COLLOQUIUM MATHEMATICUM

VOL. 107 2007 NO. 1

ON THE DIOPHANTINE EQUATION $f(x)f(y) = f(z)^2$

BY

MACIEJ ULAS (Kraków)

Abstract. Let $f \in \mathbb{Q}[X]$ and $\deg f \le 3$. We prove that if $\deg f = 2$, then the diophantine equation $f(x)f(y) = f(z)^2$ has infinitely many nontrivial solutions in $\mathbb{Q}(t)$. In the case when $\deg f = 3$ and $f(X) = X(X^2 + aX + b)$ we show that for all but finitely many $a, b \in \mathbb{Z}$ satisfying $ab \ne 0$ and additionally, if $p \mid a$, then $p^2 \nmid b$, the equation $f(x)f(y) = f(z)^2$ has infinitely many nontrivial solutions in rationals.

1. Introduction. Let $f \in \mathbb{Q}[X]$, $\deg f \le 3$ and consider the diophantine equation

$$f(x)f(y) = f(z)^2. \tag{1.1}$$

We say that a triple of rationals x, y, z satisfying (1.1) is a *nontrivial solution* if $f(x) \ne f(y)$. Throughout, by a solution we mean a nontrivial one. It is easy to observe that solving (1.1) in rationals is equivalent to finding rationals x, y, z such that $f(x), f(z), f(y)$ form a geometric progression.

The equation (1.1) for $f(X) = X^2 - 1$ was examined in [2], where it was proved that it has infinitely many solutions in integers. Similar results were obtained for polynomials of the form $f(X) = X^2 - a^2$ in [5], and of the form $f(X) = X^2 - a^2 + 2b^2$ in [6], where $a, b \in \mathbb{Z}$. In the above cases, by substituting $z = (x - y)/2$ the problem was reduced to the examination of Pell's type equations. This method cannot be used for an arbitrary polynomial of degree two, and it is natural to consider whether weakening the assumption about the solvability of (1.1) in integers will enable us to obtain new results in this case, as well as in the case when $\deg f > 2$.

It turns out that in the case when $\deg f = 2$, studying solvability of (1.1) in rationals can be reduced to the examination of a certain elliptic curve defined over the field $\mathbb{Q}(t)$. By means of this reduction we will prove that (1.1) has infinitely many solutions in $\mathbb{Q}(t)$ (Theorem 2.1, Corollary 2.2).

2000 *Mathematics Subject Classification*: Primary 11D25, 11D41; Secondary 11G99.

Key words and phrases: diophantine equations, elliptic curves, geometric progression.

The author is a participant of a project which is co-financed from the European Social Fund and Polish national budget within the Integrated Regional Operational Programme.

In the case when $\deg f = 3$ and $f(X) = X(X^2 + aX + b)$, we will show that for all but finitely many $a, b \in \mathbb{Z}$ satisfying $ab \neq 0$, and additionally, if $p \mid a$, then $p^2 \nmid b$, the equation (1.1) has infinitely many solutions in rationals (Theorem 3.1, Corollary 3.2). As in the case of a polynomial of degree two, the problem is reduced to the examination of a suitable elliptic curve over $\mathbb{Q}(t)$.

2. The equation $f(x)f(y) = f(z)^2$ for $f(X) = X^2 + k$. In this section we prove the following

THEOREM 2.1. *Let $k \in \mathbb{Z}$ and $f(X) = X^2 + k$. Then the equation $f(x)f(y) = f(z)^2$ has infinitely many solutions in the field $\mathbb{Q}(t)$ of rational functions.*

Proof. If $k = 0$ there is nothing to prove, so assume that $k \in \mathbb{Z} \setminus \{0\}$. Let t be a variable and put

$$x = T + t, \qquad y = u^2T + t, \qquad z = uT - t. \tag{2.1}$$

Then

$$f(x)f(y) - f(z)^2 = (u+1)^2 T F_u(T),$$

where $F_u(T) = 2tu^2T^2 + (u-1)^2(t^2+k)T + 2t(t^2+k)$.

