ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 36, Number 3, 2006

ON QUADRATIC SOLUTIONS OF $x^4 + py^4 = z^4$

ERIC D. MANLEY

ABSTRACT. Consider the diophantine equation $x^4+py^4 = z^4$ where p is prime and $p \equiv 3 \bmod 8$. It is well known that this equation has no nonzero integer solutions. This paper shows that all quadratic solutions are inherited. That is, all quadratic solutions can be easily obtained from integer solutions to the simpler equation $x^4 + py^4 = z^2$.

1. Introduction. One of Fermat's most well-known results is the nonexistence of nonzero integer solutions to $x^4 + y^4 = z^4$. In 1934, Aigner proved that nonzero *quadratic* solutions exist though they are rare [**1**]. In fact, $\mathbf{Q}(\sqrt{-7})$ is the only quadratic extension with nonzero solutions. Observe, $(1 + \sqrt{-7})^4 + (1 - \sqrt{-7})^4 = 2^4$. Faddeev later classified all solutions in $\mathbf{Q}(\sqrt{-7})$ [**3**]. The complexity of Faddeev's methods motivated Mordell to supply an alternative argument [**5**].

We are interested in generalizing Aigner's results to the family of equations $x^4 + Dy^4 = z^4$ with $D \in \mathbf{Z}$. We prove that the only quadratic solutions to $x^4 + py^4 = z^4$ with $p \equiv 3 \bmod 8$ are those that come from rational solutions of $x^4 + py^4 = z^2$. For example, since $(1)^4+3(1)^4 = (2)^2$, we find $(1, 1, \sqrt{2}) \in \mathbf{Q}(\sqrt{2})^3$ satisfies $x^4+3y^4 = z^4$. That is, we will prove

Theorem 1. *All quadratic solutions to $x^4+py^4 = z^4$ for $p \equiv 3 \bmod 8$ can be written in the form $(a, b, \sqrt{c})$ where (a, b, c) is a rational solution to $x^4 + py^4 = z^2$.*

Furthermore, we will show

Corollary 2. *All quadratic solutions to $x^4 + py^4 = z^4$ with $p \equiv 11 \bmod 16$ satisfy $xyz = 0$.*

Research partially supported by NSF grant DMS-0201080.
Received by the editors on June 5, 2003, and in revised form on February 27, 2004.

The solution $(1, 1, \sqrt{2})$ of $x^4 + 3y^4 = z^4$ is inherited from a rational solutions to $x^4 + 3y^4 = z^2$. This leads to the following definition.

Definition 3. If (a, b, c) is a rational solution to $x^2 + Dy^4 = z^4$, $x^4 + Dy^2 = z^4$, or $x^4 + Dy^4 = z^2$ then $(\sqrt{a}, b, c)$, $(a, \sqrt{b}, c)$, or $(a, b, \sqrt{c})$ respectively is an *inherited quadratic solution* of $x^4 + Dy^4 = z^4$.

Then, we find the following more simply stated corollary

Corollary 4. *All quadratic solutions to* $x^4 + py^4 = z^4$ *with* $p \equiv 3 \bmod 8$ *are inherited.*

It is worth noting that $x^4 + y^4 = z^4$ has no inherited quadratic solutions, so Aigner found nontrivial, noninherited solutions. This observation makes his result all the more remarkable.

2. On related equations. There are no rational solutions to

$$x^4 + py^2 = 1, \quad p \equiv 3 \bmod 8. \tag{1}$$

The proof is by descent and can be found in [**6**, p. 230].

Similarly, there are no rational solutions to

$$x^2 + py^4 = 1, \quad p \equiv 3 \bmod 8. \tag{2}$$

The proof is also by descent and can be found in [**4**, p. 23]. Note also that $x^2 + py^4 = 1$ is related to the elliptic curve $v^2 = u^3 + 4pu$. This is because if (u, v) nontrivially solves $v^2 = u^3 + 4pu$, then $((8pu - v^2)/v^2, 2u/v)$ solves $x^2 + py^4 = 1$. So, all rational solutions to

$$v^2 = u^3 + 4pu, \quad p \equiv 3 \bmod 8 \tag{3}$$

satisfy $uv = 0$.

