

Relative Densities of Ramified Primes¹

in $\mathbb{Q}(\sqrt{pq})$

Michele Elia

Politecnico di Torino, Italy
elia@polito.it

Abstract

The relative densities of rational primes q , such that a given rational prime p is a square of either a principal or a non-principal ideal in the quadratic number field $\mathbb{Q}(\sqrt{pq})$, essentially depend on the residue classes of both p and q modulo 4. The computation of these densities is complete when at least one residue of p or q is not equal to 1 modulo 4. When both residues are equal to 1 modulo 4, it is shown that the densities are related to a problem of Legendre's, and are evaluated taking as true an old conjecture on the solvability of the Pell equation $x^2 - Ny^2 = -1$. The proofs use elementary properties from algebraic number theory, and the conclusions on densities are a direct consequence of Dirichlet's density theorem.

Mathematics Subject Classification: 49Q10, 11S99

Keywords: Pell equation, ramification, fundamental unit, densities of sets of primes

1 Introduction

The separation of a composite integer into prime factors is of fundamental importance in modern cryptography. This problem had an illustrious formulation in Gauss' "*Disquisitiones Arithmeticae*" [8, p.396-406]:

¹A preliminary version of this paper has been presented at the conference "Interdisciplinary Mathematical and Statistical Technique 2007" - May 20-23, 2007 - Shanghai, China.

The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic ...

Many of the factorization methods for a composite squarefree integer N considered thus far, in particular Shank's algorithm, directly or indirectly exploit properties of binary quadratic forms and units in the quadratic number field $\mathbb{Q}(\sqrt{N})$ [3, 16, 1, 23]. Units and ramified primes in real quadratic number fields, besides their relevance to factorization, have interesting connections coming from Hilbert's Theorem 90. Let $\{1, \omega\}$ be a basis of the maximal order $\mathfrak{D}(\sqrt{N}) = \{a + b\omega : a, b \in \mathbb{Z}\}$ in $\mathbb{Q}(\sqrt{N})$, with $\omega = \frac{1+\sqrt{N}}{2}$ if $N \equiv 1 \pmod{4}$, or $\omega = \sqrt{N}$ if $N \equiv 2, 3 \pmod{4}$. The field norm of $z = a + b\omega$ is either $\mathbf{N}(z) = a^2 + ab - \frac{N-1}{4}b^2$ if $N \equiv 1 \pmod{4}$, or $\mathbf{N}(z) = a^2 - Nb^2$ if $N \equiv 2, 3 \pmod{4}$. The elements of norm ± 1 are called units; they form a multiplicative cyclic group \mathfrak{U} of infinite order whose generator is called a fundamental unit. If the norm of a fundamental unit $\mathbf{u} \in \mathfrak{D}(\sqrt{N})$ is 1, then Theorem 90 of Hilbert's establishes that \mathbf{u} can be written as a ratio $\gamma/\sigma(\gamma)$ where γ is a convenient element of $\mathfrak{D}(\sqrt{N})$, and σ is the non-trivial automorphism of $\mathbb{Q}(\sqrt{N})$, that is $\sigma(\sqrt{N}) = -\sqrt{N}$. Since $\gamma\sigma(\gamma) = N\gamma \in \mathbb{Z}$, the field norm of γ , the equalities $\mathbf{u} = \frac{\gamma}{\sigma(\gamma)} = \frac{\gamma^2}{N\gamma}$ show that $N\gamma$ is a product of rational primes that ramify, that is rational primes which are squares of principal or non-principal ideals in $\mathfrak{D}(\sqrt{N})$. An ideal is a subset of $\mathfrak{D}(\sqrt{N})$ whose elements share a common factor \mathfrak{a} . If \mathfrak{a} is a proper element of $\mathfrak{D}(\sqrt{N})$, the ideal is principal and is written as (\mathfrak{a}) ; if \mathfrak{a} is not a proper element of $\mathfrak{D}(\sqrt{N})$, the ideal is non-principal and is written as the greatest common divisor $(a, b+\omega)$ of $a \in \mathbb{Z}$ and $b+\omega \in \mathfrak{D}(\sqrt{N})$, where a is a factor of the norm $N(b+\omega)$.

