LOWER BOUNDS FOR THE SOLUTIONS
IN THE SECOND CASE OF FERMAT'S LAST THEOREM

LE MAOHUA

Abstract. Let \( p \) be an odd prime. In this paper, we prove that if \( p \equiv 3 \pmod{4} \) and \( x, y, z \) are integers satisfying \( x^p + y^p = z^p, \ p | xyz, \ 0 < x < y < z, \) then \( y > 2^{-1/p} p^{6p-2} \) and \( z - x > \frac{1}{2} p^{6p-3} \).

Let \( p \) be an odd prime. In [1] and [2], Inkeri showed that if \( x, y, z \) are integers satisfying

\[
\begin{align*}
\text{(1)} \quad & x^p + y^p = z^p, \quad \gcd(x, y) = 1, \ p | xyz, \ 0 < x < y < z, \\
\end{align*}
\]

then \( y > \frac{1}{2} p^{3p-1} \) and \( z - x > (2p^{20/7})^p \). In this paper, we prove the following result:

Theorem. If \( p \equiv 3 \pmod{4} \) and \( x, y, z \) are integers satisfying (1), then \( y > 2^{-1/p} p^{6p-2} \) and \( z - x > \frac{1}{2} p^{6p-3} \).

Proof. It is a well-known fact that (1) is impossible for \( p = 3 \), so we may assume that \( p > 3 \). We first deal with the case that \( p | z \). Let \( \zeta \) be a \( p \)-th primitive root of 1. Let \( S \) be the set of nonzero squares \( \pmod{p} \), and let \( \theta = \prod_{i \in S} (x + y \zeta^i) \). Since \( S \) represents \( \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{-p})) \), it follows that \( \theta \) is an algebraic integer in \( \mathbb{Q}(\sqrt{-p}) \), so \( \theta = A + B \sqrt{-p} \), where \( A, B \in \mathbb{Z} \). Note that \( \theta_0 = \prod_{i \in S} (1 - \zeta^i) \) is an algebraic integer in \( \mathbb{Q}(\sqrt{-p}) \) with norm \( p \); hence, it must be \( \pm \sqrt{-p} \). From

\[
\theta \equiv \begin{cases} 
\theta_0 = \pm \sqrt{-p} \pmod{2}, & 2 \nmid x, \ 2 \nmid y, \\
\prod_{i \in S} 1 = 1 \pmod{2}, & 2 \nmid x, \ 2 | y, \\
\prod_{i \in S} \zeta^i = 1 \pmod{2}, & 2 | x, \ 2 \nmid y, 
\end{cases}
\]

we find that \( A + B \sqrt{-p} \) is congruent modulo 2 to an element of \( \mathbb{Z}(\sqrt{-p}) \), so \( A, B \in \mathbb{Z} \). Further, since

\[
\theta \equiv \prod_{i \in S} (x - x \zeta^i) = 0 \pm x^{(p-1)/2} \sqrt{-p} \pmod{x + y},
\]

Received by the editors November 11, 1989 and, in revised form, March 27, 1990. 1980 Mathematics Subject Classification (1985 Revision). Primary 11D41.
we get
\[ A \equiv 0 \pmod{x+y}. \]

Let \( p^a \mid z \). Classical relations due to Abel [4, p. 54] imply that
\[ \begin{align*}
& x + y = p^{\alpha p - 1} d^p, \quad \frac{x^p + y^p}{x + y} = p b^p, \quad z = p^a \cdot a b,
\end{align*} \]
where \( a, b \) are positive integers satisfying \( p \nmid ab \) and \( 2 \nmid b \). From the above, we have \( p b^p = A^2 + p B^2 \). Hence \( p \mid A, p \nmid B \), and
\[ b^p = p A' + B^2, \]
where \( A' = A/p \). By (2) and (3), we get
\[ A' \equiv 0 \pmod{p^a - 2}. \]

The factors \( x + y \zeta^i \) are pairwise relatively prime for \( 1 \leq i \leq p-1 \), except for factors of \( 1 - \zeta \). Therefore \( \prod_{i \in S} (x + y \zeta^i) = A + B \sqrt{-p} \) and \( \prod_{i \in S} (x + y \zeta^i) = A - B \sqrt{-p} \) are relatively prime, except for primes above \( p \). Recall that \( p \nmid B \).

