ON THE EQUATION \( s^2 + y^{2p} = \alpha^3 \)

IMIN CHEN

Abstract. We describe a criterion for showing that the equation \( s^2 + y^{2p} = \alpha^3 \) has no non-trivial proper integer solutions for specific primes \( p > 7 \). This equation is a special case of the generalized Fermat equation \( x^p + y^q + z^r = 0 \). The criterion is based on the method of Galois representations and modular forms together with an idea of Kraus for eliminating modular forms for specific \( p \) in the final stage of the method (1998). The criterion can be computationally verified for primes \( 7 < p < 10^7 \) and \( p \neq 31 \).

1. Introduction

A solution \( (\alpha, s, y) \in \mathbb{Z}^3 \) to the equation \( s^2 + y^{2p} = \alpha^3 \) is said to be non-trivial if \( sy \neq 0 \), and proper if \( (\alpha, s, y) = 1 \). In this paper, we describe a criterion for showing that equation \( s^2 + y^{2p} = \alpha^3 \) has no non-trivial proper integer solutions for specific primes \( p > 7 \). This equation is a special case of the generalized Fermat equation \( x^p + y^q + z^r = 0 \) (cf. [5] and its references for a recent survey of this equation).

The proper solutions to the diophantine equation \( s^2 + y^{2p} = \alpha^3 \) naturally arise as certain suitably-defined integral points on a twist of the modular curve associated to the subgroup \( \Gamma_3 \) of index 2 of \( SL_2(\mathbb{Z}) \) (for a description of this viewpoint as applied to familiar cases, see [3]). This was in fact the initial motivation for considering the above diophantine equation. A uniformizer for this genus 0 modular curve is usually denoted \( \gamma_3 \) in the classical literature.

For \( p > 3 \) a prime and \( q \) a prime of the form \( np + 1 \), let \( \Omega_{p,q} \) be the subset of elements \( \zeta \in \mathbb{F}_q \) such that \( \zeta = A^p \) and \( \zeta + \frac{1}{27} = U^2 \) for some \( A \in \mathbb{F}_q^* \), \( U \in \mathbb{F}_q^* \). For \( \zeta \in \Omega_{p,q} \), let \( E_{\zeta} \) denote the isomorphism class of the elliptic curve over \( \mathbb{F}_q \) given by \( Y^2 = X^3 + 2UX^2 + \frac{1}{27}X \) where \( \zeta + \frac{1}{27} = U^2 \) (note the choices of \( U \) give rise to elliptic curves which are twists of each other). Let \( E_0 \) denote an elliptic curve over \( \mathbb{Q} \) of conductor 96.

Theorem 1. Let \( p > 7 \) be a prime. Suppose there exists a prime \( q \) of the form \( np + 1 \) such that \( a_q(E_0)^2 \neq 4 \) (mod \( p \)) and for all \( \zeta \in \Omega_{p,q} \) we have \( a_q(E_{\zeta})^2 \neq a_q(E_0)^2 \) (mod \( p \)). Then there are no triples \( (\alpha, s, y) \in \mathbb{Z}^3 \) satisfying \( s^2 + y^{2p} = \alpha^3 \) with \( (\alpha, s, y) = 1 \) and \( sy \neq 0 \).

Corollary 2. Let \( 7 < p < 10^7 \) and \( p \neq 31 \) be a prime. Then there are no triples \( (\alpha, s, y) \in \mathbb{Z}^3 \) satisfying \( s^2 + y^{2p} = \alpha^3 \) with \( (\alpha, s, y) = 1 \) and \( sy \neq 0 \).
Corollary 3. Let \( p > 7 \) be a prime such that \( q = 2p + 1 \) is prime. If \( \left( \frac{q}{13} \right) = 1 \) and \( \left( \frac{a}{13} \right) = (-1)^{\frac{a-1}{2}} \), then there are no triples \((a, s, y)\) \in \mathbb{Z}^3\) satisfying \( s^2 + y^2p = \alpha^3 \) with \((a, s, y) = 1\) and \( sy \neq 0 \).

For instance, the hypotheses of Corollary 3 are satisfied for
\[
p = 100000000000000014611, \quad q = 200000000000000029223.
\]
Based on the conjectures described in [6], the conclusion of the above theorem should hold if \( p > 3 \).

2. Proof of Theorem 1

We first recall the parametrization of solutions to the equation \( s^2 + t^2 = \alpha^3 \).

