CANADIAN THESES

THÈSES CANADIENNES

NOTICE

The quality of this microfiche is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Previously copyrighted materials (journal articles, published tests, etc.) are not filmed.

Reproduction in full or in part of this film is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30.

AVIS

La qualité de cette microfiche dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

Les documents qui font déjà l'objet d'un droit d'auteur (articles de revue, examens publiés, etc.) ne sont pas microfilmés.

La reproduction, même partielle, de ce microfilm est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30.

THIS DISSERTATION
HAS BEEN MICROFILMED
EXACTLY AS RECEIVED

LA THÈSE A ÉTÉ
MICROFILMÉE TELLE QUE
NOUS L'AVONS REÇUE

Canada

On the Vanishing of the Iwasawa Invariant λ for Totally Real Fields

Nelson R. Petulante

A Thesis

in

The Department

of

Mathematics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science at
Concordia University
Montreal, Quebec, Canada

January 1986

ISBN 0-315-30659-9

ABSTRACT

On the Vanishing of the Iwasawa Invariant λ for Totally Real Fields

Nelson R. Petulante

According to a conjecture of Greenberg , the Iwasawa invariant λ vanishes for all totally real fields . Various criteria are known which verify this conjecture for special cases provided certain conditions are satisfied . One of these criteria derives from an unpublished theorem of Kisilevsky . In this thesis the strengths and limitations of this criterion are examined . Based upon computations for several million pairs (p,K) where p is a splitting prime in a real quadratic field K, and upon similar computations for several thousand pairs (p',K') where p' is a splitting prime in a real cubic-cyclic field K', it is found that Kisilevsky's criterion implies that $\lambda = 0$ for all except a rare number of the cases tested . On the other hand it is shown that the criterion fails to determine the value of λ for infinitely many cases.

*

Acknowledgements

In the first place I want to thank my teacher Hershy Kisilevsky, originator of the idea behind this project. I remain especially grateful to him for having stimulated my interest in this superb subject.

In all fairness I must concede that a large part of the credit for the success of these computations must go to David Ford of the computer science department of Concordia University. In all, he has devoted several hundred hours of his time to helping me with this project.

Using the programming language ALGEB, developed by David Ford at The Ohio State University, it was possible to carry these computations to levels of integer precision unattainable with less suitable programming languages like FORTRAN, BASIC, or PASCAL. As suggested by its name, ALGEB is expressly designed for handling algebraic computations. Its main advantage for Number Theory is that it permits the use of integers of virtually unlimited size.

All of the computations for this thesis were done on a PDP1173 micro-computer and on a VAX mainframe computer, both of which were made accessible to me through David Ford

and John McKay at Concordia University's computer science department.

Finally I wish to express my warmest thanks to all members of the staff of Concordia University's mathematics department, especially professors Proppe, Malik, and Raphael.

Contents

Introduction 1

Chapter 1 : Preliminaries 3

Chapter 2 : The Quadratic Case 15

Chapter 3 : The Cubic Case 24

Chapter 4 : Some Questions 34

Appendix A : Tables

Appendix B : Program Listings

References

List of Symbols

$\mathbb{Z}$: rational integers

$\mathbb{Q}$: rational numbers

$\mathbb{C}$: field of complex numbers

$\mathbb{Z}_p$: ring of p-adic integers

$\mathbb{Q}_p$: p-adic metric completion of $\mathbb{Q}$

$\mathcal{O}_K$: ring of algebraic integers of K

S(K) : set of rational primes that split in K

R[x] : ring of polynomials in x over the ring R

$\mathfrak{M}$: Minkowski units of a number field (page 5)

$\mathfrak{M}_p$: p-Minkowski units of a number field (page 6)

Gal(K/Q) : Galois group of K/Q

$\mathfrak{P}$: prime ideal lying over a rational prime p

$\mathfrak{F}(p,x)$: page 34

$\langle\beta\rangle$: principal ideal generated by β

$\emptyset$: empty set

λ , μ , ν : Iwasawa invariants (page 2)

$\xi(p,K)$: page 6

$\eta(p,K)$: page 6

$R(\beta) = R_{p,K}(\beta)$: page 4

$R_p(K)$: Leopoldt's p-adic regulator

$\log_p(\beta)$: p-adic logarithm

h(K) : class number of K

$\mu_\beta(x)$: minimum polynomial of β

ζ_m : primitive m-th root of unity

$v_p(\beta)$: p-adic valuation of $\beta \in \mathbb{Q}_p$

1 : identity element of a multiplicative group

Introduction

Let p be a rational prime and let K be an algebraic number field. An infinite tower of extensions $K = K_0 \subset K_1 \subset K_2 \subset \ldots$ is called a Z_p-tower if $Gal(K_n/K) \cong Z/p^n Z$ for all $n \geq 1$.

Denote by K_∞ the union $\bigcup \{ K_n : n \geq 0 \}$. Relative to the system of restriction maps:

$$Gal(K_m/K) \cong Z/p^m Z \xrightarrow{\phi_{m,n}} Z/p^n Z \cong Gal(K_n/K) ,$$

where $m \geq n$, $Gal(K_\infty/K)$ is isomorphic to the inverse limit of the family $\{Gal(K_n/K) : n \geq 0\}$. It follows that $Gal(K_\infty/K) \cong Z_p$, the additive group of p-adic integers. The extension K_∞/K is called a Z_p-extension.

Every number field K has at least one Z_p-extension, namely the cyclotomic Z_p-extension, which can be constructed as follows:

Let $q = 4$ if $p = 2$, otherwise let $q = p$. Denote by B_n the subfield of $Q(\zeta_{qp^n})$ (unique unless $p = 2$ and $n = 1$) which is cyclic of degree p^n over Q. Then $Q = B_0 \subset B_1 \subset B_2 \subset \ldots$ is a Z_p-tower and B_∞/Q is a Z_p-extension, where $B_\infty = \bigcup \{ B_n : n \geq 0 \}$. Let $K_\infty = K B_\infty$. Then K_∞/K is itself a Z_p-extension, called the cyclotomic Z_p-extension of K.

Let $K = K_0 \subset K_1 \subset K_2 \subset \ldots$ be a Z_p-tower, and let p^{e_n} denote the exact power of p dividing the class number of K_n. According to a theorem of Iwasawa [1], there exist integers $\lambda = \lambda(p,K) \geq 0$, $\mu = \mu(p,K) \geq 0$ and $\nu = \nu(p,K)$ (known as the Iwasawa invariants) such that $e_n = \lambda n + \mu p^n + \nu$ for all n sufficiently large.

A conjecture of Iwasawa [2] holds that the invariant μ vanishes whenever K_∞/K is the cyclotomic Z_p-extension. This has been proved by Ferrero - Washington [3] in the case where $K/\mathbb{Q}$ is abelian.

On the other hand, it has been conjectured by Greenberg [4] that λ vanishes for all totally real number fields K.

In this thesis, heuristic evidence shall be given to support Greenberg's conjecture, at least as it pertains to quadratic and cubic-cyclic fields. The computations are based upon a criterion of Kisilevsky [5] which enables the conclusion that $\lambda = 0$ whenever the p-adic valuation of a certain regulator is minimal.

*

Chapter 1

1.1

Let $K/\mathbb{Q}$ be a totally real abelian extension of degree d, class number $h = h(K)$, and Galois group $\Delta = \{\sigma_1, \ldots, \sigma_d\}$. By the Normal Basis Theorem there exists in $\mathcal{O}_K$ an element θ such that $K = \mathbb{Q}(\theta)$ and $\{\sigma_1(\theta), \ldots, \sigma_d(\theta)\}$ is a basis for K over $\mathbb{Q}$.

Denote by $S(K)$ the set of all rational primes p that split completely in K. If $f(x)$ is the minimal polynomial of θ, then, for all but finitely many $p \in S(K)$, Kummer's lemma implies that $f(x) \equiv (x-r_1)\ldots(x-r_d) \bmod p$, where the roots $0 \leq r_i \leq p-1$ are distinct. If $\langle p \rangle = \mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_d$ where $\mathfrak{P}_1, \ldots, \mathfrak{P}_d$ are the prime ideals of K lying over p, then, without loss of generality, it may be assumed that $\mathfrak{P}_i = \langle p, \theta - r_i \rangle$, $(i = 1, \ldots, d)$.

By Hensel's lemma there exist in Z_p elements $\hat{\theta}_1, \ldots, \hat{\theta}_d$ such that $\hat{\theta}_i \equiv r_i \bmod p$ $(i = 1, \ldots, d)$ and $\hat{f}(x) = (x-\hat{\theta}_1)\ldots(x-\hat{\theta}_d)$ where $\hat{f}(x)$ denotes the image of $f(x)$ in $Z_p[x]$.

Let $D = \operatorname{disc}(\sigma_1(\theta), \ldots, \sigma_d(\theta)) \in \mathbb{Q}$. Then, for all but finitely many $p \in S(K)$, $v_p(D) = 0$. Since the ideals $\mathfrak{P}_i^h$

are principal , there exists some $\alpha \in \mathcal{O}_K$ such that $\mathfrak{P}_i^h = \langle \sigma_i(\alpha) \rangle$, $(i = 1,\ldots,d)$.

Since $\{\sigma_1(\theta),\ldots,\sigma_d(\theta)\}$ is a basis for K over $\mathbb{Q}$, there exist $c_{ij} \in \mathbb{Q}$, $(i,j = 1,\ldots,d)$ such that

$$\sigma_i(\alpha) = \sum_{j=1}^{d} c_{ij}\, \sigma_j(\theta)$$

Correspondingly , let $\hat{\alpha}_i \in \mathbb{Q}_p$ be defined by

$$\hat{\alpha}_i = \sum_{j=1}^{d} c_{ij}\, \hat{\theta}_j$$

If $v_p(D) = 0$ then $\hat{\alpha}_i \in Z_p$. Since $\sigma_1(\alpha)\ldots\sigma_d(\alpha) = \pm p^h$, exactly one of the $\hat{\alpha}_i$, say $\hat{\alpha}_1$, must satisfy $\hat{\alpha}_1 \equiv 0 \bmod p$. There exists an isomorphism $\phi : K_{\mathfrak{P}_1} \cong \mathbb{Q}_p$ such that $\phi(\sigma_i(\alpha)) = \hat{\alpha}_i$, $(i = 1,\ldots,d)$, and such that $v_p(\phi(\beta)) = \mathrm{ord}_{\mathfrak{P}_1}(\langle\beta\rangle)$ for all $\beta \in K$.

From here on , if $\beta \in K$, the expression $v_p(\beta)$ will be understood to mean $v_p(\phi(\beta))$.

1.2

For any $\beta \in K$ let

$$R_{p,K}(\beta) = \det(\log_p \sigma\tau^{-1}\beta)$$

where $\sigma, \tau \in \Delta$, $\sigma \neq 1$, $\tau \neq 1$. If there exists in K a unit ε which together with its conjugates generates the full group of units of $\mathcal{O}_K$, then $R_{p,K}(\varepsilon) = R_p(K)$ coincides with Leopoldt's p-adic regulator. The Leopoldt p-adic regulator is defined in terms of the value of the p-adic L-series at 1 [6].

In general , if $E = E(K)$ denotes the full group of units of $\mathcal{O}_K$ and if F denotes the subgroup of E generated by an arbitrary unit $\omega \in E$ together with its conjugates and ± 1, then $R_{p,K}(\omega) = [E : F]R_p(K)$. A conjecture of Leopoldt [7] holds that $R_p(K) \neq 0$ for all totally real number fields K. This has been proven for K/Q abelian [8].

As in section 1.1, let $p \in S(K)$, where $\langle p \rangle = \mathfrak{P}_1 \ldots \mathfrak{P}_d$, and let $E' = E'(p,K)$ denote the group of all $\nu \in \mathcal{O}_K$ for which $\mathrm{ord}_{\mathfrak{P}}(\langle \nu \rangle) = 0$ for all primes $\mathfrak{P} \notin \{\mathfrak{P}_1, \ldots, \mathfrak{P}_d\}$. There exists in E an element ε (called a Minkowski unit) which together with its conjugates generates a subgroup $M = M(\varepsilon)$ of finite index in E . Denote by $B = B(\alpha)$ the subgroup of E' generated by α and its conjugates (where, as before, $\langle \alpha \rangle = \mathfrak{P}_1^h$). Then $M \cap B = \{1\}$ and $E \times B$ is of finite index in E' . The index $c = [E' : M \times B]$ is bounded independently of p .

For any nontrivial character $\chi : \Delta \longrightarrow \mathbf{C}$ where $\Delta = \mathrm{Gal}(K/\mathbf{Q})$ and any $\beta \in K$ define

$$f_\chi(\beta) = \sum_{\sigma \in \Delta} \chi(\sigma) \log_p \sigma(\beta)$$

Then, if $\beta \in E'$,

$$R_{p,K}(\beta) = |\Delta|^{-1} \prod_{\chi \neq 1} f_\chi(\beta)$$

(for a proof see [8]).

Definition: Let $\varepsilon \in E$ be a Minkowski unit, and let $M = M(\varepsilon)$ denote the subgroup of E generated by ε and its conjugates. If $p \nmid [E : M(\varepsilon)]$ then ε is called a p-Minkowski unit. The set of all p-Minkowski units of K will be denoted by $\mathfrak{M}_p = \mathfrak{M}_{p,K}$ (possibly the empty set), while $\mathfrak{M} = \mathfrak{M}_K$ will denote the set of all Minkowski units (never empty).

In addition, define:

$$\eta(p,K) = \min \{ v_p(R_{p,K}(\varepsilon)) : \varepsilon \in \mathfrak{M} \}$$

$$\xi(p,K) = \min_{\omega \in E} \min_{\varepsilon \in \mathfrak{M}} \sum_{\chi \neq 1} \min\{v_p(f_\chi(\varepsilon)), v_p(f_\chi(\alpha\omega))\}$$

The computations in this thesis are based upon the following theorem of Kisilevsky [5]. Let c, h, d, $\lambda(p,K)$ be as above:

Theorem: Let $p \in S(K)$. Suppose that $p \nmid \mathrm{cnd}$. If $\xi(p,K) = d-1$ then $\lambda(p,K) = 0$.

1.3

The main task of this thesis is to compute $\eta(p,K)$ and $\xi(p,K)$ for certain pairs (p,K) where $p \in S(K)$. The computations are simplified by taking note of some elementary properties of the regulator $R = R_{p,K}$ and the related quantities $f(\chi,\cdot)$, η and ξ.

Proposition 1a: Suppose $\mathfrak{M}_p \neq \emptyset$. If $\omega \in E$ and $\varepsilon \in \mathfrak{M}_p$ then, for every $\chi \neq 1$,

$$v_p(f_\chi(\omega)) \geq v_p(f_\chi(\varepsilon))$$

Proof: Let $n = [E : M(\varepsilon)]$. There exist integers n_δ, $\delta \in \Delta$, $\delta \neq 1$, such that

$$\omega^n = \prod_{\substack{\delta \in \Delta \\ \delta \neq 1}} \delta(\varepsilon)^{n_\delta}$$

Thus $v_p(f_\chi(\omega)) = v_p(nf_\chi(\omega))$

$$= v_p(f_\chi(\omega^n))$$

$$= v_p(f_\chi(\prod_\delta \delta(\varepsilon)^{n_\delta}))$$

$$= v_p(\sum_\delta n_\delta f_\chi(\delta\varepsilon))$$

$$= v_p(\sum_\delta n_\delta \chi(\delta^{-1}) f_\chi(\varepsilon))$$

$$= v_p((\sum_\delta n_\delta \chi(\delta^{-1})) f_\chi(\varepsilon))$$

$$\geq v_p(f_\chi(\varepsilon))$$

Corollary (i): If $\mathfrak{M}_p \neq \emptyset$ and $\varepsilon, \varepsilon' \in \mathfrak{M}_p$ then

$$v_p(f_\chi(\varepsilon)) = v_p(f_\chi(\varepsilon'))$$

Corollary (ii): If $\mathfrak{M}_p \neq \emptyset$ and $\varepsilon \in \mathfrak{M}_p$ then

$$\xi(p,K) = \min_{\omega \in E} \sum_{\chi \neq 1} \min\{v_p(f_\chi(\varepsilon)), v_p(f_\chi(\alpha\omega))\}$$

Corollary (iii): If $\mathfrak{M}_p \neq \emptyset$ and $\varepsilon \in \mathfrak{M}_p$ then

$$\xi(p,K) = \sum_{\chi \neq 1} \min\{v_p(f_\chi(\varepsilon)), v_p(f_\chi(\alpha))\}$$

Proof of (iii): Since $v_p(f_\chi(\omega)) \geq v_p(f_\chi(\varepsilon))$ for all $\chi \neq 1$,

then $\min\{v_p(f_\chi(\varepsilon)), v_p(f_\chi(\alpha\omega))\}$

$$= \min\{v_p(f_\chi(\varepsilon)), v_p(f_\chi(\alpha)+f_\chi(\omega))\}$$

$$= \min\{v_p(f_\chi(\varepsilon)); v_p(f_\chi(\alpha))\}$$

Corollary (iv): If $\mathfrak{M}_p \neq \emptyset$ and $\varepsilon \in \mathfrak{M}_p$ then

$$\eta(p,K) = v_p(R_{p,K}(\varepsilon))$$

Proof of (iv): $v_p(R_{p,K}(\varepsilon)) = \sum_{\chi \neq 1} v_p(f_\chi(\varepsilon))$ is minimal for every $\varepsilon \in \mathfrak{M}_p$.

Proposition 1b: Let $\mathfrak{M}_p \neq \emptyset$, then

$$\eta(p,K) \geq \xi(p,k) \geq d-1$$

Proof: Let $\varepsilon \in \mathfrak{M}_p$. Then

$$\eta(p,K) = v_p(R(\varepsilon)) = \sum_{\chi \neq 1} v_p(f_\chi(\varepsilon))$$

$$\xi(p;K) = \sum_{\chi \neq 1} \min\{v_p(f_\chi(\varepsilon)), v_p(f_\chi(\alpha))\}$$

Since $\min\{v_p(f_\chi(\varepsilon)), v_p(f_\chi(\alpha))\} \leq v_p(f_\chi(\varepsilon))$ for each $\chi \neq 1$, it follows that $\eta \geq \xi$.

To show that $\xi \geq d-1$ it suffices to show that each of the terms

$$\min\{v_p(f_\chi(\varepsilon)), v_p(f_\chi(\alpha))\} \geq 1$$

For any $\beta \in \mathcal{O}_K$, $v_p(\log \beta) \geq 1$. Thus $v_p(f_\chi(\beta)) = v_p(\sum_{\sigma \in \Delta} \chi(\sigma) \log \sigma(\beta)) \geq 1$.

Proposition 1c: If $\beta \in E'$ then $v_p(R(\beta)) = v_p(R(\sigma\beta))$ for every $\sigma \in \Delta$.

Proof: $v_p(R(\beta)) = v_p(|\Delta|^{-1} \prod_{\chi \neq 1} f_\chi(\beta))$

$$= \sum_{\chi \neq 1} v_p(f_\chi(\beta))$$

So it suffices to show that $v_p(f_\chi(\sigma\beta)) = v_p(f_\chi(\beta))$ for every $\chi \neq 1$.

$$v_p(f_\chi(\sigma\beta)) = v_p(\sum_{\tau \in \Delta} \chi(\tau) \log \tau\sigma\beta)$$

$$= v_p(\sum_{\tau \in \Delta} \chi(\tau\sigma^{-1}) \log \tau\beta)$$

$$= v_p(\chi(\sigma^{-1}) \sum_{\tau \in \Delta} \chi(\tau) \log \tau\beta)$$

$$= v_p(\chi(\sigma^{-1}) f_\chi(\beta))$$

$$= v_p(f_\chi(\beta))$$

Proposition 1d: Let $\mathfrak{M}_p \neq \emptyset$, $\varepsilon \in \mathfrak{M}_p$. There exist integers r, s such that either $r=0$ and $s=1$ or $r=1$ and $0 \leq s \leq d-2$ such that $\xi(p,K) = v_p(R(\alpha^r \varepsilon^s))$.

Proof: For any r, $s \geq 0$:

$$v_p(R(\alpha^r \varepsilon^s)) = \sum_{\chi \neq 1} v_p(rf_\chi(\alpha) + sf_\chi(\varepsilon))$$

$$\xi(p,K) = \sum_{\chi \neq 1} \min\{v_p(f_\chi(\alpha)), v_p(f_\chi(\varepsilon))\}$$

So it suffices to find r, s of the required type such that, for every $\chi \neq 1$,

$$v_p(rf_\chi(\alpha)+sf_\chi(\varepsilon)) \geq \min\{v_p(f_\chi(\alpha)), v_p(f_\chi(\varepsilon))\}$$

Let's agree to say that a pair (r,s) is "okay for χ" if r, s, χ satisfy the above equation.

If $v_p(f_\chi(\varepsilon)) \leq v_p(f_\chi(\alpha))$ for all $\chi \neq 1$ then $(0,1)$ is okay for all $\chi \neq 1$.

