PACIFIC JOURNAL OF MATHEMATICS
Vol. 119, No. 2, 1985

THE DIOPHANTINE EQUATION $ax + by = c$ IN $Q(\sqrt{5})$ AND OTHER NUMBER FIELDS

DAVID ROSEN

Solving in rational integers the linear diophantine equation

(1) $$ax + by = c, \qquad (a, b)|c, a, b, c, \in Z$$

is very well known. Let $d = (a, b)$, and put $A = a/d, B = b/d, C = c/d$, then equation (1) becomes

(1′) $$Ax + By + C, \qquad (A, B) = 1, A, B, C, \in Z.$$

The purpose of this note is to discuss the solutions of this equation when A, B, C are integers in $Q(\sqrt{5})$ and the solutions are integers in $Q(\sqrt{5})$. What makes the discussion interesting is that an algorithm which mimics the continued fraction algorithm that solves the rational integer case can be implemented.

A brief summary of the continued fraction algorithm for the rational case is as follows: To solve (1′): find the regular simple continued fraction for A/B; i.e.

$$\frac{A}{B} = r_0 + \cfrac{1}{r_1 + \ddots + \cfrac{1}{r_n}}$$

which we write as $A/B = (r_0; r_1, \ldots, r_n)$. Since A/B is rational, the continued fraction is finite. The $(m + 1)$th convergent of a continued fraction is denoted by $P_m/Q_m = (r_0; r_1 \cdots r_m)$. If $A/B = P_n/Q_n$ then the penultimate convergent P_{n-1}/Q_{n-1} provides a solution to $Ax + By = 1$ because of the well-known relation.

(2) $$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n+1}.$$

It suffices therefore to take $x = (-1)^{n+1}Q_{n-1}$, $y = (-1)^nP_{n-1}$. To solve (1) we take $x = (-1)^{n+1}dCQ_{n-1}$ and $y = (-1)^{n+1}dCP_{n-1}$.

It is well known that the integers in $Q(\sqrt{5})$ have the form $s + t\lambda$, where $s, t \in Z$ and $\lambda = (1 + \sqrt{5})/2$. (See Hardy and Wright [1] or Niven and Zuckerman [3] for a complete discussion of this algebraic number field.) The elements in $Q(\sqrt{5})$ are of course the quotients of integers in the

field. In order to mimic the solution procedure above we would require a continued fraction development that essentially parallels the ordinary continued fraction representation of real numbers, that is the elements of $Q(\sqrt{5})$ should have a unique finite continued fraction representation and every other real number has a unique infinite continued fraction representation. Such a representation exists and the continued fractions will be referred to as λ_5-fractions [4].

These continued fractions were presented by the author in connection with studies on the Hecke groups [4], and are one example of the more general λ_q-fractions where $\lambda = 2\cos(\pi/q)$. It was shown in [4], that every finite λ_q-fraction is an element in the algebraic number field $Q(\lambda_q)$, and Leutbecher [2] showed that only in the case $q = 5$, every element in $Q(\sqrt{5}) = Q(\lambda_5)$ has a finite λ_5-fraction. Hence a real number is an element of $Q(\sqrt{5})$ if and only if it has a finite λ_5-continued fraction representation and every real number has a unique λ_5-fraction representation. Thus we will show that the algorithm that solves the rational integer case (which is the case $q = 3$) will work in the $Q(\sqrt{5})$ case.

What are the λ_q-fractions? These are continued fractions of the form

$$r_0\lambda + \cfrac{\varepsilon_1}{r_1\lambda + \cfrac{\varepsilon_2}{r_2\lambda + \ddots}}$$

where, in general, for fixed q, $\lambda = 2\cos(\pi/q)$, $q \in Z^+$ and $q \geq 3$, $\varepsilon_i = \pm 1$, and $r_i \in Z^+$, $i \geq 1$, $r_0 \in Z$. The continued fraction is developed by a nearest integer algorithm. If ξ is a real number we seek the nearest integral multiple of λ. This means, if $\{\ \}$ denotes the nearest integer, then we write $\{\xi/\lambda\} = r_0$, where we specify $-1/2 \leq r_0 - \xi/\lambda < 1/2$; i.e. r_0 is uniquely determined by the inequality.

