

**Math 104B, Number Theory, Winter 2003.**

**Lecture 23. Brahmagupta-Bhaskara equation.**

Last time we showed that if  $d$  is a positive integer which is not a perfect square and if  $p_k/q_k$  is the  $k$ th convergent of the continued fraction expansion of  $\sqrt{d}$  which has smallest period  $m$ , then  $x^2 - dy^2 = 1$  are the numbers  $(x, y) = (p_{jm-1}, q_{jm-1})$  where

$$j = \begin{cases} 1, 2, \dots & m \text{ even,} \\ 2, 4, \dots, & m \text{ odd.} \end{cases}$$

We see that when  $m$  is even or odd, the solutions are  $(p_{jm-1}, q_{jm-1})$  and  $jm - 1$  is odd. Hence  $p_{jm-1}/q_{jm-1}$  is a decreasing sequence as  $j$  increases. The first solution is  $(a, b) = (p_{m-1}, q_{m-1})$  if  $m$  is even and  $(a, b) = (p_{2m-1}, q_{2m-1})$  if  $m$  is odd. It is called the **fundamental solution**.

**Theorem 14.5.8** Once we have found the fundamental solution then all other solutions  $(x, y)$  can be obtained from computing

$$x + y\sqrt{d} = (a + \sqrt{db})^k$$

for  $k = 2, 3, \dots$ . This is quicker than computing more terms in the continued fraction expansion, especially if the period  $m$  is large.

**Units of the ring  $\mathbb{Z}[\sqrt{d}]$ .** The ring  $\mathbb{Z}[\sqrt{d}]$  is the set of numbers of the form  $a + b\sqrt{d}$  where  $a$  and  $b$  are integers, with the operations addition and multiplication. For  $z = a + b\sqrt{d}$ , the conjugate is  $\bar{z} = a - b\sqrt{d}$ . Notice that  $a^2 - b^2d = z\bar{z}$ . We see that  $\overline{(zw)} = \bar{z}\bar{w}$  and  $\overline{(z/w)} = \bar{z}/\bar{w}$ . We also see that if  $w$  is an inverse to  $z = a + b\sqrt{d}$  in  $\mathbb{Z}[\sqrt{d}]$ , then  $w = \pm\bar{z}$  and so  $a^2 - b^2d = \pm 1$ .

(To see this, notice that if  $w = e + f\sqrt{d}$  then  $(a + b\sqrt{d})(e + f\sqrt{d}) = 1$  so  $ae + bfd = 1$  and  $af + be = 0$ . Hence we see that  $(ae, bfd) = 1$  which implies  $(a, b) = 1$  and  $(e, f) = 1$ . But then from  $af + be = 0$  we get  $e = \pm a$  and  $f = \mp b$ .)

We gave the proof of Theorem 14.5.8 from the book.

We see that the equation  $x^2 - y^2d = -1$  is also interesting because solutions give units  $x + d\sqrt{y}$  in  $\mathbb{Z}[\sqrt{d}]$ . We find that if  $(x, y)$  is a solution of this equation and  $x > 0, y > 0$ , then  $x/y$  is a best approximation to  $\sqrt{d}$  and hence is a convergent of the continued fraction expansion of  $\sqrt{d}$ . Now recalling that

$$p_k^2 - q_k^2d = (-1)^{k+1}B_{k+1},$$

we see that this can equal  $-1$  if and only if the period  $m$  of the continued fraction expansion of  $\sqrt{d}$  is odd. It is not hard to show that in this case the solutions are

$k = mj - 1$  where  $j$  is odd. The first solution is  $(p_{m-1}, q_{m-1})$  and it is not hard to show that all the solutions  $(x, y)$  solving  $x^2 - y^2d = \pm 1$  with  $x, y > 0$  are given by

$$x + y\sqrt{d} = (p + q\sqrt{d})^k$$

for  $k = 1, 2, \dots$ . In general it is not possible to characterize the numbers  $d$  such that the period  $m$  of the continued fraction expansion of  $\sqrt{d}$  is odd, but we have the following results.

**Example 14.2.3.** The equation  $x^2 - y^2d = -1$  has no solutions if  $d \equiv 3 \pmod{4}$ .

We gave the simple proof in the book.

**Proposition 14.5.11** (Lagrange). If  $p$  is a prime such that  $p \equiv 1 \pmod{4}$  then the equation  $x^2 - py^2 = -1$  has a solution.