Otherwise there is some character $\chi' \neq 1$ such that $v_p(f_{\chi'}(\varepsilon)) = v_p(f_{\chi'}(\alpha))$. Fix $r = 1$. If $v_p(f_\chi(\varepsilon)) \geq$

$v_p(f_\chi(\alpha))$ for all $\chi \neq 1$ then $(1,0)$ is okay for all $\chi \neq 1$. Otherwise there must exist some χ'' such that $v_p(f_{\chi''}(\varepsilon)) < v_p(f_{\chi''}(\alpha))$. Hence there are at most d-3 characters χ such that $v_p(f_\chi(\varepsilon)) = v_p(f_\chi(\alpha))$.

Let $\chi_1, \ldots, \chi_n$ $(n \leq d-3)$ be the characters satisfying

$$v_p(f_{\chi_i}(\varepsilon)) = v_p(f_{\chi_i}(\alpha))$$

Suppose a value s , $0 \leq s \leq d-2$, could be found such that $(1,s)$ is okay for $\chi_1, \ldots, \chi_n$. A moment's reflection shows that if $s \not\equiv 0 \bmod p$ then $(1,s)$ is okay for all remaining characters as well.

Hence the proposition will be completely proved if it could be shown that there exists $s \not\equiv 0 \bmod p$ such that $(1,s)$ is okay for $\chi_1, \ldots, \chi_n$. Since $p > d$ (by hypothesis), it suffices to find s in the range $1 \leq s \leq d-2$ such that $(1,s)$ is okay for $\chi_1, \ldots, \chi_n$.

Let

$$f_{\chi_i}(\alpha) = a_i p^{n_i} \ , \ f_{\chi_i}(\varepsilon) = b_i p^{n_i}$$

where a_i , b_i $(i = 1, \ldots, n)$ are units in Z_p. It suffices to find s ; $1 \leq s \leq d-2$, such that

$$a_i + sb_i \not\equiv 0 \bmod p \quad (i = 1, \ldots, n)$$

Each of these incongruences (of which there are at most d-3) is satisfied by all except possibly one value of s in the range $1 \leq s \leq d-2$. Hence there is at least one value of s in the range $1 \leq s \leq d-2$ which satisfies all the incongruences simultaneously.

<u>Corollary (i)</u>: Let K be a real quadratic field and let ε be the fundamental unit of K, then

$$\xi(p,K) = \min\{v_p(R(\varepsilon)), v_p(R(\alpha))\}$$

<u>Corollary (ii)</u>: Let K be a real cubic-cyclic field and let ε be a fundamental unit for K, then

$$\xi(p,K) = \min\{v_p(R(\varepsilon)), v_p(R(\alpha)), v_p(R(\alpha\varepsilon))\}$$

1.4

This chapter will conclude with a brief description of the steps used to compute $\eta(p,K)$ and $\xi(p,K)$.

Suppose $p \in S(K)$ and $\mathfrak{M}_p \neq \emptyset$. Since $\eta \geq \xi \geq d-1$ it is logical to first compute $\eta = v_p(R(\varepsilon))$. To do this it is

necessary to find a p-Minkowski unit ε of K. Except for the simplest fields this is not easy to do. Given ε, if it turns out that $\eta = d-1$ (as occurs in the great majority of cases tested) then $\xi = d-1$ and $\lambda = 0$.

On the other hand if $\eta > d-1$ then it is necessary to compute ξ by some other means. To do this, a generator α must be found for the principal ideal $\mathfrak{P}^h$ where $\mathfrak{P}$ is a prime ideal lying over p. In practice if $\alpha \in \mathcal{O}_K$ is chosen such that

$$N_{K/\mathbb{Q}}(\alpha) = \pm p^h$$

and $v_p(\hat{\alpha}_i) = h$ for some $\hat{\alpha}_i$ (as defined in section 1.1) then α generates $\mathfrak{P}^h$ for some prime $\mathfrak{P}$ lying over p. In general it is no easier to compute α than it is to compute ε. Given α, ξ is effectively determined by the formula

$$\xi = \min\{v_p(R(\alpha^r \varepsilon^s))\}$$

where either $r = 0$ and $s = 1$ or $r = 1$ and $0 \leq s \leq d-2$.

*

Chapter 2

2.1

Throughout this chapter K will denote a real quadratic field $\mathbb{Q}(\sqrt{D})$ where $D > 0$ is square-free, and $p > 2$ will denote a prime that splits in K.

To compute η and ξ for the pair (p,K), it is necessary to find a fundamental unit ε of $\mathcal{O}_K$. This can be accomplished quite efficiently using the well-known continued fraction algorithm.

Let $\varepsilon = e+f\sqrt{D}$ be the fundamental unit of K where e, f are integers (if $D \equiv 2, 3 \bmod 4$) or half-integers (if $D \equiv 1 \bmod 4$). Then

$$\eta = v_p(R(\varepsilon)) = v_p(\log_p \varepsilon)$$

To compute $v_p(\log_p \varepsilon)$ it is useful to observe that

$$\begin{aligned} v_p(\log_p \varepsilon) &= v_p((p-1)\log_p \varepsilon) \\ &= v_p(\log_p(1-(1-\varepsilon^{p-1})) \\ &= v_p(1-\varepsilon^{p-1}) \end{aligned}$$

Thus the problem is reduced to that of finding an approximation to the image of $\varepsilon = e+f\sqrt{D}$ in Z_p. Evidently it suffices to find the image of $\sqrt{D}$ in Z_p. By the Hensel lifting theorem one has only to find a solution of $x^2 \equiv D \bmod p$ then refine to Z_p .

Based upon the ideas in [9] , an algorithm can be devised for solving $x^2 \equiv D \bmod p$ which is , in my opinion , a rather good one ; especially since it can be modified to solve $x^n \equiv D \bmod p$ for $n > 2$, provided a solution is known to exist.

2.2

Suppose D is a quadratic residue mod p . To find a solution of $x^2 \equiv D \bmod p$, proceed as follows:

First choose a quadratic non-residue g mod p . It is thought that this can always be done in $O(\log^2 p)$ steps although the proof depends upon the Generalized Riemann Hypothesis [10] . The rest of the algorithm is easily seen to be of order $O(\log p)$.

Let $p-1 = 2^s m$ where $m = 2n+1$ is odd. Let $1 \leq t \leq s$ be the largest integer such that

$$D^{(p-1)2^{-t}} \equiv 1 \bmod p$$

If $t = s$, then

$$D^{a} \equiv x^{2a} \equiv 1 \bmod p$$

$$x^{a} \equiv \pm 1 \bmod p$$

$$x^{2n+1} \equiv \pm 1 \bmod p$$

$$D^{n+1} \equiv \pm x \bmod p .$$

Therefore both roots of $D \equiv x^2 \bmod p$ are obtainable by a power algorithm of order $O(\log p)$.

On the other hand, suppose $t < s$. Let $c_0 = 1$, $\delta_1 = 2$. Then

$$D^{(p-1)2^{-t-1}} \equiv -1 \equiv g^{\delta_1 (p-1)/2} g^{c_0 (p-1)2^{-1}} \bmod p$$

$$\equiv g^{c_1 (p-1)2^{-1}} \bmod p$$

where $c_1 = c_0 + \delta_1$.

In general , if $k \geq 1$ and if

$$D^{(p-1)2^{-t-k}} \equiv g^{c_k(p-1)2^{-k}} \mod p$$

Then

$$D^{(p-1)2^{-t-(k+1)}} \equiv \pm g^{c_k(p-1)2^{-(k+1)}} \mod p$$

$$\equiv g^{\delta_{k+1}(p-1)/2} g^{c_k(p-1)2^{-(k+1)}} \mod p$$

where $\delta_{k+1} = \begin{cases} 2 & \text{if the } + \text{ sign holds} \\ 1 & \text{if the } - \text{ sign holds} \end{cases}$

Therefore

$$D^{(p-1)2^{-t-(k+1)}} \equiv g^{c_{k+1}(p-1)2^{-(k+1)}} \mod p \qquad (2.21)$$

where $c_{k+1} = c_k + 2^k \delta_{k+1}$.

Since $s \geq t \geq 1$, $(p-1)2^{-(s-t)}$ is even , so let

$$y = g^{(p-1)2^{-(s-t)-1}} ,$$

then

$$D^{(p-1)2^{-s}} \equiv g^{(p-1)2^{-(s-t)}} \mod p \qquad (2.22)$$

(obtained from (2.21) by letting $k = s-t-1$). Thus:

$$D^m \equiv y^2 \mod p ,$$

where $m = (p-1)2^{-s} = 2n+1$. If x is a solution of $D \equiv x^2 \mod p$ then

$$x^m \equiv \pm y \mod p ,$$

$$x^{2n}x \equiv \pm y \mod p ,$$

$$D^n x \equiv \pm y \mod p .$$

The last congruence determines both solutions of $D \equiv x^2 \mod p$.

2.3

If $\eta(p,K) = 1$ then $\xi(p,K) = 1$, and so $\lambda = 0$. On the other hand, if $\eta > 1$ then ξ must be computed independently.

To do this , a generator $\alpha \in \mathcal{O}_K$ must be found for the principal ideal $\mathfrak{B}^h$ where $\mathfrak{B}$ is a prime lying over p and h is the class number of K . It suffices to find $\alpha \in \mathcal{O}_K$ such that

$$N(\alpha) = \pm p^h$$

and $\mathfrak{B} \nmid \langle \alpha \rangle$. The problem reduces to finding solutions x, y in integers (if $D \equiv 2, 3 \bmod 4$) or half integers (if $D \equiv 1 \bmod 4$) of the equation

$$x^2 - Dy^2 = \pm p^h \qquad (2.31)$$

such that $p \nmid xy$.

If a solution of (2.31) is known to exist , an algorithm based upon the "cyclic method" (see [11] for details) always yields a solution.

For example, suppose a solution is known to exist of the equation

$$x^2 - Dy^2 = m \ . \qquad (2.32)$$

For simplicity, assume that $D \not\equiv 1 \bmod 4$. Since (2.32) has a solution in integers x , y , D must be a quadratic residue mod m . Let r be a solution of

$$D \equiv r^2 \bmod m \ .$$

If u , v is a solution of

$$mu^2 + 2ruv + m^{-1}(r^2-D)v^2 = 1 \qquad (2.33)$$

then $x = mu+rv$, $y = v$ is a solution of (2.32) and $(x,y) = 1$. Thus , to solve (2.32) , it suffices to have available a method for solving

$$au^2 + buv + cv^2 = 1 \ .$$

A concrete example may best suffice to illustrate how the cyclic method works:

Suppose a solution in integers x_0, x_1 is sought of the equation

$$-7x_0^2 + 4x_0x_1 + 9x_1^2 = 1 \qquad (1)$$

Note that $x_0 > x_1$ is a necessary condition for a solution to exist . On the other hand , if $x_0 \geq 2x_1$ then $-7x_0^2+4x_0x_1+9x_1^2 \leq 0$. So let $x_0 = x_1+x_2$ where $x_1 > x_2 \geq 0$. Substituting this value for x in (1) produces:

$$6x_1^2 - 10x_1x_2 - 7x_2^2 = 1 \qquad (2)$$

If $x_1 < x_2$ then $6x_1^2-10x_1x_2-7x_2^2 < 0$, while if $x_1 \geq 3x_2$

then $6x_1^2-10x_1x_2-7x_2^2 > 1$. So let $x_1 = 2x_2+x_3$ where $x_2 > x_3 \geq 0$. Substituting in (2) produces:

$$-3x_2^2 + 14x_2x_3 + 6x_3^2 = 1 \qquad (3)$$

One final substitution with $x_2 = 5x_3+x_4$ begets:

$$x_3^2 - 16x_3x_4 - 3x_4^2 = 1 \qquad (4)$$

The last equation has the obvious solution $x_3 = 1$, $x_4 = 0$. A solution of (1) can now be recovered from the sequence of equations $x_2 = 5x_3+x_4$, $x_1 = 2x_2+x_3$, $x_0 = x_1+x_2$.

2.4

Using the algorithms described above together with some other standard number-theoretic routines (see Appendix B for program listings) we were able to compute $\eta(p,K)$ and $\xi(p,K)$ for all fields $K = \mathbb{Q}(\sqrt{D})$ and all splitting primes p in the ranges:

(1) $3 \leq D \leq 4111$; $3 \leq p \leq 547$

(2) $3 \leq D \leq 497$; $3 \leq p \leq 104729$

Tables summarizing the results of these computations are given in the first part of Appendix A.

No discrepancies have been found between these tables and the tables of Fukuda and Komatsu [12], which cover the range:

$$3 \leqslant D \leqslant 2000 \quad ; \quad p = 3, 5, 7$$

In Chapter 4 I shall take up a discussion of an unexpected heuristic found in connection with the quadratic case.

Chapter 3

3.1

Let $q \equiv 1 \bmod 3$ be a rational prime and let $K = K_q$ denote the unique cubic-cyclic field of conductor q. This means that q is the smallest positive integer such that $K \subset \mathbb{Q}(\zeta_q)$ where ζ_q is a primitive q-th root of unity. The discriminant of K_q is exactly q^2.

There exists $\theta \in \mathcal{O}_K$, and rational integers $a \equiv 1 \bmod 3$, $b > 0$, such that:

(i) $a^2 + 27b^2 = 4q$

(ii) The minimal polynomial of θ satisfies
$$27\mu_\theta(x) = 27x^3 + 27x^2 + 9(1-q)x - q(a+3) + 1$$

(iii) $\{1, \theta, \sigma(\theta)\}$ is a Z-basis for $\mathcal{O}_K$ where σ is a generator of $Gal(K/\mathbb{Q})$.

(iv) The discriminant of $\mu_\theta(x)$ is q^2b^2.

For a proof of these statements and related facts see [13].

It is known that there exists a unit $\epsilon \in \mathcal{O}_K$ (called a fundamental unit) with the property that ϵ together with

its conjugates generates the full group of units of $\mathcal{O}_K$. For all except a small number of values of m , Marie Nicole Gras [14] has computed the numbers a, b ; the coefficients of the minimal polynomial $\mu_\varepsilon(x)$ of the fundamental unit of K_m ; and the class number $h = h(K_m)$ for all cubic-cyclic fields of conductor $m < 4000$. The only values of m for which $\mu_\varepsilon(x)$ was not computed were those producing coefficients of $\mu_\varepsilon(x)$ of a size too large to be handled by the FORTRAN language. The smallest such value of m is $m = 919$.

3.2

As before , let $K = K_q$ denote the unique cubic-cyclic field of prime conductor q. Assume that a, b, $\mu_\varepsilon(x)$, and $h = h(K)$ are given. A rational prime p splits completely in K_q if and only if $p \neq q$ and p is a cubic residue mod q.

Assume that an isomorphism $K_{\mathfrak{P}} \longrightarrow \mathbb{Q}_p$ has been established , where $\mathfrak{P}$ is a prime of K lying over p.

If $\beta \in \mathcal{O}_K$ is such that $N_{K/\mathbb{Q}}(\beta) = \pm p^n$ for some $n \geq 0$, then

$$R_{p,K}(\beta) = \log_p^2\beta - \log_p\sigma(\beta)\log_p\sigma^2(\beta)$$

where $\sigma \in Gal(K/\mathbb{Q})$, $\sigma \neq 1$. To compute $v_p(R(\beta))$, it is useful to note that

$$v_p(R(\beta)) = v_p(\log_p^2(1-\gamma)) - \log_p(1-\sigma(\gamma))\log_p(1-\sigma^2(\gamma))$$

where $\gamma = 1-\beta^{p-1} \in pZ_p$. Since each of the terms $\log^2(1-\gamma)$, $\log(1-\sigma(\gamma))$, $\log(1-\sigma^2(\gamma))$ can be expanded in a power series, the highest power of p dividing $R(\beta)$ equals the highest power of p dividing a rational expression in γ, $\sigma(\gamma)$, $\sigma^2(\gamma)$. Thus $v_p(R(\beta))$ is effectively computable provided a sufficiently accurate approximation is obtainable to the images of β and its conjugates in Z_p.

If $\mu_\beta(x)$ is the minimum polynomial of β and if p does not divide $disc(\mu_\beta)$ then $\mu_\beta(x) \equiv 0 \bmod p$ has three distinct roots $0 \leq r_1, r_2, r_3 < p$. By Hensel's lemma these roots can be refined to solutions of $\mu_\beta(x) = 0$ in Z_p. Thus to compute the image of β and its conjugates in Z_p it is desirable to have available a method for solving $\mu_\beta(x) \equiv 0 \bmod p$.

3.3

In this section I will describe a method for obtaining the roots of a cubic congruence $f(x) \equiv 0 \bmod p$ provided it is known that the polynomial $f(x) \in Z[x]$ splits into distinct linear factors mod p.

To illustrate the method, suppose $f(x) = x^3 - a_0x^2 - b_0x - c_0$ and suppose it is known that $f(x) \equiv 0 \bmod p$ has three distinct roots, a situation that arises whenever $p \nmid \mathrm{disc}(f)$ and p splits completely in the splitting field of $f(x)$. To avoid trivialities assume that $p \geq 7$, and $c_0 \not\equiv 0 \bmod p$. If x is any one of the roots of $f(x) \equiv 0 \bmod p$, then

$$x^3 \equiv a_0x^2 + b_0x + c_0 \bmod p \qquad (1)$$

Multiply through by x:

$$x^4 \equiv a_0x^3 + b_0x^2 + c_0x \bmod p \qquad (2)$$

Substitute in (2) the expression for x^3 given by (1):

$$x^4 \equiv (a_0^2+b_0)x^2 + (a_0b_0+c_0)x + a_0c_0 \bmod p \qquad (3)$$

Multiply through by x again, and substitute in the new congruence the expression for x^3 given in (1), and so on...

In general if

$$x^{3+n} \equiv a_nx^2 + b_nx + c_n \bmod p$$

then

$$x^{3+n+1} \equiv a_{n+1}x^2 + b_{n+1}x + c_{n+1} \bmod p$$

where

$$\begin{bmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{bmatrix} = \begin{bmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \\ c_0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix}$$

Even better:

$$\begin{bmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{bmatrix} = \begin{bmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \\ c_0 & 0 & 0 \end{bmatrix}^{n+1} \begin{bmatrix} a_o \\ b_o \\ c_o \end{bmatrix}$$

If $n = (p-7)/2$ then by Fermat's Little Theorem:

$$x^{3+n} = x^{(p-1)/2} \equiv \pm 1 \mod p$$

And so

$$a_n x^2 + b_n x + c_n \equiv \pm 1 \mod p \qquad (3.31)$$

The original cubic congruence has thus been reduced to two quadratic congruences. Unless $a_n \equiv b_n \equiv 0 \mod p$ and $c_n \equiv \pm 1 \mod p$., all the roots of $f(x) \equiv 0 \mod p$ must be among the roots of (3.31). These roots can be obtained using the method described in section 2.2 .

What if it should turn out that $a_n \equiv b_n \equiv 0 \bmod p$ and $c_n \equiv \pm 1 \bmod p$, then what? Evidently this cannot happen unless all the three roots of $f(x) \equiv 0 \bmod p$ are either quadratic residues or quadratic nonresidues mod p.

To circumvent this problem define a new polynomial $f_1(x) = f(x+1)$. Apply the above algorithm using $f_1(x)$ instead of $f(x)$. Should the same problem arise, let $f_2(x) = f_1(x+1)$ and so on. By the same reasoning as in section 2.2, it should be possible in approximately $O(\log^2 p)$ steps to find a polynomial $f_k(x)$ having both a quadratic residue and a quadratic nonresidue among its roots.

The above method has been successfully implemented in the program GREEN3 which computes η and ξ for certain pairs (p,K) where K is a cubic-cyclic field and p is a splitting prime. For details see the program listings in Appendix B.

Although the details are harder to visualize, it appears possible to generalize the above method to solve congruences of the form $f(x) \equiv 0 \bmod p$ where $f(x)$ is a polynomial of degree $n \geq 3$.

3.4

If $\beta \in \mathcal{O}_K$ and p splits in $K = \mathbb{Q}(\beta)$, the above method for finding the image of β and its conjugates in Z_p works well provided that p does not divide the discriminant of $\mu_\beta(x)$. If $p \mid \mathrm{disc}(\mu_\beta)$ then an alternate approach is called for.

A feasible strategy is to find an element $\beta' = c_0 + c_1\beta + c_2\beta^2 \in \mathbb{Q}(\beta)$ such that $v_p(\mathrm{disc}(\mu_{\beta'})) \neq 0$. Then $\mu_{\beta'}(x) \equiv 0 \bmod p$ has three distinct roots which can be found using the algorithm of section 3.3. By Hensel's lemma these roots can be refined to the images of β' and its conjugates in Z_p. The image of β and its conjugates in Z_p can then be recovered from the relation $\beta' = c_0 + c_1\beta + c_2\beta^2$.

Based upon ideas from his Phd Thesis [15], David Ford has developed an algorithm which functions precisely as described in the preceding paragraph. This algorithm has been incorporated in GREEN3. For further details refer to GLOBAL PROCEDURE NEWPHI in Appendix B.

