

AperTO - Archivio Istituzionale Open Access dell'Università di Torino

QUADRATIC FIELDS and CLASS NUMBER FORMULA

This is the author's manuscript

Original Citation:

Availability:

This version is available <http://hdl.handle.net/2318/1910> since

Publisher:

Maplesoft

Terms of use:

Open Access

Anyone can freely access the full text of works made available as "Open Access". Works made available under a Creative Commons license can be used according to the terms and conditions of said license. Use of all other works requires consent of the right holder (author or publisher) if not exempted from copyright protection by the applicable law.

(Article begins on next page)

QUADRATIC FIELDS and CLASS NUMBER FORMULA

Miriam Ciavarella
Università degli Studi di Torino
Italy
miriam.ciavarella@unito.it

Marina Marchisio
Università degli Studi di Torino
Italy
marina.marchisio@unito.it

Introduction

The aim of this document is to give some procedures in order to work explicitly with quadratic fields; in particular the idea of work was born in order to find a useful procedure to compute the class number of a quadratic field.

Many problems of number theory lead to another important question in the arithmetic of algebraic number fields, the question of decomposition of algebraic numbers into prime factors. We shall define a procedure *Dec* which returns the decomposition of algebraic numbers into prime factors in a quadratic field. The problems of factorization are very closely connected with Fermat's (last) theorem. Historically, it was precisely the problem of Fermat's theorem which led Kummer to his fundamental work on the arithmetic of algebraic numbers.

The number of divisor classes is a characteristic of the set of all divisors of the field. It is well known the important role of the number h of divisor classes of algebraic number field play in the arithmetic of the field. Thus one would like to have an explicit formula for the number h in terms of simpler values which depend on the field. Although this has not been accomplished for arbitrary algebraic number fields, for certain fields of great interest, such as quadratic fields, such formulas as been found.

Since all divisors are products of prime divisors and the number of prime divisors is infinite, then to compute the number h in a finite number of steps we must use some infinite processes. This is why, in the determination of h , we shall have to consider infinite products, series and other analytic concepts.

Notation:

In the sequel of this work we shall use the following notation:

- \mathcal{Q} the field of rational numbers;
- \mathcal{Z} the ring of integer numbers.

Initialization

restart

Quadratic Fields

A *quadratic field* is an algebraic number field K of degree two over \mathcal{Q} .

Any quadratic field has the form $\mathcal{Q}(\sqrt{d})$, where $d \in \mathcal{Q}$ and $\sqrt{d} \notin \mathcal{Q}$. $\mathcal{Q}(\sqrt{d_1}) = \mathcal{Q}(\sqrt{d_2})$ if and only if $d_1 = c^2 d_2$, where $c \in \mathcal{Q}$. Therefore any quadratic field has the form $\mathcal{Q}(\sqrt{d})$, where d is a square-free integer that is uniquely determined by the field.

When $d > 0$, $\mathcal{Q}(\sqrt{d})$ is called a *real* and when $d < 0$ an *imaginary*, quadratic field.

Procedure Definition

We give a procedure *QuadraticField* for writing the quadratic field for any integer (not necessarily square-free).

Input datum is d (not necessarily square-free) an integer number.

Output datum is the quadratic field determined by d .

```
QuadraticField := proc(d :: integer)
```

```
  local m, i, a;
```

```
  if d > 0 then for i from 1 to d do
```

```
    if type( $\frac{d}{i^2}$ , integer) = true then a :=  $\frac{d}{i^2}$  end if; end do; print("The quadratic filed is'
```

```
  '  $\mathcal{Q}(\sqrt{a})$  ) end if;
```

```
  if d < 0 then m := -d; for i from 2 to m do
```

```
    if type( $\frac{m}{i^2}$ , integer) = true then m :=  $\frac{m}{i^2}$  end if; end do; print("The quadratic filed is'
```

```
  '  $\mathcal{Q}(\sqrt{-m})$  ) end if;
```

```
  end proc
```

```
proc(d::integer)
```

