SQUARE VALUES OF QUADRATIC POLYNOMIALS

R.G.E. Pinch

Department of Pure Mathematics and Mathematical Statistics,
University of Cambridge

16 September 1997 10:4

Abstract. We show that a quadratic polynomial symmetric about an integer point which is not a perfect square can not take more than five distinct integer square values about the centre of symmetry.

0. Introduction.

Allinson [1] asks whether a quadratic polynomial symmetric about an integer point which is not a perfect square can take more than five integer square values about the centre of symmetry. We show that it can not by reducing the problem to finding the rational points on certain elliptic curve. We show that the problem is equivalent to an old result of Pocklington [3].

1. Simultaneous quadratic forms.

It is well-known that the intersection of two space quadrics is in general an elliptic curve. We give an explicit parametrisation in the case of interest.

Proposition 1.1. *Suppose the simultaneous quadratic forms*

$$\begin{aligned} ax^2 - by^2 &= cz^2, \\ dx^2 - ey^2 &= ft^2 \end{aligned} \tag{1.1}$$

have a non-trivial solution (p, q, r, s) and that $\delta = ae - bd$ is non-zero. Then they define an elliptic curve, isomorphic to the plane cubic C:

$$\begin{aligned} Y^2 = -8f^2s^4(X-1)&(afs^2X + (adp^2 - (2bd - ae)q^2)) \\ &(bfs^2X + ((2ae - bd)p^2 - beq^2)). \end{aligned} \tag{1.2}$$

Given a point (X, Y) on C, define (u, v) by

$$\begin{aligned} u &= 4fs^2pq\delta(X-1) + Y \\ v &= 2f^2s^4(X^2-1). \end{aligned} \tag{1.3}$$

1991 *Mathematics Subject Classification.* Primary 12A15; Secondary 10A10.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Then (x, y, z, t) *are given by*

$$
\begin{aligned}
x &= pu^2 + 2bquv + abpv^2 \\
y &= qu^2 + 2apuv + abqv^2 \\
z &= r(u^2 - abv^2) \\
t &= su^2X + abv^2 - 2pq\delta uv/fs^2 \\
&= -4fs^3(X-1) \\
&\qquad (-pq\delta XY + pq\delta Y + abf^3s^6X^3 \\
&\qquad + f^2s^4(4a^2ep^2 - abfs^2 - 4b^2dq^2)X^2 \\
&\qquad + fs^2(4a^2dep^4 + 8a^2e^2p^2q^2 - 2abd^2p^4 - 20abdep^2q^2 \\
&\qquad\qquad - 2abe^2q^4 + abf^2s^4 + 8b^2d^2p^2q^2 + 4b^2deq^4)X \\
&\qquad + fs^2(-4a^2e^2p^2q^2 + 8abdep^2q^2 + abf^2s^4 - 4b^2d^2p^2q^2)).
\end{aligned} \tag{1.4}
$$

Proof. We may parametrise the conic $ax^2 - by^2 = cz^2$ by projection from the point $x = p$, $y = q$, $z = r$ onto the projective line with coordinate u/v parallel to the tangent to obtain

$$
\begin{aligned}
x &= pu^2 + 2bquv + abpv^2 \\
y &= qu^2 + 2apuv + abqv^2 \\
z &= r(u^2 - abv^2).
\end{aligned}
$$

Substituting, we have

$$
\begin{aligned}
ft^2 = fs^2u^4 - 4pq\delta u^3v + 2u^2v^2(2b^2q^2d - 2a^2p^2e + abfs^2) \\
- 4abpq\delta uv^3 + a^2b^2fs^2v^4
\end{aligned}
$$