3.5

So far nothing has been said about the problem of finding a generator α for the principal ideal $\mathfrak{P}^h$ where $\mathfrak{P}$ is a

prime of K lying above p. If the class number h=1, it suffices to find $\alpha \in \mathcal{O}_K$ such that

$$N_{K/\mathbb{Q}}(\alpha) = \pm p$$

Using the Z-basis $\{1, \theta, \sigma(\theta)\}$ defined in section 3.1 , if $\alpha = x+y\theta+z\sigma(\theta)$, and if $\mu_\theta(x) = x^3-tx^2+sx-n$, then

$$N_{K/\mathbb{Q}}(\alpha) = x^3 + n(y^3+z^3) + tx^2(y+z) + sx(y^2+z^2) + dzy^2 + eyz^2 + fxyz \qquad (3.51)$$

where the coefficients d, e, f are determined by

$$2d = st - 3n + \delta$$
$$2e = st - 3n - \delta$$
$$f = t^2 - s$$
$$\delta^2 = \mathrm{disc}(\mu_\theta)$$

and where δ corresponds to the choice of $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ by the equation:

$$\delta = (\theta-\sigma(\theta))(\sigma(\theta)-\sigma^2(\theta))(\theta-\sigma^2(\theta)) .$$

At present, no simple computational strategy seems to be known for solving equations of type (3.51) . Since it is known that a solution exists, one might try looking for a solution near the origin on the lattice Z^3 .

The integer procedure NF3SOL (see Appendix B for details) starts at the origin , moves out along the yz-plane using an exhaustive search routine , and along the x-axis using a binary search routine , until a solution cf (3.51) is eventually encountered. Unfortuately this type of search can be a costly one . For this reason it was necessary in our application of this procedure to implement controls to abort the search if more than a reasonable length of time had elapsed.

Under these controls , solutions of (3.51) were found , where required , for all except four of the pairs (p,K) tested. For these four pairs the values of $\xi(p,K)$ and hence of $\lambda(p,K)$ remain undetermined.

3.6

Based upon the data given in [14] , the program GREEN3 (see Appendix B) was put to work computing $\eta(p,K)$ and $\xi(p,K)$ for all pairs (p,K) where $K = K_q$ is a real cubic-cyclic field of class number $h = 1$ and of prime conductor q in the range

$$7 \leq q \leq 907$$

and where p is a splitting prime in the range

$$5 \leq p < 10,000 .$$

There are 75 real cubic-cyclic fields with class number 1 and conductor q in the range $7 \leq q \leq 907$, and there are 1227 primes in the range $5 \leq p < 10,000$. Only 33 pairs (p,K) were found with $\eta(p,K) \geq 3$. For four of these pairs, NF3SOL failed to find a solution of (3.51) and so $\xi(p,K)$ remains undetermined. For all except these four pairs it was found that $\xi(p,K) = 2$ and so $\lambda(p,K) = 0$.

The results of the cubic computations are summarized in Table VI (Appendix B).

*

Chapter 4

4.1

For all except a rare number of the pairs (p,K) tested by GREEN2 and GREEN3 it has been found that $\xi(p,K) = d-1$. By Kisilevsky's Theorem (section 1.2), $\lambda(p,K) = 0$ for all except these rare cases. One might ask: just how rare are the cases for which Kisilevsky's Theorem fails to imply that $\lambda = 0$? Are there only finitely many such cases ?

Fix a rational prime p. Let $\mathcal{F}(p,x)$ denote the family of real quadratic fields $\mathbb{Q}(\sqrt{D})$ such that D is square-free, $D \leq x$, and p splits in $\mathbb{Q}(\sqrt{D})$. What is the probability of finding $K \in \mathcal{F}(p,x)$ such that $\eta(p,K) > 1$?

The remainder of this thesis is devoted to these and related questions. Throughout this chapter K will denote a real quadratic field and p will denote an odd prime that splits in K.

4.2

For a given pair (p,K) where p is an odd splitting prime in a quadratic field K, Kisilevsky's Theorem fails to determine the value of $\lambda(p,K)$ if either (i) the class number h(K) is divisible by p or (ii) $p \nmid h(K)$ and $\xi(p,K) \geq 2$.

To answer the first question above, we shall construct, for a fixed prime p, an infinite class of fields K such that Kisilevsky's Theorem fails to determine the value of $\lambda(p,K)$. Two lemmas are needed:

Lemma 1: Let p be an odd prime. Let $u(n) = 4p^{2n}+1$ ($n = 0, 1, 2, \ldots$). There exist infinitely many distinct fields of the form $\mathbb{Q}(\sqrt{u(n)})$.

Proof: The lemma follows easily from a result of C. L. Stewart [16] which (in diluted form) says: *let r, s, u(0), u(1) be integers and* $u(n) = ru(n-1)+su(n-2)$, $(n \geq 2)$. *Let A, B be the roots of* $x^2-rx-s = 0$. *Provided* $A \neq B$, *set* $a = ((u(1)-u(0)A)/(A-B)$ *and* $b = (u(0)B-u(1))/(A-B)$. *Suppose* $abAB \neq 0$ *and* A/B *is not a root of unity. Let* $q(u(n))$ *denote the greatest square-free factor of* $u(n)$. *Then*

$$q(u(n)) \geq C(n/(\log n)^2)^{1/d}$$

where C, d are positive constants independent of n.

Now let p be the given odd prime. Set $u(0) = 5$, $u(1) = 4p^2+1$, $r = p^2+1$, $s = -p^2$. Then $u(n) = ru(n-1)+su(n-2) = 4p^{2n}+1$. The conditions of Stewart's Theorem are easily seen to be satisfied and thus it follows that there exist infinitely many distinct fields in the sequence of fields $K_n = \mathbb{Q}(\sqrt{u(n)})$,

Acknowledgement: The proof of the above lemma is due to William Adams of the University of Maryland who showed me how to apply Stewart's result to this problem.

Lemma 2: Let p be an odd prime which splits in K. Suppose p does not divide the class number h of K, and suppose there exists an algebraic integer $\beta \in K$ such that $N(\beta) = p^r$ and $v_p(\beta) = r$. If $p \nmid r$ then $\xi(p,K) = \min\{v_p(\log\varepsilon), v_p(\log\beta)\}$ where ε is the fundamental unit of K.

Proof: The conditions on β imply that $\langle\beta\rangle$ (the principal ideal generated by β) $= \mathfrak{B}^r$ where $\mathfrak{B}$ is a prime ideal lying over p. So $\langle\beta^h\rangle = (\mathfrak{B}^h)^r$ where $\mathfrak{B}^h$ is principal. If $\mathfrak{B}^h = \langle\alpha\rangle$, then $\beta^h = \alpha^r\varepsilon^t$ where ε is the fundamental unit of K and $t \in Z$. Since $p \nmid r$, we may choose α such that $p \nmid t$. Then

$$\begin{aligned}
\xi(p,K) &= \min\{v_p(\log\alpha), v_p(\log\varepsilon)\} \\
&= \min\{v_p(\log\alpha^r), v_p(\log\varepsilon^t)\} \\
&= \min\{v_p(\log\alpha^r\varepsilon^t), v_p(\log\varepsilon^t)\} \\
&= \min\{v_p(\log\beta^h), v_p(\log\varepsilon^t)\} \\
&= \min\{v_p(\log\beta), v_p(\log\varepsilon)\}
\end{aligned}$$

Proposition 4a: Let $u(s) = 4p^{2s}+1$ $(s = 1, 2, 3, \ldots)$ and $K_s = Q(\sqrt{u(s)})$. For large enough s, if $p \nmid h(K_s)$ and $p \nmid s$ then $\xi(p,K_s) \geq 2$.

Proof: Let $q(s)$ denote the square-free part of $u(s)$ and let $\varepsilon = x+y\sqrt{q(s)}$ be the fundamental unit of K_s. Let

$$\omega = 2p^s + \sqrt{u(s)} = 2p^s + c\sqrt{q(s)}$$

where $u(s) = c^2 q(s)$. Then

$$N(\omega) = (2p^s + \sqrt{u(s)})(2p^s - \sqrt{u(s)})$$

$$= 4p^{2s} - (4p^{2s}+1) = -1$$

which implies that $\omega = \varepsilon^t$ for some $t \geq 1$. Let us first show that for s sufficiently large $v_p(\log\varepsilon) \geq 2$.

Note that $\sqrt{u(s)} \equiv \pm 1 \bmod p^s Z_p$ so that $\omega \equiv \pm 1 \bmod p^s Z_p$. Therefore

$$v_p(\log\omega) = v_p(\omega^{p-1}-1) \geq s$$

Since $\omega = \varepsilon^t$ it follows that

$$v_p(\log\varepsilon) + v_p(t) \geq s$$

If $v_p(\log\varepsilon) \leq 1$ then $v_p(t) \geq s-1$. But this renders impossible the equation

$$2p^s + c\sqrt{q(s)} = (x + y\sqrt{q(s)})^t$$

for s large enough. Thus we have shown that $v_p(\log\varepsilon) \geq 2$ for large enough s.

On the other hand, let $\beta = (1+\sqrt{u(s)})/2$ (this is an integer in K_s because $u(s)$ is of the form $4N+1$). Then $\beta \equiv 0$ or $1 \bmod p^s Z_p$ depending upon which square root of $u(s)$ is represented in Z_p. Without loss of generality assume that $\beta \equiv 0 \bmod p^s Z_p$ (then $\bar{\beta}$ (conjugate of β) $\equiv 1 \bmod p^s Z_p$). We have $N(\beta) = -p^{2s}$, and so, by lemma 2, if $p \nmid s$ then

$$\xi(p,K_s) = \min\{v_p(\log\varepsilon), v_p(\log\beta)\}$$

But $v_p(\log\beta) = v_p(\log\bar{\beta})$

$$= v_p(\bar{\beta}^{p-1} - 1)$$

$$\geq s$$

Therefore $\xi(p,K_s) \geq 2$.

4.3

In the preceding section it was shown that for a fixed p there exist infinitely many fields K such that either $p \mid h(K)$ or $\xi(p,K) \geq 2$ (in either case Kisilevsky's Theorem fails to determine the value of $\lambda(p,K)$). The analogous question for $\eta(p,K)$ is whether, given a fixed p, there exist infinitely many K such that $\eta(p,K) \geq 2$. Note that this question is unrelated to the divisibility properties of h(K) relative to p.

Proposition 4b: Let $p \geq 5$ and let $n \geq 1$. There exist infinitely many real quadratic fields K such that $\eta(p,K) = n$.

Proof: Let g be a primitive root for all powers of p. Let $x = r_0$ be the least positive solution of the linear congruence:

$$2g^{p^{n-1}} x \equiv g^{2p^{n-1}} + 1 \bmod p^{n+1}$$

Observe that $r_0 \equiv \pm 1 \bmod p$ is impossible if $p \geq 5$.

For $m = 1, 2, 3, \ldots$ set $a(m) = r_0 + mp^{n+1}$, $u(m) = a(m)^2 - 1$, and let $q(m)$ denote the greatest square-free part of $u(m)$. Since $a(m)+1 = r_0 + 1 + mp^{n+1}$ and $r_0 + 1$ is relatively prime to p, it follows by Dirichlet's Theorem on primes in arithmetic progressions that $a(m)+1$ is prime for infinitely many m. Therefore $q(m) > \sqrt{u(m)}$ for infinitely many m.

Let $\varepsilon = x+y\sqrt{q(m)}$ denote the fundamental unit of $\mathbb{Q}(\sqrt{u(m)})$ and let $\omega = a(m)+\sqrt{u(m)} = a(m)+c\sqrt{q(m)}$ where $u(m) = c^2 q(m)$. Then $N(\omega) = a(m)^2 - u(m) = 1$. Therefore $\omega = \varepsilon^t$ for some $t \geq 1$. But if m is chosen such that $q(m) > \sqrt{u(m)}$, then $a(m) = \sqrt{u(m)+1} \leq q(m)$, making the equation

$$a(m) + c\sqrt{q(m)} = (x + y\sqrt{q(m)})^t$$

impossible unless $t = 1$.

We have shown that there exist infinitely many distinct fields $K_m = \mathbb{Q}(\sqrt{u(m)})$ such that $\omega = a(m)+\sqrt{u(m)} = \varepsilon$ is the fundamental unit of K_m. It only remains to show that $\eta(p,K_m) = n$ for each of these fields. In other words, it only remains to show that $v_p(\varepsilon^{p-1} - 1) = n$ for each of these fields:

$$u(m) = a(m)^2 - 1$$

$$\equiv r_o^2 - 1 \bmod p^{n+1}\mathbb{Z}_p$$

$$\equiv (g^{2p^{n-1}} + 2 + g^{-2p^{n-1}})/4 - 1 \bmod p^{n+1}\mathbb{Z}_p$$

$$\equiv (g^{p^{n-1}} - g^{-p^{n-1}})^2/4 \bmod p^{n+1}\mathbb{Z}_p$$

$$\sqrt{u(m)} \equiv \pm(g^{p^{n-1}} - g^{-p^{n-1}})/2 \bmod p^{n+1}\mathbb{Z}_p$$

So $\varepsilon = a + \sqrt{u(m)} \equiv g^{\pm p^{n-1}} \bmod p^{n+1}\mathbb{Z}_p$. Therefore

$$\varepsilon^{p-1} \equiv 1 \bmod p^n\mathbb{Z}_p$$

which implies that $\eta(p,K_m) \geq n$. On the other hand the congruence

$$\varepsilon \equiv g^{\pm p^{n-1}} \bmod p^{n+1}\mathbb{Z}_p$$

also implies that $\varepsilon^{p-1} \equiv g^{\pm p^{n-1}(p-1)} \mod p^{n+1} Z_p$. But since g is a primitive root for all powers of p

$$g^{\pm p^{n-1}(p-1)} \not\equiv 1 \mod p^{n+1} Z_p .$$

Therefore $\eta(p, K_m) = n$ exactly.

4.4

As in section 4.1, let $\mathcal{F}(p,x)$ denote the family of real quadratic fields $K = Q(\sqrt{D})$ such that D is square-free , $D \leq x$, and p splits in $Q(\sqrt{D})$. Denote by $N(p,x)$ the cardinality of $\mathcal{F}(p,x)$ and by $n(p,x)$ the number of fields K in $\mathcal{F}(p,x)$ such that $\eta(p,K) \geq 2$. Let

$$\mathcal{F}(p) = \bigcup_{x=1}^{\infty} \mathcal{F}(p,x)$$

The actual probability $\text{prob}(p)$ that $\eta(p,K) \geq 2$ for a field K selected at random from $\mathcal{F}(p)$ is by definition

$$\text{prob}(p) = \lim_{x \to \infty} \frac{n(p,x)}{N(p,x)}$$

Starting from a naive point of view, it would seem fairly easy to form an estimate of $\text{prob}(p)$. In the absence of any information indicating otherwise , it is not unreason-

able to expect that for different fields $K \in \mathcal{F}(p)$ the fundamental units $\varepsilon = \varepsilon(K)$ should be randomly distributed mod $p^2 Z_p$. That is, naively one would expect that for any $a \not\equiv 0 \bmod p$ the event

$$\varepsilon(K) \equiv a \bmod p^2 Z_p$$

should occur with probability independent of a. In particular, the event

$$\varepsilon^{p-1} \equiv 1 \bmod p^2 Z_p$$

should occur with probability

$$\frac{p-1}{p^2-p} = \frac{1}{p}$$

How well does this expected figure compare with computed estimates of prob(p)? According to the data in Table II (see Appendix A) which gives $N(p,x)$ and $n(p,x)$ for all primes p in the range $3 \leq p \leq 547$ with $x = 4111$, the estimates for $p = 3, 5, 7$ are as follows:

prob(p)	1/p
prob(3) ≈ 262/935 ≈ .280	.333
prob(5) ≈ 197/1031 ≈ .191	.200
prob(7) ≈ 150/1091 ≈ .138	.143

It is seen that the computed estimates for prob(p) differ significantly from the expected figures at the right, which is somewhat of a mystery. The same reasoning that leads us to expect that prob(p) = 1/p also leads us to expect that the convergence of $n(p,x)/N(p,x)$ to prob(p) should be rather rapid as $x \longrightarrow \infty$. One is led to conclude that either prob(p) $\neq$ 1/p or there is some unknown principle at work which makes the convergence very slow.

Subsequent computations at the University of Maryland using the SPERRY UNIVAC mainframe (research sponsored by Lawrence Washington) have turned up the following figures for p = 3, 5 and $x = 10^6 + 1$.

$$n(3, 10^6+1)/N(3, 10^6+1) \approx .3187$$

$$n(5, 10^6+1)/N(5, 10^6+1) \approx .1975$$

Although these figures are closer to the expected values of prob(p), there is still enough difference to shed serious doubt on the conjecture that prob(p) = 1/p.

*

APPENDIX A

TABLES

Contents

Table I A-1

Lists all pairs (D,p) in the range $3 \leq D \leq 4111$, $3 \leq p \leq 547$, for which $\eta(p,K) \geq 2$, where p is a splitting prime in $K = \mathbb{Q}(\sqrt{D})$.

Table II A-13

Tabulates frequencies of values of $\eta(p,K)$ where $3 \leq D \leq 4111$, $3 \leq p \leq 547$, and p splits in $K = \mathbb{Q}(\sqrt{D})$. Column N displays the number of fields K for which $\eta(p,K) \geq N$.

Table III A-14

Tabulates frequencies of values of $\xi(p,K)$ where $3 \leq D \leq 4111$, $3 \leq p \leq 547$, and p splits in $K = \mathbb{Q}(\sqrt{D})$. Column N displays the number of fields K for which $\xi(p,K) \geq N$.

Table IV A-15

Lists all pairs (D,p) in the range $3 \leq D \leq 4111$, $3 \leq p \leq 547$, for which $\eta(p,K) \geq 2$, and for which the class number of $K = \mathbb{Q}(\sqrt{D})$ is divisible by the splitting prime p.

Table V A-16

Lists all pairs (D,p), in the range $3 \leq D \leq 497$, $3 \leq p \leq 104729$, for which $\eta(p,K) \geq 2$, where p is a splitting prime in $K = \mathbb{Q}(\sqrt{D})$.

Table VI A-19

Lists all pairs (q,p) in the range $7 \leq q \leq 907$, $5 \leq p < 10,000$, for which $\eta(p,K) \geq 3$, where p is a splitting prime in K, and K is a real cubic-cyclic field of conductor q and class number 1.

T A B L E I

The following table lists all pairs (D,P) in the range $3 \leq D \leq 4111$, $3 \leq P \leq 547$, for which eta(P,K) > 1, where K is the real quadratic field of discriminant D. An asterisk at the extreme right indicates that xi(P,K) > 1.