(3.1.1)

```
  local m, i, a;
```

```
  if 0 < d then
```

```
    for i to d do if type(d/i^2, integer) = true then a := d/i^2 end if end do;
```

```
    print("The * quadratic * filed * is" *  $\mathcal{Q}(\text{sqrt}(a))$  )
```

```
  end if;
```

```
  if d < 0 then
```

```
    m := -d;
```

```
    for i from 2 to m do
```

```
      if type(m/i^2, integer) = true then m := m/i^2 end if
```

```

    end do;
    print('The *quadratic* field is' * Q(sqrt(-m)))
  end if
end proc

```

Examples

$QuadraticField(12)$

'The quadratic field is' $Q(\sqrt{3})$ (3.2.1)

$QuadraticField(-12)$

'The quadratic field is' $Q(i\sqrt{3})$ (3.2.2)

Discriminant

The *discriminant* of an algebraic number field is a numerical invariant that, loosely speaking, measures the size of the (ring of integers of the) algebraic number field. More specifically, it is related to the volume of the fundamental domain of the ring of integers, and it regulates which primes are ramified.

The discriminant is one of the most basic invariants of a number field, and occurs in several important analytic formulas such as the functional equation of the Dedekind zeta function of K , and the analytic class number formula for K . An old theorem of Hermite states that there are only finitely many number fields of bounded discriminant, however determining this quantity is still an open problem, and the subject of current research.

Let K be an algebraic number field, and let O_K be its ring of integers. Let b_1, \dots, b_n be an integral basis of O_K (i.e. a basis as a Z -module), and let $\{\sigma_1, \dots, \sigma_n\}$ be the set of embeddings of K into the complex numbers (i.e. ring homomorphisms $K \rightarrow C$). The *discriminant* of K is the square of the determinant of the n by n matrix B whose (i,j) -entry is $\sigma_i(b_j)$.

Procedure Definition

The procedure *DiscriminantQ* computes the discriminant of $Q(\sqrt{d})$.

Input datum is d (not necessarily square-free) a integer number which defines $Q(\sqrt{d})$.

Output datum is the discriminant of $Q(\sqrt{d})$.

```

DiscriminantQ := proc(d)
local DiscriminantQ, m, i, a;
if d > 0 then for i from 1 to d do
if type( $\frac{d}{i^2}$ , integer) = true then a :=  $\frac{d}{i^2}$  end if; end do; end if;
if d < 0 then m := -d; for i from 2 to m do

```

```

if  $\text{type}\left(\frac{m}{i^2}, \text{integer}\right) = \text{true}$  then  $m := \frac{m}{i^2}$  end if;  $a := -m$  end do; end if;

if  $\text{modp}(a, 4) = 1$  then  $\text{Discriminant}Q := a$  else  $\text{Discriminant}Q := 4 \cdot a$  end if;
end proc

```

Examples

$$\text{Discriminant}Q(12 \cdot 7) \qquad \qquad \qquad 21 \qquad \qquad \qquad (4.2.1)$$

$$\text{Discriminant}Q(-12 \cdot 3) \qquad \qquad \qquad -4 \qquad \qquad \qquad (4.2.2)$$

Ring of Integers of a Quadratic Field

The *ring of integers* of an algebraic number field K , often denoted by O_K , is the ring of algebraic integers contained in K .

Procedure Definition

We give a procedure *RingInteger* which computes the ring of integers of $Q(\sqrt{d})$.

Input datum is d (not necessarily square-free) a integer number which defines $Q(\sqrt{d})$.

Output datum is the ring of integers of $Q(\sqrt{d})$.

```

RingInteger := proc( $d$ )
local  $m, i, a$ ;
if  $d > 0$  then for  $i$  from 1 to  $d$  do
if  $\text{type}\left(\frac{d}{i^2}, \text{integer}\right) = \text{true}$  then  $a := \frac{d}{i^2}$  end if; end do; end if;
if  $d < 0$  then  $m := -d$ ; for  $i$  from 2 to  $m$  do
if  $\text{type}\left(\frac{m}{i^2}, \text{integer}\right) = \text{true}$  then  $m := \frac{m}{i^2}$  end if;  $a := -m$  end do; end if;
if  $\text{modp}(a, 4) = 2$  or  $\text{modp}(a, 4) = 3$  then print( "The integer ring of"  $Q(\sqrt{a})$  "is "  $Z$ 
+  $\sqrt{a}Z$  ) end if;
if  $\text{modp}(a, 4) = 1$  then print( "The integer ring of"  $Q(\sqrt{a})$  " is "  $Z + \frac{1 + \sqrt{a}}{2}Z$  ) end if;
end proc
proc( $d$ ) (5.1.1)
local  $m, i, a$ ;
if  $0 < d$  then
for  $i$  to  $d$  do