Now define X by

$$fst = fs^2u^2X - 2pq\delta uv + fs^2abv^2. \tag{1.5}$$

We have

$$f^2s^4(X^2-1)u^2 - 4pqfs^2\delta(X-1)uv + (2f^2s^4ab(X-1) + 4dec^2r^4)v^2 = 0$$

and so the discriminant of this quadratic equation in u/v must be a square, that is,

$$
\begin{aligned}
Y^2 = -8f^2s^4(X-1)(afs^2X + (adp^2 - (2bd - ae)q^2)) \\
(bfs^2X + ((2ae - bd)p^2 - beq^2))
\end{aligned}
$$

for some Y and then, up to a scale factor,

$$
\begin{aligned}
u &= 4pqfs^2\delta(X-1) + Y \\
v &= 2f^2s^4(X^2-1).
\end{aligned}
$$

We now obtain t from (1.5) to give (1.3). $\square$

2. Quadratics symmetric about an integer.

Suppose that $f(n)$ is a quadratic polynomial symmetric about an integer point and taking five integer square values about its axis. We assume that the centre of symmetry is 0 so that we have $f(0) = y^2$, $f(\pm 1) = x^2$, $f(\pm 2) = z^2$, $f(\pm 3) = t^2$. But now the sequence $f(n)$, $n \in \mathbb{Z}$, has constant second difference, so that $f(2) - 2f(1) + f(0) = f(1) - 2f(0) - f(-1) = 2x^2 - 2y^2$, giving $z^2 = 4x^2 - 3y^2$. Similarly, $t^2 = 9x^2 - 8y^2$. These simultaneous equations have an obvious solution corresponding to the polynomial $f(n) = n^2$, namely $x = 1$, $y = 0$, $z = 2$, $t = 3$. Substituting into equation (1.3) we have

$$\begin{aligned} Y^2 &= -2^3 3^4 (X-1)(36X+36)(27X+37) \\ &= -2^5 (27X-27)(27X+27)(27X+37) \end{aligned}$$

and so

$$(Y/2)^2 = (-54X+54)(-54X-54)(-54X-74).$$

Putting $y = Y/16$ and $4x = -54X - 74$ we have

$$64y^2 = 4x(4x+20)(4x+128),$$

that is,

$$y^2 = x(x+5)(x+32). \tag{2.1}$$

The trivial solution $x = 1$, $y = 0$ corresponds to $u = 1$, $v = 0$ in (1.2) and hence to $Y = 0$, $X = 1$ in (1.3), and $x = 0$, $y = 0$ in (2.1). We note that by inspection the curve (2.1) has rational points $(0,0)$, $(-5,0)$ and $(-32,0)$ of order 2; $(-20,\pm 60)$ of order 3 and $(-8,\pm 24)$, $(4,\pm 36)$ and $(40,\pm 360)$ of order 6.

Proposition 2.1. *The only rational points on the curve*

$$y^2 = x(x+5)(x+32)$$

are the 12 torsion points.

Proof. Suppose that $(x,y;z) = (x/z^2, y/z^3)$ is a rational point in lowest terms. Then

$$y^2 = x(x+5z^2)(x+32z^2).$$

Denote by $[x]$ the class of a rational number x modulo rational squares, with $[0] = [1]$. Then

$$\phi \ : \ (x,y;z) \mapsto ([x], [x+5z^2], [x+32z^2])$$

defines ϕ to be a group homomorphism from $E(\mathbb{Q})$ to $(\mathbb{Q}/\mathbb{Q}^2)^3$ with kernel $2E(\mathbb{Q})$: see Mordell [2] chapter 16. The terms x, $x+5z^2$, $x+32z^2$ are coprime except for possible factors in common with the discriminant $5.27.(-32) = -2^5 3^3 5$ so we must have

$$\begin{aligned} x &= (-1)^{a_1} 2^{b_1} 3^{c_1} 5^{d_1} u^2 \\ x + 5z^2 &= (-1)^{a_2} 2^{b_2} 3^{c_2} 5^{d_2} v^2 \\ x + 32z^2 &= (-1)^{a_3} 2^{b_3} 3^{c_3} 5^{d_3} w^2 \end{aligned}$$

where u, v, w are integers, the a_i, b_i, c_i and d_i are all either 0 or 1 with $\sum a_i$, $\sum b_i$, $\sum c_i$, $\sum d_i$ all even.