Lemma 4. A triple \((\alpha, s, t)\) \in \mathbb{Z}^3\) with \((\alpha, s, t) = 1\) satisfies \( s^2 + t^2 = \alpha^3 \) only if \((\alpha, s, t) = (u^2 + v^2, u(u^2 - 3v^2), v(3u^2 - v^2))\) for some \((u, v)\) \in \mathbb{Z}^2\).

Proof. Cf. Lemma 3.2.2 in [3].

Lemma 5. Let \( p \) be an odd prime. Suppose \((u, v)\) \in \mathbb{Z}^2\) gives rise to a triple \((\alpha, s, t) = (u^2 + v^2, u(u^2 - 3v^2), v(3u^2 - v^2))\) satisfying \((\alpha, s, t) = 1\) and \( st \neq 0 \). Then the constraint that \( t = y^p \) for some \( y \in \mathbb{Z} \) implies either

\[
\begin{align*}
(1) & \quad v = r^p \text{ and } 3u^2 - v^2 = a^p \text{ for some } a, r \text{ with } 3 \nmid a, r \text{ and } a, r, u \text{ are non-zero pairwise coprime}, \\
(2) & \quad v = 3^{p-1}r^p \text{ and } 3u^2 - v^2 = 3a^p \text{ for some } a, r \in \mathbb{Z} \text{ and positive } j \in \mathbb{Z}, \text{ where } 3 \nmid a, r, u \text{ and } a, r, u \text{ are non-zero pairwise coprime}.
\end{align*}
\]

Proof. Since \((\alpha, s, y) = 1\), it is necessary that \((u, v) = 1\). If \( d \mid v \) and \( d \mid 3u^2 - v^2 \), then \( d \mid 3u^2 \). Since \((u, v) = 1\), we have that \( d \mid 3 \). Hence, \((v, 3u^2 - v^2) \mid 3 \).

If \( 3 \nmid v \), then \( v, 3u^2 - v^2 = 1 \). The condition that \( t = v(3u^2 - v^2) = y^p \) for some \( y \in \mathbb{Z} \) implies by unique factorization that \( v = r^p \) and \( 3u^2 - v^2 = a^p \) for coprime \( a, r, u \in \mathbb{Z} \). It now follows that \( 3 \nmid a, r \) and \( a, r, u \) are pairwise coprime.

If \( 3 \mid v \), then \( v, 3u^2 - v^2 = 3 \). The condition that \( t = v(3u^2 - v^2) = y^p \) for some \( y \in \mathbb{Z} \) implies by unique factorization that \( v = 3^p r^p \) and \( 3u^2 - v^2 = 3^n a^p \) for coprime \( a, r, m \in \mathbb{Z}, \text{ where } 3 \nmid a, r \), and positive \( n \in \mathbb{Z} \). It is now easily checked that \( 3 \nmid u, m = 1 \), \( n = pj - 1 \) for some positive \( j \in \mathbb{Z} \), and \( a, r, u \) are pairwise coprime.

Corollary 6. Let \( p \) be an odd prime. Suppose \((u, v)\) \in \mathbb{Z}^2\) gives rise to a triple \((\alpha, s, t) = (u^2 + v^2, u(u^2 - 3v^2), v(3u^2 - v^2))\) satisfying \((\alpha, s, t) = 1\) and \( st \neq 0 \). Then the constraint that \( t = y^p \) for some \( y \in \mathbb{Z} \) implies there are non-zero pairwise coprime \( a, r, u \in \mathbb{Z} \) and positive \( j \in \mathbb{Z} \) satisfying either

\[
\begin{align*}
(1) & \quad a^p + (r^2)^p = 3u^2 \text{ with } 3 \nmid a, r, \\
(2) & \quad a^p + 3^{p-1}r^p = u^2 \text{ with } 3 \nmid a, u.
\end{align*}
\]

Theorem 7. Let \( p > 3 \) be a prime. Suppose \((a, r, u)\) \in \mathbb{Z}^3\) satisfies \( a^p + (r^2)^p = 3u^2 \) with \( a, r, u \) pairwise coprime and \( 3 \nmid a, r \). Then \( aru = 0 \).

Proof. This is a special case of Theorem 1.1 in [1].