```

```

        if type(d/i^2, integer) = true then a := d/i^2 end if
    end do
end if;
if d < 0 then
    m := -d;
    for i from 2 to m do
        if type(m/i^2, integer) = true then m := m/i^2 end if; a := -m
    end do
end if;
if modp(a, 4) = 2 or modp(a, 4) = 3 then
    print("The * integer* ring * of* Q(sqrt(a)) * 'is'* Z + sqrt(a) * Z)
end if;
if modp(a, 4) = 1 then
    print("The * integer* ring * of* 'Q(sqrt(a))'* 'is'* Z + (1/2 + 1/2 * sqrt(a))
    * Z)
end if
end proc

```

Examples

`RingInteger(-5·9)`

The integer ring of $Q(\mathbb{I}\sqrt{5})$ 'is' $Z + \mathbb{I}\sqrt{5} Z$ (5.2.1)

`RingInteger(20·3)`

The integer ring of $Q(\sqrt{15})$ 'is' $Z + \sqrt{15} Z$ (5.2.2)

Fundamental Unit of a Real Quadratic Field

The *units* of a number field K are the invertible elements of the ring of integers. If $K = Q(\sqrt{d})$ is a real quadratic field then the positive units form a multiplicative group which is isomorphic to \mathbb{Z} . This group admits a generator >1 ; this generator is called *fundamental unit* of K .

Let us recall that in the case of $d \equiv 2$ or $3 \pmod{4}$ the units of K are the natural integer solutions of the Pell-Fermat equation; thus if $a_1 + b_1\sqrt{d}$ is the fundamental unit of K and we put

$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n$ then the sequence (a_n, b_n) gives all the solutions of the Pell-Fermat equation.

Procedure Definition

We give a procedure *FU* which computes the fundamental unit of a real quadratic field.

Input datum is d (not necessarily square-free) a positive integer number which defines $Q(\sqrt{d})$.
Output datum is the fundamental unit of $Q(\sqrt{d})$.

```

FU :=proc(d)
  local b, m, i, a, FU;
  if d > 0 then for i from 1 to d do
    if type( $\frac{d}{i^2}$ , integer) = true then a :=  $\frac{d}{i^2}$  end if; end do; end if;
  if d < 0 then m := -d; for i from 2 to m do
    if type( $\frac{m}{i^2}$ , integer) = true then m :=  $\frac{m}{i^2}$  end if; a := -m end do; end if;
  if modp(a, 4) = 2 or modp(a, 4) = 3 then b := 1;
  while type( $\sqrt{a \cdot b^2 + 1}$ , integer) = false and type( $\sqrt{a \cdot b^2 - 1}$ , integer) = false do
    b := b + 1 end do;
  if type( $\sqrt{a \cdot b^2 - 1}$ , integer) = true and type( $\sqrt{a \cdot b^2 + 1}$ , integer) = false then FU :=  $\sqrt{a \cdot b^2 - 1}$ 
    + b· $\sqrt{a}$  end if;
  if type( $\sqrt{a \cdot b^2 + 1}$ , integer) = true and type( $\sqrt{a \cdot b^2 - 1}$ , integer) = false then FU :=  $\sqrt{a \cdot b^2 + 1}$ 
    + b· $\sqrt{a}$  end if;
  if type( $\sqrt{a \cdot b^2 - 1}$ , integer) = true and type( $\sqrt{a \cdot b^2 + 1}$ , integer) = true then FU :=  $\sqrt{a \cdot b^2 - 1}$ 
    + b· $\sqrt{a}$  end if;
  end if;
  if modp(a, 4) = 1 then b := 1;
  while type( $\sqrt{a \cdot b^2 + 4}$ , integer) = false and type( $\sqrt{a \cdot b^2 - 4}$ , integer) = false do
    b := b + 1 end do;
  if type( $\sqrt{a \cdot b^2 - 4}$ , integer) = true and type( $\sqrt{a \cdot b^2 + 4}$ , integer) = false then FU
    :=  $\frac{1}{2}(\sqrt{a \cdot b^2 - 4} + b \cdot \sqrt{a})$  end if;
  if type( $\sqrt{a \cdot b^2 + 4}$ , integer) = true and type( $\sqrt{a \cdot b^2 - 4}$ , integer) = false then FU
    :=  $\frac{1}{2}(\sqrt{a \cdot b^2 + 4} + b \cdot \sqrt{a})$  end if;
  if type( $\sqrt{a \cdot b^2 - 4}$ , integer) = true and type( $\sqrt{a \cdot b^2 + 4}$ , integer) = true then FU
    :=  $\frac{1}{2}(\sqrt{a \cdot b^2 - 4} + b \cdot \sqrt{a})$  end if;
  end if; FU
end proc
proc(d)
  local b, m, i, a, FU;
  if 0 < d then
    for i to d do
      if type(d/i^2, integer) = true then a := d/i^2 end if
    end do
  end if;