$$r_0\lambda - \frac{\lambda}{2} < \xi \leq r_0\lambda + \frac{\lambda}{2}. \tag{3}$$

Hence $\xi = r_0\lambda + \varepsilon_1/\xi_1$, where it is seen that $\xi_1 = \varepsilon_1/(\xi - r_0\lambda) > 0$, since $\varepsilon_1 > 0$ if $r_0\lambda < \xi$ and $\varepsilon_1 < 0$ if $r_0\lambda > \xi$. If $\xi = n\lambda + \lambda/2 = (n+1)\lambda - \lambda/2$, then because of inequality (3) $r_0 = n$ and $\varepsilon_1 = 1$. Then $r_0\lambda - \lambda/2 < \xi \leq r_0\lambda + \lambda/2$ implies $\xi_1 \geq 2/\lambda > 1 > \lambda/2$ and hence $r_1 = \{\xi_1/\lambda\} \geq 1$. Continuing in this way we find that $\xi_m > \lambda/2$ which implies that $r_m \geq 1$ $(m \geq 1)$. Henceforth, λ-fraction will refer to λ_5-fraction. The λ-fraction is unique provided that the following few simple rules indicated in [4] are obeyed.

(i) If $\lambda - 1/r\lambda$ occurs, then $r \geq 2$.

(ii) If

$$\cfrac{\varepsilon_1}{\lambda - \cfrac{1}{\cfrac{}{2\lambda - \cfrac{1}{\cfrac{}{\lambda + \cfrac{\varepsilon_2}{\ddots}}}}}}$$

occurs, then $\varepsilon_1 = \varepsilon_2 = 1$.

We point out that in $Q(\sqrt{5})$,

$$\lambda - \cfrac{1}{2\lambda - \cfrac{1}{\lambda}} = \frac{2}{\lambda}.$$

(iii) If the λ-fraction terminates as

$$\cfrac{\varepsilon}{\lambda - \cfrac{1}{\lambda}},$$

then $\varepsilon = 1$. In $Q(\sqrt{5})$, $\lambda - 1/\lambda = 1$, which yields the equation

$$\lambda^2 - \lambda - 1 = 0. \tag{4}$$

A λ-fraction satisfying these criteria is called a *reduced* λ-fraction. Similar criteria will yield unique λ_q-fractions. Because of (4) the rolled up finite continued fraction produces the quotient of two polynomials in λ which can be reduced to the form

$$(a + b\lambda)/(c + d\lambda), \qquad a, b, c, d \in Z. \tag{5}$$

This in turn can be put in the form

$$(a' + b'\lambda)/c' \tag{6}$$

by multiplying numerator and denominator by the conjugate of $c + d\lambda$, which is $(c + d) - d\lambda$. One finds that $a' = ac + ad - bc$, $b' = bc - ad$, $c' = c^2 + cd - d^2$—the norm of $c + d\lambda$.

As observed on p. 550 of [4] consecutive convergents P_{n-1}/Q_{n-1} and P_n/Q_n of a λ-fraction satisfy a determinant relation similar to (2):

$$P_nQ_{n-1} - P_nQ_n = (-1)^{n-1}\varepsilon_1\varepsilon_2 \cdots \varepsilon_n = 1. \tag{7}$$

Finally we remark that the units in $Q(\sqrt{5})$ are λ^n which can be written in terms of consecutive Fibonnaci numbers. If F_n is the nth Fibonnaci

number, then $\lambda^n = F_{n-1} + F_n\lambda$. This can be proved as follows:

Let $F_0 = 0$, $F_1 = 1$, $F_2 = 1$ then $\lambda^1 = 0 + \lambda$, $\lambda^2 = F_1 + F_2\lambda = \lambda + 1$, which is a consequence of (4). By induction then if $\lambda^k = F_{k-1} + F_k\lambda$, then

$$\lambda^{k+1} = F_{k-1}\lambda + F_k\lambda^2 = F_k + (F_{k-1} + F_k)\lambda = F_k + F_{k+1}\lambda,$$

as desired. If $n < 0$ one determines first from (4) that $1/\lambda = \lambda - 1$; hence $\lambda^{-2} = (\lambda - 1)^2 = 2 - \lambda$. By induction, one determines that $\lambda^{-n} = -F_{n+1} + F_n\lambda$ if n is odd and $\lambda^{-n} = F_{n+1} - F_n\lambda$ if n is even. To show that λ^n is a unit, we observe that the norm of $F_k + F_{k+1}\lambda$ is $F_k^2 + F_kF_{k+1} - F_{k+1}^2$. But the last expression is precisely the determinant relation (2) for the consecutive convergents. F_k/F_{k+1}, F_{k+1}/F_{k+2} of the regular continued fraction $(1; 1, 1 \cdots) = \lambda$. Thus each λ^n, $n > 0$, is indeed a unit. For n negative $= -m$, the norm $N(1/\lambda^m) = 1/N(\lambda^m) = \pm 1$ too, so λ^n is a unit for all integers n. We now state and prove the main theorem.

THEOREM 1. *Let $p, q, r \in Z(\sqrt{5})$, and suppose that, except for units, p, q, r are relatively prime. Then the diophantine equation $px + qy = r$ has integer solutions in $Q(\sqrt{5})$. If x_0, y_0 is a particular solution, then any other solution has the form $x = x_0 + qt, y = y_0 - pt$. If $(p, q) = d$ and $d|r$, then*

$$\frac{p}{d}x + \frac{q}{d}y = \frac{r}{d}$$

is solvable in $Q(\sqrt{5})$.

Proof. As in the rational integer case, we first solve $px + qy = 1$. This is done by expanding p/q in its unique λ-fraction. The penultimate convergent will supply the values for x and y. To sove $px + qy = r$ multiply the x and y values by r.

As in the rational case we note that if a particular solution is x_0, y_0 then an infinity of solutions is obtained using the usual trick namely putting $x = x_0 + qt$, $y = y_0 - pt$, which satisfies the equation for all $t \in Z(\lambda)$. Moreover if a and b is any solution $\in Z(\sqrt{5})$, i.e., $pa + qb = r$ then $a = x_0 + qt$, $b = y_0 - pt$, for some t. This is clear because from $pa + qb = r$ and $px_0 + qy_0 = r$ we obtain $p(x_0 - a) + q(y_0 - b) = 0$. Hence $p(x - a) = -q(y_0 - b)$. Since $(p, q) = 1$, it follows that $p|(y_0 - b)$. Thus $pl = y_0 - b$. But now $p(x - a) = -qpl$, hence $x - a = -ql$. This result has a bearing on the Hecke group $\Gamma(\lambda)$ in determining which solutions to $px + qy = 1$ provide a substitution that belongs to $\Gamma(\lambda)$.

Finally, the last statement of the theorem follows easily from the first statement since $p/d, q/d, r/d$ are relatively prime.

There is one wrinkle in this method which does not arise in the rational case. The λ-fraction when rolled up and reduced to the form (5) may not be identical with the original fraction unless a suitable unit is factored out from numerator and denominator.

Consider the following example: Solve

$$(3 + 7\lambda)x + (5 - 2\lambda)y = 6 + 5\lambda. \tag{8}$$

One can verify that

$$\frac{3 + 7\lambda}{5 - 2\lambda} = 5\lambda + \cfrac{1}{20\lambda - \cfrac{1}{\lambda - \cfrac{1}{3\lambda}}}.$$

The right side, when rolled up and reduced using (4), becomes

$$\frac{487 + 788\lambda}{97\lambda + 60}.$$

The numerator is $(34 + 55\lambda)(3 + 7\lambda)$ and the denominator is

$$(34 + 55\lambda)(5 - 2\lambda), (55\lambda + 34 = \lambda^{10}).$$

The penultimate convergent is

$$5\lambda + \cfrac{1}{20\lambda - \cfrac{1}{\lambda}} = \frac{196\lambda + 100}{20\lambda + 19}.$$

