1\colon 0.237604;$$
$$r \geqslant 2\colon 0.002063.$$

(d) $\mathscr{M}(p^{nr_p(H_K)}) = \sum_{i=0}^{n} p^{i(n-i)}(p)_n/((p)_i(p)_{n-i})$.

Examples.

$$n = 1\colon 2; \quad n = 2\colon p + 3.$$

(e) $\mathscr{M}(h_K) = \infty$.

(1.2) *Real quadratic fields.*

$$(r_1 = 2,\ r_2 = 0),$$
$$\mathscr{M}(f) = M_{\neq 2}^{\mathbf{Z}}(f; 1).$$

(a)
$$\operatorname{pr}(H_K \simeq H) = \left(2h(2)_\infty C(\mathbf{Z})\,|\operatorname{Aut} H|\right)^{-1},$$
$$\operatorname{pr}(h_K = h) = \left(2h^2(2)_\infty C(\mathbf{Z}) \prod_{p^\alpha \| h}(p)_\alpha\right)^{-1}.$$

Examples.

$$h = 1\colon 0.754458; \quad h = 3\colon 0.125743;$$
$$h = 5\colon 0.037723; \quad h = 7\colon 0.017963;$$
$$h = 9\colon 0.015718\ \left(H \simeq \mathbf{Z}/9\mathbf{Z}\colon 0.013971;\ H \simeq (\mathbf{Z}/3\mathbf{Z})^2\colon 0.001746\right).$$

(b) $\mathrm{pr}(m \mid h_K) = \prod_{p^\alpha \| m}(1 - ((p)_\infty/(p)_1)\Sigma_{0 \leqslant \beta \leqslant \alpha}(p^{2\beta}(p)_\beta)^{-1})$.
Examples.

$$m = 3\colon 0.159811; \quad m = 5\colon 0.049584;$$
$$m = 7\colon 0.023739; \quad m = 9\colon 0.019779.$$

(c) $\mathrm{pr}(r_p(H_K) = r) = p^{-r(r+1)}(p)_\infty/((p)_r(p)_{r+1})$.
Examples.

$$p=3\colon r = 0\colon 0.840189; \quad r = 1\colon 0.157535;$$
$$r \geqslant 2\colon 0.002275;$$
$$p=5\colon r = 0\colon 0.950416; \quad r = 1\colon 0.049501;$$
$$r \geqslant 2\colon 0.000083.$$

(d) $\mathscr{M}(p^{nr_p(H_K)}) = \sum_{i=0}^{n} p^{i(n-i-1)}(p)_n/((p)_i(p)_{n-i})$.
Examples.

$$n = 1\colon 1 + p^{-1}; \quad n = 2\colon 2 + p^{-1} + p^{-2}.$$

(e) $\mathscr{M}(H_K) = \infty$.
(f) (Also conjectured by C. Hooley [11])

$$\sum_{\substack{p \leqslant x \\ p \text{ prime},\ p \equiv 1 \pmod 4}} h_{\mathbf{Q}(\sqrt{p})} \sim \frac{x}{8} \quad \text{as } x \to \infty.$$

(2) *Cyclic Cubic Fields.*

K	$\Gamma = \mathbf{Z}/3\mathbf{Z}$
$3 \mid$	bad prime: $\ell = 3$
$\mathbf{Q}$	$A = \mathbf{Z}[j] \quad (j = e^{2i\pi/3})$

K is totally real $\quad (r_1 = 3, r_2 = 0)$,

$$\mathscr{M}(f) = M^A_{\neq 3}(f; 1).$$

(a)
$$\mathrm{pr}(H_K \simeq_A H) = \left(\frac{9\sqrt{3}}{2\pi} h(3)_\infty C(A) |\mathrm{Aut}_A H|\right)^{-1},$$
$$\mathrm{pr}(h_K = h) = \left(\frac{9\sqrt{3}}{2\pi} h^2(3)_\infty C(A)\right)^{-1} \sum_{N\mathfrak{a} = h} \prod_{\mathfrak{p}^\alpha \| \mathfrak{a}} (N\mathfrak{p})^{-1}_\alpha.$$

Here, $\mathfrak{a}$ runs through all integral ideals of A of norm h, and $\mathfrak{p}$ through prime ideals dividing $\mathfrak{a}$.
Examples.

$h = 1$: 0.850072; $\quad h = 4$: 0.070839 $\left(\text{here } H \simeq_{\mathbf{Z}} (\mathbf{Z}/2\mathbf{Z})^2\right)$;

$h = 7$: 0.040480 (50% for each of the two A-isomorphism classes);

$h = 13$: 0.010898 (50% for each of the two A-isomorphism classes);

$h = 16$: 0.004723 $\left(H \simeq_{\mathbf{Z}} (\mathbf{Z}/4\mathbf{Z})^2\colon 0.004427;\ H \simeq_{\mathbf{Z}} (\mathbf{Z}/2\mathbf{Z})^4\colon 0.000295\right)$.