```

(6.1.1)

```

if  $d < 0$  then
   $m := -d$ ;
  for  $i$  from 2 to  $m$  do
    if  $\text{type}(m/i^2, \text{integer}) = \text{true}$  then  $m := m/i^2$  end if;  $a := -m$ 
  end do
end if;
if  $\text{modp}(a, 4) = 2$  or  $\text{modp}(a, 4) = 3$  then
   $b := 1$ ;
  while  $\text{type}(\sqrt{a * b^2 + 1}, \text{integer}) = \text{false}$  and  $\text{type}(\sqrt{a * b^2 - 1}, \text{integer}) = \text{false}$  do
     $b := b + 1$ 
  end do;
  if  $\text{type}(\sqrt{a * b^2 - 1}, \text{integer}) = \text{true}$  and  $\text{type}(\sqrt{a * b^2 + 1}, \text{integer}) = \text{false}$  then
     $FU := \sqrt{a * b^2 - 1} + b * \sqrt{a}$ 
  end if;
  if  $\text{type}(\sqrt{a * b^2 + 1}, \text{integer}) = \text{true}$  and  $\text{type}(\sqrt{a * b^2 - 1}, \text{integer}) = \text{false}$  then
     $FU := \sqrt{a * b^2 + 1} + b * \sqrt{a}$ 
  end if;
  if  $\text{type}(\sqrt{a * b^2 - 1}, \text{integer}) = \text{true}$  and  $\text{type}(\sqrt{a * b^2 + 1}, \text{integer}) = \text{true}$  then
     $FU := \sqrt{a * b^2 - 1} + b * \sqrt{a}$ 
  end if
end if;
if  $\text{modp}(a, 4) = 1$  then
   $b := 1$ ;
  while  $\text{type}(\sqrt{a * b^2 + 4}, \text{integer}) = \text{false}$  and  $\text{type}(\sqrt{a * b^2 - 4}, \text{integer}) = \text{false}$  do
     $b := b + 1$ 
  end do;
  if  $\text{type}(\sqrt{a * b^2 - 4}, \text{integer}) = \text{true}$  and  $\text{type}(\sqrt{a * b^2 + 4}, \text{integer}) = \text{false}$  then
     $FU := 1/2 * \sqrt{a * b^2 - 4} + 1/2 * b * \sqrt{a}$ 
  end if;
  if  $\text{type}(\sqrt{a * b^2 + 4}, \text{integer}) = \text{true}$  and  $\text{type}(\sqrt{a * b^2 - 4}, \text{integer}) = \text{false}$  then
     $FU := 1/2 * \sqrt{a * b^2 + 4} + 1/2 * b * \sqrt{a}$ 
  end if;
  if  $\text{type}(\sqrt{a * b^2 - 4}, \text{integer}) = \text{true}$  and  $\text{type}(\sqrt{a * b^2 + 4}, \text{integer}) = \text{true}$  then

