Far East J. Math. Sci. (FJMS) 3(1) (2001), 129-132

ON THE RELATIVE SIZES OF A AND B IN $p = A^2 + B^2$, WHERE p IS A PRIME $\equiv 1$ (MOD 4)

KENNETH S. WILLIAMS

(Received June 30, 2000)

Submitted by K. K. Azad

Abstract

Let p be a prime $\equiv 1 \pmod 4$ such that the norm of the fundamental unit of $\mathbb{Q}(\sqrt{2p})$ is -1. A necessary and sufficient condition is given for A to be larger than B in the representation $p = A^2 + B^2$, $A \equiv 1 \pmod 2$, $B \equiv 0 \pmod 2$, $A > 0$, $B > 0$.

Let p be a prime with $p \equiv 1 \pmod 4$. It is a classical result that there exist unique positive integers A and B such that

$$p = A^2 + B^2, \quad A \equiv 1 \pmod 2, \quad B \equiv 0 \pmod 2. \tag{1}$$

We consider the problem of giving a necessary and sufficient condition for A to be larger than B. By making use of results of Kaplan and Williams [2], we are able to solve this problem when the norm of the fundamental unit $T + U\sqrt{2p}$ (> 1) of the real quadratic field $\mathbb{Q}(\sqrt{2p})$ is -1, so that

$$T^2 - 2pU^2 = -1. \tag{2}$$

2000 Mathematics Subject Classification: 11E25.

Key words and phrases: sums of two squares.

Research supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

By a result of Dirichlet [1], this is always the case when $p \equiv 5 \pmod 8$. From (2), we see that

$$T \equiv U \equiv 1 \pmod 2. \tag{3}$$

We let L denote the length of the period of the continued fraction expansion of $\sqrt{2p}$. By a theorem of Lagrange (see for example [3, Satz 3.18, p. 93]), we have

$$L \equiv 1 \pmod 2 \tag{4}$$

in view of (2). We prove

Theorem. *$A > B$ if and only if $L \equiv T \pmod 4$.*

Proof. In view of (4), by [2, Lemma 2], there exists exactly one pair of positive integers (a, b) with

$$2p = a^2 + b^2, \quad \gcd(a, 2b) = 1, \tag{5}$$

such that the binary quadratic form $ax^2 + 2bxy - ay^2$ lies in the principal class of the group under composition of equivalence classes of primitive integral binary quadratic forms of discriminant $8p$. Then, by [2, Lemma 3, eqns. (2.6), (2.8)] there exist integers k and l such that

$$U = k^2 + l^2 \tag{6}$$

and

$$(-1)^{(L-1)/2}\, a + Tb = 2p(k^2 - l^2). \tag{7}$$

From (3) and (6), we deduce that

$$k \not\equiv l \pmod 2. \tag{8}$$

From (1), we have

$$2p = (A + B)^2 + (A - B)^2. \tag{9}$$

As there are exactly eight representations of $2p$ as a sum of two squares, these representations must be by (9)

$$(\pm(A + B), \pm(A - B)), \quad (\pm(A - B), \pm(A + B)). \tag{10}$$

Hence, from (5) and (10), we have

$$(a, b) = (A + B, |A - B|) \quad \text{or} \quad (|A - B|, A + B),$$

that is

$$(a, b) = \begin{cases} (A + \varepsilon B, A - \varepsilon B), & \text{if } A > B, \\ (\varepsilon A + B, -\varepsilon A + B), & \text{if } A < B, \end{cases} \tag{11}$$

for some $\varepsilon = \pm 1$. Set

$$\begin{cases} \theta = \phi = 1, & \text{if } A > B, \\ \theta = -\phi = \varepsilon, & \text{if } A < B. \end{cases} \tag{12}$$

From (12), we see that

$$\theta\phi = \begin{cases} 1, & \text{if } A > B, \\ -1, & \text{if } A < B. \end{cases} \tag{13}$$

From (11) and (12), we have

$$(a, b) = (\theta(A + \varepsilon B), \phi(A - \varepsilon B)). \tag{14}$$

From (7) and (14), we deduce that

$$(-1)^{(L-1)/2}\theta(A + \varepsilon B) + T\phi(A - \varepsilon B) = 2p(k^2 - l^2). \tag{15}$$

Appealing to (1), (4) and (8), we see that

$$\pm \varepsilon B \equiv B \pmod 4, \quad (-1)^{(L-1)/2} \equiv L \pmod 4, \quad k^2 - l^2 \equiv 1 \pmod 2.$$

Then, taking (15) modulo 4, we obtain

$$(\theta L + \phi T)(A + B) \equiv 2 \pmod 4. \tag{16}$$

Further, as $\theta L + \phi T \equiv 0 \pmod 2$ (by (3), (4) and (12)) and $A + B \equiv 1 \pmod 2$ (by (1)), we deduce from (16) that

$$\theta L + \phi T \equiv 2 \pmod 4. \tag{17}$$

Multiplying (17) by θ, we have

$$L + \theta\phi T \equiv 2\theta \equiv 2 \pmod 4. \tag{18}$$

The assertion of the theorem now follows from (3), (4), (13) and (18).

It seems unlikely that there is such a simple criterion in the case when the norm of $\mathbb{Q}(\sqrt{2p})$ is +1. To see this consider the primes $p = 89$ and $p = 233$. In the former case, we have

$$L = 6 \equiv 6 \pmod{16},\quad T = 1601 \equiv 1 \pmod{64},\quad U = 120 \equiv 56 \pmod{64},$$

and in the latter case, we have

$$L = 22 \equiv 6 \pmod{16},\quad T = 938319425 \equiv 1 \pmod{64},$$

$$U = 43466808 \equiv 56 \pmod{64},$$

so that $L \pmod{16}$, $T \pmod{64}$ and $U \pmod{64}$ are the same for both primes. However, $A < B$ in the first case $(A = 5,\ B = 8)$ whereas $A > B$ in the second case $(A = 13,\ B = 8)$.

References

[1] P. G. L. Dirichlet, Einige neue Sätze über unbestimmte Gleichungen, Abh. König. Preuss. Akad. Wissen. (1834), 649-664. (Werke, Vol. 1, pp 219-236, Chelsea (1969))

[2] P. Kaplan and K. S. Williams, Pell's equations $x^2 - my^2 = -1, -4$ and continued fractions, J. Number Theory 23 (1986), 169-182.

[3] O. Perron, Die Lehre von den Kettenbrüchen, Vol. I, B. G. Teubner, Stuttgart, 1977.

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6
e-mail: williams@math.carleton.ca