(b) $\mathrm{pr}(m \mid H_K) = P_1 P_2$, where

$$P_1 = \prod_{\substack{p^\alpha \| m \\ p \equiv 1 \pmod 3}} \left(1 - \left((p)_\infty^2/(p)_1^2\right) \sum_{0 \leqslant \beta+\gamma<\alpha} \left(p^{2\beta+2\gamma}(p)_\beta (p)_\gamma\right)^{-1}\right),$$

$$P_2 = \prod_{\substack{p^\alpha \| m \\ p \equiv 2 \pmod 3}} \left(1 - \left((p^2)_\infty/(p^2)_1\right) \sum_{0 \leqslant \beta<\alpha/2} \left(p^{4\beta}(p^2)_\beta\right)^{-1}\right).$$

Examples.

$m = 2$ and $m = 4$: 0.081950; $m = 5$: 0.001667;
$m = 7$: 0.046914; $m = 8$ and $m = 16$: 0.005446.

(c) $\mathrm{pr}(r_{\mathfrak{p}}^A(H_K) = r) = (N\mathfrak{p})^{-r(r+1)}(N\mathfrak{p})_\infty/((N\mathfrak{p})_r(N\mathfrak{p})_{r+1})$.

If $p \equiv 1 \pmod 3$, then

$$\mathrm{pr}\left(r_p^{\mathbf{Z}}(H_K) = r\right) = (p)_\infty^2 \sum_{t+u=r} p^{-t(t+1)-u(u+1)}/((p)_t(p)_{t+1}(p)_u(p)_{u+1}).$$

If $p \equiv 2 \pmod 3$, then

$$\mathrm{pr}\left(r_p^{\mathbf{Z}}(H_K) = r\right) = \begin{cases} 0 & \text{if } r \text{ is odd,} \\ p^{-r(r+2)/2}(p^2)_\infty/\left((p^2)_{r/2}(p^2)_{(r/2)+1}\right) & \text{otherwise.} \end{cases}$$

Examples.

$p=2$: $r = 0$: 0.918050; $r = 2$: 0.081604;
$r \geqslant 4$: 0.000346;
$p=5$: $r = 0$: 0.998333; $r \geqslant 2$: 0.001667;
$p=7$: $r = 0$: 0.953086; $r = 1$: 0.046331;
$r \geqslant 2$: 0.000583.

(d) If $p \equiv 1 \pmod 3$ then

$$\mathscr{M}\left(p^{nr_{\mathfrak{p}}^A(H_K)}\right) = \sum_{i=0}^{n} p^{i(n-i-1)}(p)_n/((p)_i(p)_{n-i}),$$

$$\mathscr{M}\left(p^{nr_p^{\mathbf{Z}}(H_K)}\right) = \left(\mathscr{M}\left(p^{nr_{\mathfrak{p}}^A(H_K)}\right)\right)^2.$$

Examples.

$$n = 1\colon (1 + p^{-1})^2; \quad n = 2\colon (2 + p^{-1} + p^{-2})^2.$$

If $p \equiv 2 \pmod 3$ then

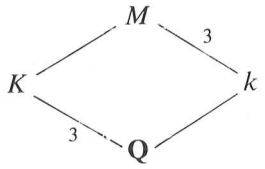
$$\mathscr{M}\left(p^{2nr_{\mathfrak{p}}^A(H_K)}\right) = \mathscr{M}\left(p^{nr_p^{\mathbf{Z}}(H_k)}\right) = \sum_{i=0}^{n} p^{2i(n-i-1)}(p^2)_n/\left((p^2)_i(p^2)_{n-i}\right).$$

Examples.

$$n = 1\colon 1 + p^{-2}; \quad n = 2\colon 2 + p^{-2} + p^{-4}.$$

(e) $\mathscr{M}(h_K) = \infty$.

(3) *Non-Galois Cubic Fields.*



$\Gamma = S_3$
bad prime: $\ell = 3$
$A = \mathbf{Z}$
$H_{M/k} \simeq H_K \times H_K$

(3.1) *Complex cubic fields.*

$$(r_1 = 1,\ r_2 = 1),$$
$$\mathscr{M}(f) = M^{\mathbf{Z}}_{\neq 3}(f;1).$$

(a)
$$\operatorname{pr}(H_K \simeq H) = \left(\frac{3}{2}h(3)_\infty C(\mathbf{Z})|\operatorname{Aut} H|\right)^{-1},$$
$$\operatorname{pr}(h_K = h) = \left(\frac{3}{2}h^2(3)_\infty C(\mathbf{Z})\prod_{p^\alpha \| h}(p)_\alpha\right)^{-1}.$$

Examples.

$h = 1$: 0.518642; $h = 2$: 0.259321;

$h = 4$: 0.086440 $\left(H \simeq \mathbf{Z}/4\mathbf{Z}$: 0.064830; $H \simeq (\mathbf{Z}/2\mathbf{Z})^2$: 0.021610$\right)$;

$h = 5$: 0.025932.

(b) $\operatorname{pr}(m \mid h_K) = \prod_{p^\alpha \| m}(1 - ((p)_\infty/(p)_1)\sum_{0 \leqslant \beta < \alpha}(p^{2\beta}(p)_\beta)^{-1})$.

Examples.