D	P	ETA	XI	D	P	ETA	XI	D	P	ETA	XI
6	523	2	1	114	5	2	1	247	3	4	1
10	191	2	1	123	7	2	2 *	251	11	2	1
15	181	2	1	123	17	2	1	253	3	2	2 *
19	79	2	1	130	167	2	1	253	7	2	1
23	7	2	1	131	23	2	1	259	5	2	2 *
31	157	2	1	134	5	2	1	262	41	2	1
33	29	2	1	139	3	2	2 *	265	241	2	1
33	37	2	1	139	5	3	1	265	263	2	1
34	37	2	1	139	23	2	1	266	37	2	1
34	547	2	1	142	73	2	1	267	7	2	1
35	23	2	1	145	17	2	1	267	11	2	1
37	7	2	1	145	37	2	1	267	31	2	1
39	5	2	1	149	7	2	1	267	131	2	1
39	7	2	1	151	3	2	1	269	11	2	1
43	3	2	1	161	5	2	1	271	3	3	1
51	5	2	1	165	199	2	1	271	5	2	1
57	59	2	1	173	227	2	1	281	17	2	1
58	3	2	1	179	7	2	1	285	89	2	1
58	23	2	1	181	3	2	1	286	173	2	1
62	263	2	1	185	139	2	1	295	3	2	2 *
67	3	3	2 *	186	5	2	2 *	295	7	2	1
67	11	2	1	187	29	2	1	301	107	2	1
69	5	2	1	191	5	3	2 *	302	19	2	1
69	17	3	1	199	3	2	1	303	7	2	1
71	67	2	1	199	19	2	1	303	107	2	1
73	41	2	1	201	211	2	1	307	97	2	1
74	7	2	1	202	3	2	1	309	11	2	1
79	3	2	1	209	167	2	1	310	3	2	1
82	3	2	1	210	37	2	1	313	11	2	1
82	11	2	1	210	41	2	1	314	5	2	1
85	3	2	1	211	5	2	1	317	23	2	1
87	17	2	1	211	31	2	1	318	41	2	1
89	5	3	1	213	19	2	1	319	139	2	1
91	41	2	1	214	5	2	1	322	3	2	1
103	3	2	2 *	214	7	2	1	323	11	3	1
103	13	2	1	215	19	2	1	326	5	2	1
106	3	2	2 *	218	7	2	1	327	19	2	1
106	379	2	1	218	11	2	1	329	71	2	1
109	3	2	1	219	7	2	1	330	227	2	1
109	5	2	1	219	109	2	1	331	3	2	1
110	29	2	1	223	11	2	1	337	3	2	1
111	107	2	1	238	3	3	2 *	337	7	2	1
113	53	2	1	241	5	2	1	341	13	2	2 *

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
347	79	2	1		491	13	2	1		593	31	2	1	
349	41	2	1		494	7	2	1		593	337	2	1	
355	457	2	1		494	43	2	1		602	283	2	1	
358	89	2	1		501	5	2	2	*	606	5	4	1	
362	211	2	1		501	7	2	1		606	19	2	1	
365	233	2	1		502	3	2	1		606	61	2	1	
366	5	2	1		503	19	2	1		607	3	2	2	*
370	113	2	1		503	233	2	1		607	13	2	1	
381	23	2	1		505	3	2	2	*	610	3	4	2	*
389	19	2	1		505	7	2	1		626	5	2	1	
390	11	2	1		506	347	2	1		627	251	2	1	
391	3	2	1		509	5	2	1		629	5	2	1	
394	23	2	1		509	11	2	1		634	3	4	1	
397	3	2	2	*	509	29	2	1		634	5	4	1	
397	73	2	1		511	3	4	1		634	23	2	1	
401	29	2	1		514	5	3	1		634	443	2	1	
403	7	2	1		515	11	2	1		651	73	2	1	
406	3	2	1		515	61	2	1		653	19	2	1	
406	41	2	1		519	5	2	1		654	103	2	1	
407	139	2	1		519	7	2	1		661	43	2	1	
413	13	2	1		521	11	2	2	*	663	11	2	1	
415	7	2	1		526	5	2	1		663	137	2	1	
415	13	2	1		526	29	2	1		665	37	2	1	
417	7	2	2	*	526	47	2	1		667	3	2	1	
417	227	2	1		527	263	2	1		674	5	2	1	
417	433	2	1		530	61	2	1		679	3	2	2	*
418	3	2	2	*	533	103	2	1		679	17	2	1	
426	5	2	1		534	5	2	2	*	679	23	2	1	
426	17	2	1		534	31	2	1		679	41	2	1	
430	61	2	1		534	103	2	1		681	17	2	1	
434	5	3	2	*	535	31	2	1		683	29	2	2	*
443	11	2	1		535	89	2	1		683	439	2	1	
445	23	2	1		535	173	2	1		685	19	2	1	
445	193	2	1		537	13	2	1		685	439	2	1	
446	131	2	1		541	5	2	1		687	37	2	1	
449	7	3	1		542	11	2	1		694	3	2	1	
451	109	2	1		543	31	2	1		695	7	2	2	*
454	3	2	2	*	554	7	2	2	*	698	17	2	1	
455	37	2	1		554	173	2	1		699	5	2	2	*
457	3	2	1		562	197	2	1		705	13	2	1	
458	13	2	1		571	3	2	1		706	383	2	1	
462	23	2	1		574	5	2	1		710	61	2	1	
462	251	2	1		581	5	2	1		714	19	2	2	*
463	19	2	1		583	7	2	1		715	373	2	1	
466	5	2	1		589	5	3	1		717	61	2	1	
470	7	2	1		589	101	2	1		718	271	2	1	
478	7	2	1		590	101	2	1		719	5	2	1	
478	23	2	1		591	31	2	1		727	3	3	2	*
478	397	2	1		591	191	2	1		730	3	3	1	
489	5	2	1		593	19	2	1		731	13	2	1	

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
731	53	2	1		851	11	2	1		971	251	2	1	
731	229	2	1		854	17	2	1		973	11	2	1	
733	3	3	1		854	29	2	1		977	11	3	1	
734	5	2	2	*	857	29	2	1		977	31	2	1	
741	521	2	1		861	43	2	1		977	193	2	1	
742	43	2	1		862	11	2	1		978	311	2	1	
745	3	2	2	*	862	139	2	1		979	3	2	1	
749	29	2	1		862	163	2	1		979	79	2	1	
749	37	2	1		863	29	2	1		982	17	2	1	
749	73	2	1		863	293	2	1		983	103	2	1	
751	3	2	1		865	3	2	1		989	7	2	1	
751	7	2	1		869	5	2	1		989	19	2	1	
754	3	2	1		871	3	2	1		991	23	2	1	
755	47	2	1		871	109	2	1		994	3	2	2	*
758	7	2	1		874	3	2	1		995	7	2	2	*
761	5	2	1		874	5	2	1		997	3	2	1	
763	17	2	1		877	3	3	1		998	37	2	1	
763	29	2	1		878	19	2	1		1002	17	3	1	
767	7	2	1		878	23	2	1		1006	3	3	1	
767	17	2	1		881	5	2	2	*	1007	509	2	1	
767	283	2	1		886	3	2	2	*	1009	3	3	1	
770	173	2	1		890	29	2	2	*	1011	101	2	1	
770	269	2	1		897	59	2	1		1015	149	2	1	
771	7	2	1		897	229	2	1		1023	211	2	1	
771	23	2	1		898	13	2	1		1027	3	3	1	
773	11	2	1		899	23	2	1		1031	5	2	2	*
777	13	2	1		903	293	2	1		1034	197	2	1	
778	53	2	1		910	19	2	1		1037	211	2	1	
778	433	2	1		911	53	2	1		1039	11	2	1	
778	461	2	1		917	17	2	1		1041	5	2	1	
779	109	2	1		921	19	2	1		1041	13	2	1	
781	13	2	1		922	73	2	1		1043	23	2	1	
786	163	2	1		926	163	2	1		1045	7	2	1	
787	3	2	2	*	929	11	2	1		1047	113	2	1	
789	5	2	1		929	53	2	1		1049	11	2	1	
790	3	2	2	*	938	59	2	1		1049	19	2	1	
791	5	2	2	*	938	373	2	1		1051	3	3	1	
797	107	2	1		939	457	2	1		1051	5	3	2	*
798	79	2	1		941	397	2	1		1057	37	2	1	
802	3	2	1		946	283	2	1		1063	89	2	1	
803	59	2	1		951	29	2	1		1065	193	2	1	
807	11	2	1		953	103	2	1		1069	131	2	1	
807	17	2	1		955	11	2	1		1073	7	2	1	
809	109	2	1		958	37	2	1		1074	5	2	1	
809	347	2	1		959	13	2	1		1074	59	2	1	
823	109	2	1		966	5	2	1		1079	5	2	2	*
826	347	2	1		966	19	2	1		1086	5	2	1	
830	11	2	1		969	233	2	1		1086	131	2	1	
834	7	3	2	*	969	257	2	1		1087	23	2	1	
835	37	3	1		971	13	2	1		1102	3	2	2	*

D	P	ETA	XI	D	P	ETA	XI	D	P	ETA	XI
1102	271	2	1	1226	53	2	1	1322	13	2	1
1103	7	2	1	1231	5	2	1	1322	19	2	2 *
1109	37	2	1	1231	71	2	1	1322	251	2	1
1109	233	2	1	1237	3	2	1	1327	19	2	1
1111	5	2	2 *	1237	197	2	1	1327	23	2	1
1111	19	2	1	1241	11	2	1	1329	11	2	1
1111	227	2	1	1246	3	3	1	1330	3	4	1
1114	3	2	1	1246	47	2	1	1330	17	2	1
1114	13	2	1	1246	151	2	1	1330	347	2	1
1114	79	2	1	1247	7	2	1	1333	3	2	2 *
1115	113	2	1	1247	31	2	1	1333	107	2	1
1115	277	2	1	1247	89	2	1	1338	61	2	1
1117	3	3	1	1249	3	2	1	1339	3	3	1
1117	199	2	1	1258	3	3	1	1339	5	2	1
1118	17	2	1	1258	11	2	2 *	1339	127	2	1
1119	43	2	1	1258	23	2	1	1342	13	3	1
1121	7	2	1	1259	17	2	1	1342	37	2	1
1126	3	2	1	1261	3	2	2 *	1342	149	2	1
1131	11	2	1	1261	5	2	2 *	1343	31	2	1
1133	271	2	1	1261	409	2	1	1346	197	2	1
1135	3	3	1	1265	31	2	1	1347	23	2	1
1135	17	2	1	1265	71	2	1	1351	5	2	1
1135	491	2	1	1267	17	2	1	1353	7	2	1
1146	89	2	1	1270	157	2	1	1354	71	2	1
1147	29	2	1	1271	29	2	2 *	1354	449	2	1
1153	3	2	2 *	1271	173	2	1	1358	167	2	1
1154	83	2	1	1273	109	2	1	1361	31	2	1
1162	3	2	1	1279	5	3	1	1365	11	3	1
1165	3	3	1	1279	11	2	1	1366	5	2	1
1167	13	2	1	1281	5	2	2 *	1366	13	2	1
1169	11	2	1	1283	67	2	1	1367	71	2	1
1171	7	2	1	1286	131	2	1	1370	29	2	1
1173	167	2	1	1286	439	2	1	1370	223	2	1
1181	47	2	1	1289	5	2	1	1373	7	3	3 *
1181	61	2	1	1294	3	2	2 *	1373	19	2	1
1191	5	2	1	1294	41	2	1	1374	131	2	1
1194	5	3	1	1297	3	2	1	1374	311	2	1
1194	7	2	1	1297	101	2	1	1379	67	2	1
1194	151	2	1	1299	11	2	1	1381	13	2	2 *
1195	3	2	1	1301	5	2	1	1383	7	2	1
1195	131	2	1	1303	11	2	1	1383	31	2	1
1198	293	2	1	1306	7	4	1	1383	467	2	1
1199	23	2	1	1306	73	2	1	1389	5	2	1
1201	167	2	1	1307	109	2	1	1389	11	2	2 *
1211	109	2	1	1310	263	2	1	1390	3	4	3 *
1213	3	7	1	1310	379	2	1	1397	83	2	1
1214	5	2	1	1311	7	2	1	1399	3	2	1
1219	11	2	1	1318	3	2	2 *	1401	197	2	1
1222	3	2	1	1319	347	2	1	1406	5	2	1
1226	13	2	1	1321	5	2	1	1414	47	2	1

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
1415	7	3	1		1574	11	2	1		1691	79	2	1	
1415	61	2	1		1574	283	2	1		1699	3	2	1	
1418	47	2	1		1578	41	2	1		1699	5	2	1	
1419	311	2	1		1579	3	2	1		1702	7	2	1	
1426	5	2	1		1579	43	2	1		1702	227	2	1	
1429	3	3	1		1582	19	3	1		1709	7	2	1	
1434	5	2	1		1582	61	2	1		1709	47	2	1	
1441	5	2	1		1585	3	2	1		1709	457	2	1	
1446	7	2	1		1586	5	2	1		1714	3	2	2	*
1446	17	2	1		1586	43	2	1		1721	281	2	1	
1447	17	2	1		1589	11	2	1		1726	3	2	2	*
1451	7	2	1		1590	7	2	2	*	1726	431	2	1	
1453	3	4	1		1595	43	2	1		1730	67	2	1	
1454	353	2	1		1599	29	2	1		1731	5	3	1	
1455	29	2	1		1603	3	2	1		1738	3	2	2	*
1457	59	2	1		1609	3	2	2	*	1738	13	2	1	
1461	5	2	1		1609	13	3	1		1738	17	2	2	*
1462	3	2	2	*	1610	11	2	1		1741	5	2	1	
1465	31	2	1		1613	13	2	1		1743	17	2	1	
1466	29	2	1		1615	13	2	1		1743	47	2	1	
1477	3	3	1		1615	179	2	1		1751	7	4	1	
1477	89	2	1		1621	5	3	1		1753	3	2	2	*
1479	5	2	1		1622	149	2	1		1753	73	2	1	
1486	3	2	1		1622	157	2	1		1754	5	2	2	*
1486	7	2	2	*	1622	541	2	1		1754	7	2	1	
1486	11	2	1		1627	53	2	1		1758	11	2	1	
1495	31	2	1		1627	433	2	1		1759	7	2	1	
1497	23	2	1		1630	53	2	2	*	1761	5	2	1	
1498	3	2	1		1631	5	2	1		1763	11	2	1	
1499	19	2	1		1634	89	2	1		1765	29	2	1	
1501	3	2	1		1635	7	2	1		1771	19	2	1	
1507	3	3	1		1639	13	2	1		1774	29	2	1	
1511	23	2	1		1641	5	4	1		1778	13	2	1	
1518	457	2	1		1642	3	2	2	*	1783	17	2	1	
1522	11	2	1		1642	541	2	1		1785	13	2	1	
1526	41	2	1		1645	3	2	1		1786	5	2	1	
1529	5	2	1		1657	29	2	1		1786	43	2	1	
1531	5	2	1		1659	31	2	1		1789	7	2	1	
1533	107	2	1		1662	31	2	1		1789	17	2	1	
1533	197	2	1		1663	3	2	1		1795	3	2	1	
1534	223	2	1		1669	3	2	2	*	1795	13	2	1	
1538	47	2	1		1669	23	2	1		1798	11	2	1	
1542	139	2	1		1670	19	2	1		1801	53	2	1	
1542	439	2	1		1670	173	2	1		1803	41	2	1	
1546	3	3	1		1671	59	2	1		1806	13	2	1	
1555	3	2	1		1678	3	3	1		1810	3	2	2	*
1565	47	2	1		1678	13	2	1		1811	17	2	1	
1567	11	2	1		1678	103	2	1		1821	61	2	1	
1567	47	2	1		1686	5	2	1		1822	89	2	1	
1569	73	2	1		1686	43	2	1		1829	5	2	1	

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
1829	11	2	1		1959	131	2	1		2045	347	2	1	
1829	43	2	1		1963	17	2	1		2047	11	2	1	
1830	23	2	1		1966	3	4	1		2047	73	2	1	
1834	3	2	1		1966	5	2	1		2047	181	2	1	
1834	5	2	1		1969	5	2	2	*	2049	19	2	1	
1835	23	2	1		1973	17	2	1		2053	13	2	1	
1843	257	2	1		1973	37	2	1		2059	3	3	3	*
1846	449	2	1		1974	11	2	1		2069	7	2	2	*
1851	5	2	1		1978	7	2	1		2069	71	2	1	
1853	11	2	1		1979	73	2	1		2074	3	2	1	
1853	503	2	1		1982	109	2	1		2078	113	2	1	
1855	3	3	1		1982	269	2	1		2081	37	2	1	
1858	3	2	1		1982	541	2	1		2082	11	2	1	
1858	23	2	1		1985	7	2	1		2082	19	2	1	
1861	5	2	2	*	1986	5	3	1		2082	379	2	1	
1861	101	2	1		1993	3	2	1		2083	3	2	1	
1865	31	2	1		1994	89	2	1		2083	13	2	1	
1867	3	6	2	*	1995	313	2	1		2085	47	2	1	
1870	3	2	1		1999	5	2	1		2087	31	2	1	
1874	5	2	1		2003	13	2	1		2089	47	2	1	
1879	17	2	2	*	2005	3	2	1		2091	67	2	1	
1882	3	3	1		2006	149	2	2	*	2094	7	3	1	
1887	7	2	1		2006	307	2	1		2101	5	2	2	*
1889	17	2	1		2010	7	2	1		2102	23	2	1	
1891	5	2	1		2011	41	2	1		2102	47	2	1	
1893	43	2	1		2014	5	3	1		2105	127	2	1	
1894	3	3	2	*	2018	7	2	2	*	2109	79	2	1	
1897	3	2	1		2018	11	2	1		2110	3	4	1	
1897	47	2	1		2018	107	2	1		2111	5	2	1	
1898	7	2	1		2021	17	2	1		2113	53	2	1	
1903	3	2	1		2022	11	3	1		2117	271	2	1	
1903	17	2	1		2022	43	2	1		2119	5	2	1	
1903	101	2	1		2026	3	2	1		2121	61	2	1	
1914	5	2	2	*	2026	61	2	1		2122	3	2	2	*
1921	3	2	1		2029	3	2	2	*	2123	61	2	1	
1921	5	3	1		2029	13	2	1		2135	53	2	1	
1921	23	2	1		2030	113	2	1		2135	149	2	1	
1923	67	2	1		2031	13	2	1		2137	3	3	1	
1934	7	2	1		2031	29	2	1		2137	11	2	1	
1934	257	2	1		2031	97	2	1		2141	41	3	1	
1942	211	2	1		2035	3	2	1		2146	3	2	1	
1945	3	2	1		2037	13	2	1		2147	29	2	1	
1945	79	2	1		2037	181	2	1		2149	3	4	4	*
1951	3	3	1		2037	547	2	1		2153	31	2	1	
1951	17	2	1		2038	7	2	1		2155	3	2	1	
1954	7	2	1		2038	13	2	1		2155	31	2	1	
1954	13	2	1		2038	157	2	1		2157	7	2	1	
1954	19	2	1		2039	19	2	1		2157	13	2	1	
1958	79	2	1		2042	107	2	1		2158	3	2	2	*
1959	5	2	2	*	2045	41	2	1		2158	167	2	1	

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
2161	3	3	1		2278	3	4	1		2411	337	2	1	
2165	359	2	1		2279	5	2	1		2413	3	2	1	
2167	3	2	1		2279	23	2	1		2418	47	2	1	
2170	23	2	1		2279	103	2	1		2423	71	2	1	
2171	5	2	1		2281	3	2	1		2426	61	2	1	
2173	239	2	1		2283	163	2	1		2429	17	2	1	
2179	7	2	2	*	2283	293	2	1		2431	3	2	2	*
2183	13	2	1		2285	13	4	1		2431	61	2	1	
2185	3	2	1		2287	13	2	1		2433	73	2	1	
2186	7	3	1		2289	11	2	1		2435	11	2	1	
2189	5	2	2	*	2290	53	2	1		2435	13	2	1	
2189	19	3	1		2290	139	2	1		2442	461	2	1	
2194	3	2	1		2293	271	2	1		2443	11	2	1	
2194	19	2	1		2302	31	2	1		2445	13	2	1	
2198	149	2	1		2310	43	2	1		2445	29	2	1	
2199	7	2	1		2311	7	2	2	*	2446	23	2	1	
2201	107	2	1		2314	3	2	1		2454	311	2	1	
2202	43	2	1		2314	29	2	1		2459	5	2	2	*
2203	23	2	1		2315	89	2	1		2461	7	2	1	
2210	37	2	1		2318	7	2	1		2463	331	2	1	
2211	19	2	1		2326	3	2	1		2465	7	2	1	
2215	3	2	1		2326	5	3	1		2467	19	2	1	
2215	19	2	1		2327	31	3	1		2467	31	2	1	
2218	43	2	1		2327	211	3	1		2469	17	3	1	
2221	3	3	2	*	2329	3	2	1		2470	3	3	1	
2226	11	2	1		2333	11	2	1		2471	5	2	1	
2226	17	2	1		2333	239	2	1		2473	3	3	1	
2230	3	2	2	*	2334	5	2	1		2479	11	2	1	
2230	7	2	2	*	2343	19	2	1		2485	73	2	1	
2231	17	2	1		2347	7	4	1		2486	13	2	1	
2233	3	3	1		2355	29	2	1		2487	359	2	1	
2234	5	2	1		2358	5	2	1		2490	23	2	1	
2237	7	2	2	*	2362	3	5	1		2490	97	2	1	
2237	11	2	1		2363	59	2	1		2490	277	2	1	
2242	17	2	1		2371	3	2	2	*	2491	283	2	1	
2243	17	5	1		2374	3	3	1		2495	17	2	1	
2245	13	2	1		2374	251	2	1		2498	11	2	1	
2246	37	2	1		2374	269	2	1		2498	31	2	1	
2247	293	2	1		2382	7	2	1		2501	5	2	2	*
2249	71	2	1		2386	5	2	1		2501	89	2	1	
2251	3	2	1		2391	5	2	1		2501	193	2	1	
2263	3	2	2	*	2395	421	2	1		2506	83	2	1	
2266	3	3	1		2399	5	2	1		2510	263	2	1	
2266	37	2	1		2402	7	2	1		2513	13	2	1	
2266	67	2	1		2402	167	2	1		2515	3	2	2	*
2266	139	2	1		2402	523	2	1		2517	419	2	1	
2269	7	2	1		2405	7	2	1		2518	3	3	1	
2269	29	2	1		2406	5	2	1		2521	3	3	2	*
2270	17	2	1		2410	3	3	2	*	2530	3	2	1	
2273	61	2	1		2411	5	3	1		2531	7	2	1	