If $a_3 = 1$, then since $x < x + 5z^2 < x + 32z^2$ we would have all $a_i = 1$. We conclude that $a_1 = a_2 = a$, say, and $a_3 = 0$.

If 2 divides z, then all the b_i must be zero. For if 2 exactly divides x then each of the b_i would be 1, and if 4 does divide x then we must have 8 dividing y, so that a common factor can be extracted in x/z^2 and y/z^3. If 2 does not divide z, then $b_2 = 1$ would imply that b_1 and b_3 would both be 0. In any case we conclude that $b_2 = 0$ and $b_1 = b_3 = b$, say.

Arguing as for the prime 2, we also conclude that $c_1 = 0$, $c_2 = c_3 = c$, say, and $d_3 = 0$ and $d_1 = d_2 = d$, say.

Hence

$$\begin{aligned} x &= (-1)^a\, 2^b \, 5^d\, u^2 \\ x + 5z^2 &= (-1)^a \, 3^c\, 5^d\, v^2 \\ x + 32z^2 &= \, 2^b\, 3^c \, w^2 \end{aligned}$$

with a, b, c, d taken modulo 2. The possibilities $(a, b, c, d) = (0, 0, 0, 0)$, $(0, 1, 0, 1)$, $(1, 0, 1, 1)$ and $(1, 1, 1, 0)$ correspond to the known torsion points. We may rule out the possibilities $c = 1, a+b+d = 1$ by considering quadratic residues modulo 3 and rule out $(0, 0, 1, 0)$ and $(1, 0, 0, 1)$ by considering residues modulo 5. Since the set of values (a, b, c, d) must form a subgroup of $(\mathbb{Z}/2\mathbb{Z})^4$, the values corresponding to torsion points are the only ones.

This is sufficient to show that $E(\mathbb{Q})$ does not have a torsion-free part. For suppose that P is a torsion-free generator in $E(\mathbb{Q})$. Then for some torsion point T we have $P - T = 2Q$ for some point Q. But then $6P = 12Q$ so that P cannot be a generator.

We now show that the points already found are the only torsion points. Reduction modulo 7 gives a curve with just 12 points over GF(7): but by the Lutz–Nagell Theorem (Mordell [2] chapter 16 theorem 10) a torsion point must be 7-integral and hence reduction modulo 7 is one-to-one on the torsion group. □

Theorem 2.2. *The only quadratic polynomials symmetric about an integer point which take five integer square values about the centre of symmetry are the perfect squares.*

Proof. By the discussion above we know that such polynomials correspond to the rational points on (2.1).

The points of order 2 on (2.1) correspond to the trivial solution $(1, 0, 2, 3)$ and hence $f(n) = n^2$. All the other torsion points correspond to a constant polynomial f.

The result follows. □

3. Squares in an arithmetic progression.

Pocklington [3] proves the following result.

Proposition 3.1. *The first, second, fifth and tenth terms of an arithmetical progression cannot all be squares, unless the first term is zero or all are equal.* □

We can now see that this is equivalent to Theorem 2.2. Suppose that $f(n) = an^2 + c$ takes square values about the centre of symmetry 0, so that $f(0) = c$, $f(\pm 1) = a + c$, $f(\pm 2) = 4a + c$ and $f(\pm 3) = 9a + c$ are all square. These values are the first, second, fifth and tenth values of the arithmetic progression with first term c and difference a. Theorem 2.2 is now equivalent to the statement that a and c are not both non-zero.

Acknowledgements.

The author is grateful to Prof. J. Leech for discussions on the subject of squares in arithmetic progression and for pointing out the equivalence of Pocklington's result.

References

1. D. Allison, *On square values of quadratics*, Math. Proc. Cambridge Philos. Soc. **99** (1986), 381–383.
2. L.J. Mordell, *Diophantine equations*, Academic Press, London, 1969.
3. H.C. Pocklington, *Some Diophantine impossibilities*, Proc. Cambridge Philos. Soc. **42** (1913), 108–121.

University of Cambridge, Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane, Cambridge CB2 1SB, U.K.