```



```

    FU := 1/2 * sqrt(a * b^2 - 4) + 1/2 * b * sqrt(a)
  end if
end if;
FU
end proc

```

Examples

$FU(33)$

$$23 + 4\sqrt{33} \quad (6.2.1)$$

$FU(33 \cdot 4)$

$$23 + 4\sqrt{33} \quad (6.2.2)$$

Decomposition of primes in Quadratic Fields

Any prime number p gives rise to an ideal pO_K in the ring of integers O_K of a quadratic field K . In line with general theory of splitting of prime ideals in Galois extensions, this may be:

p is *inert* :

(p) is a prime ideal; the quotient ring is the finite field with p^2 elements: $O_K/pO_K = F_{p^2}$.

p *splits* :

(p) is a product of two distinct prime ideals of O_K ; the quotient ring is the product $O_K/pO_K = F_p \times F_p$.

p is *ramified* :

(p) is the square of a prime ideal of O_K ; the quotient ring contains non-zero nilpotent elements.

The third case happens if and only if p divides the discriminant D . The first and second cases occur when the Kronecker symbol equals -1 and $+1$, respectively. The first two cases are in a certain sense equally likely to occur as p runs through the primes, see Chebotarev density theorem.

The law of quadratic reciprocity implies that the splitting behaviour of a prime p in a quadratic field depends only on p modulo D , where D is the field discriminant.

Procedure Definition

We give a procedure Dec which returns how each rational prime p factors as a product of prime divisors in $Q(\sqrt{d})$.

Input data are d (not necessarily square-free) a positive integer number which defines $Q(\sqrt{d})$ and p a prime number.

Output datum is the decomposition of the prime p in $Q(\sqrt{d})$.

$Dec := \mathbf{proc}(d, p)$

local $m, i, a;$

```

if  $d > 0$  then for  $i$  from 1 to  $d$  do
if  $\text{type}\left(\frac{d}{i^2}, \text{integer}\right) = \text{true}$  then  $a := \frac{d}{i^2}$  end if; end do; end if;
if  $d < 0$  then  $m := -d$ ; for  $i$  from 2 to  $m$  do
if  $\text{type}\left(\frac{m}{i^2}, \text{integer}\right) = \text{true}$  then  $m := \frac{m}{i^2}$  end if; a := -m; end do; end if;
if  $\text{type}(p, \text{prime}) = \text{false}$  then  $\text{print}(\text{'The number } p \text{ must be a prime'})$  end if;
 $\text{with}(\text{numtheory})$  :
if  $p \neq 2$  and  $\text{legendre}(a, p) = 1$  then  $\text{print}(\text{'The prime } p \text{ splits'})$  end if;
if  $p \neq 2$  and  $\text{legendre}(a, p) = -1$  then  $\text{print}(\text{'The prime } p \text{ is inert'})$  end if;
if  $p \neq 2$  and  $\text{type}\left(\frac{a}{p}, \text{integer}\right) = \text{true}$  then  $\text{print}(\text{'The prime } p \text{ is ramified'})$  end if;
if  $p = 2$  then
if  $\text{modp}(a, 8) = 1$  then  $\text{print}(\text{'2 splits'})$  end if;
if  $\text{modp}(a, 8) = 5$  then  $\text{print}(\text{'2 is inert'})$  end if;
if  $\text{modp}(a, 4) = 2$  or  $\text{modp}(a, 4) = 3$  then  $\text{print}(\text{'2 splits'})$  end if; end if;
end proc

```

```

proc( $d, p$ )

```

(7.1.1)

```

  local  $m, i, a$ ;

```

```

  if  $0 < d$  then

```

```

    for  $i$  to  $d$  do

```

```

      if  $\text{type}(d/i^2, \text{integer}) = \text{true}$  then  $a := d/i^2$  end if

```

```

    end do

```

```

  end if;

