SQUARES FROM SUMS OF FIXED POWERS

Mark Bauer and Michael A. Bennett
University of Calgary and University of British Columbia, Canada

Abstract. In this paper, we show that if p and q are positive integers, then the polynomial exponential equation $p^x + q^x = y^2$ can have at most two solutions in positive integer x and y. If such solutions exists, we are able to precisely characterize them. Our proof relies upon a result of Darmon and Merel, and Chabauty's method for finding rational points on curves of higher genus.

1. Introduction

More than two centuries ago, in the Gentleman's Diary, J. Saul [12] exhibited a pair of positive integers $(p, q) = (184, 345)$ with the property that

$$p + q, \;\; p^2 + q^2 \;\; \text{and} \;\; p^3 + q^3$$

are simultaneously squares of integers. Such questions, while undoubtedly odd by modern standards, enjoyed a long vogue, stemming from work of Diophantus of Alexandria. As is the case for much of classical number theory, the best place to find references to such problems is Dickson [7]. In 1986, Bremner [1] put a modern spin on Saul's result, showing that all such pairs (p, q) may be derived from a certain binary recurrence sequence arising from the rational points on a particular elliptic curve (of positive rank over $\mathbb{Q}$).

In a more recent paper, Gica [9] used the arithmetic of a real quadratic field to show that, for $(p, q) = (5, 11)$, $p^x + q^x$ is square only when $x = 1$. As with the above, this falls within the framework of the following more general question :

Given integers p and q, for what values of x do we have $p^x + q^x$ square?

2000 *Mathematics Subject Classification.* ????, ????
Key words and phrases. template, glasnik, LaTeXstyle.

The answer to this is somewhat surprising in three regards. Firstly, it is possible with current methods to answer such a question completely, provided p and q are coprime. Secondly, to carry this out really does seem to require modern techniques of some sophistication. Finally, if p and q fail to be coprime, then this apparently innocent question leads us into very deep waters and well beyond the limits of current technology.

Our main result in this paper is the following.

THEOREM 1.1. *If p and q are relatively prime positive integers, then the equation*

$$p^x + q^x = y^2 \tag{1.1}$$

possesses at most two solutions in positive integers x and y, all of which satisfy $x \leq 3$. If there are two solutions $(x_1, y_1), (x_2, y_2)$, with $x_1 < x_2$, then one of p or q, say p, is even and there exist coprime integers m and n such that either

$$x_1 = 1, \;\; x_2 = 2, \;\; p = 4mn\left(m^2 - 2mn + 2n^2\right)$$

and

$$q = \left(m^2 + 2n^2\right)\left(m^2 - 4mn + 2n^2\right),$$

or

$$x_1 = 1, \;\; x_2 = 3, \;\; p = \frac{1}{4}(n-m)(3n-m)(m^2+3n^2)$$

and

$$q = m\,n\,(m^2 - 3mn + 3n^2).$$

In this latter case, we may assume that both m and n are odd.

An immediate corollary (which yields the aforementioned result of Gica as a special case) is the following.

COROLLARY 1.2. *If p and q are odd relatively prime positive integers, then equation (1.1) has at most a single solution in positive integers x and y, which necessarily satisfies $x \in \{1, 3\}$.*

The outline of this paper is as follows. We begin by invoking a striking result of Darmon and Merel [6] which reduces the problem to one of small exponents x in (1.1) (in particular, to $x \leq 3$). Easy elementary arguments then allow us to classify precisely when we can find solutions with $(x_1, x_2) = (1, 2)$ and $(1, 3)$. To complete our proof, it remains to exclude the possibility that we have two solutions with $(x_1, x_2) = (2, 3)$. In this situation, we are led to the problem of determining the set of rational points on a particular hyperelliptic curve of genus 2, via the methods of Chabauty [2], techniques which over the past twenty years or so have proven to be remarkably successful in finding rational points on higher genus curves. We conclude with some comments on the surprisingly difficult situation that arises if we do not insist that the integers p and q are coprime.