When $N = pq$ is a product of two different odd primes p and q congruent 3 modulo 4, it is well known [4, Theorem 7, p.188] that p and q are squares of principal ideals in $\mathfrak{D}(\sqrt{pq})$. When either p or q is not congruent 3 modulo 4, the more complex situation may be analyzed by considering, for a given p , the set \mathcal{P} of rational primes q partitioned into subsets \mathcal{P}_i depending on the ramification of 2 or p or $2p$ into principal or non-principal ideals in $\mathfrak{D}(\sqrt{pq})$. Section 2 addresses the cases when either p or q is congruent 3 modulo 4. When both p and q are congruent 1 modulo 4, the relative densities of \mathcal{P}_i s are only conjectured [22] as they depend on Diophantine problems concerning the negative Pell equation, dating back to Euler and Legendre, which are still open [12, 13, 14]. Section 3 collects remarks and comments concerning factorization, statistics of numerical investigations, and open problems.

2 Main Propositions

In $\mathfrak{D}(\sqrt{pq})$ the only rational primes that ramify into principal or non-principal ideals are p , q , and possibly 2. Let us recall for easy reference the well known splitting of 2 [5, 9, 16, 11]:

i) If pq is congruent 5 modulo 8, then 2 is inert, which means that 2 is a prime in any order of $\mathbb{Q}(\sqrt{pq})$, and correspondingly the equation $x^2 - pqy^2 = \pm 8$ is not solvable in integers.

ii) If pq is congruent 1 modulo 8, then 2 splits into the product of either principal or non-principal ideals, which means that 2 is a product of two conjugate ideals \mathfrak{I}_2 and $\sigma(\mathfrak{I}_2)$. If 2 splits into the product of principal ideals, the equation $x^2 - pqy^2 = \pm 2$ is solvable in integers.

iii) If pq is congruent 3 or 7 modulo 8, then 2 ramifies, which means that 2 is a square of a principal or a non-principal ideal.

The following theorem is reported from [4, p.188] together with its proof, because it started this investigation and plays a fundamental part in the results.

Theorem 1 ([4]). *For two different rational primes $p \equiv q \equiv -1 \pmod{4}$, the field $\mathbb{Q}(\sqrt{pq})$ has the property that the factors \mathfrak{p} , \mathfrak{q} of $(p) = \mathfrak{p}^2$, $(q) = \mathfrak{q}^2$ are principal.*

PROOF. Since $pq \equiv 1 \pmod{4}$, the only ramified primes are p and q . Therefore the candidates for γ are the factor ideals \mathfrak{p} , \mathfrak{q} , and their product $\mathfrak{p}\mathfrak{q}$ which is certainly a principal ideal because $\mathfrak{p}\mathfrak{q} = \sqrt{pq}\mathfrak{v}$, with \mathfrak{v} a unit. However $\gamma = \sqrt{pq}\mathfrak{v}$ does not give a fundamental unit, since we have $\mathfrak{u} = \frac{(\sqrt{pq}\mathfrak{v})^2}{pq} = \mathfrak{v}^2$ and a square is not fundamental. Then, from Hilbert's Theorem 90, the fundamental unit is

$$\mathfrak{u} = \frac{\mathfrak{p}^2}{p}$$

therefore $\gamma = \mathfrak{p}$, and \mathfrak{p} is a principal ideal. It follows that also \mathfrak{q} is principal because the product $\mathfrak{p}\mathfrak{q}$ is principal.

□

Theorem 2. *Let p be a rational prime congruent 5 modulo 8; the set of rational primes $q > p$ congruent 3 modulo 4 is partitioned into two subsets of relative density 1/2, such that either p or $2p$ is a square of a principal ideal in $\mathbb{Q}(\sqrt{pq})$.*

PROOF. Since $pq \equiv 3 \pmod{4}$, the ramified primes are 2, p , and q ; however, the ideal $\mathfrak{I}_2 = (2, 1 - \sqrt{pq})$ is non-principal, since 2 cannot be represented by the

form $x^2 - pqy^2$ because it is a quadratic non-residue modulo p .

If p is a quadratic residue modulo q , then $x^2 - pqy^2 = p$ admits of an integer solution, $x = a, y = b$, thus $\pi_p = a + b\sqrt{pq}$ is a factor of p in $\mathbb{Q}(\sqrt{pq})$. Clearly, $\pi_p^2 = pu$, and u is a fundamental unit, with $\gamma = \pi_p$.