We have \( \gcd(A, B) = 1 \). It also follows that \( A' \sqrt{-p} + B \) and \( A' \sqrt{-p} - B \) are relatively prime in \( \mathbb{Z}[\rho] \), where \( \rho = (-1 + \sqrt{-p})/2 \). Hence they are \( p \)th powers of ideals. Since the class number of \( \mathbb{Z}[\rho] \) is less than \( p \), it is prime to \( p \). Therefore \( A' \sqrt{-p} + B \) is the \( p \)th power of a number in \( \mathbb{Z}[\rho] \). It implies that
\[ (6) \]
\[ A' \sqrt{-p} + B = (X_1 + Y_1 \sqrt{-p})^p, \]
where \( X_1, Y_1 \in \frac{1}{2} \mathbb{Z} \). If \( X_1 + Y_1 \sqrt{-p} \notin \mathbb{Z}(\sqrt{-p}) \), then \( X_1 = u/2, \ Y_1 = v/2 \), with \( u, v \in \mathbb{Z} \) and \( u \equiv v \equiv 1 \pmod{2} \). By Waring’s formula [3, Formula 1.76], we get from (4) and (6) that \( u^2 + p v^2 = 4b \) and
\[ 2B = \left( \frac{u + v \sqrt{-p}}{2} \right)^p + \left( \frac{u - v \sqrt{-p}}{2} \right)^p \]
\[ = \sum_{j=0}^{(p-1)/2} (-1)^j \frac{(p - j - 1)!}{(p - 2j)! j!} u^{p - 2j} b^j \equiv \sum_{j=0}^{(p-1)/2} (-1)^j \frac{(p - j - 1)!}{(p - 2j)! j!} \]
\[ = \left( \frac{1 + \sqrt{5}}{2} \right)^p + \left( \frac{1 - \sqrt{5}}{2} \right)^p = L_p \pmod{2}, \]
where \( L_p \) is the \( p \)th Lucas number. Since \( L_p \equiv 0 \pmod{2} \) only if \( p = 3 \), it follows that \( X_1 + Y_1 \sqrt{-p} \notin \mathbb{Z}(\sqrt{-p}) \), and
\[ (7) \]
\[ X_1^2 + p Y_1^2 = b, \quad X_1, Y_1 \in \mathbb{Z}. \]

We get from (6) that
\[ (8) \]
\[ A' = \binom{p}{1} X_1^{p-1} Y_1 - \binom{p}{3} p X_1^{p-3} Y_1^3 + \cdots + (-1)^{(p-1)/2} \binom{p}{p} p^{(p-1)/2} Y_1^p. \]
Since \( p \nmid b \), we have \( p \nmid X_1 \) by (7), and hence

\[
Y_1 \equiv 0 \pmod{p^{\alpha p-3}}
\]

by (5) and (8). If \( Y_1 = 0 \), then \( A = 0, B = \pm 1 \), and \( b = 1 \) by (4). Since \( (x^p + y^p)/(x+y) \geq 2^{p-2} + 1 \), it is impossible that \( p > 3 \). Therefore \( Y_1 \neq 0 \) and \( |Y_1| > p^{\alpha p-3} \) by (9), and \( z = p^\alpha ab > p^{2\alpha p + \alpha - 5} \) by (7). Note that \( \alpha \geq 3 \), by [5]. We obtain \( z > p^{6p-2} \). Using the same method, we can prove that \( y > p^{6p-2} \) or \( x > p^{6p-2} \) correspond to \( p | y \) or \( p | x \). Thus \( y > 2^{-1/p} p^{6p-2} \) since \( 2^{1/p} y > z \).

Simultaneously, we have

\[
z - x = \frac{y^p}{z^{p-1} + xz^{p-2} + \cdots + x^{p-1}} > \frac{y^p}{pz^{p-1}} > \frac{y^p}{p(2^{1/p} y)^{p-1}}
\]

\[
= \frac{y}{2^{p-1/p} p} > \frac{1}{2} p^{6p-3}.
\]

The theorem is proved.

ACKNOWLEDGMENT

The author would like to thank the referee for his valuable suggestions.

REFERENCES


Research Department, Changsha Railway Institute, Changsha, Hunan, People’s Republic of China