Now, for $p \equiv 11 \bmod 16$, all rational solutions to

$$x^4 + py^4 = z^2 \tag{4}$$

satisfy $xyz = 0$. The proof is by descent and can be found in [**4**, p. 23]. Now consider (4) with $p \equiv 3 \bmod 16$. Note that (4) is related to the elliptic curve

$$v^2 = u(u^2 + p). \tag{5}$$

Following [**2**, p. 258], either u or pu must be a square. If pu is a square, then $(pv/u^2)^2 = (p/u)^3 + p(p/u)$, so we may assume we have a solution to (5) where u is a square. Then we obtain a solution to (4) by letting $u = x^2/y^2$ and $v = xz/y^3$ with $\gcd(x, y) = 1$. Now according to [**7**, Chapter X, Remark 6.4], conjecturally (5) has rank 1 for $p \equiv 3 \bmod 16$. This leads us to observe that, for $p \equiv 3 \bmod 16$, (4) may have infinitely many solutions. For example, when $p = 3$, $(1, 2)$ solves (5) so $(1, 1, 2)$ solves (4). When $p = 19$, $(9, 30)$ solves (5) so $(3, 1, 10)$ solves (4). When $p = 67$, $((2401/225), (148274/3375))$ solves (5) so $(49, 15, 3026)$ solves (4).

Finally, we consider an unrelated equation. Note that all rational solutions to

$$px^4 - 4y^4 = z^2, \quad p \equiv 3 \bmod 8 \tag{6}$$

satisfy $xyz = 0$ because -1 is not a quadratic residue of p.

3. Proof of Theorem 1. The proof of Theorem 1 is based on [**5**].

Since $z \neq 0$, we focus on solutions of

$$x^4 + py^4 = 1 \tag{7}$$

where $x, y \in K$ where K is some quadratic extension of $\mathbf{Q}$. Given any solution to (7) with $y \neq 0$, define $t = (1 - x^2)/y^2$. Note that $x^2 = -ty^2 + 1$. Substituting for x^2 in (7), we may solve for y^2. Then,

$$x^2 = \frac{p - t^2}{p + t^2}, \quad y^2 = \frac{2t}{p + t^2}. \tag{8}$$

Since $x, y \in K$, $t \in K$. There are two cases to consider. Either t is rational or t is irrational. In the latter case, we will show there are no quadratic solutions and only inherited quadratic solutions in the former.

Suppose first that t is rational. Then, noting (8), x^2 and y^2 are rational. If x is rational and y is irrational, then letting $y^2 = y_1$, we get a rational solution to $x^4 + py_1^2 = 1$. If y is rational and x is irrational, then letting $x^2 = x_1$, we get a rational solution to $x_1^2 + py^4 = 1$. If both x and y are irrational then $x = x_1\sqrt{d}$ and $y = y_1\sqrt{d}$ for some $d \in \mathbf{Q}$ so we get a rational solution to $x_1^4 + py_1^4 = (1/d)^2$. According to Definition 3, these quadratic solutions are inherited. However, by (1) and (2), both $x^4 + py^2 = 1$ and $x^2 + py^4 = 1$ have no nonzero rational solutions, so all inherited solutions come from $x^4 + py^4 = z^2$.

Now suppose that t is irrational. So $K = \mathbf{Q}(t)$ and $F(t) = t^2 + Bt + C = 0$ for some rational constants B and C. We would prefer polynomials in t to the rational expressions in t for x^2 and y^2 given in (8). Let $X = (p + t^2)xy$ and $Y = (p + t^2)y$. Note then that $X^2 = 2t(p - t^2)$ and $Y^2 = 2t(p + t^2)$. Since $X, Y \in K$, there are $a, b, a_1, b_1 \in \mathbf{Q}$ such that $X = a + bt$ and $Y = a_1 + b_1 t$. Substituting for X, Y, it is clear that t is a root of the two cubic polynomials $(a+bz)^2 - 2z(p-z^2)$ and $(a_1+b_1z)^2 - 2z(p+z^2)$. So both polynomials are divisible by $F(z)$.