If p is a quadratic non-residue modulo q , then either $x^2 - pqy^2 = 2p$ or $x^2 - pqy^2 = -2p$ admits of an integer solution because either $(2p|q) = 1$ or $(-2p|q) = 1$, and $\mathfrak{I}_2\mathfrak{p}$ is a principal ideal, although \mathfrak{I}_2 and \mathfrak{p} separately are not.

The densities of prime p that are or are not quadratic residues modulo q are clearly equal, by Dirichlet's density theorem, and the conclusion on densities of the partition of \mathcal{P} is a consequence of the reciprocity theorem since $(q|p) = (p|q)$.

□

Theorem 3. *Let p be a rational prime congruent 1 modulo 8; the set of rational primes $q > p$ congruent 3 modulo 4 that are quadratic residues modulo p can be partitioned into four subsets of relative density $1/4$, such that either 2, or p , or $2p$, or all three together are squares of principal ideals in $\mathbb{Q}(\sqrt{pq})$.*

PROOF. Since $pq \equiv 3 \pmod{4}$, the ramified primes are 2, p , and q . We consider separately $q \equiv 7 \pmod{8}$ and $q \equiv 3 \pmod{8}$. If $q \equiv 7 \pmod{8}$, the ideal $\mathfrak{I}_2 = (2, 1 - \sqrt{pq})$ is principal, since $(2|p) = (2|q) = 1$; moreover, if $(p|q) = 1$, \mathfrak{p} is a principal ideal, thus 2, p , and $2p$ are squares of principal ideals, whereas if $(p|q) = -1$, \mathfrak{p} is a non-principal ideal, thus also $2p$ is non-principal.

If $q \equiv 3 \pmod{8}$ the ideal $\mathfrak{I}_2 = (2, 1 - \sqrt{pq})$ is non-principal, since $(2|q) = -1$; moreover, if $(p|q) = 1$, \mathfrak{p} is a principal ideal, whereas if $(p|q) = -1$, \mathfrak{p} is a non-principal ideal; in the latter case, the product $\mathfrak{I}_2\mathfrak{p}$ is a principal ideal. The conclusions on the densities of the partition sets of \mathcal{P} are a direct consequence of Dirichlet's density theorem.

□

When p and q are primes congruent 1 modulo 4, it is useful to consider the following property, dating back to works by Euler and Legendre, [12, 13, 14], which essentially is Theorem 9.5, p.163 in Buell's book [2]. The reported proof is a slight modification of the classical one.

Lemma 1 ([2, Theorem 9.5, p.163]). *Let p and q be primes congruent 1 mod 4. The equation $x^2 - pqy^2 = -1$ is solvable if and only if neither $qu^2 - pv^2 = +1$ nor $qu^2 - pv^2 = -1$ is solvable in integers.*

PROOF. Let (x_1, y_1) be the minimal solution of $x^2 - pqy^2 = 1$, which considered modulo 4 shows that $x_1 = 2x_0 + 1$ and $y_1 = 2y_0$. Thus we have

$$x_0(x_0 + 1) = pqy_0^2$$

which is equivalent to four possible pairs of equations, since x_0 and $x_0 + 1$ are relatively prime:

$$\begin{cases} x_0 = pq u_0^2 \\ x_0 + 1 = v_0^2 \end{cases} \quad \begin{cases} x_0 = v_0^2 \\ x_0 + 1 = pq u_0^2 \end{cases} \quad \begin{cases} x_0 = p u_0^2 \\ x_0 + 1 = q v_0^2 \end{cases} \quad \begin{cases} x_0 = q u_0^2 \\ x_0 + 1 = p v_0^2 \end{cases}$$

The first system implies $v_0^2 - pq u_0^2 = 1$ which is impossible because the inequality $|u_0| < |x_1|$ contradicts the minimality of x_1 . The second system implies $v_0^2 - pq u_0^2 = -1$, and the third and fourth systems imply $q v_0^2 - p u_0^2 = \pm 1$. If $(p|q) = -1$ the equation $q v_0^2 - p u_0^2 = \pm 1$ is impossible, thus necessarily $x^2 - pqy^2 = -1$ has the solution (v_0, u_0) . If $(p|q) = 1$, one of the two equations $q v_0^2 - p u_0^2 = \pm 1$ may have a solution, in which case we have $q = (q v_0)^2 - p u_0^2$, or $-q = (q v_0)^2 - p q u_0^2$; in any case, $N = pq$ is split by the unit, which means that the period of the continued fraction representing \sqrt{pq} is even and the norm of the fundamental unit is $+1$, thus equation $x^2 - pqy^2 = -1$ is impossible.