2. Proof of Theorem 1.1

The main ingredient in our proof is the following beautiful theorem of Darmon and Merel (Theorem 1 of [6]) :

Theorem 2.1. *(Darmon and Merel) If p and q are coprime integers for which equation (1.1) has a solution in positive integers x and y, then we have $1 \leq x \leq 3$.*

This result follows from arguments somewhat analogous to Wiles' work on Fermat's Last Theorem, but with significant additional complications. With Theorem 2.1 in hand, we know that equation (1.1) has, trivially, at most three solutions. To strengthen this conclusion, we analyze the constraints placed upon the integers p and q through their satisfying (1.1) with $1 \leq x \leq 3$. In each case, we determine parametrizations of p and q in terms of integers m and n enabling us to generate all possible values of p and q satisfying the given constraint.

2.1. *Solutions to $p + q = a^2,\ p^2 + q^2 = b^2$.* Let us begin by supposing that equation (1.1) has solutions with both $x = 1$ and $x = 2$; i.e. that there exist integers a and b for which

$$p + q = a^2 \quad \text{and} \quad p^2 + q^2 = b^2.$$

Since p and q are coprime, we may apply the theory of primitive Pythagorean Triples and assume that p is even to deduce that there exist coprime integers r and s such that $p = 2rs$ and $q = r^2 - s^2$ with

$$a^2 = (r^2 - s^2) + 2rs = (r + s)^2 - 2s^2,$$

so that

$$(r + s - a)\,(r + s + a) = 2s^2.$$

Examining the factors on the left-hand side of the latter equation, we realize that their greatest common divisor divides $2(r + s), 2a$ and s. Since r and s are coprime, we conclude that their greatest common divisor is in fact 2 and thus s is even. Hence we can find coprime integers m and n, with m odd, such that

$$r + s \pm a = 2m^2,\ r + s \mp a = 4n^2, \ \text{ and } \ s = 2mn,$$

whence

$$r = m^2 - 2mn + 2n^2.$$

Since $p = 2rs$ and $q = r^2 - s^2$, we can parametrize p and q by

$$p = 4m^3n - 8m^2n^2 + 8mn^3, \ \ q = m^4 - 4m^3n + 4m^2n^2 - 8mn^3 + 4n^4.$$

2.2. *Solutions to $p+q=a^2,\ p^3+q^3=b^2$.* Let us now suppose that (1.1) has solutions with both $x=1$ and $x=3$; i.e. that there exist integers a and b for which

$$p+q=a^2 \quad \text{and} \quad p^3+q^3=b^2.$$

From the fact that $(p+q)^3=p^3+q^3$ modulo 3, it is easy to see that a^2 and b^2 are congruent modulo 3. If $3 \mid a$, then, from the coprimality of p and q, we may assume that 3 fails to divide pq. Since

$$a^4-3pq=p^2-pq+q^2=\frac{p^3+q^3}{p+q}=(b/a)^2,$$

we thus have that $(b/a)^2 \equiv \pm 3 \mod 9$, a contradiction. It follows that $a^2 \equiv b^2 \equiv 1 \mod 3$ and hence, in

$$b^2=p^3+q^3=(p+q)\left(p^2-pq+q^2\right),$$

the factors on the right hand side are necessarily coprime, whereby there exists a positive integer c, also coprime to 3, for which

$$p^2-pq+q^2=c^2. \tag{2.2}$$

If p and q are odd, then from $p+q=a^2$, it follows that

$$pq \equiv -1 \mod 4,$$

contradicting (2.2) modulo 4. We may thus suppose that one of p or q, say p, is even.

Write

$$4c^2-(2p-q)^2=(2c-2p+q)(2c+2p-q)=3q^2.$$

Examining the sum and difference of the factors in the middle, we conclude that the factors are relatively prime, whence there exist positive integers r and s such that

$$2c \pm (2p-q)=r^2,\ 2c \mp (2p-q)=3s^2,\ rs=q.$$

If we have

$$2c-(2p-q)=r^2,\ 2c+(2p-q)=3s^2,$$

then

$$c=\frac{r^2+3s^2}{4} \ \text{ and } \ q-2p=\frac{r^2-3s^2}{2}.$$

After a little work, we find from the equation $p+q=a^2$, that

$$a^2+r^2=3\left(\frac{r+s}{2}\right)^2.$$

Considering this equation modulo 3 leads us to a contradiction of the fact that a is coprime to 3.