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
2539	3	2	1		2642	479	2	1		2755	269	2	1	
2539	29	2	1		2647	7	2	1		2757	13	2	1	
2539	157	2	1		2651	13	3	1		2758	17	2	1	
2542	11	2	1		2653	503	2	1		2759	59	2	1	
2543	37	2	1		2654	5	2	1		2761	43	2	1	
2546	5	2	1		2657	23	2	2	*	2767	3	2	1	
2553	353	2	1		2657	139	2	1		2769	7	2	1	
2554	3	2	1		2658	23	2	1		2770	3	2	1	
2554	59	2	1		2659	3	3	2	*	2773	11	2	1	
2566	5	2	1		2661	5	3	1		2774	7	2	2	*
2570	179	2	1		2663	37	2	1		2778	349	2	1	
2571	5	3	3	*	2666	41	2	1		2779	19	2	1	
2571	257	2	1		2666	193	2	1		2779	181	2	1	
2573	223	2	1		2669	379	2	1		2785	103	2	1	
2578	7	2	2	*	2671	5	2	1		2786	13	2	1	
2579	5	2	1		2687	17	2	1		2791	3	2	1	
2586	197	2	1		2690	17	2	1		2794	3	3	2	*
2587	3	3	1		2694	5	2	1		2797	11	2	1	
2587	179	2	1		2698	11	2	1		2798	13	2	2	*
2589	101	2	1		2698	61	2	1		2802	7	2	2	*
2591	7	3	1		2699	7	2	1		2806	43	2	1	
2591	13	2	1		2701	3	5	3	*	2810	163	2	1	
2593	3	3	2	*	2701	17	2	1		2811	523	2	1	
2594	7	2	1		2701	419	2	1		2818	19	2	1	
2595	19	2	1		2702	37	3	1		2818	31	2	1	
2599	5	2	2	*	2707	3	2	1		2821	3	2	1	
2602	89	2	1		2715	137	2	1		2829	5	2	1	
2602	157	2	1		2717	7	2	1		2830	7	2	1	
2603	23	2	1		2719	3	2	1		2831	23	2	1	
2605	29	2	1		2719	173	2	1		2833	3	3	1	
2609	5	2	1		2721	19	2	1		2833	37	2	2	*
2609	19	2	1		2722	11	2	1		2837	59	2	1	
2611	3	3	1		2722	43	2	1		2841	71	2	1	
2613	443	2	1		2723	59	2	1		2845	61	2	1	
2613	487	2	1		2730	281	2	1		2846	13	2	1	
2614	3	4	1		2731	5	3	1		2847	43	2	1	
2615	7	2	1		2731	11	2	1		2851	5	2	1	
2621	167	2	1		2733	13	2	1		2851	7	2	1	
2623	3	2	1		2734	7	2	1		2857	17	2	1	
2627	7	2	1		2737	3	2	2	*	2859	59	2	1	
2627	101	2	1		2739	5	2	1		2859	73	2	1	
2629	3	3	1		2741	5	2	1		2863	43	2	1	
2633	7	4	1		2741	17	2	1		2870	293	2	1	
2633	193	2	1		2741	263	2	1		2874	7	2	2	*
2634	5	2	1		2743	3	3	2	*	2877	17	2	1	
2635	167	2	1		2743	11	2	1		2885	11	2	1	
2638	47	2	1		2746	5	2	1		2885	19	2	1	
2639	17	2	1		2746	7	2	1		2885	37	2	1	
2641	47	2	1		2749	401	2	1		2885	113	2	1	
2641	97	2	1		2753	7	4	1		2885	227	2	1	

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
2886	5	2	1		2993	17	2	1		3131	29	2	1	
2886	7	2	1		2994	5	2	1		3133	3	5	3	*
2887	167	2	1		2995	3	2	1		3139	83	2	1	
2887	271	2	1		2998	313	2	1		3139	433	2	1	
2894	197	2	1		3001	3	2	2	*	3142	3	2	1	
2899	83	2	1		3001	11	2	1		3147	7	2	1	
2902	41	2	1		3003	229	2	1		3147	13	2	1	
2905	19	2	1		3005	17	2	1		3149	11	2	1	
2909	7	2	1		3007	3	3	1		3157	3	3	1	
2911	5	2	1		3007	13	2	1		3165	29	2	1	
2913	13	2	1		3010	3	2	1		3166	5	2	2	*
2914	3	3	1		3013	17	2	1		3167	23	2	1	
2914	7	3	1		3019	23	2	1		3169	5	3	1	
2915	13	2	1		3021	191	2	1		3170	19	2	1	
2917	3	3	3	*	3022	17	2	1		3171	17	2	1	
2919	41	2	1		3026	7	2	2	*	3173	13	2	1	
2922	239	2	1		3026	139	2	1		3178	19	2	1	
2923	179	2	1		3035	17	2	1		3183	11	2	1	
2926	3	2	1		3039	5	3	2	*	3187	3	3	1	
2927	7	3	1		3039	13	2	1		3187	31	3	1	
2929	3	2	1		3041	5	3	1		3189	7	2	1	
2931	5	2	1		3046	7	2	1		3190	3	2	2	*
2931	257	2	1		3046	29	2	1		3190	97	2	1	
2935	13	2	1		3054	5	2	1		3191	11	3	1	
2935	167	2	1		3055	41	2	1		3193	41	2	1	
2939	47	2	1		3057	19	2	1		3194	5	2	1	
2939	389	2	1		3059	5	2	2	*	3194	11	2	1	
2942	181	2	1		3065	53	2	1		3197	13	2	1	
2945	257	2	1		3065	89	2	1		3199	3	2	2	*
2946	11	2	1		3067	3	2	1		3199	29	2	1	
2946	31	2	1		3077	7	2	1		3202	487	2	1	
2947	3	3	1		3082	3	3	1		3203	31	2	1	
2949	7	2	1		3085	13	2	1		3205	3	3	1	
2949	11	2	1		3085	71	2	1		3206	5	2	1	
2949	139	2	1		3094	3	2	2	*	3209	17	4	1	
2951	19	2	1		3095	23	2	1		3210	163	2	1	
2957	11	2	1		3098	7	2	2	*	3210	379	2	1	
2963	7	2	1		3101	5	3	2	*	3214	61	2	1	
2966	5	3	2	*	3101	79	2	1		3226	3	2	2	*
2966	101	2	1		3101	157	2	1		3226	5	2	1	
2966	173	2	1		3106	23	2	1		3227	19	2	1	
2967	59	2	1		3111	5	2	1		3227	223	2	1	
2969	73	2	1		3113	79	2	1		3233	13	2	1	
2973	19	2	1		3115	349	2	1		3235	3	2	2	*
2974	29	2	1		3119	103	2	1		3237	41	2	1	
2977	17	2	2	*	3121	23	2	1		3238	7	2	2	*
2981	19	2	1		3129	17	2	1		3239	103	2	1	
2986	3	3	1		3130	3	2	1		3241	3	2	1	
2991	5	2	1		3130	179	2	1		3241	13	2	1	
2993	11	3	1		3131	7	2	1		3242	7	2	1	

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
3243	71	2	1		3355	37	2	1		3497	19	2	1	
3251	5	3	1		3358	41	2	1		3499	5	2	1	
3254	307	2	1		3369	5	2	1		3502	3	2	1	
3257	463	2	1		3373	239	2	1		3502	29	2	1	
3259	3	5	1		3374	5	2	1		3503	29	2	1	
3263	31	2	1		3382	7	2	1		3506	5	2	2	*
3266	37	2	1		3385	13	2	1		3513	53	2	1	
3269	5	3	1		3386	29	2	1		3514	353	2	1	
3269	233	2	1		3386	47	2	1		3515	151	2	1	
3270	449	2	1		3387	277	2	1		3517	3	2	1	
3274	3	2	1		3387	383	2	1		3521	11	2	1	
3277	3	2	2	*	3391	3	4	2	*	3526	5	2	2	*
3278	181	2	1		3391	5	2	1		3526	89	2	2	*
3279	23	2	1		3397	3	2	1		3531	37	2	1	
3281	5	2	1		3397	29	2	1		3541	5	2	1	
3287	7	3	1		3397	37	2	1		3543	7	2	1	
3289	5	3	1		3401	17	2	1		3545	11	3	1	
3290	103	2	1		3401	419	2	1		3545	19	2	1	
3291	7	3	1		3409	5	2	1		3545	29	2	1	
3293	53	2	1		3409	127	2	1		3551	19	2	1	
3297	67	2	1		3414	11	2	1		3551	29	2	1	
3299	5	2	1		3418	137	2	1		3551	43	2	1	
3299	109	2	1		3421	271	2	1		3553	7	2	1	
3302	29	2	1		3422	43	2	1		3554	5	2	1	
3306	13	2	1		3427	19	2	1		3554	17	2	1	
3306	191	2	1		3434	227	2	1		3557	7	2	2	*
3307	3	2	1		3435	43	2	1		3557	233	2	1	
3307	293	2	1		3443	101	2	1		3565	13	2	1	
3309	179	2	1		3446	43	2	1		3566	13	2	1	
3311	5	2	1		3451	3	4	1		3566	409	2	1	
3311	233	2	1		3451	5	2	1		3567	163	2	1	
3314	139	2	1		3454	3	3	1		3569	5	2	1	
3322	97	2	1		3455	31	2	1		3571	3	2	2	*
3326	11	2	1		3455	137	2	1		3571	7	2	1	
3327	157	2	1		3457	29	2	1		3571	157	2	1	
3335	487	2	1		3458	151	2	1		3574	5	2	1	
3337	3	2	1		3459	19	2	1		3587	13	2	1	
3337	31	2	1		3462	7	2	1		3589	19	2	1	
3337	127	2	1		3466	151	2	1		3589	47	2	1	
3338	11	2	1		3469	3	2	2	*	3590	331	2	1	
3341	17	2	1		3469	5	2	1		3593	7	2	1	
3343	7	2	2	*	3470	13	2	1		3594	61	2	1	
3343	109	2	1		3470	53	2	1		3595	103	2	1	
3345	47	2	1		3471	5	2	1		3602	7	4	3	*
3345	53	2	1		3478	3	2	1		3605	31	2	1	
3349	5	3	2	*	3485	37	2	1		3606	7	4	1	
3349	43	2	1		3486	19	2	1		3606	67	2	1	
3353	19	2	1		3489	83	2	1		3607	331	2	1	
3354	7	2	2	*	3490	3	2	2	*	3615	31	2	1	
3355	3	2	2	*	3493	3	2	1		3619	3	4	1	

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
3619	443	2	1		3767	103	2	1		3873	113	2	1	
3622	17	2	1		3769	3	3	1		3873	157	2	1	
3622	103	2	1		3777	7	2	2	*	3877	13	2	1	
3631	11	2	1		3777	73	2	1		3886	11	2	1	
3637	3	2	1		3778	3	3	1		3893	7	3	1	
3639	5	2	1		3781	3	2	2	*	3893	139	3	1	
3641	53	2	1		3781	281	2	1		3895	3	3	2	*
3642	11	2	1		3782	7	2	1		3895	509	2	1	
3646	23	2	1		3782	283	2	1		3902	47	2	1	
3649	7	2	1		3783	17	2	2	*	3902	167	2	1	
3649	19	2	1		3786	5	3	2	*	3905	467	2	1	
3651	37	2	1		3787	3	2	2	*	3910	13	2	1	
3655	11	2	1		3797	19	2	1		3911	5	2	1	
3658	463	2	1		3797	59	2	1		3911	211	3	1	
3661	5	3	1		3799	3	2	1		3913	41	2	1	
3666	5	2	1		3799	5	2	2	*	3918	293	2	1	
3667	3	2	2	*	3803	7	2	1		3919	5	2	1	
3671	199	2	1		3811	11	2	1		3919	11	2	1	
3673	3	4	2	*	3813	79	2	1		3919	23	2	1	
3678	43	2	1		3814	31	2	1		3922	3	2	1	
3683	7	2	1		3814	97	2	1		3923	13	2	1	
3685	3	3	1		3818	367	2	1		3927	97	2	1	
3691	5	2	1		3819	7	2	1		3930	269	2	1	
3693	13	2	1		3819	13	2	1		3931	3	2	1	
3693	19	2	1		3823	17	2	1		3931	5	2	1	
3693	43	2	1		3826	3	2	1		3931	7	2	1	
3694	5	2	1		3829	5	2	2	*	3934	3	4	1	
3697	11	2	1		3830	347	2	1		3934	41	2	1	
3705	337	2	1		3831	73	2	1		3935	23	2	1	
3706	23	2	1		3833	7	2	2	*	3935	193	2	1	
3709	3	2	1		3833	31	2	1		3937	3	2	1	
3709	5	2	1		3835	521	2	1		3937	53	2	1	
3713	227	2	1		3845	13	3	1		3938	19	2	1	
3715	13	2	1		3845	443	2	1		3939	131	2	1	
3715	179	2	1		3847	3	2	2	*	3941	307	2	1	
3719	151	2	1		3847	13	2	1		3943	29	2	1	
3727	3	2	1		3849	13	2	1		3943	59	2	1	
3727	17	2	1		3853	3	3	1		3943	349	2	1	
3729	23	2	1		3854	31	2	1		3945	23	2	1	
3730	13	2	1		3855	101	2	1		3945	59	2	1	
3738	31	2	1		3855	491	2	1		3946	17	2	1	
3739	3	2	2	*	3858	7	2	1		3946	31	2	1	
3739	7	2	1		3858	43	2	1		3949	61	2	1	
3745	3	2	1		3859	37	2	1		3954	11	2	1	
3755	277	2	1		3859	71	2	1		3955	3	2	1	
3761	83	2	1		3859	89	2	1		3958	3	2	1	
3766	13	2	1		3862	31	2	1		3959	5	2	1	
3766	17	2	1		3866	5	2	1		3959	127	2	1	
3766	59	2	1		3866	11	2	1		3961	5	2	1	
3767	23	2	1		3873	37	2	1		3961	431	2	1	

D	P	ETA	XI		D	P	ETA	XI		D	P	ETA	XI	
3965	269	2	1		4013	11	2	1		4065	353	2	1	
3966	281	2	1		4019	47	2	1		4078	3	2	1	
3967	3	2	1		4021	3	3	1		4081	3	3	3	*
3970	3	2	1		4026	29	2	1		4082	61	2	1	
3970	223	2	1		4027	11	2	1		4087	3	2	1	
3973	3	2	1		4029	5	2	1		4089	101	2	1	
3977	7	2	1		4029	19	2	1		4091	269	2	1	
3979	3	3	2	*	4029	109	2	1		4093	3	3	1	
3981	5	2	1		4034	7	2	1		4093	67	2	1	
3982	13	2	1		4035	67	2	1		4094	101	2	1	
3982	29	2	1		4038	241	2	1		4099	3	2	2	*
3986	5	4	1		4038	263	2	1		4109	5	2	1	
3989	5	2	1		4039	13	2	1		4109	61	2	1	
3991	7	2	2	*	4039	317	2	1		4109	271	2	1	
3995	23	2	1		4053	71	2	1		4110	7	2	1	
3997	3	2	2	*	4061	5	3	1		4110	19	2	1	
3997	11	2	1		4061	7	2	1		4110	37	2	1	
3999	[redacted]	2	1		4061	433	2	1		4111	71	2	1	
3999	7	2	1		4061	461	2	1						
3999	53	2	1		4062	7	2	1						

TABLE II

P	1	2	3	4	5	6	7
3	935	262	88	23	6	2	1
5	1041	197	35	4	.	.	.
7	1091	150	19	7	.	.	.
11	1143	98	7	.	.	.	.
13	1160	86	5	1	.	.	.
17	1179	70	5	2	1	.	.
19	1187	65	2	.	.	.	.
23	1195	53	.	.	.	.	.
29	1208	47	.	.	.	.	.
31	1211	40	2	.	.	.	.
37	1214	34	2	.	.	.	.
41	1218	24	1	.	.	.	.
43	1222	29	.	.	.	.	.
47	1219	24	.	.	.	.	.
53	1228	20	.	.	.	.	.
59	1226	18	.	.	.	.	.
61	1231	24	.	.	.	.	.
67	1231	11	.	.	.	.	.
71	1224	14	.	.	.	.	.
73	1229	16	.	.	.	.	.
79	1229	12	.	.	.	.	.
83	1232	7	.	.	.	.	.
89	1238	16	.	.	.	.	.
97	1240	8	.	.	.	.	.
101	1235	13	.	.	.	.	.
103	1228	14	.	.	.	.	.
107	1232	9	.	.	.	.	.
109	1237	13	.	.	.	.	.
113	1236	7	.	.	.	.	.
127	1232	5	.	.	.	.	.
131	1237	9	.	.	.	.	.
137	1236	4	.	.	.	.	.
139	1237	12	1	.	.	.	.
149	1240	6	.	.	.	.	.
151	1240	6	.	.	.	.	.
157	1244	10	.	.	.	.	.
163	1243	7	.	.	.	.	.
167	1233	12	.	.	.	.	.
173	1238	8	.	.	.	.	.
179	1234	7	.	.	.	.	.
181	1243	6	.	.	.	.	.
191	1229	4	.	.	.	.	.
193	1241	7	.	.	.	.	.
197	1236	8	.	.	.	.	.
199	1235	3	.	.	.	.	.
211	1246	7	1	.	.	.	.
223	1236	5	.	.	.	.	.
227	1237	8	.	.	.	.	.
229	1243	3	.	.	.	.	.
233	1248	7	.	.	.	.	.

P	1	2	3
239	1227	4	.
241	1245	2	.
251	1245	5	.
257	1241	6	.
263	1234	7	.
269	1250	7	.
271	1227	8	.
277	1249	4	.
281	1241	4	.
283	1237	6	.
293	1244	8	.
307	1247	3	.
311	1222	4	.
313	1244	2	.
317	1247	1	.
331	1242	3	.
337	1244	3	.
347	1241	7	.
349	1243	3	.
353	1243	4	.
359	1226	2	.
367	1240	1	.
373	1251	2	.
379	1246	5	.
383	1224	2	.
389	1250	1	.
397	1251	2	.
401	1248	1	.
409	1244	2	.
419	1233	3	.
421	1243	1	.
431	1226	2	.
433	1235	5	.
439	1231	4	.
443	1243	4	.
449	1243	3	.
457	1239	4	.
461	1243	3	.
463	1235	2	.
467	1236	2	.
479	1227	1	.
487	1247	3	.
491	1246	2	.
499	1241	.	.
503	1232	2	.
509	1247	2	.
521	1244	2	.
523	1243	3	.
541	1243	3	.
547	1249	2	.

TABLE III

P	1	2	3	4
3	935	82	7	1
5	1041	38	1	.
7	1091	29	2	.
11	1143	3	.	.
13	1160	3	.	.
17	1179	4	.	.
19	1187	2	.	.
23	1195	1	.	.
29	1208	3	.	.
31	1211	.	.	.
37	1214	1	.	.
41	1218	.	.	.
43	1222	.	.	.
47	1219	.	.	.
53	1228	1	.	.
59	1226	.	.	.
61	1231	.	.	.
67	1231	.	.	.
71	1224	.	.	.
73	1229	.	.	.
79	1229	.	.	.
83	1232	.	.	.
89	1238	1	.	.
97	1240	.	.	.
101	1235	.	.	.
103	1228	.	.	.
107	1232	.	.	.
109	1237	.	.	.
113	1236	.	.	.
127	1232	.	.	.
131	1237	.	.	.
137	1236	.	.	.
139	1237	.	.	.
149	1240	1	.	.
151	1240	.	.	.
157	1244	.	.	.
163	1243	.	.	.
167	1233	.	.	.
173	1238	.	.	.
179	1234	.	.	.
181	1243	.	.	.
191	1229	.	.	.
193	1241	.	.	.
197	1236	.	.	.
199	1235	.	.	.
211	1246	.	.	.
223	1236	.	.	.
227	1237	.	.	.
229	1243	.	.	.
233	1248	.	.	.
239	1227	.	.	.
241	1245	.	.	.
251	1245	.	.	.
257	1241	.	.	.
263	1234	.	.	.
269	1250	.	.	.
271	1227	.	.	.
277	1249	.	.	.
281	1241	.	.	.
283	1237	.	.	.
293	1244	.	.	.
307	1247	.	.	.
311	1222	.	.	.
313	1244	.	.	.
317	1247	.	.	.
331	1242	.	.	.
337	1244	.	.	.
347	1241	.	.	.
349	1243	.	.	.
353	1243	.	.	.
359	1226	.	.	.
367	1240	.	.	.
373	1251	.	.	.
379	1246	.	.	.
383	1224	.	.	.
389	1250	.	.	.
397	1251	.	.	.
401	1248	.	.	.
409	1244	.	.	.
419	1233	.	.	.
421	1243	.	.	.
431	1226	.	.	.
433	1235	.	.	.
439	1231	.	.	.
443	1243	.	.	.
449	1243	.	.	.
457	1239	.	.	.
461	1243	.	.	.
463	1235	.	.	.
467	1236	.	.	.
479	1227	.	.	.
487	1247	.	.	.
491	1246	.	.	.
499	1241	.	.	.
503	1232	.	.	.
509	1247	.	.	.
521	1244	.	.	.
523	1243	.	.	.
541	1243	.	.	.
547	1249	.	.	.

TABLE I-V

D	H	F	ETA	XI	
79	3	3	2	1	
730	12	3	3	1	
733	3	3	3	1	
874	6	3	2	1	
1111	10	5	2	2	*
1339	6	3	3	1	
1546	6	3	3	1	
1641	5	5	4	1	
1714	12	3	2	2	*
1882	6	3	3	1	
1934	7	7	2	1	
2230	6	3	2	2	*
2233	6	3	3	1	
2263	6	3	2	2	*
2399	5	5	2	1	
2554	6	3	2	1	
2659	3	3	3	2	*
2914	12	3	3	1	
2917	3	3	3	3	*
3251	5	5	3	1	
3391	3	3	4	2	*
3667	6	3	2	2	*
3739	3	3	2	2	*
3955	12	3	2	1	
3958	3	3	2	1	
3973	6	3	2	1	

TABLE V

The followins table lists all pairs (D,P) in the ranse $3 \leq D \leq 497$, $3 \leq P \leq 104729$ for which eta(P,K) > 1, where K is the real quadratic field of discriminant D. An asterisk at the extreme right indicates that xi(P,K) > 1.