□

Corollary 1. *Let p and q be two primes congruent 1 modulo 4, then of the three Diophantine equations*

$$\begin{aligned} X^2 - pqY^2 &= -1 \\ X^2 - pqY^2 &= -p \\ X^2 - pqY^2 &= p \end{aligned} \tag{1}$$

only one is solvable in integers.

Corollary 2. *Let p and q be primes congruent 1 modulo 4, and let \mathbf{u} be a fundamental unit in $\mathbb{Q}(\sqrt{pq})$ assumed to be of norm -1 . Then p and q ramify in $\mathbb{Q}(\sqrt{pq})$ into primes which are non-principal ideals.*

PROOF. Assuming, contrary to the theorem statement, that p ramifies into a principal ideal \mathfrak{p} , we may write $\mathfrak{p}^2 = p\mathfrak{v}$, with \mathfrak{v} a unit. Taking the field norm of both sides we have $(N\mathfrak{p})^2 = NpN\mathfrak{v}$, which implies $N\mathfrak{v} = 1$. It follows that \mathfrak{v} is an even power, say \mathbf{u}^{2k} , of the fundamental unit. From $\mathfrak{p}^2 = p\mathfrak{v}$ we obtain $p = (\sigma(\mathbf{u})^k \mathfrak{p})^2$, which is clearly impossible because \sqrt{p} is not in $\mathbb{Q}(\sqrt{pq})$, thus the Corollary is proved.

□

Corollary 3. *Let p and q be primes congruent 1 modulo 4; if $(p|q) = -1$ then $X^2 - pqY^2 = -1$ is solvable in integers.*

The description of the set of relative densities concerning ramified primes is completed by the following theorem, whose conjectural proof, given here (also supported by extensive numerical computations) is a direct consequence of a conjecture formulated by Stevenhagen [22, p.127].

Theorem 4. *Let p be a prime congruent 1 modulo 4; the set \mathcal{P} of primes q congruent 1 modulo 4 that are quadratic residues modulo p , is partitioned into three subsets \mathcal{P}_1 , \mathcal{P}_2 , and \mathcal{P}_3 of relative density $1/3$, depending on which of the equations (1) is solvable in integers. The set \mathcal{P} of primes congruent 1 modulo 4 is partitioned into two subsets of relative densities $2/3$ and $1/3$, such that p is, or is not, a square of a principal ideal.*

PROOF. Since $pq \equiv 1 \pmod{4}$, p and q are the only primes that ramify in $\mathbb{Q}(\omega)$. If $(p|q) = -1$, then both \mathfrak{p} and \mathfrak{q} are non-principal, and the fundamental unit has norm -1 . If $(p|q) = 1$ and the fundamental unit has norm -1 , necessarily both \mathfrak{p} and \mathfrak{q} are non-principal. If the fundamental unit has norm 1, then \mathfrak{p} and \mathfrak{q} are principal ideals. If it is true (and this is an open problem) that for every pair of primes congruent 1 modulo 4 the fundamental unit norm takes the values $+1$ and -1 with the same frequency, then the conclusion on the density follows directly.

□

3 Comments and Applications

The conclusions of the theorems on densities are summarized in the following table, where d_i denotes the density of the subset $\mathcal{P}_i \subseteq \mathcal{P}$, and specifically \mathcal{P}_1 denotes the set of primes q such that p is a square of a principal ideal, \mathcal{P}_2 denotes the set of primes q such that p is a square of a non-principal ideal, lastly \mathcal{P}_3 and \mathcal{P}_4 have the meanings specified in Theorem 3

p	q	d_1	d_2	d_3	d_4
3 mod 4	3 mod 4	1	0	0	0
1 mod 8	3 mod 4	1/4	1/4	1/4	1/4
5 mod 8	3 mod 4	1/2	1/2	0	0
1 mod 4	1 mod 4	1/3	2/3	0	0

The ramification of primes in $\mathbb{Q}(\sqrt{N})$ has a direct consequence on the factorization of N through the fundamental unit $\mathbf{u} = u_0 + \sqrt{N}u_1$ when its norm is $+1$. We say that \mathbf{u} is split (for N) whenever $u_0 + 1$ and $u_0 - 1$ are divisible by some proper factors m_1 and m_2 of $N = m_1m_2$.