$m = 2$: 0.422424; $m = 4$: 0.133636;
$m = 5$: 0.049584; $m = 7$: 0.023739.

(c) $\operatorname{pr}(r_p(H_K) = r) = p^{-r(r+1)}(p)_\infty/((p)_r(p)_{r+1})$.

Examples.

$p = 2$: $r = 0$: 0.577576; $r = 1$: 0.385051;
$r = 2$: 0.036672; $r \geqslant 3$: 0.000702.

For $p \geqslant 5$ see 1.2(c).

(d), (e) See 1.2(d) and 1.2(e).

(3.2) *Totally real non-Galois cubic fields.*

$$(r_1 = 3,\ r_2 = 0),$$
$$\mathscr{M}(f) = M^{\mathbf{Z}}_{\neq 3}(f;2).$$

(a)
$$\operatorname{pr}(H_K \simeq H) = \left(\frac{81}{8\pi^2}h^2(3)_\infty C(\mathbf{Z})|\operatorname{Aut} H|\right)^{-1},$$
$$\operatorname{pr}(h_K = h) = \left(\frac{81}{8\pi^2}h^3(3)_\infty C(\mathbf{Z})\prod_{p^\alpha \| m}(p)_\alpha\right)^{-1}.$$

Examples.

$h = 1$: 0.758339; $h = 2$: 0.189585;

$h = 4$: 0.031597 $\left(H \simeq \mathbf{Z}/4\mathbf{Z}$: 0.023698; $H \simeq (\mathbf{Z}/2\mathbf{Z})^2$: 0.007899$\right)$.

(b) $\operatorname{pr}(m \mid h_K) = \prod_{p^\alpha \| m}(1 - ((p)_\infty/(p)_2)\Sigma_{0 \leqslant \beta < \alpha}(p^{3\beta}(p)_\beta)^{-1})$.

Examples.

$m = 2$: 0.229898; $m = 4$: 0.037373;
$m = 5$: 0.009983; $m = 7$: 0.003400.

(c) $\operatorname{pr}(r_p(H_K) = r) = p^{-r(r+2)}(p)_\infty/((p)_r(p)_{r+2})$.

Examples.

$p=2$: $r = 0$: 0.770102; $r = 1$: 0.220029;
$r = 2$: 0.009779; $r \geqslant 3$: 0.000090;
$p=5$: $r = 0$: 0.990017; $r = 1$: 0.009980;
$r \geqslant 2$: 3.3×10^{-6}.

(d) $\mathscr{M}(p^{nr_p(H_K)}) = \sum_{i=0}^{n} p^{i(n-i-2)}(p)_n/((p)_i(p)_{n-i})$.

Examples.

$$n = 1: 1 + p^{-2}; \quad n = 2: 1 + p^{-1} + p^{-2} + p^{-4}.$$

(e) $\mathscr{M}(h_K) = 4\pi^2/27 = 1.462164$.

(4) *Cyclic Quartic Fields.*

$$\begin{array}{c} K \\ | \\ k \\ | \\ \mathbf{Q} \end{array} \qquad \begin{array}{c} \Gamma = \mathbf{Z}/4\mathbf{Z} \\ \text{bad prime: } \ell = 2 \\ H_K \simeq H_k \times H_{K/k} \\ \text{hence only } H_{K/k} \text{ is interesting} \\ A = \mathbf{Z}[i] \end{array}$$

(4.1) *Totally complex cyclic quartic fields.*

$$(r_1 = 0, r_2 = 2).$$

Here, k is real quadratic.

$$\mathscr{M}(f) = M^A_{\neq 2}(f; 0).$$

Remark. If one wants the full class group H_K, then the template is

$$\mathscr{M}(f) = M^B_{\neq 2}(f; 1, 0),$$

where $B = \mathbf{Z} \times \mathbf{Z}[i]$.

(a) $\mathrm{pr}(H_{K/k} \simeq_A H) = 0$, $\mathrm{pr}(h_{K/k} = h) = 0$.

(b) $\mathrm{pr}(m \mid h_{K/k}) = P_1 P_3$, where

$$P_1 = \prod_{\substack{p^\alpha \| m \\ p \equiv 1 \pmod 4}} \left(1 - (p)_\infty^2 \sum_{0 \leqslant \beta + \gamma < \alpha} (p^{\beta+\gamma}(p)_\beta(p)_\gamma)^{-1}\right),$$

$$P_3 = \prod_{\substack{p^\alpha \| m \\ p \equiv 3 \pmod 4}} \left(1 - (p^2)_\infty/(p^2)_{[(\alpha-1)/2]}\right).$$

Examples.

$$m = 3: \ 0.123440; \quad m = 5: \ 0.421894;$$
$$m = 7: \ 0.020825; \quad m = 9: \ 0.123440;$$
$$m = 11: 0.008333; \quad m = 13: 0.158813.$$

(c) $\mathrm{pr}(r_\mathfrak{p}^A(H_{K/k}) = r) = (N\mathfrak{p})^{-r^2}(N\mathfrak{p})_\infty/(N\mathfrak{p})_r^2$.