We may thus suppose that

$$2c+(2p-q)=r^2,\ 2c-(2p-q)=3s^2,$$

whereby

$$p = \frac{r^2 + 2rs - 3s^2}{4},\ q = rs. \tag{2.3}$$

We now appeal to the fact that $p + q = a^2$ which, with (2.3), leads us to the equation

$$\left(\frac{r+3s}{2}\right)^2 - a^2 = 3s^2$$

and hence to the conclusion that there exist integers m and n for which

$$\frac{r+3s}{2} \pm a = m^2,\ \frac{r+3s}{2} \mp a = 3n^2,\ s = mn,$$

i.e.

$$r = m^2 - 3mn + 3n^2,\ s = mn.$$

Substituting these values into (2.3), we find that

$$p = \frac{1}{4}(n-m)(3n-m)(m^2+3n^2)$$

and

$$q = m\,n\,(m^2 - 3mn + 3n^2).$$

It is worth noting that this combines the pair of parametrizations given by Mordell (page 235 of [11]) for this case into a single form.

2.3. *The case* $p^2 + q^2 = a^2,\ p^3 + q^3 = b^2$. To complete the proof of Theorem 1.1, it remains to show that there do not exist integers a and b for which

$$p^2 + q^2 = a^2,\ p^3 + q^3 = b^2,$$

provided p and q are coprime. If there are such integers, then using Pythagorean Triples again we may write $p = 2mn$ and $q = m^2 - n^2$ for relatively prime nonzero integers m and n, of opposite parity, to conclude that

$$b^2 = (m^2 + 2mn - n^2)(m^4 - 2m^3n + 2m^2n^2 + 2mn^3 + n^4). \tag{2.4}$$

Defining a curve $\mathcal{C}$ by

$$\mathcal{C}\ :\ y^2 = x^6 - 3x^4 + 8x^3 + 3x^2 - 1 = (x^2 + 2x - 1)(x^4 - 2x^3 + 2x^2 + 2x + 1),$$

a triple of integers (m, n, b) satisfying equation (2.4) therefore yields a (rational) point $(x, y) = (\frac{m}{n}, \frac{b}{n^3})$ on $\mathcal{C}$.

Let J denote the Jacobian of $\mathcal{C}$. We now show how the computer algebra package MAGMA can be used to find the structure of $J(\mathbb{Q})$. The following commands

```
> _<x>:=PolynomialRing(Rationals());
> C:=HyperellipticCurve(x^6-3*x^4 + 8*x^3 + 3*x^2-  1);
> J:=Jacobian(C);
> T,mapTtoJ:=TorsionSubgroup(J);
> T;
```

```
 > {mapTtoJ(t):t in T};
```

yield the output

```
 Abelian Group isomorphic to Z/2
 Defined on 1 generator
 Relations:
  2*P[1] = 0
{ (x^2 + 2*x - 1, 0, 2), (1, 0, 0) }
```

This tells us that $J(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2$. To understand the arithmetic structure of $J(\mathbb{Q})$, it remains to determine the rank r of $J(\mathbb{Q})$ and (if possible) the r free generator(s). We can use a 2-descent to compute an upper bound $\hat{r}$ on the rank, then search for independent points in $J(\mathbb{Q})$ and hope we find $\hat{r}$ of them, thus verifying that $\hat{r}$ is indeed the rank of $J(\mathbb{Q})$.

```
 > r:=TwoSelmerGroupData(J); r;
 > R:=RationalPoints(J:Bound:=1000);
 > B:=ReducedBasis(R); B;
```

yields

```
 1
[ (x^2 - 10/7*x + 5/7, 180/49*x - 48/49, 2) ]
```

We thus have an upper bound of 1 on the rank and, since we found a torsion-free element, $J(\mathbb{Q})$ has rank 1. Therefore

$$J(\mathbb{Q}) \simeq \mathbb{Z}/2 \times \mathbb{Z}.$$

Note that we cannot immediately conclude that

$$\mathcal{A} = (x^2 - 10x/7 + 5/7, 180x/49 - 48/49)$$

generates the free part of $J(\mathbb{Q})$; it could be a multiple of a generator. Let us suppose that $\mathcal{G}$ is a generator of the free part of $J(\mathbb{Q})$ and that $\mathcal{A} = n\mathcal{G}$ for some integer n. Then, taking (canonical) heights, we find that $\hat{h}(\mathcal{A}) = n^2\hat{h}(\mathcal{G})$. If $\mathcal{A}$ is not a generator then $n \geq 2$ and so