Hence $x = (20\lambda + 19)$ and $y = -(196\lambda + 100)$ solves $(487 + 788\lambda)x + (97\lambda + 60)y = 1$. It follows that $x' = (20\lambda + 19)(5\lambda + 6) = 214 + 315\lambda$ and $y' = -(196\lambda + 100)(5\lambda + 6) = -(2656\lambda + 1580)$ solves $(487 + 788\lambda)x' + (97\lambda + 60)y' = 6 + 5\lambda$. Thus to solve (8) we incorporate the common unit factor $(34 + 55\lambda)$ with x' and y'. Then $(3 + 7\lambda)x'' + (5 - 2\lambda)y'' = 6 + 5\lambda$ has as solution

$$\begin{aligned} x'' &= (214 + 315\lambda)(34 + 55\lambda) = 24601 + 39805\lambda \\ y'' &= -(1580 + 2656\lambda)(34 + 55\lambda) = -(199800 + 3223284\lambda). \end{aligned} \tag{9}$$

Knowing one solution thus gives all solutions; $x = x'' + qt$, $y = y'' - pt$ where $t \in Z(\sqrt{5})$ and we assume that $(p, q) = 1$.

It is interesting to observe here that solving one diophantine equation automatically solves a class of equations. Recalling that the units λ^n can be written as integers in $Z(\sqrt{5})$ and noting that

$$\lambda^n (= F_{n-1} + F_n\lambda) \text{ times } \lambda^{-n} (= F_{n+1} - F_n\lambda \text{ or } -F_{n+1} + F_n\lambda) = 1$$

then a solution to $px + qy = n$ provides a solution to $(F_{n-1} + F_n\lambda)px' + (F_{n-1} + F_n\lambda)qy' = n$. Clearly, the solution is $x' = (F_{n+1} - F_n\lambda)x$, $y' = (F_{n+1} - F_n\lambda)y$ or $x' = (-F_{n+1} + F_n\lambda)x$, $y' = (-F_{n+1} + F_n\lambda)y$, depending on the parity of n. As an example, the equation

$$(7 + 10\lambda)x' + (-2 + 3\lambda)y' = 6 + 5\lambda,$$

which is

$$\lambda(3 + 7\lambda)x + \lambda(5 - 2\lambda)y = 6 + 5\lambda,$$

is solved by $x' = 15204 + 24601\lambda$, $y' = -(123484 + 199800\lambda)$. This solution is obtained from (9) by dividing x'' and y'' by λ, i.e., multiplying by $\lambda - 1$.

The above procedures could be extended to other number fields if a suitable continued fraction representation were available. A continued fraction representation for the number fields $Q(2\cos(\pi/q))$ similar to the foregoing was developed in [**4**], but as Wolfart showed [**5**] the only possible q's for which all the rational elements in $Q(\lambda_q)$ have a finite λ_q-fraction are $q = 3, 5, 9$. It appears therefore that it is true only for the fields $q = 3$ and $q = 5$; while for $q = 9$ the questions is still open. For other values of q, equation (1) can be solved in $Z(\lambda_q)$ provided a/b has a finite λ_q-fraction. The formal statement is:

THEOREM 2. *If* $\lambda_q = 2\cos(\pi/q)$, *q an integer* ≥ 4, *then if* $a, b \in Z(\lambda_q)$, *then the diophantine equation* $az + by = 1$ *has solutions in* $Z(\lambda_q)$ *if and only if* $(a, b) = d$ *and* $d|c$, *d is not a unit*; *and if* a/b *has a finite* λ_q*-fraction representation.*