```

```

  if  $d < 0$  then

```

```

     $m := -d$ ;

```

```

    for  $i$  from 2 to  $m$  do

```

```

      if  $\text{type}(m/i^2, \text{integer}) = \text{true}$  then  $m := m/i^2$  end if; a := -m

```

```

    end do

```

```

  end if;

```

```

  if  $\text{type}(p, \text{prime}) = \text{false}$  then  $\text{print}(\text{'The * number* } p \text{ * must* be* a * prime'})$  end if;

```

```

   $\text{with}(\text{numtheory})$ ;

```

```

  if  $p \neq 2$  and  $\text{legendre}(a, p) = 1$  then  $\text{print}(\text{'The * prime* } p \text{ * splits'})$  end if;

```

```

  if  $p \neq 2$  and  $\text{legendre}(a, p) = -1$  then  $\text{print}(\text{'The prime } p \text{ is inert'})$  end if;

```

```

  if  $p \neq 2$  and  $\text{type}(a/p, \text{integer}) = \text{true}$  then  $\text{print}(\text{'The prime } p \text{ is ramified'})$ 

```

```

  end if;

```

```

  if  $p = 2$  then

```

```

    if  $\text{modp}(a, 8) = 1$  then  $\text{print}(\text{'2 splits'})$  end if;

```

```

    if  $\text{modp}(a, 8) = 5$  then  $\text{print}(\text{'2 is inert'})$  end if;

```

```

    if  $\text{modp}(a, 4) = 2$  or  $\text{modp}(a, 4) = 3$  then  $\text{print}(\text{'2 splits'})$  end if

```

```

  end if

```

```

end proc

```

Examples

$Dec(3 \cdot 4, 7)$

"The prime p is inert"

(7.2.1)

$Dec(15, 3)$

"The prime p is ramified"

(7.2.2)

Dirichlet Character of a Quadratic Field

The type of decomposition of a prime number p depends only on its residue modulo $|D|$, so that all prime numbers having the same residue have the same decomposition. The Dirichlet character χ of the field $Q(\sqrt{d})$ makes this form of the decomposition rule more clear.

The character χ is a Dirichlet character modulo $|D|$ where D is the discriminant of the field $Q(\sqrt{d})$ and the decomposition of a prime p in $Q(\sqrt{d})$ is given the conditions:

- $p = pp'$, $p \neq p'$ if $\chi(p) = 1$;
- $p = p$ if $\chi(p) = -1$;
- $p = p^2$ if $\chi(p) = 0$.

This character is fundamental for the computation of the class number of $Q(\sqrt{d})$.

Procedure Definition

We now give a procedure *Car* which gives the Dirichlet character χ of the field $Q(\sqrt{d})$.

Note that *Car* procedure needs *DiscriminantQ* procedure to be clicked.

Input data are d (not necessarily square-free) a positive integer number which defines $Q(\sqrt{d})$ and x an integer number.

Output datum is the value $\chi(x)$.

Car := **proc**(d, x)

local m, i, a, Car ;

if $d > 0$ **then for** i **from** 1 **to** d **do**

if $\text{type}\left(\frac{d}{i^2}, \text{integer}\right) = \text{true}$ **then** $a := \frac{d}{i^2}$ **end if; end do; end if;**

if $d < 0$ **then** $m := -d$; **for** i **from** 2 **to** m **do**

if $\text{type}\left(\frac{m}{i^2}, \text{integer}\right) = \text{true}$ **then** $m := \frac{m}{i^2}$ **end if; a := -m; end do; end if;**

with(numtheory) :

if $\text{gcd}(x, \text{DiscriminantQ}(a)) = 1$ **then**

if $\text{modp}(a, 4) = 1$ **then** $Car := \text{jacobi}(x, \text{abs}(a))$ **end if;**

if $\text{modp}(a, 4) = 3$ **then** $Car := (-1)^{\left(\frac{x-1}{2}\right)} \cdot \text{jacobi}(x, \text{abs}(a))$ **end if;**

```

if  $\text{type}\left(\frac{a}{2}, \text{integer}\right) = \text{true}$  then  $Car := (-1)^{\left(\left(\frac{x^2-1}{8}\right) + \left(\frac{x-1}{2}\right) \cdot \left(\frac{\frac{a}{2}-1}{2}\right)\right)}$   $\cdot \text{jacobi}\left(x,$ 
   $\text{abs}\left(\frac{a}{2}\right)\right)$  end if;