If $p \equiv 1 \pmod 4$, then

$$\mathrm{pr}\left(r_p^{\mathbf{Z}}(H_{K/k}) = r\right) = (p)_\infty^2 \sum_{t+u=r} p^{-t^2-u^2}/\left((p)_t^2(p)_u^2\right).$$

If $p \equiv 3 \pmod 4$, then

$$\mathrm{pr}\left(r_p^{\mathbf{Z}}(H_{K/k}) = r\right) = \begin{cases} 0 & \text{if } r \text{ is odd,} \\ p^{-r^2/2}(p^2)_\infty/(p^2)_{r/2}^2 & \text{otherwise.} \end{cases}$$

Examples.

$$p=3: \ r = 0: 0.876560; \quad r = 2: 0.123266;$$
$$r \geqslant 4: 0.000173;$$
$$p=5: \ r = 0: 0.578106: \quad r = 1: 0.361316;$$
$$r = 2: 0.059592; \quad r \geqslant 3: 0.000986.$$

(d) If $p \equiv 1 \pmod 4$, then

$$\mathscr{M}\left(p^{nr_v^A(H_{K/k})}\right) = \sum_{i=0}^{n} p^{i(n-i)}(p)_n/((p)_i(p)_{n-i}),$$

$$\mathscr{M}\left(p^{nr_p^{\mathbf{Z}}(H_{K/k})}\right) = \left(\mathscr{M}\left(p^{nr_v^A(H_{K/k})}\right)\right)^2.$$

Examples.

$$n = 1: 4; \quad n = 2: (p+3)^2.$$

If $p \equiv 3 \pmod 4$, then

$$\mathscr{M}\left(p^{2nr_v^A(H_{K/k})}\right) = \mathscr{M}\left(p^{nr_p^{\mathbf{Z}}(H_{K/k})}\right) = \sum_{i=0}^{n} p^{2i(n-i)}(p^2)_n/((p^2)_i(p^2)_{n-i}).$$

Examples.

$$n = 1: 2; \quad n = 2: p^2 + 3.$$

(e) $\mathscr{M}(h_{K/k}) = \infty$.

(4.2) *Totally real cyclic quartic fields.*

$$(r_1 = 4, r_2 = 0),$$
$$\mathscr{M}(f) = M_{\neq 2}^A(f; 1).$$

Remark. For the full class group H_K,

$$\mathscr{M}(f) = M_{\neq 2}^B(f; 1, 1),$$

where $B = \mathbf{Z} \times \mathbf{Z}[i]$.

(a)

$$\mathrm{pr}(H_{K/k} \simeq_A H) = \left(\frac{8}{\pi} h(2)_\infty C(A) |\mathrm{Aut}_A H|\right)^{-1},$$

$$\mathrm{pr}(h_{K/k} = h) = \left(\frac{8}{\pi} h^2(2)_\infty C(A)\right)^{-1} \sum_{N\mathfrak{a}=h} \prod_{\mathfrak{p}^\alpha \| \mathfrak{a}} (N\mathfrak{p})_\alpha^{-1}.$$

Here, $\mathfrak{a}$ runs through all integral ideals of A of norm h, and $\mathfrak{p}$ through prime ideals dividing $\mathfrak{a}$.

Examples.

$h = 1$: 0.864608;

$h = 5$: 0.086461 (50% for each of the two A-isomorphism classes);

$h = 9$: 0.012008 (here, $H \simeq_{\mathbf{Z}} (\mathbf{Z}/3\mathbf{Z})^2$);

$h = 13$: 0.011085 (50% for each of the two A-isomorphism classes).

(b) $\mathrm{pr}(m \mid h_{K/k}) = P_1 P_3$, where

$$P_1 = \prod_{\substack{p^\alpha \| m \\ p \equiv 1 \pmod 4}} \left(1 - ((p)_\infty^2/(p)_1^2) \sum_{0 \le \beta+\gamma < \alpha} (p^{2\beta+2\gamma}(p)_\beta(p)_\gamma)^{-1}\right),$$

$$P_3 = \prod_{\substack{p^\alpha \| m \\ p \equiv 3 \pmod 4}} \left(1 - ((p^2)_\infty/(p^2)_1) \sum_{0 \le \beta < \alpha/2} (p^{4\beta}(p^2)_\beta)^{-1}\right).$$

Examples.

$$m = 3\colon\ 0.013870; \quad m = 5\colon\ 0.096709;$$
$$m = 7\colon\ 0.000425; \quad m = 9\colon\ 0.013870;$$
$$m = 11\colon 0.000069; \quad m = 13\colon 0.012774.$$

(c) $\mathrm{pr}(r_{\mathfrak{p}}^{A}(H_{K/k}) = r) = (N\mathfrak{p})^{-r(r+1)}(N\mathfrak{p})_{\infty}/((N\mathfrak{p})_{r}(N\mathfrak{p})_{r+1})$.