Let $[a_0, \overline{a_1, a_2, \dots, a_2, a_1, 2a_0}]$ be the periodic continued fraction representation of \sqrt{N} , where the overbar denotes the period of length τ :

$$\sqrt{N} = a_0 + \frac{1}{a_1 + \frac{1}{\dots + \frac{1}{2a_0 + \frac{1}{a_1 + \frac{1}{\dots}}}}}$$

Let $\frac{A_j}{B_j}$ be the j -th convergent and set $\Delta_j = A_j^2 - NB_j^2$; the following properties are well known

1. $|\Delta_j| < 2\sqrt{N}$ for every $j > 1$
2. For a given $|a| < \sqrt{N}$, the Diophantine equation $X^2 - NY^2 = a$ is solvable if and only if $a = \Delta_j$ for some j , [10, 18].
3. The sequence $\Delta_j = A_j^2 - NB_j^2$ is periodic with a symmetric part around the term $(\tau - 2)/2$, thus $\Delta_j = \Delta_{\tau-j-2}$.
4. $\Delta_{\tau-1} = (-1)^\tau$, thus $A_{\tau-1} + \sqrt{N}B_{\tau-1}$ is a unit in $\mathbb{Q}(\sqrt{N})$ and the matrix

$$M_{\tau-1} = \begin{bmatrix} A_{\tau-1} & -NB_{\tau-1} \\ B_{\tau-1} & -A_{\tau-1} \end{bmatrix}$$

is involutory, that is $M_{\tau-1}^2 = I$, with eigenvalues 1 and -1 if $\Delta_{\tau-1} = 1$, otherwise $M_{\tau-1}^2 = -I$ and the eigenvalues are i and $-i$.

When $\Delta_{\tau-1} = 1$, let $(A_{\tau-1} + 1, B_{\tau-1})^T/d$ be the eigenvector of $M_{\tau-1}$ corresponding to the eigenvalue 1 , with $d = \gcd\{A_{\tau-1} - 1, B_{\tau-1}\}$. It is immediately seen that the $(\tau/2 - 1)$ -th convergent is $\frac{A_{\tau/2-1}}{B_{\tau/2-1}} = \frac{A_{\tau-1}-1}{B_{\tau-1}}$.

The following can now be proved

Theorem 5. *If the norm of the fundamental unit $\mathbf{u} \in \mathbb{Q}(\sqrt{N})$ is 1 , and some factor of N is a square of a principal integral ideal in $\mathbb{Q}(\sqrt{N})$, then \mathbf{u} is split for N .*

PROOF. If \mathbf{u} is split, then $A_{\tau-1}^2 - NB_{\tau-1}^2 = 1$ implies $m_1\lambda_1 = A_{\tau-1} - 1$ and $m_2\lambda_2 = A_{\tau-1} + 1$. Now we know that

$$A_m^2 - NB_m^2 = 2(-1)^m \frac{A_{\tau-1} + (-1)^{m-1}}{\theta^2} = 2(-1)^m \frac{A_m}{\theta} \tag{2}$$

where $m = \frac{\tau-2}{2}$, and $\theta = \gcd\{A_{\tau-1} + (-1)^{m-1}, B_{\tau-1}\}$. Therefore, either $\theta = A_m$ or $\frac{A_m}{\theta}$ is a proper divisor of N . The assumption that \mathfrak{u} is split implies the second instance, thus either $\frac{A_m}{\theta}$ or $2\frac{A_m}{\theta}$ is a square of a principal ideal.

Conversely, let d be a divisor of N and a square of a principal ideal; it is not restrictive to assume that d is less than \sqrt{N} , thus it occurs in the sequence Δ_n with appropriate sign. It follows that $d = 2\frac{A_m}{\theta} > 1$, thus \mathfrak{u} is split.

□

Corollary 4. *Under the same assumptions as Theorem 5, the smaller of the two factors of $N = pq$ is a factor of $\Delta_{\frac{\tau-2}{2}} = A_{\frac{\tau-2}{2}}^2 - NB_{\frac{\tau-2}{2}}^2$. In particular, if p and q are congruent 3 mod 4, with $p < q$, then $\Delta_{\frac{\tau-2}{2}} = (q|p)p$.*

PROOF. The hypotheses imply that the period τ of the continued fraction representation of \sqrt{N} is even. Moreover, the period τ is equal to $4k$ or to $4k + 2$ if Δ_m is positive or negative, respectively.