D	P	ETA	XI	
6	523	2	1	
10	191	2	1	
10	643	2	1	
15	181	2	1	
19	79	2	1	
23	7	2	1	
26	2683	2	1	
31	157	2	1	
33	29	2	1	
33	37	2	1	
34	37	2	1	
34	547	2	1	
34	4733	2	1	
35	23	2	1	
35	577	2	1	
37	7	2	1	
39	5	2	1	
39	7	2	1	
41	7211	2	1	
43	3	2	1	
51	5	2	1	
51	4831	2	1	
55	571	2	1	
57	59	2	1	
57	28927	2	1	
58	3	2	1	
58	23	2	1	
58	4639	2	1	
62	263	2	1	
65	8831	2	1	
66	21023	2	1	
67	3	3	2	*
67	11	2	1	
67	953	2	1	
67	57301	2	1	
69	5	2	1	
69	17	3	1	
71	67	2	1	
71	8863	2	1	
73	41	2	1	
74	7	2	1	
74	1171	2	1	
78	62591	2	1	
79	3	2	1	
79	4049	2	1	
79	6199	2	1	
82	3	2	1	
82	11	2	1	
82	769	2	1	
85	3	2	1	
86	1231	2	1	
86	5779	2	1	
87	17	2	1	
87	1123	2	1	
89	5	3	1	
91	41	2	1	
95	10937	2	1	
97	3331	2	1	
102	10487	2	1	
103	3	2	2	*
103	13	2	1	
106	3	2	2	*
106	379	2	1	
106	4969	2	1	
109	3	2	1	
109	5	2	1	
109	809	2	1	
110	29	2	1	
111	107	2	1	
113	53	2	1	
113	20219	2	1	
114	5	2	1	
114	2801	2	1	
123	7	2	2	*
123	17	2	1	
123	853	2	1	
129	5419	2	1	
130	167	2	1	
131	23	2	1	
134	5	2	1	
138	3863	2	1	
139	3	2	2	*
139	5	3	1	
139	23	2	1	
139	17747	2	1	
142	73	2	1	
145	17	2	1	
145	37	2	1	
149	7	2	1	
151	3	2	1	

D	P	ETA	XI		D	P	ETA	XI	
151	18127	2	1		253	2953	2	1	
154	859	2	1		253	11159	2	1	
155	7877	2	1		254	3163	2	1	
157	9613	2	1		254	31123	2	1	
161	5	2	1		255	30071	2	1	
165	199	2	1		258	1873	2	1	
173	227	2	1		259	5	2	2	*
174	6133	2	1		262	41	2	1	
179	7	2	1		263	21179	2	1	
181	3	2	1		265	241	2	1	
183	829	2	1		265	263	2	1	
185	139	2	1		265	1987	2	1	
185	2389	2	1		266	37	2	1	
186	5	2	2	*	267	7	2	1	
187	29	2	1		267	11	2	1	
191	5	3	2	*	267	31	2	1	
199	3	2	1		267	131	2	1	
199	19	2	1		267	1987	2	1	
201	211	2	1		269	11	2	1	
202	3	2	1		271	3	3	1	
202	1999	2	1		271	5	2	1	
209	7	2	1		281	17	2	1	
209	82613	2	1		285	89	2	1	
210	37	2	1		285	2083	2	1	
210	41	2	1		285	3863	2	1	
211	5	2	1		286	173	2	1	
211	31	2	1		291	1667	2	1	
211	55667	2	1		295	3	2	2	*
213	19	2	1		295	7	2	1	
213	787	2	1		295	53611	2	1	
214	5	2	1		298	757	2	1	
214	7	2	1		298	56437	2	1	
215	19	2	1		301	107	2	1	
218	7	2	1		302	19	2	1	
218	11	2	1		302	2791	2	1	
218	2549	2	1		303	7	2	1	
219	7	2	1		303	107	2	1	
219	109	2	1		305	2713	2	1	
223	11	2	1		307	97	2	1	
226	1277	2	1		307	2179	2	1	
230	5641	2	1		309	11	2	1	
233	1499	2	1		310	3	2	1	
237	3221	2	1		310	19447	2	1	
238	3	3	2	*	311	797	2	1	
238	20161	2	1		311	3517	2	1	
241	5	2	1		313	11	2	1	
246	13151	2	1		314	5	2	1	
247	3	4	1		317	23	2	1	
251	11	2	1		318	41	2	1	
253	3	2	2	*	319	139	2	1	
253	7	2	1		319	20161	2	1	

D	P	ETA	XI	
321	911	2	1	
321	1039	2	1	
322	3	2	1	
323	11	3	1	
326	5	2	1	
327	19	2	1	
329	71	2	1	
330	2[illegible]	2	1	
330	15269	2	1	
330	29123	2	1	
331	3	2	1	
331	4729	2	1	
337	3	2	1	
337	7	2	1	
339	1063	2	1	
341	13	2	2	*
345	613	2	1	
347	79	2	1	
349	41	2	1	
355	457	2	1	
357	6299	2	1	
358	89	2	1	
362	211	2	1	
365	233	2	1	
366	5	2	1	
370	113	2	1	
373	2003	2	1	
381	23	2	1	
385	4513	2	1	
389	19	2	1	
390	11	2	1	
391	3	2	1	
391	709	2	1	
393	21283	2	1	
394	23	2	1	
397	3	2	2	*
397	73	2	1	
399	1579	2	1	
401	29	2	1	
401	3251	2	1	
403	7	2	1	
406	3	2	1	
406	41	2	1	
407	139	2	1	
407	1571	2	1	
407	1993	2	1	
409	2633	2	1	
413	13	2	1	
415	7	2	1	
415	13	2	1	
417	7	2	2	*
417	227	2	1	
417	433	2	1	
418	3	2	2	*
419	89753	2	1	
426	5	2	1	
426	17	2	1	
427	6983	2	1	
430	61	2	1	
430	78031	2	1	
431	1427	2	1	
434	5	3	2	*
443	11	2	1	
445	23	2	1	
445	193	2	1	
446	131	2	1	
447	2207	2	1	
447	24781	2	1	
449	7	3	1	
451	109	2	1	
453	709	2	1	
454	3	2	2	*
455	37	2	1	
457	3	2	1	
457	25111	2	1	
458	13	2	1	
461	5407	2	1	
462	23	2	1	
462	251	2	1	
463	19	2	1	
463	5741	2	1	
465	757	2	1	
466	5	2	1	
466	607	2	1	
466	15187	2	1	
467	27773	2	1	
470	7	2	1	
473	739	2	1	
473	997	2	1	
478	7	2	1	
478	23	2	1	
478	397	2	1	
481	2423	2	1	
481	16447	2	1	
487	569	2	1	
487	23911	2	1	
489	5	2	1	
491	13	2	1	
494	7	2	1	
494	43	2	1	
497	9859	2	1	

TABLE VI

P	Q	ETA	XI	X	Y	Z
5	367	4	2	-247	38	-6
7	73	3	2	5	1	0
7	373	3	2	-57	4	-6
7	463	3	2	-19	2	-1
7	661	3	2	22	3	0
7	769	4	2	12	1	0
7	883	4	2	-115	10	-3
13	409	3	2	-25	1	-3
13	499	3	2	-51	6	-2
19	307	3	???			
19	373	3	2	-15	1	-2
19	661	3	2	-141	2	-15
31	619	3	2	-117	10	-8
37	421	3	2	-18	1	-2
37	457	3	???			
37	883	3	2	-42	4	-1
43	67	3	2	6	1	0
43	619	3	2	-53	4	-3
67	577	3	2	-271	22	-17
97	337	3	2	-80	7	-7
97	769	3	2	-50	5	-7
139	241	3	2	-7	1	-1
193	103	3	2	17	2	-1
523	643	3	???			
571	757	3	2	-143	12	-6
823	421	3	2	-4	1	0
877	79	3	2	-1	3	0
1873	373	3	2	-2	1	-1
2131	661	3	2	277	42	-3
3889	541	3	2	53	2	-2
5419	7	3	2	18	1	-6
5953	727	3	???			
8101	379	3	2	-26	5	-5

APPENDIX B
PROGRAM LISTINGS

Contents

Main Programs

GREEN2 ..... B-1

Computes η and ξ for real quadratic fields.

GREEN3 ..... B-7

Computes η and ξ for real cubic - cyclic fields.

Global Procedures

Procedures marked with an asterisk have been transcribed more or less unaltered from David Ford's Phd Thesis [15].