If $p \equiv 1 \pmod 4$, then

$$\mathrm{pr}\left(r_{p}^{\mathbf{Z}}(H_{K/k}) = r\right) = (p)_{\infty}^{2} \sum_{t+u=r} p^{-t(t+1)-u(u+1)}/((p)_{t}(p)_{t+1}(p)_{u}(p)_{u+1}).$$

If $p \equiv 3 \pmod 4$, then

$$\mathrm{pr}\left(r_{p}^{\mathbf{Z}}(H_{K/k}) = r\right) = \begin{cases} 0 & \text{if } r \text{ is odd,} \\ p^{-r(r+2)/2}(p^2)_{\infty}/\left((p^2)_{r/2}(p^2)_{(r/2)+1}\right) & \text{otherwise.} \end{cases}$$

Examples.

$$p=3\colon\ r = 0\colon 0.986130; \quad r = 2\colon 0.013867;$$
$$r \geqslant 4\colon 2.1 \times 10^{-6};$$
$$p=5\colon\ r = 0\colon 0.903291; \quad r = 1\colon 0.094093;$$
$$r \geqslant 2\colon 0.002617.$$

(d) If $p \equiv 1 \pmod 4$, then

$$\mathscr{M}\left(p^{nr_{\mathfrak{p}}^{A}(H_{K/k})}\right) = \sum_{i=0}^{n} p^{i(n-i-1)}(p)_{n}/((p)_{i}(p)_{n-i}),$$

$$\mathscr{M}\left(p^{nr_{p}^{\mathbf{Z}}(H_{K/k})}\right) = \left(\mathscr{M}\left(p^{nr_{\mathfrak{p}}^{A}(H_{K/k})}\right)\right)^{2}.$$

Examples.

$$n = 1\colon (1 + p^{-1})^{2}; \quad n = 2\colon (2 + p^{-1} + p^{-2})^{2}.$$

If $p \equiv 3 \pmod 4$, then

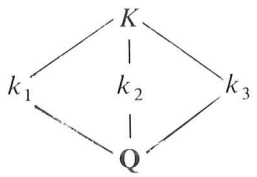
$$\mathscr{M}\left(p^{2nr_{\mathfrak{p}}^{A}(H_{K/k})}\right) = \mathscr{M}\left(p^{nr_{p}^{\mathbf{Z}}(H_{K/k})}\right) = \sum_{i=0}^{n} p^{2i(n-i-1)}(p^2)_{n}/((p^2)_{i}(p^2)_{n-i}).$$

Examples.

$$n = 1\colon 1 + p^{-2}; \quad n = 2\colon 2 + p^{-2} + p^{-4}.$$

(e) $\mathscr{M}(h_{K/k}) = \infty$.

(5) *Bicyclic Fields.*



$\Gamma = (\mathbf{Z}/2\mathbf{Z})^{2}$
bad prime: $\ell = 2$
$H_K \simeq H_{K_1} \times H_{k_2} \times H_{k_3}$

Our heuristics predict that these three groups behave independently, hence the desired conjectures for H_K or $H_{K/k_3} \simeq H_{k_1} \times H_{k_2}$ can easily be deduced from the conjectures in the quadratic case. For the sake of completeness we give the templates.

For H_K we take $A = \mathbf{Z}^3$.
For H_{K/k_3} we take $A = \mathbf{Z}^2$.
(5.1) *Totally complex bicyclic fields.*

$$(r_1 = 0,\ r_2 = 2).$$

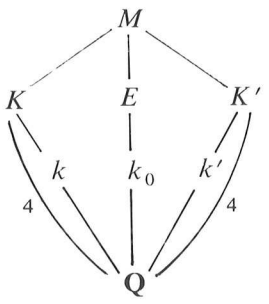
For H_K $(A = \mathbf{Z}^3)$: $\mathscr{M}(f) = M^A_{\neq 2}(f; 0, 0, 1)$.
For H_{K/k_3} $(A = \mathbf{Z}^2)$

$$\text{if } k_3 \text{ is complex:} \quad \mathscr{M}(f) = M^A_{\neq 2}(f; 0, 1),$$
$$\text{if } k_3 \text{ is real:} \quad \mathscr{M}(f) = M^A_{\neq 2}(f; 0, 0).$$

(5.2) *Totally real bicyclic fields.*

$$(r_1 = 4,\ r_2 = 0).$$

For H_K $(A = \mathbf{Z}^3)$: $\mathscr{M}(f) = M^A_{\neq 2}(f; 1, 1, 1)$.
For H_{K/k_3} $(A = \mathbf{Z}^2)$: $\mathscr{M}(f) = M^A_{\neq 2}(f; 1, 1)$ (here k_3 is real).
(6) *Dihedral Quartic Fields.*