As a consequence of Theorem 5, Δ_m is a proper multiple of p or q smaller than $2\sqrt{N}$, therefore the only possibilities are $(-1)^{m-1}p$, $2(-1)^{m-1}p$, and $q(-1)^{m-1}$. The value $q(-1)^{m-1}$ is excluded by Theorem 8.2 in Hua’s book [10, p.263]. Lastly, if p and q are congruent 3 mod 4, Theorem 1 excludes $2(-1)^{m-1}p$.

□

In conclusion, the unit of a quadratic field $\mathbb{Q}(\sqrt{pq})$ splits $N = pq$ if and only if either p , or $2p$, or both are squares of principal ideals. The "splitting" pairs are partitioned in the proportions $1/8$, $1/2$, and $3/8$ depending on whether they are the product of two primes congruent 1, of one prime congruent 1 and one congruent 3, or of two primes congruent 3 modulo 4. The "non-splitting" pairs are equally distributed between products of pairs of primes congruent 1, and products of primes one congruent 3 and the other congruent 1 modulo 4. These observations, which follow from the previous theorems on prime ramification, are summarized in the following table:

		(1)(1)	(1)(3)	(3)(3)
splitting pairs	2/3	1/8	1/2	3/8
non-splitting pairs	1/3	1/2	1/2	0

Systematic computations performed on every pair p and q of primes less than 5,000 have confirmed that about $2/3$ of the fields $\mathbb{Q}(\sqrt{pq})$ have split units, and about $1/3$ of fields do not have split units. These numerical results support Theorem 4, whose proof is based on a conjecture of Stevenhagen’s [22].

References

- [1] **E. Bach and J. Shallit**, *Algorithmic Number Theory*, vol.1, Cambridge: MIT Press, 1996.
- [2] **D.A. Buell**, *Binary Quadratic Forms*, New York: Springer-Verlag, 1989.
- [3] **H. Cohen**, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, New York, 1993.
- [4] **H. Cohn**, *Advanced in Number Theory*, Dover, New York, 1980.
- [5] **D.A. Cox**, *Primes of the form $x^2 + ny^2$* , Wiley, New York, 1989.
- [6] **H. Davenport**, *The Higher Arithmetic*, New York: Dover, 1983.
- [7] **L.E. Dickson**, *Introduction to the Theory of Number*, New York: Dover, 1957.
- [8] **C.F. Gauss**, *Disquisitiones Arithmeticae*, Springer-Verlag, New York, 1986.
- [9] **H. Hasse**, *Number Theory*, New York: Springer, 1980.
- [10] **Hua Loo Keng**, *Introduction to Number Theory*, New York: Springer, 1981.
- [11] **K. Ireland, M. Rosen**, *A Classical Introduction to Modern Number Theory*, New York: Springer, 1998.
- [12] **F. Lemmermeyer**, *Higher descent on Pell conics. I. From Legendre to Selmer*, arXiv, 18 November 2003.
- [13] **F. Lemmermeyer**, *Higher Descent On Pell Conics. II. Two Centuries Of Missed Opportunities*, arXiv, 18 November 2003.
- [14] **F. Lemmermeyer**, *Higher Descent On Pell Conics. III. The First 2-Descent*, arXiv, 18 November 2003.
- [15] **G.B. Mathews**, *Theory of Numbers*, Chelsea, New York, 1892.
- [16] **R.A. Mollin**, *Quadratics*, CRC, New York, 1996.
- [17] **H. Riesel**, *Prime Numbers and Computer Methods for Factorization*, Boston: Birkhäuser, 1984.

- [18] **W. Sierpinski**, *Elementary Theory of Numbers*, North Holland, New York, 1988.
- [19] **R. Schoof**, *Elliptic Curves over Finite Fields and the Representations of Square Roots mod p* , Math. Comp., 44, (1985), p.483-494. p.33-44.
- [20] **D. Shanks**, *Solved and Unsolved Problems in Number Theory*, Chelsea, New York, 1985.
- [21] **J. Steuding**, *Diophantine Analysis*, Chapman & Hall, New York, 2003.
- [22] **P. Stevenhagen**, *The Number of Real Quadratic Fields Having Units of Negative Norm*, Experimental Mathematics, Vol. 2, (1993), p.121-136.
- [23] **L.C. Washington**, *Elliptic Curves, Number Theory, and Cryptography*, New York: Chapman & Hall, 2003.

Received: September 17, 2007