It is enough to show that the set of $u \in \mathbb{Q}(t)$ for which the equation $F_u(T) = 0$ has roots in $\mathbb{Q}(t)$ is infinite. Equivalently, the discriminant $\Delta(u) = (t^2+k)^2(u-1)^4 - 16t^2(t^2+k)u^2$ of the polynomial F_u should be a square in the field $\mathbb{Q}(t)$. For $k \in \mathbb{Z} \setminus \{0\}$ consider the curve

$$C_k : v^2 = (t^2+k)^2(u-1)^4 - 16t^2(t^2+k)u^2 \tag{2.2}$$

over $\mathbb{Q}(t)$. The discriminant of Δ equals $D = -2^{20}kt^6(t^2+k)^8$ and $D \neq 0$ for $k \in \mathbb{Z} \setminus \{0\}$. This means that the curve C_k is smooth. Also note that the $\mathbb{Q}(t)$-rational point $Q = (0, t^2+k)$ lies on C_k. If we treat Q as a point at infinity on C_k and use the method described in [1, p. 77], we conclude that C_k is birationally equivalent by means of the mapping

$$u = \frac{Y + 108t^2(t^2+k)^2}{(t^2+k)(3X - 72t^2(t^2+k))} + 1,$$

$$v = -(t^2+k)(u-1)^2 + \frac{2X + 24t^2(t^2+k)}{9(t^2+k)}$$

to the elliptic curve with the Weierstrass equation

$$E_k : Y^2 = X^3 - 108t^2(t^2-3k)(t^2+k)^2X + 432t^4(t^2+9k)(t^2+k)^3.$$

We will prove that there are infinitely many $\mathbb{Q}(t)$-rational points on E_k. First recall that on the elliptic curve over $\mathbb{Q}(t)$ with the equation $y^2 = x^3 + a(t)x + b(t)$, where $a, b \in \mathbb{Z}[t]$, points of finite order have coordinates in $\mathbb{Z}[t]$. It is, therefore, enough to find a point lying on E_k with coordinates not in $\mathbb{Z}[t]$. It is easy to notice that there is a point on E_k of the form

$$P = (24t^2(t^2+k), 108t^2(t^2+k)^2).$$

Using the rule of addition on E_k, we obtain the point

$$2P = \left(\frac{3}{4}(t^2-3k)(11t^2-k), \frac{27}{8}(3t^2-k)(t^4+18kt^2+k^2)\right),$$

and the point $3P = (p(t), q(t))$, where

$$p(t) = \frac{24t^2(t^2+k)(13t^8-364kt^6+14k^2t^4+148k^3t^2+13k^4)}{(7t^4+22kt^2-k^2)^2},$$

$$q(t) = \frac{108(t^2-3k)(t^3+kt)^2(5t^2+k)(t^8+612kt^6-58k^2t^4+100k^3t^2+k^4)}{(7t^4+22kt^2-k^2)^3}.$$

It is enough to show that for $k \in \mathbb{Z}\setminus\{0\}$ the rational function $p(t)$ is not a polynomial. To see this, note that the remainder of division of the numerator of p by $7t^4+22kt^2-k^2$ equals $R = -2359296k^5(4727t^2-212k)/16807$ and $R \neq 0$ for $k \in \mathbb{Z}\setminus\{0\}$. Hence, the X-coordinate of the point $3P$ is not a polynomial. Therefore, P is not of finite order on E_k; hence, infinitely many $\mathbb{Q}(t)$-rational points lie on our curve.

Now it is an easy task to obtain the statement of our theorem. For $m = 2, 3, 4, \ldots$ we calculate mP on the curve E_k; next, we calculate the corresponding point (u, v) on C_k and we solve the equation $F_u(T) = 0$. We put the calculated roots into (2.1) and obtain various rational function solutions of our equation. As an example, consider the point $2P$. The corresponding point on C_k is

$$(u, v) = \left(-\frac{2(t^2+k)}{3t^2-k}, \frac{(t^2+k)(7t^4+22kt^2-k^2)}{(3t^2-k)^2}\right).$$

The substitution $u = -2(t^2+k)/(3t^2-k)$ to the equation $F_u(T) = 0$ gives

$$T_1 = -2t, \quad T_2 = -\frac{(3t^2-k)^2}{8t(t^2+k)}.$$

After substitution into (2.1), we obtain the solutions of our equation $f(x)f(y) = f(z)^2$ corresponding to T_1 and T_2:

$$x = -t, \quad y = \frac{t(t^4-22kt^2-7k^2)}{(3t^2-k)^2}, \quad z = \frac{t(t^2+5k)}{3t^2-k},$$

$$x = -\frac{t^4-14kt^2+k^2}{8t(t^2+k)}, \quad y = \frac{t^2-k}{2t}, \quad z = -\frac{t^2+k}{4t}. \blacksquare$$