$$\hat{h}(\mathcal{G}) < \frac{1}{4}\hat{h}(\mathcal{A}).$$

It follows that we need only search for points on $J(\mathbb{Q})$ up to canonical height $\frac{1}{4}\hat{h}(\mathcal{A})$ to find the generator. In MAGMA, we can search for points by naive height h. Letting HC be the height constant of $J(\mathbb{Q})$, i.e. the maximum difference between the canonical and naive height, we thus need to search up to the bound

$$\exp\left(\frac{\hat{h}(\mathcal{A})}{4} + HC\right)$$

in order to guarantee that we will find a generator. We have

```
> HC:=HeightConstant(J:Effort:=2); HC;
> A:=J![x^2 - 10/7*x + 5/7, 180/49*x - 48/49];
> hA:=Height(A); hA;
> newbound:=Exp(hA/4+HC); newbound;
> R:=RationalPoints(J:Bound:=newbound); B:=ReducedBasis(R); B;
```

with output

```
4.440714133574227037952632870 01
1.936436133936195601852927195 84
137.664995784170212641786904264
[ (x^2 - 10/7*x + 5/7, 180/49*x - 48/49, 2) ]
```

whereby it follows that $\mathcal{A}$ is indeed a generator of the free part of $J(\mathbb{Q})$.

Since we are in a situation where the rank of $J(\mathbb{Q})$ is strictly less than the genus of $\mathcal{C}$, we may appeal to classical arguments of Chabauty to attempt to determine $\mathcal{C}(\mathbb{Q})$. We try such arguments modulo an assortment of small primes; the commands

```
> P:=B[1];
> #Chabauty(P,5);
> #Chabauty(P,7);
> #Chabauty(P,11);
> #Chabauty(P,13);
> #Chabauty(P,17);
```

lead to the following outputs :

```
3
2
5
3
1
```

Thus, applying Chabauty's method at the prime 17 is enough to show that we have found all the rational points on $\mathcal{C}$ and hence conclude as desired (i.e. that equation (2.4) has no solutions in coprime, nonzero integers m and n). This completes the proof of Theorem 1.1.

3. p and q with common factors

The case where p and q have a common factor is, as it transpires, significantly more difficult to handle. If, for example, $p = q = 2k^2$, for k a fixed positive integer, then equation (1.1) has solutions for *every* odd positive integer x. If we assume that $p \neq q$, then we suspect that equation (1.1) has at most 3 solutions in positive integers x and y. If there are three such solutions, (x_i, y_i) with, say, $x_1 < x_2 < x_3$, then we would guess that

$$(x_1, x_2, x_3) = (1, 2, 3).$$

Further, if there are exactly two solutions, say with $x_1 < x_2$, then perhaps it follows that

$$(x_1, x_2) \in \{(1,2),(1,3),(1,5)\}, \quad \text{or} \quad (x_1, x_2) = (2, k) \ \text{ for } k \text{ odd}.$$

This appears to be well out of reach to prove at the present time.

In the case that we have three solutions to (1.1) given by $(x_1, x_2, x_3) = (1, 2, 3)$, let us suppose that $\gcd(p, q) = d > 1$ and write $p = dp_1, q = dq_1$. Then if $p + q, p^2 + q^2$ and $p^3 + q^3$ are all squares, it follows that both $p_1^2 + q_1^2$ and $p_1^2 - p_1q_1 + q_1^2$ are squares, whereby, from the Pythagorean Theorem, there exist positive coprime integers m and n such that, without loss of generality, $p_1 = m^2 - n^2$, $q_1 = 2mn$, and hence an integer a such that

$$a^2 = p_1^2 - p_1q_1 + q_1^2 = m^4 - 2m^3n + 2m^2n^2 + 2mn^3 + n^4.$$

Upon setting

$$y = \frac{4am}{n^3} + \frac{4m^3}{n^3} - \frac{6m^2}{n^2} + \frac{4m}{n} - \frac{2a}{n^2} + 2$$

and

$$x = \frac{2a}{n^2} + \frac{2m^2}{n^2} - \frac{2m}{n} + 1,$$

we find that

$$y^2 = x^3 - x^2 - 9x + 9$$

which is an elliptic curve E of conductor 192. In fact, it is 192A2 in Cremona's notation [5], with full rational 2-torsion, and rank 1 over $\mathbb{Q}$; i.e. we have