```

```

end if;

```

```

if  $\text{gcd}(x, \text{Discriminant}Q(a)) > 1$  then  $Car := 0$  end if;

```

```

   $Car$  end proc

```

```

proc( $d, x$ )

```

(8.1.1)

```

  local  $m, i, a, Car;$ 

```

```

  if  $0 < d$  then

```

```

    for  $i$  to  $d$  do

```

```

      if  $\text{type}(d/i^2, \text{integer}) = \text{true}$  then  $a := d/i^2$  end if

```

```

    end do

```

```

  end if;

```

```

  if  $d < 0$  then

```

```

     $m := -d;$ 

```

```

    for  $i$  from 2 to  $m$  do

```

```

      if  $\text{type}(m/i^2, \text{integer}) = \text{true}$  then  $m := m/i^2$  end if;  $a := -m$ 

```

```

    end do

```

```

  end if;

```

```

   $\text{with}(\text{numtheory});$ 

```

```

  if  $\text{gcd}(x, \text{Discriminant}Q(a)) = 1$  then

```

```

    if  $\text{mod}p(a, 4) = 1$  then  $Car := \text{numtheory}:\text{jacobi}(x, \text{abs}(a))$  end if;

```

```

    if  $\text{mod}p(a, 4) = 3$  then

```

```

       $Car := (-1)^{(1/2 * x - 1/2)} * \text{numtheory}:\text{jacobi}(x, \text{abs}(a))$ 

```

```

    end if;

```

```

    if  $\text{type}(1/2 * a, \text{integer}) = \text{true}$  then

```

```

       $Car := (-1)^{(1/8 * x^2 - 1/8 + (1/2 * x - 1/2) * (1/4 * a - 1/2))}$ 
       $* \text{numtheory}:\text{jacobi}(x, \text{abs}(1/2 * a))$ 

```

```

    end if

```

```

  end if;

```

```

  if  $1 < \text{gcd}(x, \text{Discriminant}Q(a))$  then  $Car := 0$  end if;

```

```

   $Car$ 

```

```

end proc

```

Examples

```

 $Car(15, 3)$ 

```

0

(8.2.1)

```

 $Car(21, 4)$ 

```

1

(8.2.2)

▼ Class Number for Quadratic Fields

In mathematics, the extent to which unique factorization fails in the ring of integers of an algebraic number field (or more generally any Dedekind domain) can be described by a certain group known as an ideal class group (or class group). If this group is finite, (as it is in the case of the ring of integers of a number field) then the order of the group is called the *class number*. The multiplicative theory of a Dedekind domain is intimately tied to the structure of its class group. For example, the class group of a Dedekind domain is trivial if and only if the ring is a unique factorization domain.

Let K be the an algebraic number field; let $\mathfrak{I}(\mathcal{O}_K)$ be the group of the fractional ideals of K and H be the group of the principal fractional ideals of K . Then $Cl(\mathcal{O}_K) = \frac{\mathfrak{I}(\mathcal{O}_K)}{H}$ and the *class number* is $h = |Cl(\mathcal{O}_K)|$.

The computation of the class number is closely related to the Dedekind zeta function $\zeta_K(s)$ of K , in particular it is related to the residue in $s = 1$ of $\zeta_K(s)$. If K is a quadratic field, the Dedekind zeta function is the product $\zeta_K(s) = \zeta(s)L(s, \chi)$ where $\zeta(s)$ is the zeta Riemann function and $L(s, \chi)$ is the Dirichlet L function. Thus the number h is related to the value of $L(1, \chi)$ which can be explicitly computed.

▼ Procedure Definition

We give a procedure *ClassNumber* which computes the class number of $\mathcal{O}(\sqrt{d})$. This procedure needs the *DiscriminantQ*, *Car*, *FU* procedure to be clicked.