$\Gamma = D_8$
bad prime: $\ell = 2$
Note. In this diagram $\mathrm{Gal}(M/k_0) \simeq \mathbf{Z}/4\mathbf{Z}$, while $\mathrm{Gal}(M/k) \simeq \mathrm{Gal}(M/k') \simeq (\mathbf{Z}/2\mathbf{Z})^2$. Only the relative class group $H_{K/k}$ is interesting, and we have

$$H_{M/E} \simeq H_{K/k} \times H_{K/k} \text{ and } H_{K'/k'} \simeq H_{K/k}.$$

$$A = \mathbf{Z}$$

(6.1) *Totally complex dihedral quartics with complex quadratic subfield k.*

$$(r_1 = 0,\ r_2 = 2),$$
$$\mathscr{M}(f) = M^{\mathbf{Z}}_{\neq 2}(f; 1).$$

For specific f and examples, see (1.2) (real quadratic fields).
(6.2) *Dihedral quartics of mixed signature.*

$$(r_1 = 2,\ r_2 = 1).$$

Same as (6.1).
(6.3) *Totally complex dihedral quartics with real quadratic subfield k.*

$$(r_1 = 0,\ r_2 = 2),$$
$$\mathscr{M}(f) = M^{\mathbf{Z}}_{\neq 2}(f; 0).$$

For specific f and examples, see (1.1) (complex quadratic fields).
(6.4) *Totally real dihedral quartic fields.*

$$(r_1 = 4,\ r_2 = 0),$$
$$\mathscr{M}(f) = M^{\mathbf{Z}}_{\neq 2}(f; 2).$$

(a)

$$\mathrm{pr}(H_{K/k} \simeq H) = \left(\frac{16}{\pi^2} h^2(2)_\infty C(\mathbf{Z})\, |\mathrm{Aut}\, H|\right)^{-1},$$

$$\mathrm{pr}(h_{K/k} = h) = \left(\frac{16}{\pi^2} h^3(2)_\infty C(\mathbf{Z}) \prod_{p^\alpha \| h} (p)_\alpha\right)^{-1}.$$

Examples.

$h = 1$: 0.930775; $h = 3$: 0.051710;
$h = 5$: 0.009308; $h = 7$: 0.003166;
$h = 9$: 0.002155 $\left(H \simeq \mathbf{Z}/9\mathbf{Z}\text{: } 0.001915;\ H \simeq (\mathbf{Z}/3\mathbf{Z})^2\text{: } 0.000239\right)$.

(b) $\mathrm{pr}(m \mid h_{K/k}) = \prod_{p^\alpha \| m}(1 - ((p)_\infty/(p)_2)\Sigma_{0 \leqslant \beta < \alpha}(p^{3\beta}(p)_\beta)^{-1})$.
Examples.

$m = 3$: 0.054787; $m = 5$: 0.009983;
$m = 7$: 0.003400; $m = 9$: 0.002275.

(c) $\mathrm{pr}(r_p(H_{K/k}) = r) = p^{-r(r+2)}(p)_\infty/((p)_r(p)_{r+2})$.
Examples.

$p=3$: $r = 0$: 0.945213; $r = 1$: 0.054532;
$r \geqslant 2$: 0.000256;
$p=5$: $r = 0$: 0.990017; $r = 1$: 0.009980;
$r \geqslant 2$: 3.3×10^{-6}.

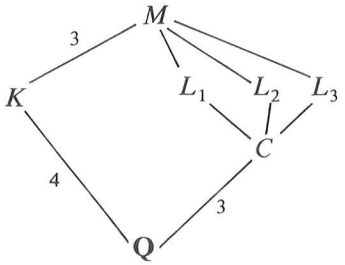
(d) $\mathscr{M}(p^{nr_p(H_{K/k})}) = \sum_{i=0}^{n} p^{i(n-i-2)}(p)_n/((p)_i(p)_{n-i})$.
Examples.

$n = 1$: $1 + p^{-2}$; $n = 2$: $1 + p^{-1} + p^{-2} + p^{-4}$.

(e) $\mathscr{M}(h_{K/k}) = \pi^2/8 = 1.233701$.

Remark. The conjectures that we obtain in the case D_8 are, as expected, the same as the ones that we would obtain for quadratic extensions of a fixed quadratic field k (such an extension being of type D_8 with probability 1).

(7) *Quartic Fields of Type A_4.*



$\Gamma = A_4$
bad prime: $\ell = 2$
$H_{M/C} \simeq H_K \times H_K \times H_K$ $(H_K \simeq H_{L_1}/C)$
$A = \mathbf{Z}$

(7.1) *Totally complex quartic fields of type A_4.*

$(r_1 = 0,\ r_2 = 2)$,
$\mathscr{M}(f) = M^{\mathbf{Z}}_{\neq 2}(f; 1)$.

For specific f and examples, see (1.2) (real quadratic fields).

(7.2) *Complex quartic fields of type A_4 of mixed signature.*

$(r_1 = 2,\ r_2 = 1)$.

These fields to not exist!

(7.3) *Totally real quartic fields of type A_4.*

$(r_1 = 4,\ r_2 = 0)$,
$\mathscr{M}(f) = M^{\mathbf{Z}}_{\neq 2}(f; 3)$.

(a)

$$\mathrm{pr}(H_K \simeq H) = \left(\frac{128}{7\pi^2\zeta(3)} h^3(2)_\infty C(\mathbf{Z})|\operatorname{Aut} H|\right)^{-1},$$

$$\mathrm{pr}(h_K = h) = \left(\frac{128}{7\pi^2\zeta(3)} h^4(2)_\infty C(\mathbf{Z}) \prod_{p^\alpha \| m} (p)_\alpha\right)^{-1}.$$

Examples.