COMPAN* B-18
DET* B-18
DISC* B-21
DISC3 ..... B-21
FUNDUN B-14
GCD B-11
HORROR B-37
IDENT B-17
INV B-11

JACOBI B-12
KDELTA* B-17
LN B-36
MATINV* B-20
MATPWR ..... B 20
NEWPHI B-29
NF3SOL B-22
NQUOT* B-19
ORDMP* B-26
POL3RT B-32
POWMOD B-12
QFSOLN B-15
REG B-38
ROWRED* B-19
SPLIT B-13
SQRT B-11
VALQEX B-16

```
BEGIN

COMMENT -- GREEN2;  Computes     eta and xi
                    for a real quadratic field;

IOCHAN 1,2;

INTEGER DLIM,D,H,PLIM,P,XI,ETA,T,J,K,L,U,Q,V,
        A,B,C,X,Y,M,N,E,F,T0,T1,T2;

ARRAY EC,XC[1:100,1:10], PRIME[1:100];

EXTERNAL INTEGER PROCEDURE SQRT;
EXTERNAL INTEGER PROCEDURE JACOBI;
EXTERNAL INTEGER PROCEDURE POWMOD;
EXTERNAL INTEGER PROCEDURE SPLIT;
EXTERNAL INTEGER PROCEDURE QFSOLN;
EXTERNAL INTEGER PROCEDURE VALQEX;

PROCEDURE WRITN2(V);
INTEGER T,U,V;
T REM U := V / 10;
WRITEN(0,T,1);
WRITEN(0,U,1)
END;

PROCEDURE WRITET(V);
INTEGER V,Q,H,M,S,T;
Q := 10*V + 3 / 6;
Q REM T := Q / 100;
Q REM S := Q / 60;
H REM M := Q / 60;
WRITEN(0,H,0);
WRITES(0,":");  WRITN2(M);
WRITES(0,":");  WRITN2(S);
WRITES(0,".");  WRITN2(T)
END;

PROCEDURE DISPLAY(X,Z);
INTEGER X;  BOOLEAN Z;
SPACE(0,3);  WRITES(0,Z);
WRITES(0," = ");  WRITEN(0,X,0)
END;
```

```
PROCEDURE REPORT(X,Y,D);
INTEGER X,Y,D,A,B,N;
IF D = 1 MOD 4 THEN
   A := X - Y / 2 ! B := Y !
    N := X*X - Y*Y*D / 4
ELSE
    A := X ! B := Y !
    N := X*X - Y*Y*D;
SPACE(0,3); WRITES(0,"N(");
IF A # 0 THEN WRITEN(0,A,0);
IF B < 0 THEN
   WRITES(0,"-")
ELSE IF B > 0 AND A # 0 THEN
    WRITES(0,"+");
IF B # 0 THEN
    BEGIN
    IF ABS(B) # 1 THEN WRITEN(0,ABS(B),0);
    WRITES(0,"w")
    END;
WRITES(0,") = "); WRITEN(0,N,0)
END;

PROCEDURE HEADER;
WRITES(2,"The following table lists all pairs (D,P) found ");
LINE(2,1);
WRITES(2,"for which eta > 1.");
LINE(2,1);
WRITES(2,"An asterisk at the extreme right indicates that ");
LINE(2,1);
WRITES(2,"xi > 1 (Kisilevsky's criterion not applicable).");
LINE(2,3);
WRITES(2,"          D          P");
WRITES(2,"       ETA        XI");
LINE(2,2)
END;
```

```
PROCEDURE STATS(M,Z);
ARRAY M[2]; BOOLEAN Z;
WRITEC(2,12);
WRITES(2,"The following table lists frequencies of values for ");
WRITES(2,Z); WRITES(2,".");
LINE(2,3);
WRITES(2,"  P");
FOR L := 1,...,10 DO WRITEN(2,L,5);
LINE(2,2);
FOR K := 1,...,PLIM DO
    BEGIN
    P := PRIME[K];
    WRITEN(2,P,3);
    FOR L := 1,...,10 DO
        IF M[K,L] = 0 THEN
            WRITES(2,"    .")
        ELSE
            WRITEN(2,M[K,L],5);
    LINE(2,1)
    END
END;

INPUT(1,"A:NTABLE.DAT");
READN(1,DLIM); READN(1,PLIM);
CLOSE(1);

INPUT(1,"B:PRIME.DAT");
READN(1,P);
IF P - 1 < PLIM THEN PLIM := P - 1;
READN(1,P);
FOR K := 1,...,PLIM DO READN(1,PRIME[K]);
CLOSE(1);

LINE(0,1);
WRITES(0,"DLIM = "); WRITEN(0,DLIM,0);
LINE(0,1);
WRITES(0,"PLIM = "); WRITEN(0,PLIM,0);
LINE(0,1);

FOR K := 1,...,PLIM DO
FOR L := 1,...,10 DO
    EC[K,L] := 0 ! XC[K,L] := 0;

OUTPUT(2,"NEL:NTABLE.TXT");

INPUT(1,"B:QUADCL.DAT");
```

```
TO := TIME;  T1 := TO;

FOR J := 1,...,DLIM DO

    BEGIN

    IF J = 1 MOD 500 THEN HEADER;

    READN(1,D);  READN(1,H);

    IF D = 1 MOD 4 THEN
        T := 2
    ELSE
        T := 1;

    IF D = 5 THEN
        E := 1 ! F := 1 ! L := -4
    ELSE
        L := QFSOLN(1,0,-D,T,E,F);

    LINE(0,1);
    DISPLAY(J,'J');
    DISPLAY(D,'D');
    DISPLAY(H,'H');
    DISPLAY(T,'T');
    REPORT(E,F,D);
    LINE(0,2);

    FOR K := 1,...,PLIM DO

        BEGIN

        P := PRIME[K];

        IF JACOBI(D,P) = 1 AND
            NOT P DIVIDES H THEN

            BEGIN

            WRITET(TIME-TO);

            Q := P^H;
            U := SPLIT(D,P,H);
            ETA := VALQEX(E,F,T,D,P,U);

            DISPLAY(D,'D');
            DISPLAY(P,'P');
            DISPLAY(Q,'Q');
            DISPLAY(U,'U');
            DISPLAY(ETA,'ETA');
```

```
    IF ETA > 1 THEN

        BEGIN

        A := Q;  B := 2*U;  C := U*U - D / Q;
        L := QFSOLN(A,B,C,T,X,Y);
        M := SQRT(L*Q+D*Y*Y);  N := Y;
        WHILE P DIVIDES M AND P DIVIDES N DO
            M := M / P ! N := N / P;

        IF M+N*U # 0 MOD P THEN
            XI := VALQEX(M,N,T,D,P,U)
        ELSE IF M-N*U # 0 MOD P THEN
            XI := VALQEX(M,-N,T,D,P,U)
        ELSE
            XI := 0;
        IF XI > ETA THEN XI := ETA;

        DISPLAY(XI,"XI");  WRITES(0,"  <<<");
        IF XI = 0 THEN WRITES(0,"  ???");

        WRITEN(2,D,10);
        WRITEN(2,P,10);
        WRITEN(2,ETA,10);
        WRITEN(2,XI,10);
        IF XI > 1 THEN
            WRITES(2,"    *")
        ELSE IF XI = 0 THEN
            WRITES(2,"    ?");
        LINE(2,1)

        END

    ELSE

        XI := 1;

    FOR L := 1,...,10 DO
        BEGIN
        IF ETA >= L THEN
            EC[K,L] := EC[K,L] + 1;
        IF XI >= L THEN
            XC[K,L] := XC[K,L] + 1
        END;

    LINE(0,1)

    END

END;
```

```
        T2 := TIME;  T1 := T2;

        LINE(0,1);
        WRITES(0,'    LAST:   '); WRITET(T1-T2);
        WRITES(0,'    TOTAL:  '); WRITET(T1-T0);
        LINE(0,1);

        IF J = 0 MOD 500 THEN
            STATS(EC,'eta') !
            STATS(XC,'xi') !
            WRITEC(2,12)

        END;

    CLOSE(1);

    CLOSE(2)

    END
```

```
BEGIN

COMMENT -- GREEN3;  Computes eta and xi for a
                    real cubic cyclic field;

IOCHAN 1,2,3;
INTEGER IMIN,IMAX,K,RCHAN,
        QLIM,QNR,FLIM,FNR,Q,P,
        QF,AF,BF,TF,UF,HF,NGP,ETA,XI,M,V,W,X,Y,Z,
        REGE,REGA,REG1,REG2,REG3;
ARRAY F,G[0:3], R,S,T[1:3];

EXTERNAL INTEGER PROCEDURE POWMOD;
EXTERNAL INTEGER PROCEDURE DISC3;
EXTERNAL INTEGER PROCEDURE REG;
EXTERNAL PROCEDURE POL3RT;
EXTERNAL PROCEDURE NF3SOL;


PROCEDURE VALETA;

M := 2;  V := P^M;  REGE := 0;

WHILE V DIVIDES REGE DO
    BEGIN
    M := M + 1;  V := P*V;
    POL3RT(F,P,M,R);
    REGE := REG(0,1,0,R,P,M)
    END;

ETA := M - 1

END;


PROCEDURE VALXI;

M := 2;  V := P^M;
REGA := 0;  REG1 := 0;
REG2 := 0;  REG3 := 0;
```

```
WHILE V DIVIDES REGA AND
      V DIVIDES REG1 AND
      V DIVIDES REG2 AND
      V DIVIDES REG3 DO

    BEGIN

    M := M + 1;  V := P*V;

    POL3RT(F,P,M,R);
    POL3RT(G,P,M,S);

    REGA := REG(X,Y,Z,S,P,M);

    T[1] := R[1]*S[1];  T[2] := R[2]*S[2];  T[3] := R[3]*S[3];

    REG1 := REG(X,Y,Z,T,P,M);

    T[1] := R[2]*S[1];  T[2] := R[3]*S[2];  T[3] := R[1]*S[3];

    REG2 := REG(X,Y,Z,T,P,M);

    T[1] := R[3]*S[1];  T[2] := R[1]*S[2];  T[3] := R[2]*S[3];

    REG3 := REG(X,Y,Z,T,P,M)

    END;

XI := M - 1

END;


PROCEDURE QMARK;
SPACE(RCHAN,3);
WRITES(RCHAN,'???')
END;


LINE(0,1);
WRITES(0,'Output (0=TT,1=LP,2=DK):  ');
READN(0,RCHAN);

LINE(0,1);
WRITES(0,'IMIN  =  ');
READN(0,IMIN);
WRITES(0,'IMAX  =  ');
READN(0,IMAX);
```

```
IF RCHAN = 1 THEN
    RCHAN := 2 ! OUTPUT(RCHAN,"LP:GREEN3.TXT")
ELSE IF RCHAN = 2 THEN
    RCHAN := 2 ! OUTPUT(RCHAN,"DK:GREEN3.TXT");
LINE(RCHAN,1);
WRITES(RCHAN,"  IMIN  IMAX");
LINE(RCHAN,1);
FOR W := IMIN,IMAX DO WRITEN(RCHAN,W,6);
LINE(RCHAN,2);

WHILE TRUE DO

BEGIN

LINE(0,1);
WRITES(0,"   Q  = ");
READN(0,Q);
WRITES(0,"   P = ");
READN(0,P);

LINE(RCHAN,1);
WRITES(RCHAN,"     Q     P   ETA    XI     X     Y     Z");
LINE(RCHAN,1);

INPUT(1,"B:CUBCL.DAT");
READN(1,FLIM);

FOR FNR := 1,...,FLIM DO

    BEGIN

    READN(1,QF);  READN(1,AF);  READN(1,BF);
    READN(1,TF);  READN(1,UF);  READN(1,HF);

    IF QF = Q THEN

        BEGIN

        LINE(RCHAN,1);
        IF RCHAN # 0 THEN LINE(0,1);
        FOR W := QF,P DO WRITEN(RCHAN,W,6);
        IF RCHAN # 0 THEN
            WRITEN(0,QF,0) ! WRITES(0,",") !
            WRITEN(0,P,0) ! LINE(0,1);
```

```
            F[0] :=  -1;
            F[1] :=  UF;
            F[2] := -TF;
            F[3] :=   1;

            VALETA;

            WRITEN(RCHAN,ETA,6);

            IF ETA > 2 THEN

                BEGIN

                NF3SOL(AF,BF,QF,HF,IMIN,IMAX,X,Y,Z,P);

                IF X = Y = Z = 0 THEN

                    QMARK

                ELSE

                    BEGIN
                    G[0] := (1 - 3*QF - QF*AF) / 27;
                    G[1] := (1 - QF) / 3;
                    G[2] := 1;
                    G[3] := 1;
                    VALXI;
                    IF XI > ETA THEN XI := ETA;
                    FOR W := XI,X,Y,Z DO WRITEN(RCHAN,W,6)
                    END

                END

            ELSE

                XI := 2 ! WRITEN(RCHAN,XI,6);

            LINE(RCHAN,1)

            END

        END;
    CLOSE(1)

    END;

    LINE(RCHAN,1); CLOSE(RCHAN)

    END
```

```
GLOBAL INTEGER PROCEDURE GCD(X,Y);

COMMENT -- Returns abs(gcd(x,y));

INTEGER X,Y;  VALUE X,Y;

WHILE Y # 0 DO
    REM X := X / Y !
    X :=: Y;

GCD := ABS(X)

END


GLOBAL INTEGER PROCEDURE SQRT(N);

COMMENT -- Returns [sqrt(n)];

INTEGER N,X,Y;

X := 2;  Y := X*X;
WHILE Y < N DO
    X :=: Y ! Y := X*X;
WHILE Y > N DO
    X := Y + N / 2*X ! Y := X*X;
SQRT := X

END


GLOBAL INTEGER PROCEDURE INV(N,M);

COMMENT -- inv*N = abs(gcd(N,M)) (mod M), abs(inv) < M;

INTEGER N,M,X,Y,A,B,Q;

X := N;  Y := M;  A := 1;  B := 0;

WHILE Y # 0 DO
    Q := X / Y !
    X := -X + Q*Y ! X :=: Y !
    A := -A + Q*B ! A :=: B;

IF X < 0 THEN
    REM INV := -A / M
ELSE
    REM INV := A / M

END
```

```
GLOBAL INTEGER PROCEDURE JACOBI(N,P);

COMMENT -- Returns (N/P) = -1, 0, +1;

INTEGER N,P,W,S,T;

W := 1;  T := P;  REM S := N / P;

IF S = 0 THEN

    W := 0

ELSE WHILE S # 1 DO

    IF 2 DIVIDES S THEN
        BEGIN
        IF T = 3 MOD 8 OR T = 5 MOD 8 THEN W := -W;
        S := S / 2
        END
    ELSE
        BEGIN
        IF S = 3 MOD 4 AND T = 3 MOD 4 THEN W := -W;
        S := T;  REM S := S / T
        END;

JACOBI := W

END


GLOBAL INTEGER PROCEDURE POWMOD(K,M,V);

COMMENT -- Returns x = k^m (mod v);

INTEGER K,M,Q,R,V,X,Y;

X := 1;  Y := K;  Q := M;
WHILE Q > 0 DO
    BEGIN
    Q REM R := Q / 2;
    IF R = 1 THEN
        REM X := Y*X / V;
    IF Q > 0 THEN
        REM Y := Y*Y / V
    END;
POWMOD := X

END
```

```
GLOBAL INTEGER PROCEDURE SPLIT(D,P,N);

COMMENT -- Solution of x^2 = D (mod p^n);

INTEGER D,P,N,G,F,H,J,K,L,M,Q,R,S,T,U,V,W;

EXTERNAL INTEGER PROCEDURE INV;
EXTERNAL INTEGER PROCEDURE JACOBI;
EXTERNAL INTEGER PROCEDURE POWMOD;

IF D # 0 MOD P THEN

BEGIN

COMMENT -- p-1 = m*2^s, m = 2*l+1;

S := 0;  M := P - 1;
WHILE 2 DIVIDES M DO
    S := S + 1 ! M := M / 2;

COMMENT -- f = (2^w)th rt of 1;

F := POWMOD(D,M,P);  W := 0;
WHILE F # 1 MOD P DO
    REM F := F*F / P ! W := W + 1;

IF W = 0 THEN
    V := 1
ELSE
    BEGIN
    G := 2;
    WHILE JACOBI(G,P) # -1 DO G := G + 1;
    T := 2^(S-W)*M;
    K := POWMOD(G,T,P);  H := INV(K,P);
    F := POWMOD(D,M,P);
    K := 2^W;  T := K / 2;  U := 1;
    FOR J := 0,...,W-1 DO
        BEGIN
        IF POWMOD(F,T,P) = -1 MOD P THEN
            REM F := F*POWMOD(H,U,P) / P !
            K := K - U;
        T := T / 2;
        U := 2*U
        END;
    T := 2^(S-W-1)*M*K;
    V := POWMOD(G,T,P)
    END;

T := M + 1 / 2;
REM U := V*POWMOD(D,T,P) / P;
COMMENT -- u*u = D (mod p);
```

```
Q := P;  R := P^N;
WHILE Q < R DO
    BEGIN
    V := D - U*U / Q;
    T := INV(2*U,Q);
    REM W := T*V / Q;
    REM U := U + Q*W / R;
    Q := Q*Q
    END;

SPLIT := U

END

ELSE SPLIT := 0

END



GLOBAL INTEGER PROCEDURE FUNDUN(D,X,Y);

COMMENT -- Finds X, Y such that |N(X+Yw)| = 1.
           If D = 1 mod 4:  w = (1+rt(D))/2 and r = 2p-q.
           Otherwise:       w = rt(D), r = p.
           In either case:  p/q is a convergent of w, and
                            r/q --> rt(D);

INTEGER D,X,Y,E,F,T,V,W,Z,A0,R0,R1,R2,Q0,Q1,Q2;

EXTERNAL INTEGER PROCEDURE SQRT;

IF D = 1 MOD 4 THEN T := 2 ELSE T := 1;
R2 := 1 - T;  R1 := T;  Q2 := 1;  Q1 := 0;
E := SQRT(T*T*D);  Z := 0;

WHILE ABS(Z) # 1 DO
    W := R1*R1 - Q1*Q1*D !
    F := SIGN(E) - SIGN(W) / 2 !
    V := E + F - R1*R2 + Q1*Q2*D !
    A0 := V / W !
    R0 := A0*R1 + R2 ! R2 :=: R1 ! R1 :=: R0 !
    Q0 := A0*Q1 + Q2 ! Q2 :=: Q1 ! Q1 :=: Q0 !
    Z := R1*R1 - D*Q1*Q1 / T*T !
    E := -E;

X := R1 + (1 - T)*Q1 / T;
Y := Q1;
FUNDUN := Z

END
```

```
GLOBAL INTEGER PROCEDURE QFSOLN(A,B,C,T,X,Y);

COMMENT -- Returns u if Axx + Bxy + Cyy = u
                     or Axx - Bxy + Cyy = u,
           with abs(u) = t**t;

INTEGER A,B,C,D,E,G,T,
        A0,A1,A2,A3,B0,B1,B2,B3,C0,C1,C2,C3,
        R0,R1,R2,R3,S0,S1,S2,S3,Q0,Q2,X,Y;

EXTERNAL INTEGER PROCEDURE SQRT;

INTEGER PROCEDURE NEWQ(A,B,E);
INTEGER A,B,E;
IF A < 0 THEN
    NEWQ := -B - E / 2*A
ELSE
    NEWQ := -B + E / 2*A
END;

D := B*B - 4*A*C;  E := SQRT(D);  G := T*T;
Q0 := NEWQ(A,B,E);
R0 := 1;  R1 := Q0;
S0 := 0;  S1 := 1;
A0 := A;  A1 := A*Q0*Q0 + B*Q0 + C;
B0 := B;  B1 := 2*A*Q0 + B;
C0 := C;  C1 := A;
Q2 := NEWQ(A,-B,E);
R2 := 1;  R3 := Q2;
S2 := 0;  S3 := 1;
A2 :=  A;  A3 := A*Q2*Q2 - B*Q2 + C;
B2 := -B;  B3 := 2*A*Q2 - B;
C2 :=  C;  C3 := A;

WHILE ABS(A1) # 1 AND ABS(A1) # G AND
      ABS(A3) # 1 AND ABS(A3) # G DO
    BEGIN
    A0 :=: A1;  B0 :=: B1;  C0 :=: C1;
    R0 :=: R1;  S0 :=: S1;  Q0 := NEWQ(A0,B0,E);
    R1 := R0*Q0 + R1;  S1 := S0*Q0 + S1;
    A1 := A0*Q0*Q0 + B0*Q0 + C0;
    B1 := 2*A0*Q0 + B0;
    C1 := A0;
    A2 :=: A3;  B2 :=: B3;  C2 :=: C3;
    R2 :=: R3;  S2 :=: S3;  Q2 := NEWQ(A2,B2,E);
    R3 := R2*Q2 + R3;  S3 := S2*Q2 + S3;
    A3 := A2*Q2*Q2 + B2*Q2 + C2;
    B3 := 2*A2*Q2 + B2;
    C3 := A2
    END;
```

```
IF ABS(A1) = G THEN
    X := R1 ! Y := S1 ! QFSOLN := A1
ELSE IF ABS(A3) = G THEN
    X := R3 ! Y := S3 ! QFSOLN := A3
ELSE IF ABS(A1) = 1 THEN
    X := T*R1 ! Y := T*S1 ! QFSOLN := G*A1
ELSE
    X := T*R3 ! Y := T*S3 ! QFSOLN := G*A3

END



GLOBAL INTEGER PROCEDURE VALQEX(A,B,C,D,P,U);

COMMENT -- P-adic valuation of (x^(p-1) - 1),
           x = (A + B*rt(D)) / C, U = sqrt(D) (mod p);

INTEGER A,B,C,D,P,U,H,Q,R,S,V,W,X,Z;

EXTERNAL INTEGER PROCEDURE INV;
EXTERNAL INTEGER PROCEDURE POWMOD;

X := U;  H := INV(2*U,P);
Q := P;  Z := 0;

WHILE Q DIVIDES Z DO
    W := D - X*X / Q !
    REM V := H*W / P !
    X := X + Q*V !
    Q := P*Q !
    R := POWMOD(A+B*X,P-1,Q) !
    S := POWMOD(C,P-1,Q) !
    REM Z := (R - S) / Q;

V := 0;  W := C;
WHILE P DIVIDES Z DO
    Z := Z / P ! V := V + 1;
WHILE P DIVIDES W DO
    W := W / P ! V := V - 2*(P - 1);

VALQEX := V

END
```

```
GLOBAL INTEGER PROCEDURE KDELTA(X,Y);
COMMENT -- Kronecker's delta function;
INTEGER X,Y;
IF X = Y THEN
    KDELTA := 1
ELSE
    KDELTA := 0
END


GLOBAL PROCEDURE IDENT(A);
COMMENT -- Set A to be the identity matrix;
INTEGER I,J,L,H;  ARRAY A[2];
EXTERNAL INTEGER PROCEDURE KDELTA;
L := LOWBD(2,A);
H := HIGHBD(2,A);
FOR I := L,...,H DO
FOR J := L,...,H DO
    A[I,J] := KDELTA(I,J)
END
```

```
GLOBAL INTEGER PROCEDURE DET(A);

COMMENT -- Determinant of matrix A;

ARRAY A[2];  INTEGER I,J,C,D,L,H;

L := LOWBD(2,A);

H := HIGHBD(2,A);

D := 1;

FOR J := L,...,H DO

    BEGIN
    FOR I := J+1,...,H DO
    WHILE A[I,J] # 0 DO
        C := A[J,J] / A[I,J] !
        ROW(J,A) := -ROW(J,A) + C*ROW(I,A) !
        ROW(I,A) :=: ROW(J,A);
    D := A[J,J]*D
    END;

DET := D

END


GLOBAL PROCEDURE COMPAN(F,A);

COMMENT -- Set A to be the companion
           matrix of the polynomial f;

INTEGER I,J,N;  ARRAY F[1],A[2];

EXTERNAL INTEGER PROCEDURE KDELTA;

N := HIGHBD(1,F);

FOR I := 0,...,N-1 DO
FOR J := 0,...,N-1 DO

    IF J < N-1 THEN
        A[I,J] := KDELTA(I,J+1)
    ELSE
        A[I,J] := -F[I]
END
```

```
GLOBAL INTEGER PROCEDURE NQUOT(X,Y);

COMMENT -- Normalized quotient q of x and y,
           such that |x/y - q| <= 1/2;

INTEGER X,Y;

IF SIGN(X) = SIGN(Y) THEN

    NQUOT := 2*X + Y / 2*Y

ELSE

    NQUOT := 2*X - Y / 2*Y

END
```

```
GLOBAL PROCEDURE ROWRED(A,RH,CH);
INTEGER R,C,Q,RL,CL,RH,CH;  ARRAY A[2];

COMMENT -- Reduces the matrix A to triangular form;

EXTERNAL INTEGER PROCEDURE NQUOT;

RL := LOWBD(1,A); CL := LOWBD(2,A);

FOR C := CL,...,CH DO
    BEGIN
    FOR R := C+1,...,RH DO
    WHILE A[R,C] # 0 DO
        Q := NQUOT(A[C,C],A[R,C]) !
        ROW(C,A) := ROW(C,A) - Q*ROW(R,A) !
        ROW(C,A) :=: ROW(R,A);
    IF A[C,C] < 0 THEN
        ROW(C,A) := -ROW(C,A);
    FOR R := RL,...,C-1 DO
    IF A[R,C] # 0 THEN
        Q := NQUOT(A[R,C],A[C,C]) !
        ROW(R,A) := ROW(R,A) - Q*ROW(C,A);
    END
END
```

```
GLOBAL PROCEDURE MATINV(X,Y,D);

COMMENT -- Set Y/D to be the inverse of
           the UPPER TRIANGULAR matrix X;

INTEGER D,I,J,K;  ARRAY X,Y[2];

EXTERNAL PROCEDURE IDENT;

K := HIGHBD(1,X);
IDENT(Y);
FOR I := 0,...,K DO
    Y[I,I] := D / X[I,I];
FOR I := 1,...,K DO
FOR J := I-1, I-2,..., 0 DO
    Y[I,J] := -ROW(I,Y)*COLUMN(J,X) / X[J,J]

END


GLOBAL ARRAY PROCEDURE MATPWR(A,K,P,M)[2];

COMMENT -- Returns B = A^k mod P^M where
           A is an n by n matrix and P is prime;

INTEGER K,P,M,N;  ARRAY A[2];

EXTERNAL PROCEDURE IDENT;

N := HIGHBD(1,A);

BEGIN

INTEGER H,J,Q,R,V;  ARRAY B,X[1:N,1:N];

IDENT(X);  B := A;  Q := K;  V := P^M;

WHILE Q > 0 DO
    BEGIN
    Q REM R := Q / 2;
    IF R = 1 THEN
        REM X := B*X / V;
    IF Q > 0 THEN
        REM B := B*B / V
    END;

MATPWR := X

END

END
```

```
GLOBAL INTEGER PROCEDURE DISC3(A,B,C);
COMMENT -- Discriminant of the polynomial xxx + Axx + Bx + C;
INTEGER A,B,C;
DISC3 := A*A*B*B - 4*B*B*B - 4*A*A*A*C - 27*C*C + 18*A*B*C
END


GLOBAL INTEGER PROCEDURE DISC(F);
COMMENT -- Discriminant of f;
INTEGER I,J,N;  ARRAY F[1];
N := HIGHBD(1,F);
BEGIN
ARRAY A[1:N,1:N];
EXTERNAL INTEGER PROCEDURE DET;
FOR I := 1,...,N DO
FOR J := 1,...,N DO
    IF I = 1 THEN
        A[I,J] := (N-J+1)*F[N-J+1]
    ELSE IF J < N THEN
        A[I,J] := A[I-1,J+1] - A[I-1,1]*F[N-J]
    ELSE
        A[I,J] := -A[I-1,1]*F[N-J];
DISC := DET(A)
END
END
```

```
GLOBAL PROCEDURE NF3SOL(AF,BF,QF,HF,IL,IH,X,Y,Z,P);

INTEGER AF,BF,QF,HF,IL,IH,P,X,Y,Z;

COMMENT -- Input:   Field parameters AF,BF,QF,HF determining the
                    totally real cubic-cyclic field of prime
                    conductor QF and class number HF.
                    IL,IH : Low and high bounds on I.
                    P : a prime to be represented by the norm-
                    form of the field.

           Output:  Three coefficients X,Y,Z which satisfy the
                    equation |normform(X,Y,Z)| = P;

INTEGER A,B,C,D,E,F,I,J,K,L,N,S,T,XL,XH,DY,DZ;

INTEGER PROCEDURE CLG(X,Y);
INTEGER X,Y;
IF Y < 0 THEN
    IF X < 0 THEN
        CLG := X + Y + 1 / Y
    ELSE
        CLG := X / Y
ELSE
    IF X < 0 THEN
        CLG := X / Y
    ELSE
        CLG := X + Y - 1 / Y
END;

INTEGER PROCEDURE FLR(X,Y);
INTEGER X,Y;
IF Y < 0 THEN
    IF X < 0 THEN
        FLR := X / Y
    ELSE
        FLR := X - Y - 1 / Y
ELSE
    IF X < 0 THEN
        FLR := X - Y + 1 / Y
    ELSE
        FLR := X / Y
END;
```

```
PROCEDURE SQRT2(N,R1,R2);
COMMENT -- r1 <-- flr(sqrt(n)),
           r2 <-- cls(sqrt(n));
INTEGER N,R1,R2,X,Y;
X := 1;  Y := 1;
WHILE Y < N DO
    X := 2*X-1 Y := 4*Y;
WHILE Y > N DO
    X := (Y + N) / 2*X ! Y := X*X;
R1 := X;
IF Y = N THEN
    R2 := X
ELSE
    R2 := X + 1
END;

INTEGER PROCEDURE NF(W);
INTEGER W;
NF := W*W*W + A*W*W + B*W + C
END;

PROCEDURE INTRVL(RL,RH);
INTEGER RL,RH,RM,FL,FH,FM;  VALUE RL,RH;
FL := NF(RL);  FH := NF(RH);
IF FL = 0 THEN
    XL := RL ! XH := RL
ELSE IF FH = 0 THEN
    XL := RH ! XH := RH
ELSE WHILE RH - RL > 1 DO
    BEGIN
    RM := (RL + RH) / 2;
    FM := NF(RM);
    IF FM = 0 THEN
        RL := RM ! RH := RM !
        XL := RM ! XH := RM
    ELSE IF SIGN(FM) = SIGN(FL) THEN
        RL := RM ! EL := FM
    ELSE
        RH := RM ! FH := FM
    END
END;
```

```
PROCEDURE NORMVAL(EPS);
INTEGER EPS,U,RDL,RDH,R1L,R1H,R2L,R2H,R3L,R3H;
IF XL # XH THEN
    BEGIN
    A := (Y + Z)*T;
    B := (Y*Y + Z*Z)*S + (Y*Z*F);
    C := Y*Z*(Y*D + Z*E) + (Y*Y*Y + Z*Z*Z)*N + EPS*P;
    SQRT2(A*A-3*B,RDL,RDH);
    R1L := FLR(-A-RDH,3);  R1H := CLG(-A-RDL,3);
    R2L := FLR(-A+RDL,3);  R2H := CLG(-A+RDH,3);
    INTRVL(R1H,R2L);
    IF XL # XH THEN
        BEGIN
        U := R2H - R1L;
        R3H := R2H + U;
        WHILE NF(R3H) < 0 DO
            U := 2*U ! R3H := R3H + U;
        INTRVL(R2H,R3H);
        IF XL # XH THEN
            BEGIN
            U := R2H - R1L;
            R3L := R1L - U;
            WHILE NF(R3L) > 0 DO
                U := 2*U ! R3L := R3L - U;
            INTRVL(R3L,R1L)
            END
        END
    END
END;
```

```
T := -1;
S := (1 - QF)/3;
N := (3*QF + QF*AF - 1) / 27;
D := (S*T - 3*N + QF*BF) / 2;
E := (S*T - 3*N - QF*BF) / 2;
F := T^2 - S;

I := IL;  XL := -1;  XH := +1;

WHILE XL # XH AND I <= IH DO
   BEGIN
    Y := I;  DY := 0;
    Z := I;  DZ := -1;
    FOR J := 1,2 DO
        BEGIN
        FOR K := 1,...,2*I DO
        IF XL # XH THEN
            Z := Z + DZ !
            Y := Y + DY !
            NORMVAL(-1) !
            NORMVAL(+1);
        DZ := DY;  DZ := -DZ
        END;
    I := I + 1
    END;

IF XL = XH THEN
    X := XL !
    K := X^3 + (Y^3+Z^3)*N + (Y*X^2+Z*X^2)*T
                + (X*Y^2+X*Z^2)*S + D*Z*Y^2 + E*Y*Z^2 + X*Y*Z*F
ELSE
    X := 0 ! Y := 0 ! Z := 0

END
```

```
        GLOBAL PROCEDURE ORDMP(F,P,E,M,DELTA);
        INTEGER N,P,E,DELTA;  ARRAY F[1],M[2];

        COMMENT -- Given f in Z[x], p prime, e the p-adic valuation
                   of disc(f), ORDMP returns a basis of a 'p-maximal'
                   Z-order in the field Q[u], u a root of f(x).  An
                   order is 'p-maximal' if its index in the maximal
                   order of Q[u] is not divisible by p.  The basis
                   is returned as polynomials in u, with coefficients
                   in the array M, all having denominator DELTA.;

        EXTERNAL INTEGER PROCEDURE GCD;
        EXTERNAL PROCEDURE IDENT;
        EXTERNAL PROCEDURE ROWRED;
        EXTERNAL PROCEDURE MATINV;

        N := HIGHBD(1,F);

        BEGIN

        INTEGER I,J,K,L,DISCR,PMAX,Q,S,U,U1;

        ARRAY   ID,COMPF,B,T,SP,JU[0:N-1,0:N-1],
                A[0:N^2-1,0:N-1], W[0:N-1,0:N-1,0:N-1];

STEP1;  DISCR := P^E;
        IDENT(ID);
        FOR I := 0,...,N-2 DO
            ROW(I,COMPF) := ROW(I+1,ID);
        FOR J := 0,...,N-1 DO
            COMPF[N-1,J] := -F[J];
        M := ID;  DELTA := 1;

        K := DISCR;
STEP2:  U := 1;
        IF P^2 DIVIDES DISCR
        AND P DIVIDES K THEN
            U := P*U ! PMAX := P;

        IF U # 1 THEN
            BEGIN
STEP3:      MATINV(M,B,DELTA);
            T := M*COMPF*B;  B := DELTA*ID;
            FOR I := 0,...,N-1 DO
                MATRIX(2,3,W,I) := M[I,0]*B;
            FOR J := 1,...,N-1 DO
                BEGIN
                B := B*T / DELTA;
                FOR I := 0,...,N-1 DO
                MATRIX(2,3,W,I) := MATRIX(2,3,W,I) + M[I,J]*B
                END;
            W := W / DELTA^2;
```

```
            IF PMAX > N THEN
                BEGIN
                SP := 0*ID;
                FOR I := 0,...,N-1 DO
                FOR J := 0,...,N-1 DO
                FOR K := 0,...,N-1 DO
                    SP[I,J] := SP[I,J]
                        + VECTOR(3,W,I,K)*VECTOR(2,W,J,K)
                END;

            FOR I := 0,...,N-1 DO
                ROW(I,A) := U*ROW(I,ID);
STEP4;      IF P DIVIDES U THEN
                BEGIN
                U1 := U/P;
                IF P > N THEN T := SP
                ELSE
                    BEGIN
                    FOR J := 0,...,N-1 DO
                        BEGIN
                        COLUMN(J,B) := COLUMN(0,ID);
                        FOR K := 1,...,P DO
                        COLUMN(J,B) :=
                            COLUMN(J,B)*MATRIX(2,3,W,J)
                        END;
                    Q := P;  K := 1;
                    WHILE Q < N DO
                        Q := P*Q ! K := K + 1;
                    T := B^K
                    END;
                FOR I := 0,...,N-1 DO
                    ROW(N+I,A) := U1*ROW(I,T);
                ROWRED(A,2*N-1,N-1)
                END;

STEP5;      FOR I := 0,...,N-1 DO
                COLUMN(I,B) := ROW(I,A);
            MATINV(B,JU,U);
            FOR K := 0,...,N-1 DO
                BEGIN
                T := JU*MATRIX(2,3,W,K)*B / U;
                L := 0;
                FOR I := 0,...,N-1 DO
                FOR J := 0,...,N-1 DO
                    A[L,K] := T[I,J] ! L := L + 1
                END;
            ROWRED(A,N^2-1,N-1);
            K := 1;
            FOR I := 0,...,N-1 DO
                K := A[I,I]*K;
```

```
STEP6:      IF K # 1 THEN
                BEGIN
                DELTA := K*DELTA;
                DISCR := DISCR / K^2;
                MATINV(MATRIX(2,1,A),B,K);
                M := B*M;
                L := DELTA;
                FOR I := 0,...,N-1 DO
                FOR J := 0,...,I DO
                    L := GCD(M[I,J],L);
                IF L > 1 THEN
                    DELTA := DELTA/L ! M := M/L;
                GOTO STEP2
                END
            END
        END

        END
```

```
GLOBAL PROCEDURE NEWPHI(F,P,G,H,D);

COMMENT -- Given cubic minimal polynomial f(x) of theta,
           p prime, p dividing disc(f), finds phi in Q(theta)
           with minimal polynomial g(x), with p not dividing
           disc(g), and polynomial h(x) with denominator d,
           such that theta = h(phi)/d;

INTEGER P,D;  ARRAY F,G,H[1];

INTEGER J,K,Q,R,E,DBAS,DPHI,DPSI;

ARRAY   MPHI[0:3],
        CTHE,CPHI,CPSI,TPHI,TPSI,ID,MBAS[0:2,0:2],
        APSI[0:3,0:2],
        BPSI[0:3,0:3];

BOOLEAN HORMSG;

EXTERNAL INTEGER PROCEDURE DISC;
EXTERNAL INTEGER PROCEDURE GCD;
EXTERNAL INTEGER PROCEDURE NQUOT;
EXTERNAL PROCEDURE ORDMP;
EXTERNAL PROCEDURE IDENT;
EXTERNAL PROCEDURE COMPAN;
EXTERNAL PROCEDURE HORROR;

INTEGER PROCEDURE VAL(X);
INTEGER X,V;  VALUE X;
IF X = 0 THEN
    V := -1
ELSE
    BEGIN
    V := 0;
    WHILE P DIVIDES X DO
        X := X / P ! V := V + 1
    END;
VAL := V
END;
```

```
IDENT(ID);

TPHI := ID;  DPHI := 1;  MPHI := F;

WHILE P DIVIDES DISC(MPHI) DO

    BEGIN

    E := VAL(DISC(MPHI));

    ORDMP(MPHI,P,E,MBAS,DBAS);

    COMPAN(MPHI,CPHI);

    CPSI := MBAS[2,0]*ID + MBAS[2,1]*CPHI + MBAS[2,2]*CPHI*CPHI;

    COMMENT -- CPSI/DBAS is PSI, where PSI belongs to
               Q adjoined the companion matrix of PHI;

    ROW(0,TPSI) := DBAS*DBAS*COLUMN(0,ID);
    ROW(1,TPSI) := DBAS*COLUMN(0,CPSI);
    ROW(2,TPSI) := COLUMN(0,CPSI*CPSI);
    DPSI := DBAS*DBAS;

    COMMENT -- TPSI/DPSI is the change-of-basis matrix between a
               basis of powers of PHI and a basis of powers of PSI;

    COMMENT -- Replace PHI by PSI;

    MPHI[3] := 1;
    MPHI[2] := - CPSI[0,0] - CPSI[1,1] - CPSI[2,2] / DBAS;
    MPHI[1] := CPSI[0,0]*CPSI[1,1] - CPSI[0,1]*CPSI[1,0]
               + CPSI[0,0]*CPSI[2,2] - CPSI[0,2]*CPSI[2,0]
                 + CPSI[1,1]*CPSI[2,2] - CPSI[1,2]*CPSI[2,1]
                   / DBAS*DBAS;
    MPHI[0] := - CPSI[0,0]*CPSI[1,1]*CPSI[2,2]
                 + CPSI[0,0]*CPSI[1,2]*CPSI[2,1]
                   - CPSI[0,1]*CPSI[1,2]*CPSI[2,0]
                     + CPSI[0,1]*CPSI[1,0]*CPSI[2,2]
                       - CPSI[0,2]*CPSI[1,0]*CPSI[2,1]
                         + CPSI[0,2]*CPSI[1,1]*CPSI[2,0]
                           / DBAS*DBAS*DBAS;

    TPHI := TPSI*TPHI;
    DPHI := DPSI*DPHI;

    END;

G := MPHI;
```

```
COMMENT -- Confirm that s annihilates PHI;

COMPAN(F,CTHE);
CPHI := TPHI[1,0]*ID + TPHI[1,1]*CTHE + TPHI[1,2]*CTHE*CTHE;
CPSI := G[0]*DPHI*DPHI*DPHI*ID + G[1]*DPHI*DPHI*CPHI
                    + G[2]*DPHI*CPHI*CPHI + G[3]*CPHI*CPHI*CPHI;
HORMSG := FALSE;
FOR J := 0,...,2 DO
FOR K := 0,...,2 DO
IF CPSI[J,K] # 0 AND NOT HORMSG THEN
    HORROR('Error expressing min pol phi!') !
    HORMSG := TRUE;

COMMENT -- Express THETA in terms of PHI;

TPSI := TPHI;  CPSI := DPHI*ID;
FOR K := 0,..,2 DO
    FOR J := K+1,...,2 DO
    WHILE TPSI[J,K] # 0 DO
        Q := NQUOT(TPSI[K,K],TPSI[J,K]) !
        ROW(K,TPSI) := ROW(K,TPSI) - Q*ROW(J,TPSI) !
        ROW(K,CPSI) := ROW(K,CPSI) - Q*ROW(J,CPSI) !
        ROW(K,TPSI) := ROW(J,TPSI) !
        ROW(K,CPSI) := ROW(J,CPSI);

J := 1;  K := 2;
Q := TPSI[J,K];  R := TPSI[K,K];
ROW(J,TPSI) := R*ROW(J,TPSI) - Q*ROW(K,TPSI);
ROW(J,CPSI) := R*ROW(J,CPSI) - Q*ROW(K,CPSI);

IF TPSI[1,1] < 0 THEN
    ROW(1,TPSI) := - ROW(1,TPSI) !
    ROW(1,CPSI) := - ROW(1,CPSI);

K := TPSI[1,1];
FOR J := 0,...,2 DO
    K := GCD(K,CPSI[1,J]);

H := ROW(1,CPSI) / K;  D := TPSI[1,1] / K;

COMPAN(F,CTHE);
CPHI := TPHI[1,0]*ID + TPHI[1,1]*CTHE + TPHI[1,2]*CTHE*CTHE;
CPSI := H[0]*DPHI*DPHI*ID + H[1]*DPHI*CPHI + H[2]*CPHI*CPHI;
Q := DPHI*DPHI*D;
HORMSG := FALSE;
FOR J := 0,...,2 DO
FOR K := 0,...,2 DO
IF CPSI[J,K] # Q*CTHE[J,K] AND NOT HORMSG THEN
    HORROR('Error expressing theta in terms of phi!') !
    HORMSG := TRUE

END
```

```
GLOBAL PROCEDURE POL3RT(ORGF,P,ORGM,ORGR);

COMMENT--Returns approximations mod p^m to the roots r1,r2,r3
        of f(x) in Zp, with the numbering chosen so that
        (r1-r2)(r2-r3)(r1-r3) = sqrt(disc(f)) > 0;

INTEGER P,ORGM;  ARRAY ORGF,ORGR[1];
INTEGER D,G,H,I,J,K,M,V,W,A,B,C,A1,B1,C1,DT,ORGV,ORGD;
ARRAY F[0:3], ORGT[0:2], R,S[1:3], T[1:3,1:3];

EXTERNAL INTEGER PROCEDURE SQRT;
EXTERNAL INTEGER PROCEDURE DISC;
EXTERNAL INTEGER PROCEDURE SPLIT;
EXTERNAL INTEGER PROCEDURE INV;
EXTERNAL INTEGER PROCEDURE JACOBI;

EXTERNAL ARRAY PROCEDURE MATPWR[1:3,1:3];

EXTERNAL PROCEDURE NEWPHI;
EXTERNAL PROCEDURE HORROR;

INTEGER PROCEDURE JAC(N,P);
INTEGER N,P; VALUE N;
WHILE N < 0 DO REM N := (N + P) / P;
IF N = 0 MOD P THEN
    JAC := 0
ELSE
    JAC := JACOBI(N,P)
END;

INTEGER PROCEDURE FO(X);
INTEGER X;
REM FO := F[3]*X*X*X + F[2]*X*X + F[1]*X + F[0] / V
END;

INTEGER PROCEDURE FN(X);
INTEGER X;
REM FN := X*X*X + A*X*X + B*X + C / P
END;

INTEGER PROCEDURE ORGFN(X);
INTEGER X;
REM ORGFN := ORGF[3]*X*X*X + ORGF[2]*X*X + ORGF[1]*X + ORGF[0] / ORGV
END;
```

```
BOOLEAN PROCEDURE MODFAC(X,Y,Z);
COMMENT -- Confirm that X1,X2,X3 are
           the roots of Y(x) mod Z;
INTEGER Z,SYM1,SYM2,SYM3;  ARRAY X,Y[1];
SYM1 := X[1] + X[2] + X[3];
SYM2 := X[1]*X[2] + X[1]*X[3] + X[2]*X[3];
SYM3 := X[1]*X[2]*X[3];
MODFAC := (SYM1 = -Y[2] MOD Z) AND
          (SYM2 =  Y[1] MOD Z) AND
          (SYM3 = -Y[0] MOD Z)
END;

PROCEDURE SOLVEL;
COMMENT -- Finds r2, r3, given f(r1) = 0 mod P;
INTEGER B1,C1,D1,E1,G1;
B1 := A + R[1];
C1 := R[1]*R[1] + A*R[1] + B;
D1 := INV(2,P);
E1 := B1*B1 - 4*C1;
G1 := SPLIT(E1,P,1);
REM R[2] := (-B1 + G1)*D1 / P;
REM R[3] := (-B1 - G1)*D1 / P
END;

PROCEDURE SOLVEQ;
COMMENT -- Finds R[1], given S[1] # 0 mod P;
INTEGER D1,E1,G1,H1;
D1 := INV(2*S[1],P);
FOR H1 := -1,1 DO
   BEGIN
   E1 := S[2]*S[2] - 4*S[1]*(S[3]+H1);
   IF FN(R[1]) # 0 THEN
   IF JAC(E1,P) # -1 THEN
      BEGIN
      G1 := SPLIT(E1,P,1);
      REM R[2] := (-S[2] + G1)*D1 / P;
      REM R[3] := (-S[2] - G1)*D1 / P;
      IF FN(R[2]) = 0 THEN R[1] := R[2];
      IF FN(R[3]) = 0 THEN R[1] := R[3]
      END
   END
END;
```

```
PROCEDURE LIFT;
COMMENT -- Lifts roots mod P to roots mod P^M;
INTEGER H,I,J,K;  ARRAY G,U[1:3], V,W[1:3,1:3];

V[1,1] := 1;          V[1,2] := 1;          V[1,3] := 1;
V[2,1] := R[2]+R[3];  V[2,2] := R[1]+R[3];  V[2,3] := R[1]+R[2];
V[3,1] := R[2]*R[3];  V[3,2] := R[1]*R[3];  V[3,3] := R[1]*R[2];

W[1,1] := 1;  W[1,2] := 0;  W[1,3] := 0;
W[2,1] := 0;  W[2,2] := 1;  W[2,3] := 0;
W[3,1] := 0;  W[3,2] := 0;  W[3,3] := 1;

FOR I := 1,...,3 DO
    BEGIN
    K := INV(V[I,I],P);
    REM ROW(I,V) := K*ROW(I,V) / P;
    REM ROW(I,W) := K*ROW(I,W) / P;
    FOR J := 1,...,3 DO
    IF J # I THEN
        K := V[J,I] !
        REM ROW(J,V) := ROW(J,V) - K*ROW(I,V) / P !
        REM ROW(J,W) := ROW(J,W) - K*ROW(I,W) / P
    END;

FOR H := 1,...,M-1 DO
    BEGIN
    K := P^H;
    U[1] := R[1] + R[2] + R[3] + A / K;
    U[2] := R[1]*R[2] + R[1]*R[3] + R[2]*R[3] - B / K;
    U[3] := R[1]*R[2]*R[3] + C / K;
    R := R - K*W*U
    END

END;


NEWPHI(ORGF,P,F,ORGT,DT);

K := DT;  M := ORGM;  ORGV := P^ORGM;
ORGD := SQRT(DISC(ORGF));
WHILE P DIVIDES K DO
    K := K / P ! M := M + 2;

V := M;  W := (P - 7) / 2;
A := F[2];  B := F[1];  C := F[0];
D := SQRT(DISC(F));
K := 0;  R[1] := 0;  S[1] := 0;  S[3] := 0;
```

```
WHILE FN(R[1]) # 0 DO
    BEGIN
    K := K+1;
    REM C := (A + B + C + 1) / V;
    REM B := (B + 2*A + 3) / V;
    REM A := (A + 3) / V;
    IF C = 0 MOD P THEN
        R[1] := 0
    ELSE IF W > 0 THEN
        BEGIN
        T[1,1] := -A;  T[1,2] := 1;  T[1,3] := 0;
        T[2,1] := -B;  T[2,2] := 0;  T[2,3] := 1;
        T[3,1] := -C;  T[3,2] := 0;  T[3,3] := 0;
        REM S := MATPWR(T,W,P,M)*COLUMN(1,T) / V;
        IF S[1] # 0 MOD P THEN SOLVEQ
        END
    END;

SOLVEL;  LIFT;

FOR J := 1,...,3 DO
    REM R[J] := R[J] + K / V;

IF NOT MODFAC(R,F,V) THEN
    HORROR('Oh, no!!!  Roots of min pol phi wrong!!!');

COMMENT <-- Convert roots of new f to roots of original f;

K := INV(DT,V);  W := P^(M-ORGM);
FOR J := 1,...,3 DO
    BEGIN
    REM H := K*(ORGT[0] + ORGT[1]*R[J] + ORGT[2]*R[J]*R[J]) / V;
    IF W DIVIDES H THEN
        ORGR[J] := H / W
    ELSE
        HORROR('Egad!!!  Impossible denominator!!!')
    END;

IF NOT MODFAC(ORGR,ORGF,ORGV) THEN
    HORROR('Min pol theta not factorized properly!!!');

FOR J := 1,...,3 DO
WHILE ORGR[J] < 0 DO
    ORGR[J] := ORGR[J] + ORGV;

W := 1;
WHILE W DIVIDES ORGD DO W := P*W;
K := 1;
FOR I := 1,2 DO
FOR J := I+1,...,3 DO
    K := K*(ORGR[I] - ORGR[J]);
IF K # ORGD MOD W THEN ORGR[1] := ORGR[2]

END
```

```
GLOBAL INTEGER PROCEDURE LN(W,P,M,N);

COMMENT -- Finds the image of
           s + s^2/2 + s^3/3 + ... + s^n/n  (mod P^m)
           where  s = 1 - w^(p-1);  n >= 1;

INTEGER W,P,M,N,V,I,L;  VALUE W;

EXTERNAL INTEGER PROCEDURE POWMOD;
EXTERNAL INTEGER PROCEDURE INV;
EXTERNAL PROCEDURE HORROR;


V := P^M;

IF W = 0 THEN
    HORROR('LN(0) is not defined!!!')
ELSE
    WHILE P DIVIDES W DO W := W / P;

L := 1 - POWMOD(W,P-1,V);

FOR I := 1,2,3,N DO

    REM L := (L + INV(I,V)*L^I) / V;

REM LN := L / V

END



GLOBAL INTEGER PROCEDURE REG(X,Y,Z,R,P,M);

COMMENT -- Approximation to the P-adic regulator;

ARRAY R[1];  INTEGER X,Y,Z,P,M;  ARRAY U[1:3];

EXTERNAL INTEGER PROCEDURE LN;

U[1] := X + Y*R[1] + Z*R[2];
U[2] := X + Y*R[2] + Z*R[3];
U[3] := X + Y*R[3] + Z*R[1];

REG := LN(U[1],P,M,M-2)^2 - LN(U[2],P,M,M-2)*LN(U[3],P,M,M-2)

END
```

```
GLOBAL PROCEDURE HORROR(Z);
COMMENT -- Display a horrifying note;
BOOLEAN Z;
LINE(0,1);
WRITES(0,Z);
WRITES(0,' <<< <<< <<< !!! ??? !!!');
LINE(0,1)
END
```