For $q = 4$, $\lambda_4 = \sqrt{2}$, and for $q = 6$, $\lambda_6 = \sqrt{3}$. The finite λ_4- and λ_6-fractions when rolled up have the form $a\sqrt{r}/b$ or $a/b\sqrt{r}$, $r = 2, 3$. Thus not all elements of $Q(\sqrt{r})$ are realizable as finite λ_4 or λ_6 continued fractions. However, consider

$$7x + 3\sqrt{2}y = 4 + 9\sqrt{2}.$$

We find the λ_4 continued fraction for $7/3\sqrt{2}$ which turns out to be $7/3\sqrt{2} = \sqrt{2} + 1/3\sqrt{2}$. Clearly

$$\frac{p_2}{q_2} = \frac{7}{3\sqrt{2}}, \quad \frac{p_1}{q_1} = \frac{\sqrt{2}}{1},$$

and $7 \cdot 1 - \sqrt{2} \cdot 3\sqrt{2} = 1$ so $x = 1$ and $y = -\sqrt{2}$ solves $7x + 3\sqrt{2}y = 1$.

Hence $x' = 4 + 9\sqrt{2}$, $y' = -\sqrt{2}(4 + 9\sqrt{2}) = -(18 + 4\sqrt{2})$ solves the original equation and of course there are an infinite of solutions of the

form $x'' = 4 + 9\sqrt{2} + (18 + 4\sqrt{2})t$, $y'' = -(18 + 4\sqrt{2}) + (4 + 9\sqrt{2})t$, $t \in Z(\lambda_4)$.

This same procedure will work for any of the algebraic fields $(2\cos(\pi/q))$. Examples can be easily found by first taking a finite λ_q-fraction and using the numerator and denominator for the coefficients. For example in λ_7, compute

$$2\lambda + \cfrac{1}{\lambda - \cfrac{1}{3\lambda}} = 2\lambda + \frac{3\lambda}{3\lambda^2 - 1} = \frac{6\lambda^3 + \lambda}{3\lambda^2 - 1}.$$

In λ_7,

$$\lambda - \cfrac{1}{\lambda - \cfrac{1}{\lambda}} = 1$$

so the rational elements will be of the form

$$\frac{a\lambda^2 + b\lambda + c}{d\lambda^2 + e\lambda + f}.$$

The equation $(6\lambda^3 + \lambda)x + (3\lambda^2 - 1)y = 1$ is solved by $x = 2\lambda$, $y = -(2\lambda^2 + 1)$, since

$$(6\lambda^3 + \lambda)2\lambda + (3\lambda^3 - 1) - (2\lambda^2 + 1) = 6\lambda^4 + \lambda^2 - (6\lambda^4 + \lambda^2 - 1) = 1.$$

We remark that there are other ways of solving the linear diophantine equation in $Q(\sqrt{5})$, but the algorithm presented above bears such a striking similarity to the usual algorithm for the rational case that it gives $Q(\sqrt{5})$ a special status. The author knows of no other algebraic field in which a continued fraction can be similarly developed.

It seems that Pell's equation $(x^2 - dy^2 = 1)$ should also be solvable in $Q(\sqrt{5})$ but there are still some difficulties in showing that $\sqrt{d}$ is a periodic λ_5-function. However, if $\sqrt{d}$ is periodic then Pell's equations can be solved as in the rational case

REFERENCES

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford: Clarendon Press, 4th edition, 1960.

[2] A. Leutbecher, *Über die Heckeschen Gruppen* $G(\lambda)$, Abh. Math. Sem., Hamburg, **31** (1967), 199–205.

[3] I. Niven and H. S. Zuckerman, *Introduction to the Theory of Numbers*, John Wiley and Sons, Inc., 2nd edition, 1966.

[4] D. Rosen, *A Class of Continued Fractions Associated with Certain Properly Discontinuous Groups*, Duke Math., **21** (1954), 549–563.
[5] J. Wolfart, *Eine Bemerkung über Heckes Modulgruppen*, Arch. der Math., **29** #1 (1977), 72–77.

Received August 4, 1983 and in revised form July 16, 1984.

SWARTHMORE COLLEGE
SWARTHMORE, PA 19081