$h = 1$: 0.978989; $h = 3$: 0.018129;
$h = 5$: 0.001958; $h = 7$: 0.000476;
$h = 9$: 0.000252 $\left(H \simeq \mathbf{Z}/9\mathbf{Z}$: 0.000224; $H \simeq (\mathbf{Z}/3\mathbf{Z})^2$: 0.000028$\right)$.

(b) $\mathrm{pr}(m \mid h_K) = \prod_{p^\alpha \| m}(1 - ((p)_\infty/(p)_3)\sum_{0 \leqslant \beta < \alpha}(p^{4\beta}(p)_\beta)^{-1})$.
Examples.

$m = 3$: 0.018433; $m = 5$: 0.001999;
$m = 7$: 0.000486; $m = 9$: 0.000256.

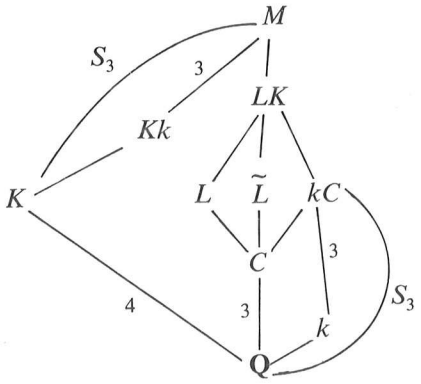
(c) $\mathrm{pr}(r_p(H_K) = r) = p^{-r(r+3)}(p)_\infty/((p)_r(p)_{r+3})$.
Examples.

$p=3$: $r = 0$: 0.981567; $r = 1$: 0.018404;
$r \geqslant 2$: 0.000029;
$p=5$: $r = 0$: 0.998001; $r \geqslant 1$: 0.001999.

(d) $\mathscr{M}(p^{nr_p(H_K)}) = \sum_{i=0}^{n} p^{i(n-i-3)}(p)_n/((p)_i(p)_{n-i})$.
Examples.

$$n = 1\text{: } 1 + p^{-3}; \quad n = 2\text{: } 1 + p^{-2} + p^{-3} + p^{-6}.$$

(e) $\mathscr{M}(h_K) = \frac{7}{8}\zeta(3) = 1.051800$.
(f) $\mathscr{M}(h_K^2) = \frac{7}{64}\pi^2\zeta(3) = 1.297606$.
(8) *Quartic Fields of Type* S_4.



$\Gamma = S_4$
bad prime: $\ell = 2$
$L = C(\sqrt{m})$ with $N_{C/\mathbf{Q}}(m) \in \mathbf{Q}^{*2}$
$H_{M/C} \simeq H_K \times H_K \times H_K$ and
$H_K \simeq H_{L/C}$
$A = \mathbf{Z}$

(8.1) *Totally complex quartic fields of type* S_4.

$$(r_1 = 0, r_2 = 2),$$
$$\mathscr{M}(f) = M^{\mathbf{Z}}_{\neq 2}(f; 1).$$

For specific f and examples, see (1.2) (real quadratic fields).
(8.2) *Quartic fields of type* S_4 *and mixed signature.*

$$(r_1 = 2, r_2 = 1),$$
$$\mathscr{M}(f) = M^{\mathbf{Z}}_{\neq 2}(f; 2).$$

For specific f and examples, see (6.4) (totally real dihedral quartic fields).

(8.3) *Totally real quartic fields of type* S_4.

$$(r_1 = 4,\ r_2 = 0),$$
$$\mathcal{M}(f) = M^{\mathbf{Z}}_{\neq 2}(f; 3).$$

For specific f and examples, see (7.3) (totally real quartics of type A_4).

3. Discussion. The tables that we have at our disposal (some of which having been extended specifically to test our conjectures) are as follows:

- Complex quadratic fields, $|D_K| \leqslant 2.5 \times 10^7$ [2].
- Real quadratic fields $\mathbf{Q}(\sqrt{p})$ with p prime, $p \leqslant 10^8$ [15].
- Cyclic cubic fields, $D_K \leqslant 2.56 \times 10^8$ ([9], [8]).
- Noncyclic complex cubic fields, $|D_K| \leqslant 2 \times 10^4$ [1].
- Pure cubic fields $\mathbf{Q}(\sqrt[3]{p})$ with p prime, $p \leqslant 10^6$ ([13], [15]).
- Noncyclic totally real cubic fields, $|D_K| \leqslant 5 \times 10^5$ [7].
- Some tables for fields of degree 4 and 6, which are not sufficiently extensive to make any significant statistics ([10], [12], [6]). In addition, C. P. Schnorr [14] kindly computed for us a few samples for $|D_K| \simeq 5 \times 10^8$ for complex quadratic fields.

The first observation is that for imaginary and real quadratic fields, and for cyclic cubics, the agreement with the tables is very good.