References

[1] Iwasawa, K. : On Z_ℓ-extensions of algebraic number fields. *Ann. of Math.* (2), 98 (1973), 246-326.

[2] Iwasawa, K. : On the μ-invariants of Z_ℓ-extensions. *Number Theory, Algebraic Geometry and Commutative Algebra*. Kinokuniya : Tokyo, 1973, 1-11.

[3] Ferrero, B. and Washington, L. : The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math.*, 109 (1979), 377-395.

[4] Greenberg, R. : On the Iwasawa invariants of totally real number fields. *Amer. J. Math.*, 100 (1978), 1235-1245.

[5] Kisilevsky, H. : A Criterion for the Vanishing of λ in Real Abelian Fields. To appear.

[6] Koblitz, N. : p-adic Analysis : A Short Course on Recent Work; *Cambridge Univ. Press* 1980 (chapter 4).

[7] Leopoldt, H.W. : Zur Arithmetik in abelschen Zahlkörpen, *J. reine angew. Math.*, 209 (1962), 54-71.

[8] Washington, L. : Introduction to Cyclotomic Fields, *Springer-Verlag* (1982). (chapter 5).

[9] LeVeque, W.J., editor : Studies in Number Theory, *(Mathematical Association of America)* Printice-Hall (1969). See article by D.H. Lehmer.

[10] Chowla, S. : The Riemann Hypothesis and Hilbert's Tenth Problem, *Gordon and Breach* (1965).

[11] Edwards, H.M. : Fermat's Last Theorem , *Springer-Verlag* (1977). (chapter 8).

[12] Fukuda, T. and Komatsu, K. : On Z_p-extensions of real quadratic fields. To appear.

[13] Borevich, Z. and Shafarevich, I. : Number Theory . *Academic Press* : London and New York, 1966.

[14] Gras, M.N. : Methodes et algorithmes pour le calcul numerique de classes et des unités des extensions cubiques cycliques de Q, *J. reine angew. Math.* , 277 (1975), 89-116.

[15] Ford, D. : Phd Thesis. The Ohio State University (1978).

[16] Stewart, C.L. : On divisors of terms of linear recurrence sequences , *J. reine angew. Math.*, 333 (1982), 12-31.