The above theorem implies

COROLLARY 2.2. *For each* $f \in \mathbb{Q}[X]$ *with* $\deg f = 2$, *the equation* $f(x)f(y) = f(z)^2$ *has infinitely many solutions in the field* $\mathbb{Q}(t)$ *of rational functions.*

3. The equation $f(x)f(y) = f(z)^2$ for $f(X) = X(X^2+X+t)$. In this section we will prove the following

THEOREM 3.1. *Let* $t \in \mathbb{Q}$ *and* $f(X) = X(X^2+X+t)$. *Then, for all but finitely many* t, *the equation* $f(x)f(y) = f(z)^2$ *has infinitely many solutions in rationals.*

Proof. Let $f(X) = X(X^2+X+t)$, where $t \neq 0, 1/4$. Now we define

$$x = T, \quad y = u^2T, \quad z = uT. \tag{3.1}$$

Then

$$f(x)f(y) - f(z)^2 = (u-1)^2u^2T^3G_u(T),$$

where $G_u(T) = u^2T^2 + t(u+1)^2T + t$. As in the proof of Theorem 2.1, it is sufficient to show that for infinitely many $u \in \mathbb{Q}(t)$, the equation $G_u(T) = 0$ has roots in $\mathbb{Q}(t)$. This is the case when the discriminant $\Delta(u) = t^2(u+1)^4 - 4tu^2$ of the polynomial G_u is a square in the field $\mathbb{Q}(t)$. Therefore, consider the curve

$$C:\ v^2 = t^2(u+1)^4 - 4tu^2 \tag{3.2}$$

over the field $\mathbb{Q}(t)$. The discriminant of the polynomial Δ equals $D = -2^{12}t^8(4t-1)$ and $D \neq 0$ in $\mathbb{Q}(t)$. This means that the curve C is smooth. Also note that the $\mathbb{Q}(t)$-rational point $Q = (0, t)$ lies on C. If we treat Q as a point at infinity on C and once again use the method from [1], we find that C is birationally equivalent by means of the mapping

$$u = \frac{Y - 27t^2}{3t(X-6t)} - 1, \quad v = -t(u+1)^2 + \frac{2(X+3t)}{9t}$$

to the elliptic curve with the Weierstrass equation

$$E:\ Y^2 = X^3 + 27t^2(3t-1)X + 27t^3(9t-2).$$

Note that the point $P = (6t, -27t^2)$ lies on E. Now, if we specialize to $t = 2$, we obtain the elliptic curve

$$E_2:\ Y^2 = X^3 + 540X + 3456$$

with the point $P_2 = (12, -108)$. Points of finite order on the elliptic curve $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, have integer coordinates ([3, p. 177]), while $2P_2 = (-15/4, 297/8)$; therefore, P_2 is not of finite order on E_2, which means that P is not of finite order on E. Therefore, E is a curve of positive rank. Hence, its set of $\mathbb{Q}(t)$-rational points is infinite.

To obtain the statement of our theorem, we have to use Silverman's theorem ([3, p. 368]), which states that if E is an elliptic curve over $\mathbb{Q}(t)$

with positive rank, then for all but finitely many $t_0 \in \mathbb{Q}$, the curve E_{t_0} obtained from E by the specialization $t = t_0$ has positive rank. From this result we see that for all but finitely many $t \in \mathbb{Q}$ our initial problem has infinitely many solutions in rationals. ∎

From the above theorem we obtain two interesting corollaries.

Corollary 3.2. *Put $f(X) = X(X^2+aX+b)$. Then, for all but finitely many $a, b \in \mathbb{Z}$ satisfying $ab \neq 0$ and if $p \mid a$, then $p^2 \nmid b$, the equation $f(x)f(y) = f(z)^2$ has infinitely many solutions in rationals.*

Proof. Let $F(X) = a^3X(X^2 + X + t)$, where $t = b/a^2$. Then $f(X) = F(X/a)$ and it suffices to show the statement for the polynomial F. From Theorem 3.1, the diophantine equation $F(x)F(y) = F(z)^2$ has infinitely many solutions in rationals for all but finitely many rational numbers t.

