METHOD

4(10), April 1, 2013

ISSN
2278–5469
EISSN
2278–5450

Discovery

Enhanced methods of calculation in real quadratic fields on unit norm

Renganathan K

Department of Mathematics, K. Ramakrishnan College of Technology, Trichy, E-mail: renga81@gmail.com

Publication History
Received: 16 February 2013
Accepted: 20 March 2013
Published: 1 April 2013

Citation
Renganathan K. Enhanced methods of calculation in real quadratic fields on unit norm. *Discovery*, 2013, 4(10), 16-18

ABSTRACT

In particular, a great amount of effort has been expended on the simplest algebraic extensions of the rationales' quadratic fields. These are intimately linked to binary quadratic forms and have proven to be a good testing ground for algebraic number theorists because, although computing with ideals and field elements is relatively easy, there are still many unsolved and difficult problems remaining. For example, it is not known whether there exist infinitely many real quadratic fields with class number one, and the best unconditional algorithm known for computing the class number has complexity Q(D$^{1/2+€}$)**.**Those properties are applied to the theory of the fundamental unit of $Q(D^{1/2})$The main result is as follows. Take some unit $\tau=\left[\frac{(a+b\,(D)^{1/2})}{2}\right]$whose norm = 1. If the number b satisfies a certain condition, then $\varepsilon=\tau_0^{2r}$ for some r where ε_0 is the fundamental unit of Q((D)l/2.

Keywords: Prime factor, GCD, Quadratic fields

1. INRODUCTION

Let $\tau=\frac{(t+u(D)^{1/2})}{2}$be a unit of $Q(D^{1/2})$ with D square-free whose norm = 1. We investigate the properties of the factors of the number u_r which is defined by $\tau^r=\frac{(t_r+u_r(D)^{1/2})}{2}$Those properties are applied to the theory of the fundamental unit of $Q(D^{1/2})$ The main result is as follows. Take some unit $\tau^{'}=\left[\frac{(a^{'}+b^{'}(D)^{1/2})}{2}\right]q/p^{'}$ here $\tau>1$whose norm = 1. If the number b satisfies a certain condition, then $\tau=\varepsilon_0^{2r}$ for some r, where ε_0 is the fundamental unit of $Q(D^{1/2})$, (Ankeny et al. 1965; Degert, 1958: Hasse, 1965; Nagell, 1938; Redei, 1935; Richaud, 1866).

Let D(>0) be a positive real integer and $Q(D^{1/2})$ be the real quadratic field of discriminant D. Take the fundamental unit ε is commonly normalized so that |ε| > 1and some unit $\varepsilon>1$ of $Q(D^{1/2})$ whose norm = 1. We denote this unit by $\tau=\frac{(t+u(D)^{1/2})}{2}$ and fix it in the following.

We denote $\tau^r=\frac{(t_r+u_r(D)^{1/2})}{2},r\geq 1$ (i)

The aim of this paper is to investigate the properties of the number u_r, and apply those properties to the theory of the fundamental unit of a real quadratic field.

We use the following notation:

Q-the field of rational numbers;

N -the set of positive rational integers;
(a, b)- the greatest common divisor of a and b;
a / b means a divides b.
Sice the norm of $\mathcal{E}$ is 1 , from the identity

$$\tau-\tau^{-r}=(\tau+\tau^{-1})(\tau^{(r-1)}-\tau^{-(r-1)})-(\tau^{(r-2)}-\tau^{-(r-2)}), r\in N, r\geq 3$$

We can deduce the relation

$u_r = tu_{r-1}-u_{r-2}$ here $u_1 = u$ and (ii)

By virtue of the relations (ii), we can obtain u_r, inductively and we may express u_r , in the form

$u_r = uP_r(t)$ where $P_r(t)\in N$ (iii)

Here $P_r(t)$ satisfies the following inductive relations similar to (ii):

$$P_r(t)=tP_{r-1}(t)-P_{r-2}(t) \quad r\geq 3 \qquad \text{(iv)}$$

$$P_1=1, P_2=t$$

PROPOSITION 1:

Those numbers $P_r(r\in N)$ have the following properties.