For non-zero \( a, d \in \mathbb{Z} \), let \( \text{Rad}_d(a) \) be the product of primes dividing \( a \) but not \( d \).
Proposition 8. Let $p > 3$ be a prime. Suppose $(a, r, u) \in \mathbb{Z}^3$ satisfies $a^p + 3^{2^{p-3}}(r^2)^p = u^2$ with $a, r, u$ non-zero pairwise coprime, $3 \nmid a, u$, and positive $j \in \mathbb{Z}$. Associate to $(a, r, u)$ the elliptic curve $E$ over $\mathbb{Q}$ given by

1. $Y^2 = X^3 + 2uX^2 + 3^{2^{p-3}}r^2X$ if $ar$ is odd,
2. $Y^2 + XY = X^3 + \frac{\pm u-1}{4}X^2 + \frac{2^{2^{p-3}}(r^2)^p}{64}X$ if $ar$ is even,

where the sign in $\pm u$ is chosen so that $\pm u \equiv 1 \pmod{4}$. Then the conductor $N$ of $E$ and the Artin conductor $M$ of $\rho_{E,p}$ are given in each case by

1. $N = 96 \cdot \text{Rad}_q(ab)$ and $M = 96$,
2. $N = 6 \cdot \text{Rad}_q(ab)$ and $M = 6$.

Furthermore, the representation $\rho_{E,p}$ is flat at $p$.

Proof: This follows from Lemma 2.1 of [1].

The above proposition allows us to invoke the machinery of galois representations and modular forms to establish Theorem 1.

Proof of Theorem 1. Suppose $(a, s, y) \in \mathbb{Z}^3$ satisfies $s^2 + y^2p = a^2$ with $(s, t, \alpha) = 1$ and $sy \neq 0$. By Corollary 6 we obtain non-zero pairwise coprime $a, r, u \in \mathbb{Z}$ satisfying $a^p + (r^2)^p = 3u^2$ with $3 \nmid a, r$, or non-zero pairwise coprime $a, r, u \in \mathbb{Z}$ and positive $j \in \mathbb{Z}$ satisfying $a^p + 3^{2^{p-3}}(r^2)^p = u^2$ with $3 \nmid a, u$. In the former case, Theorem 7 allows us to deduce that $aru = 0$, a contradiction. In the latter case, let $E$ be the elliptic curve over $\mathbb{Q}$ associated to $(a, r, u)$ by Proposition 8. Since $E$ is modular [2], it follows that $\rho_{E,p}$ is modular.

The elliptic curve $E$ has one odd prime of multiplicative reduction, namely $q = 3$. By Corollary 4.4 in [3], $E$ having at least one prime odd prime $q$ of multiplicative reduction and $\rho_{E,p}$ reducible implies that $p = 2, 3, 5, 7, 13$. If $p = 13$ however, then $E$ would give rise to a non-cuspidal rational point on $X_0(26)$ as $E$ also has a rational point of order 2, contradicting [10]. Since $p > 7$ we may assume now that $\rho_{E,p}$ is irreducible. Since $\rho_{E,p}$ has Artin conductor $M = 6$ or $M = 96$ and is flat at $p$, it follows by level lowering [11] that $\rho_{E,p} \cong \rho_{g,p}$ where $g$ is a weight 2 newform on $\Gamma_0(M)$. There are no weight 2 newforms on $\Gamma_0(6)$, so we are left with the case that $M = 96$.

There are two possibilities for $g$ corresponding to the isogeny classes labelled as 96A, 96B respectively in Cremona’s tables [4]. Let $E_0$ be the elliptic over $\mathbb{Q}$ corresponding to $g$.

If $q$ is a prime and $q \neq 2, 3, p$, then the fact that $\rho_{E,p} \cong \rho_{E_0,p}$ implies $p \mid a_q(E_0)^2 - a_q(E_0)$ if $E$ has good reduction at $q$ and $p \mid a_q(E_0)^2 - (q+1)^2$ if $E$ has multiplicative bad reduction at $q$. If $E_0$ does not have a rational point of order 2, then it is possible to find a prime $q$ (independently of the exponent $p$ and the solution $(a, r, u)$) so that $a_q(E_0)$ is odd. On the other hand, $a_q(E)$ is even so that $a_q(E) - a_q(E_0)$ is non-zero. The quantity $a_q(E_0)^2 - (q+1)^2$ is non-zero by Hasse’s bounds. Hence, we obtain a bound on $p$. This method to bound $p$ is used in the proof of Theorem 7 [12].

Unfortunately, all elliptic curves over $\mathbb{Q}$ of conductor 96 have a rational point of order 2. Thus, it is not possible to use the above method to bound $p$. However, in this situation, the method in [7] can be used to obtain a contradiction for specific $p$.