Let now $t_0 = p/q$ be a rational number for which the curve E_{t_0} from the proof of Theorem 3.1 has rank zero. Are there only finitely many a, b such that $b/a^2 = p/q$? Since $(p, q) = 1$, we then have $p \mid b$, $b = pb_1$ and $a^2 = qb_1$. For a fixed q, there are only finitely many a, b_1 satisfying this equation and the condition that if $s \mid a$, then $s^2 \nmid b$. Because there are only finitely many possibilities for t_0, there are only finitely many corresponding numbers a, b. ∎

Remark 3.3. The condition that $p \mid a$ implies $p^2 \nmid b$, which appears in the formulation of Corollary 3.2, is not very restrictive. Indeed, let $f(X) = X(X^2 + aX + b)$ and suppose $a, b \in \mathbb{Z}$ do not satisfy this condition. Then there exist integers r, a', b' such that $a = ra'$, $b = r^2b'$ and if $p \mid a'$, then $p^2 \nmid b'$. It follows that for all but finitely many a', b' the equation $h(x)h(y) = h(z)^2$, where $h(X) = X(X^2 + a'X + b')$, has infinitely many solutions in rationals, say (x_i, y_i, z_i) for $i = 1, 2, \ldots$. Then the triples $(x_i/r, y_i/r, z_i/r)$ for $i = 1, 2, \ldots$ solve $f(x)f(y) = f(z)^2$.

Corollary 3.4. *If $N \in \mathbb{N}_+$, then there are infinitely many polynomials $f \in \mathbb{Q}[X]$ of degree three without multiple roots such that the equation $f(x)f(y) = f(z)^2$ has at least N solutions in integers.*

Proof. Let $f(X) = X(X^2+X+t)$ and $t = p/q$ be such that the equation $f(x)f(y) = f(z)^2$ has infinitely many solutions in rationals. From the previous theorem we know that all but finitely many $t \in \mathbb{Q}$ satisfy this condition. Take N distinct rational solutions of our equation, say $(p_i/q_i, p'_i/q'_i, p''_i/q''_i)$ for $i = 1, \ldots, N$, and let

$$d = \mathrm{LCM}(q, q_1, q'_1, q''_1, \ldots, q_N, q'_N, q''_N).$$

If we now define $F(X) = X(X^2 + dX + td^2)$, then the equation $F(x)F(y) = F(z)^2$ has solutions $(dp_i/q_i, dp'_i/q'_i, dp''_i/q''_i)$ for $i = 1, \ldots, N$, which are triples of integers. ∎

4. A few questions. The results presented in the previous sections lead to several interesting questions connected with the equation $f(x)f(y) = f(z)^2$.

QUESTION 4.1. *Does there exist an irreducible polynomial $f \in \mathbb{Q}[X]$ of degree three such that the equation $f(x)f(y) = f(z)^2$ has infinitely many solutions in rationals?*

Corollary 3.4 says that for every $N \in \mathbb{N}$ there exists a polynomial f such that the equation $f(x)f(y) = f(z)^2$ has at least N solutions in integers. This leads to the following

QUESTION 4.2. *Does there exist a polynomial $f \in \mathbb{Q}[X]$ of degree three without multiple roots such that the equation $f(x)f(y) = f(z)^2$ has infinitely many solutions in integers?*

And finally

QUESTION 4.3. *Does there exist a polynomial $f \in \mathbb{Q}[X]$ of degree greater than three without multiple roots such that the equation $f(x)f(y) = f(z)^2$ has infinitely many solutions in rationals?*

Acknowledgments. I would like to thank the anonymous referee for his valuable comments and Professors A. Schinzel and K. Rusek for remarks improving the presentation.

REFERENCES

[1] L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.

[2] A. Schinzel et W. Sierpiński, *Sur l'équation diophantienne* $(x^2 - 1)(y^2 - 1) = [((y - x)/2)^2 - 1]^2$, Elem. Math. 18 (1963), 132–133.

[3] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[4] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

[5] K. Szymiczek, *On a diophantine equation*, Elem. Math. 22 (1967), 37–38.

[6] M. Ulas, *On the diophantine equation* $(x^2 + k)(y^2 + k) = (z^2 + k)^2$, Rocky Mountain J. Math., to appear.

Institute of Mathematics
Jagiellonian University
Reymonta 4
30-059 Kraków, Poland
E-mail: Maciej.Ulas@im.uj.edu.pl

Received 5 January 2006 (4713)