The second observation is that for noncyclic complex cubic fields, the agreement is not so good. Now in the non-Galois cubic case, as will be explained in [4], we have every reason to believe that the prime 2 behaves like a good prime. The poor agreement with the tables would seem to indicate that, either our whole strategy in the non-Galois case is wrong, or at least that 2 should be considered also a bad prime. However, the discriminants involved in the table of [1] are *not* very large. If we look at the subtable of pure cubic fields, the discriminant of $\mathbf{Q}(\sqrt[3]{p})$ is $3p^2$ or $27p^2$, according as $p \equiv \pm 1 \pmod 9$ or not, hence in the table of [15] the discriminants go up to more than 3×10^{12}. If we assume that, as a whole, pure cubics behave like any other complex cubics, then ordering them as usual by discriminants (and *not* by p!) we find very good agreement with the tables. Thus we believe that the poor agreement with [1] is due to the fact that the discriminants are not sufficiently large.

However, there is another phenomenon which has been stressed several times ([13], [15]) and which we repeat here: If one considers only $\mathbf{Q}(\sqrt[3]{p})$ with $p \equiv 2 \pmod 3$ prime (so as not to be bothered by the 3-part), and if one distinguishes between $p \equiv -1 \pmod 9$ and $p \equiv 2, 5 \pmod 9$, one notes a marked distinction in the behavior of the class group. For example, class number 1 seems to occur with probability 0.60 for $p \equiv -1 \pmod 9$, but with probability 0.40 for $p \equiv 2, 5 \pmod 9$. This is apparently due to the higher 2-part of the class group in the second case, and although a sort of reinterpretation of this phenomenon has been given in [5], no satisfactory heuristic explanation has yet been found.

Since $D_K \leqslant x$ is equivalent to $p \leqslant \sqrt{x/3}$ for $p \equiv -1 \pmod 9$ and $p \leqslant \sqrt{x/27}$ for $p \equiv 2, 5 \pmod 9$, by taking together all the $\mathbf{Q}(\sqrt[3]{p})$ with $p \equiv 2 \pmod 3$ and discrimi-

nant $\leqslant x$, we find an approximate probability of

$$\tfrac{3}{5} \times 0.60 + \tfrac{2}{5} \times 0.40 = 0.52$$

of having class number 1, very close to the predicted probability 0.5186.

A similar remark can be made about quartic extensions of type A_4 and S_4: The prime 3 *could* be bad. However, we think that this is not the case.

Acknowledgments. We are very grateful to D. A. Buell, H. C. Williams and D. Shanks for computing for us, or making available to us, tables which we used to check the validity of our conjectures. It is also a pleasure to thank G. Henniart, H. W. Lenstra, Jr., and J. Oesterlé for very fruitful discussions.

U.A. au C.N.R.S. No. 040226
U.E.R. de Mathématique et Informatique
Université de Bordeaux I
351, cours de la Libération
F-33405 Talence, Cedex, France

1. I. O. ANGELL, "A table of complex cubic fields," *Bull. London Math. Soc.*, v. 5, 1973, pp. 37–38.

2. D. A. BUELL, "The expectation of success using a Monte-Carlo factoring method—Some statistics on quadratic class numbers," *Math. Comp.*, v. 43, 1984, pp. 313–327.

3. H. COHEN & H. W. LENSTRA, JR., "Heuristics on class groups of number fields," *Number Theory* (Noordwijkerhout, 1983), Lectures Notes in Math., vol. 1068, pp. 33–62, Springer-Verlag, Berlin and New York, 1984.

4. H. COHEN & J. MARTINET, "Étude heuristique des groupes de classes." (In preparation.)

5. H. EISENBEIS, G. FREY & B. OMMERBORN, "Computation of the 2-rank of pure cubic fields," *Math. Comp.*, v. 32, 1978, pp. 559–569.

6. V. ENNOLA, S. MÄKI & R. TURUNEN, "On real cyclic sextic fields," *Math. Comp.*, v. 45, 1985, pp. 591–611.

7. V. ENNOLA & R. TURUNEN, "On totally real cubic fields," *Math. Comp.*, v. 44, 1985, pp. 495–518.

8. V. ENNOLA & R. TURUNEN, "On cyclic cubic fields," *Math. Comp.* v. 45, 1985, pp. 585–589.

9. M.-N. GRAS, "Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de **Q**," *J. Reine Angew. Math.*, v. 277, 1975, pp. 89–116.

10. M.-N. GRAS, "Classes et unités des extensions cycliques réelles de degré 4 de **Q**," *Ann. Inst. Fourier* (*Grenoble*), v. 29, 1979, pp. 107–124.

11. C. HOOLEY, "On the Pellian equation and the class number of indefinite binary quadratic forms," *J. Reine Angew. Math.*, v. 353, 1984, pp. 98–131.

12. S. MÄKI, *The Determination of Units in Real Cyclic Sextic Fields*, Lecture Notes in Math., vol. 797, Springer-Verlag, Berlin and New York, 1980.

13. D. SHANKS & H. C. WILLIAMS, "A note on class-number one in pure cubic fields," *Math. Comp.*, v. 33, 1979, pp. 1317–1320.

14. C. P. SCHNORR, Personal communication.

15. M. TENNENHOUSE & H. C. WILLIAMS, "A note on class-number one in certain real quadratic and pure cubic fields," *Math. Comp.*, v. 46, 1986, pp. 333–336.