Input datum is d (not necessarily square-free) a positive integer number which defines $\mathcal{O}(\sqrt{d})$.
Output datum is the class number of $\mathcal{O}(\sqrt{d})$.

```

ClassNumber := proc(d)
local h, x, a, i, m;
if d > 0 then for i from 1 to d do
if type( $\frac{d}{i^2}$ , integer) = true then a :=  $\frac{d}{i^2}$  end if; end do; end if;
if d < 0 then m := -d; for i from 2 to m do
if type( $\frac{m}{i^2}$ , integer) = true then m :=  $\frac{m}{i^2}$  end if; a := -m :end do; end if;
with(numtheory) :
if a > 0 then
h := 0 : for x from 1 to  $\frac{DiscriminantQ(a)}{2}$  do
if gcd(x, DiscriminantQ(a)) = 1 then

```

$h := h + Car(a, x) \cdot \ln\left(\sin\left(\frac{\pi \cdot x}{DiscriminantQ(a)}\right)\right)$ end if:

end do: $h := -\frac{1}{\ln(FU(a))} \cdot h$

end if:

if $a < 0$ then

$h := 0$: for x from 1 to $\text{abs}(DiscriminantQ(a))$ do

if $\text{gcd}(x, DiscriminantQ(a)) = 1$ then

$h := h + Car(a, x) \cdot x$ end if:

end do: $h := -\frac{1}{\text{abs}(DiscriminantQ(a))} \cdot h$

end if:

h

end proc

proc(d)

(9.1.1)

local h, x, a, i, m ;

if $0 < d$ then

for i to d do

if $\text{type}(d/i^2, \text{integer}) = \text{true}$ then $a := d/i^2$ end if

end do

end if;

if $d < 0$ then

$m := -d$;

for i from 2 to m do

if $\text{type}(m/i^2, \text{integer}) = \text{true}$ then $m := m/i^2$ end if; $a := -m$

end do

end if;

with(numtheory);

if $0 < a$ then

$h := 0$;

for x to $1/2 * DiscriminantQ(a)$ do

if $\text{gcd}(x, DiscriminantQ(a)) = 1$ then

$h := h + Car(a, x) * \ln(\sin(\pi * x / DiscriminantQ(a)))$

end if

end do;

$h := -h / \ln(FU(a))$

end if;

if $a < 0$ then

$h := 0$;

for x to $\text{abs}(DiscriminantQ(a))$ do

if $\text{gcd}(x, DiscriminantQ(a)) = 1$ then $h := h + Car(a, x) * x$ end if

end do;

$h := -h / \text{abs}(DiscriminantQ(a))$

```

end if;
h
end proc

```

Examples

$ClassNumber(-163)$

1

(9.2.1)

$ClassNumber(-5)$

2

(9.2.2)

$ClassNumber(33)$

$$-\frac{1}{\ln(23 + 4\sqrt{33})} \left(\ln\left(\sin\left(\frac{1}{33}\pi\right)\right) + \ln\left(\sin\left(\frac{2}{33}\pi\right)\right) + \ln\left(\sin\left(\frac{4}{33}\pi\right)\right) \right) \quad (9.2.3)$$

$$- \ln\left(\sin\left(\frac{5}{33}\pi\right)\right) - \ln\left(\sin\left(\frac{7}{33}\pi\right)\right) + \ln\left(\sin\left(\frac{8}{33}\pi\right)\right) - \ln\left(\sin\left(\frac{10}{33}\pi\right)\right)$$

$$- \ln\left(\sin\left(\frac{13}{33}\pi\right)\right) - \ln\left(\sin\left(\frac{14}{33}\pi\right)\right) + \ln\left(\sin\left(\frac{16}{33}\pi\right)\right)$$

at 5 digits
→

1.0000

(9.2.4)

References

[1] Z.I.Borevich and I.R.Shafarevich, Number Theory, Academic Press, Inc., 1966

[2] P.Samuel, Théorie Algébrique des Nombres, Hermann, Editeurs des Sciences et des Arts, 1971.