(1) $(P_{r+1}, P_r)=1$ for any r ∈ N

(2) k,r ∈ N, k/r ⇒ P_k / P_r.

(3) k,r ∈ N,(k,r)=1⇒ $(P_k, P_r)=1$

(4) *If* r ∈ N is odd and n=2ℓ+1,ℓ ∈ N,then

$$P_r = P^2{}_{\ell+1} - P^2{}_{\ell}$$
$$=(P_{\ell+1}-P_\ell)(P_{\ell+1}+P_\ell)$$

Proof of (1)

By virtue of the inductive relations (4),

$(P_2, P_1)=(P_3, P_2)=......=(P_{r+1}, P_r)=1$

This proves (1).

Proof of (2)

For two (positive) integers r and k, the properties of their greatest common divisor gcd and the least common multiple lcm come in pairs; the phenomenon is partly explained by the formula gcd(k,r) × lcm(k, r) = k × r. The basic fact that "P being a factor of Q" and "Q being a multiple of P" are equivalent also contributes to a certain kind of symmetry in properties of gcd and lcm. (Above, as below, the symbols k,r, P, Q stand for positive integers.)
P|r and P|k ⇒ P|gcd(r, k),
r|P and k|P ⇒ lcm(r, k)|P.
Lemma
For integers N_1, ..., N_k, k ≥ 2,
lcm(gcd(N_1, k), gcd(N_2,k), ..., gcd(Nr, k)) = gcd(lcm(N_1, ..., Nr), k)
gcd(lcm(N_1, k), lcm(N_2, k), ..., lcm(Nr,k)) = lcm(gcd(N_1, ..., Nr), k).
As with the union and intersection of the sets, gcd and lcm satisfy two distributive laws.

Now we can express t_r as $t_r = S_r(t)$ satisfies the following inductive relations. $S_r = tS_{r-1}-S_{r-2}$

$$S_1 = t \;, S_2 = t^2 - 2$$

Take $\tau^k = \dfrac{(t_k + u_k(D)^{1/2})}{2}$, $\tau^k = \dfrac{(S_k(t)+P_k(t)u\ (D)^{1/2})}{2}$ for the unit $\mathcal{E}$ of equation (ii)

Then the relation (iii) shows if k/r , then $P_r(t)=P_k(t)\cdot P_{r/k}(S_k(t))=P_k(t)\cdot$

Proof of (3)

For two numbers $k, r\in N$ such that (k, r) = 1, there exist two numbers $a,b\in N$ such that ku = rb + 1. Then from property (1), we have $(P_{ka}, P_{rb})=1$, and from property (2),

P_k / P_{ka} and P_r / P_{ra} ·

So we can obtain assertion (3) immediately.
Assertion (4) follows from the following identity:

$$\frac{(\tau^{\ell+1}-\tau^{-(\ell+1)})}{(\tau-\tau^{-1})^2}-\frac{(\tau^{\ell}-\tau^{-\ell})}{(\tau-\tau^{-1})^2}=\frac{(\tau-\tau^{-1})^2(\tau^{\ell+1}-\tau^{-(\ell+1)})-(\tau-\tau^{-1})^2(\tau^{\ell}-\tau^{-\ell})}{(\tau-\tau^{-1})^2}$$
$$=\frac{(\tau^{2\ell+1}-\tau^{-2(\ell+1)})(\tau\ -\tau^{-1})}{(\tau-\tau^{-1})^2}$$
$$=\frac{(\tau^{2\ell+1}-\tau^{-2(\ell+1)})}{(\tau-\tau^{-1})} \qquad (1.1)$$

Since $N(\varepsilon)$=1 and $\varepsilon>1$,t satisfies the inequality $t>(D)^{1/2}$ we can assume that $t\geq 3$

PROPOSITION 2:

For $r\in N$ then the following inequiality is satisfied

$$P_{r+1}>(t-1)P_r$$

Proof:

We prove it by induction. Since $P_1 = 1$ and $P_2 = t$

The assertion is trivial for r = 1. By virtue of the relations (1.1) and the inductive assumption for n - 1, we have

$$P_{r+1}=tP_r-P_{r-1}>tP_r-P_r$$
$$P_{r+1}>(t-1)P_r$$

Note: Relation (1.1) $\Rightarrow tP_r \geq P_{r+1} \Leftrightarrow r=1$

Result: (a) Both factor given in the property (4) of Proposition :(1) are larger than 1

We can prove *If* r ∈ N is odd and n=2ℓ+1,ℓ ∈ N

$$P_r = P^2{}_{\ell+1}-P^2{}_{\ell}$$
$$=(P_{\ell+1}-P_\ell)(P_{\ell+1}+P_\ell)>1$$

Result (b): For any $l\in N$,then the following inequality holds.

$$1<t(t-1)<\frac{(P_{l+1}+P_l)}{(P_{l+1}-P_l)}$$
$$<\frac{(t+1)}{(t-2)}$$
$$\leq 4$$

If the discriminant D is given we may take $\dfrac{D^{1/2}+1}{D^{1/2}-2}$ instead of 4.

Now we merge the results of Proposition (1) and (2) we can get the following theorems.

Theorem 1

For the number of factors of P_r then we can obtain the following estimates.

(A) P_{2^k} (k ∈ N) has at least m factors.

(B) If ℓ is odd prime, then P_{l^k} (k ∈ N) has at least k + 1 factors.

(C) If r n is of the form $r=2^{e_0} l^{e_1}{}_1 ....l_9$ where $e_0 \geq 0\ e_i\in N, 1\leq i\leq s$ where the l_i are different odd

Primes, then P_r , has at least

$$s+e_0+e_1+e_2+e_3+e_4+e_5+e_6+e_7+e_8+e_9$$

factors.

Proof:

By the virtue property (2) $P_{a^k} / P_{a^{k+1}}$ for $\mathrm{a} \geq 2$, $\mathrm{k} \in \mathrm{N}$ and k<r implies $P_k<P_r$

Since P_2 =t>1,assertion (i) follows immediately and assertion (ii) follows fro result (a) of proposition (2). Then assertion (iii) is an easy consequence of property (3)

Remark: since $u_r = uP_r$, the number of the factors of u_r is the sum of that of u and of P_r .

Let $n > 1$ be any integer and let $\operatorname{lpf}(n)$(also denoted $\operatorname{LD}(n)$) be the least integer greater than 1 that divides n, i.e., the number p_1 in the factorization

$$n = p_1^{a_1} \cdots p_k^{a_k},$$

with for . The least prime factor is implemented in *Mathematica* as FactorInteger[*n*][[1,1]].

For $n = 2$, 3, ..., the first few are 2, 3, 2, 5, 2, 7, 2, 3, 2, 11, 2, 13, 2, 3, ...

If n is composite then $[\operatorname{lpf}(n)]^2 \leq n$, with equality for $n$the square of a prime.

A plot of the least prime factor function resembles a jagged terrain of mountains, which leads to the appellation of "twin peaks" to a pair of integers (x, y)such that

1. $x < y$,
2. $\operatorname{lpf}(x) = \operatorname{lpf}(y)$,
3. For all z, $x < z < y$implies $\operatorname{lpf}(z) < \operatorname{lpf}(x)$.

The least *multiple* prime factors for squareful integers are 2, 2, 3, 2, 2, 3, 2, 2, 5, 3, 2, 2, 2,

We have several applications to theory of the fundamental unit of a real quadratic fields as follows,

A unit is an element in a ring that has a multiplicative inverse. If $a$is an algebraic integer which divides very algebraic integer in the field, $a$is called a unit in that field. A given field may contain infinity of units. The units of $\mathbb{Z}_n$are the elements relatively prime to n. The units in $\mathbb{Z}_n$which are squares are called quadratic residues. All real quadratic fields $Q(D^{1/2})$have the two units ± 1.