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

On this curve, we find the point $(x, y) = (51, 360)$, corresponding to $(m, n) = (4, 1)$. This value leads to $p_1 = 15, q_1 = 8$ whereby $d = 23$. We thus recover Saul's example $(p, q) = (345, 184)$. For further details on this case, the reader is directed to the paper of Bremner [1]. Something similar occurs if one has two solutions to (1.1) of the shape $(x_1, x_2) = (1, 5)$ – one finds that $p^4 - p^3q + p^2q^2 - pq^3 + q^4$ is necessarily square, which leads, after some work, to the curve

$$y^2 = x^3 + x^2 - 3x - 2,$$

of conductor 200 and rank 1.

Similarly, the cases where we have solutions $(x_1, x_2, x_3) = (1, 2, 5)$ or $(1, 3, 5)$ correspond to rational points on the curves

$$C_2 \ : \ y^2 = x^6 - x^5 + 2x^4 - 2x^3 + 2x^2 - x + 1$$

and

$$C_3 \ : \ y^2 = x^6 - 2x^5 + 3x^4 - 3x^3 + 3x^2 - 2x + 1,$$

respectively. Applying Chabauty arguments, we may show that all such points either lie at infinity, or correspond to $(x, y) = (0, \pm 1)$ or $(1, \pm 1)$. In no cases do these lead us to examples of (p, q) for which (1.1) has solutions with $(x_1, x_2, x_3) = (1, 2, 5)$ or $(1, 3, 5)$.

If we restrict our attention to the situation where (1.1) has two solutions given by $x_1 = 1$ and $x_2 = n$, then we are led to the Diophantine equation

$$\frac{x^n + y^n}{x + y} = z^2,$$

where we may now suppose that $\gcd(x, y) = 1$ and, via [6], that $n > 5$ is odd. It appears to be extremely difficult to fully treat this equation. Presumably, the true state of affairs (see Conjecture 1 of [13]) is that the equation has no coprime positive solutions other than $(x, y) = (1, 1)$. While this conjecture has been established provided n is divisible by one of

$$3, 7, 11, 13 \text{ or } 25$$

(see [10] and [13]), in general, with current methods, this lies well beyond the provable.

References

[1] A. Bremner, *A Diophantine system,* Internat. J. Math. Math. Sci. **9** (1986), no. 2, 413–415.

[2] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité,* C. R. Acad. Sci. Paris **212** (1941), 882-885.

[3] H. Cohen, Number Theory, Vol. II : Analytic and Modern Tools, Springer-Verlag, GTM 240, 2007.

[4] R. Coleman, *Effective Chabauty,* Duke Math. J. **52** (1985), 765–770.

[5] J. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, 1992.

[6] H. Darmon and L. Merel, J. Reine Angew. Math. **490** (1997), 81–100.

[7] L. E. Dickson, History of the theory of numbers. Vol. II: Diophantine analysis, Chelsea Publishing Co., New York 1966.

[8] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern,* Invent. Math. **73** (1983), no. 3, 349-366.

[9] A. Gica, *The Diophantine equation* $5^x + 11^x = y^2$*,* Rev. Roumaine Math. Pures Appl. **49** (2004), no. 5-6, 455–459.

[10] W. Ivorra, *Sur les courbes hyperelliptiques cyclotomiques et les équations* $x^p - y^p = cz^2$*,* Dissertationes Mathematicae **44** (2007), 46pp.

[11] L.J. Mordell, Diophantine Equations, Academic Press, 1969.

[12] J. Saul, The Gentleman's Quarterly, 1795.

[13] P. G. Walsh, *Squares in Lucas sequences with rational roots,* Integers **5** (3) (2005), #A15.

Mark Bauer
Department of Mathematics
University of Calgary
Calgary, AB
Canada
E-mail: mbauer@math.ucalgary.ca

Michael A. Bennett
Department of Mathematics
University of British Columbia
Vancouver, B.C.
Canada
E-mail: bennett@math.ubc.ca