We will show that there is no irreducible quadratic that divides both of these cubics which will prove no such t exists. Let $M + Nz$ and $M_1 + N_1 z$ denote the two quotients. So

$$(a + bz)^2 - 2z(p - z^2) = F(z)(M + Nz), \tag{9}$$

$$(a_1 + b_1 z)^2 - 2z(p + z^2) = F(z)(M_1 + N_1 z), \tag{10}$$

where M, N, M_1, and N_1 are rational constants and $N, N_1 \neq 0$.

Clearly, $-M/N$ and $-M_1/N_1$ are roots of the lefthand sides of (9) and (10) respectively. So rational solutions exist for the equations $(a + bz)^2 = 2z(p - z^2)$ and $(a_1 + b_1 z)^2 = 2z(p + z^2)$. What are they?

First, note that if we let $v = 2(a_1 + b_1 z)$ and $u = 2z$, then we get $v^2 = u^3 + 4pu$ whose only solution is $u = v = 0$ (Section 2, equation (3)), so $z = 0$ is the only solution to $(a_1 + b_1 z)^2 = 2z(p + z^2)$. Thus, we see that $0 = M_1/N_1$. So $M_1 = 0$ and also looking at (10), $a_1 = 0$. Therefore,

$$N_1 F(z) = -2z^2 + b_1^2 z - 2p.$$

We have a characterization of $F(z)$ and now show that this $F(z)$ cannot satisfy (9) as well. To do so, substitute $F(z)$ into equation

(9) and compare the coefficients. Note $(a + bz)^2 - 2z(p - z^2) = (-2z^2 + b_1^2 z - 2p)(M + Nz)/N_1$. Expand this equation, and look at the coefficient of z^3. Then we see that $N_1 = -N$. Now look at the constant term. Thus $-M/N = -a^2/(2p)$. Recall that the zero in the righthand side of equation (9) was $-M/N$. That is, the zero in (9) must have the form $-a^2/(2p)$ with $a \in \mathbf{Q}$, or $-u^2/(2pv^2)$ with $u, v \in \mathbf{Z}$ and $\gcd(u, v) = 1$. So, from the left-hand side of (9) we see that $2(-u^2/(2pv^2))(p - (-u^2/(2pv^2))^2)$ is a square. Therefore, $((u^2)(u^4 - 4p^3v^4))/(4(v^6)(p^3))$ is a square, which means $p(u^4 - 4p^3v^4)$ is a square. We can then obtain a solution to (6) which means no such a exists.

We have shown that all quadratic solutions to equation (7) are inherited from $x^4 + py^4 = z^2$, and the proof of Theorem 1 is complete.

Acknowledgments. I would like to thank my advisor, Dr. Griff Elder, for providing me with the direction, tools, and support needed to complete this paper. Thanks to the referee for providing some insightful comments. I also thank the NSF for the grant DMS-0201080 which partially supported this research.

REFERENCES

1. Alexander Aigner, *Über die Möglichkeit von $x^4 + y^4 = z^4$ in quadratische Körper*, J. Math. Verein. **43** (1934), 226–228.

2. A. Bremner and J.W.S. Cassels, *On the equation $Y^2 = X(X^2 + p)$*, Math. Comp. **42** (1984), 257–264.

3. D.K. Faddeev, *Group of divisor classes on the curve defined by the equation $x^4 + y^4 = 1$*, Soviet Math. Dokl. **1** (1960), 1149–151.

4. L.J. Mordell, *Diophantine equations*, Pure Appl. Math., vol. 30, Academic Press, London, 1969.

5. ———, *The diophantine equation $x^4 + y^4 = 1$ in algebraic number fields*, Acta Arith. **14** (1967/1968), 347–355.

6. Trygve Nagell, *Introduction to number theory*, 2nd ed., Chelsea Publishing Co., New York, 1964.

7. Joseph H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math., vol. 106, Springer-Verlag, New York, 1986.

Department of Mathematics, University of Nebraska at Omaha, Omaha, NE 68182
E-mail address: edmanley@mail.unomaha.edu