The numbers of units in the imaginary quadratic field $Q(-D^{1/2})$for $D = 1$, 2, ... are 4, 2, 6, 4, 2, 2, 2, 2, 4, 2, 2, 6, 2, ... (Sloane's A092205). There are four units for $D = 1$, 4, 9, 16, ... (Sloane's A000290; the square numbers), six units for $D = 3$, 12, 27, 48, ... (Sloane's A033428; three times the square numbers), and two units for all other imaginary quadratic fields, i.e., $D = 2$, 5, 6, 7, 8, 10, 11, ... (Sloane's A092206). The following table gives the units for small D. In this table, $\omega$is a cube root of unity.

Theorem 2

Let $Q(D^{1/2})$ be areal quadratic field of discriminate D>0, and let τ_0 >1 be the fundamental unit of $Q(D^{1/2})$. Take some unit τ >1 of $Q(D^{1/2})$ whose norm =1,and express it in the form $\tau = \frac{(a+b(D)^{1/2})}{2}$.

If b=p where p is the prime number, thenexcept for the case $\tau = \left[\frac{(1+(5)^{1/2})}{2}\right]^4$, we have $\tau = \tau_0 \text{ (or) } \tau_0^{\,2} (or) \tau_0^{\,4}$; and if

$\tau = \tau_0 \text{ (or) } \tau^2{}_0$,then τ_0 is of the form $\tau_0 = \left[\frac{(p+(D)^{1/2})}{2}\right]$,

$\mathrm{D= p^2 \pm 4}$.

(II) If $b = p^n$ " where p is an odd prime number and p > 4 and $r \geq 2$,then $\tau = \tau_0 \text{ (or) } \tau_0^{\,2}$;and if $\tau = \tau_0 \text{ (or) } \tau_0^{\,2}$,then τ_0 is of the form $\tau_0 = \left[\frac{(p^r+(D)^{1/2})}{2}\right]$, $\mathrm{D= p^{2r} \pm 4}$.

(III) If $b = p \times q$ where p and q are prime numbers such that 4p<q, then $\tau = \tau_0 \text{ (or) } \tau_0^{\,2} (or) \tau_0^{\,4}$.

(IV)If b=nq where q is the prime number such that $4n \leq q$,then $\tau = \tau_0^{\,2l}$ for some $l = 0$ or $l \in N$.

Proof:

By virtue of (B) of theorem (1) and the two results of proposition (2) under condition in (I),(II),(III) or (IV) ,the unit τ cannot power of odd degree of another unit of $Q(D^{1/2})$. (Since t>u-2 ,for unit $\frac{(t+u(D)^{1/2})}{2}$ (>1), under the condition in (IV), τ cannot be a power of another unit τ' which is of the form $\tau' = \left[\frac{(a'+b'(D)^{1/2})}{2}\right]$where q / p'). That is, $\tau = \tau_0^{\,2l}$ for some l =0 or $l \in N$. In each case of (I) to (IV), it is easy to check all possible l 's and deduce the result.

Remark 1

If we are given the value of D, the condition (II), (III), (IV) may be improved by taking $((D)^{\frac{1}{2}}+1)/((D)^{\frac{1}{2}}-2)$ instead of the number 4 in the inequalities.

REFERENCE

1. Ankeny NC, Chowla S, Hasse H. On the class number of the real subfield of a cyclotomic field. *J. reine angew. Math*. 1965, 217, 217-220
2. Degert G. Uber die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahl- korper. *Abh. math. Sem. Univ*. Hamburg, 1958, 22, 92-97
3. Hasse H. Uber mehrklassige, aber eingeschlechtige reell-quadratische Zahlkorper. *Elemente der Mathematik*, 1965, 20, 49-59
4. Nagell T. Bemerkung ber die Klassenzahl reell-quadratischer Zahlkorper. Det Konge- lige Norske Videnskabens Selskab, *Forhandlinger* 1938, 11, 7-10
5. Redei L. Uber die Pellsche Gleichung 2-du2 -. *J. reine angew. Math*. 1935, 73, 193-221
6. Richaud C, Sur la resolution des equations x2–y2 1. Atti Accad. pontif. *Nuovi Lincei* 1866, 177-182