The method works as follows. Recall we are in the situation where we have obtained non-zero pairwise coprime $a, r, u \in \mathbb{Z}$ and positive $j \in \mathbb{Z}$ satisfying $a^p + 3^{2^{p-3}}(r^2)^p = u^2$ with $3 \nmid a, u$, and this solution gave rise to the elliptic curve $E$ over
\[ \mathbb{Q} \text{ given by } Y^2 = X^3 + 2uX^2 + 3^{3p-3}r^{-2p}X. \] For a fixed exponent \( p \), we search for \( q = np + 1 \) prime such that \( a_q(E_0)^2 \equiv 4 \pmod{p} \) and \( a_q(E_\zeta)^2 \not\equiv a_q(E_0)^2 \pmod{p} \) for all \( \zeta \in \Omega_{p,q}. \)

The existence of such a prime \( q \) for the given \( p \) now yields a contradiction as follows. If \( E \) were to have multiplicative reduction modulo \( q \), then we would have that \( a_q(E_0)^2 \equiv (q+1)^2 \equiv 4 \pmod{p} \), a contradiction. Hence, \( E \) has good reduction modulo \( q \). By Lemma 2.1 in [1], the discriminant of \( E \) is equal to \( a^3r^4p \) up to factors of 2 and 3. Hence, both \( a, r \) are non-zero modulo \( q \). If we let \( A = \frac{-a}{r} \) and \( U = \frac{-U}{r} \), then \( \zeta + \frac{1}{2}U = U^2 \) where \( \zeta = A^2 \). The elliptic curve \( E \) is isomorphic to \( Y^2 = X^3 + 2UX^2 + \frac{1}{2}X \) over \( \mathbb{Q}(\sqrt{3p^3r^2}) \) which also has good reduction modulo \( q \).

Hence, the reduction modulo \( q \) of \( E \) is isomorphic to a twist of \( E_\zeta \) where \( \zeta \in \Omega_{p,q} \) is the reduction modulo \( q \) of \( \zeta \). Now, \( a_q(E)^2 = a_q(E_\zeta)^2 \). But then we would have that \( p \mid a_q(E)^2 - a_q(E_\zeta)^2 = a_q(E_\zeta - a_q(E_0)^2 \), a contradiction.

Notice that the elliptic curves 96A and 96B are twists of each other and that the criterion above only depends on \( E_0 \) up to twist.

Although it is possible to treat the diophantine equation \( s^2 + y^{2p} = a^3 \) using the elliptic curves classified by the modular curve associated to \( \Gamma_3 \) directly, many of the arguments are essentially equivalent to the work incorporated into the proof of Theorem 1.1 of [1].

**Proof of Corollary 2**. We were able to computationally verify the criterion of Theorem 1 for \( 7 < p < 10^7 \) and \( p \neq 31 \) using MAGMA.

Curiously, it is sometimes the case that \( \Omega_{p,q} \) is empty for specific \( p, q \) (e.g. \( p = 11, q = 23 \)). When this is the case, this last portion of the argument becomes completely elementary (but note the overall argument still requires [1]).

For example, suppose \( p > 3 \) and \( n = 2 \) so \( q = 2p+1 \) is prime. The set \( \Omega_{p,q} \) is not empty if and only if \( \pm 27 + 1 = 3x^2 \) for some \( x \in \mathbb{F}_q^\times \), in other words if and only if \( (\frac{26}{q}) = (\frac{3}{q}) \) or \( (\frac{-26}{q}) = (\frac{3}{q}) \). Using quadratic reciprocity, we find that the set \( \Omega_{p,q} \) is empty if and only if \( (\frac{3}{q}) = 1 \) and \( (\frac{q}{13}) = (-1)\frac{q+1}{12} \). This proves Corollary 3.

**Algorithm 1**: Verifying the criterion in Theorem 1 for specific primes \( p, q \)

- **input**: primes \( p, q \) such that \( p > 7 \) and \( q = np + 1 \)
- **output**: true if criterion of Theorem 1 is satisfied for \( p, q \); false otherwise
- if \( a_q(E_0)^2 \equiv 4 \pmod{p} \) then
  - return false;
- end
- forall \( \zeta \in \mu_n(\mathbb{F}_q^\times) \) do
  - if \( \zeta + \frac{1}{2}U = U^2 \) and \( p \mid a_q(E_\zeta)^2 - a_q(E_0)^2 \) then
    - return false
  - end
- end
- return true;
ON THE EQUATION $s^2 + y^p = \alpha^3$

Acknowledgements

I would like to thank M. Bennett and N. Bruin for useful discussions. I would also like to thank the referee for suggestions which simplified the criterion and improved its computational efficiency.

References


Department of Mathematics, Simon Fraser University, Burnaby, B.C., Canada V5A 1S6 E-mail address: ichen@math.sfu.ca