PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 111, Number 4, April 1991

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

LE MAOHUA

(Communicated by William Adams)

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

$$(1) \qquad x^p + y^p = z^p, \qquad \gcd(x, y) = 1, \ p|xyz, \ 0 < x < y < z,$$

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 ζ be a pth primitive root of 1. Let S be the set of nonzero squares $\bmod p$, and let $\theta = \prod_{i \in S}(x + y\zeta^i)$. Since S represents $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{-p}))$, it follows that θ is an algebraic integer in $\mathbb{Q}(\sqrt{-p})$, so $\theta = A + B\sqrt{-p}$, where $A, B \in \frac{1}{2}\mathbb{Z}$. Note that $\theta_0 = \prod_{i \in S}(1 - \zeta^2)$ 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

$$A \equiv 0 \pmod{x+y}. \tag{2}$$

Let $p^\alpha \| z$. Classical relations due to Abel [4, p. 54] imply that

$$x+y = p^{\alpha p-1}a^p, \qquad \frac{x^p+y^p}{x+y} = pb^p, \qquad z = p^\alpha ab, \tag{3}$$

where a, b are positive integers satisfying $p \nmid ab$ and $2 \nmid b$. From the above, we have $pb^p = A^2 + pB^2$. Hence $p|A$, $p \nmid B$, and

$$b^p = pA'^2 + B^2, \tag{4}$$

where $A' = A/p$. By (2) and (3), we get

$$A' \equiv 0 \pmod{p^{\alpha p-2}}. \tag{5}$$

The factors $x+y\zeta^i$ are pairwise relatively prime for $1 \le i \le p-1$, except for factors of $1-\zeta$. Therefore $\prod_{i\in S}(x+y\zeta^i) = A + B\sqrt{-p}$ and $\prod_{i\notin S}(x+y\zeta^i) = A - B\sqrt{-p}$ 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 pth 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 pth power of a number in $\mathbb{Z}[\rho]$. It implies that

$$A'\sqrt{-p} + B = (X_1 + Y_1\sqrt{-p})^p, \tag{6}$$

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 $u^2 + pv^2 = 4b$ and

$$\begin{aligned} 2B &= \left(\frac{u+v\sqrt{-p}}{2}\right)^p + \left(\frac{u-v\sqrt{-p}}{2}\right)^p \\ &= \sum_{j=0}^{(p-1)/2} (-1)^j \frac{(p-j-1)!p}{(p-2j)!j!} u^{p-2j} b^j \equiv \sum_{j=0}^{(p-1)/2} (-1)^j \frac{(p-j-1)!p}{(p-2j)!j!} \\ &= \left(\frac{1+\sqrt{5}}{2}\right)^p + \left(\frac{1-\sqrt{5}}{2}\right)^p = L_p \pmod 2, \end{aligned}$$

where L_p is the pth Lucas number. Since $L_p \equiv 0 \pmod 2$ only if $p = 3$, it follows that $X_1 + Y_1\sqrt{-p} \in \mathbb{Z}[\sqrt{-p}]$, and

$$X_1^2 + pY_1^2 = b, \qquad X_1, Y_1 \in \mathbb{Z}. \tag{7}$$

We get from (6) that

$$A' = \binom{p}{1} X_1^{p-1} Y_1 - \binom{p}{3} p X_1^{p-3} Y_1^3 + \cdots + (-1)^{(p-1)/2} \binom{p}{p} p^{(p-1)/2} Y_1^p. \tag{8}$$

Since $p \nmid b$, we have $p \nmid X_1$ by (7), and hence

$$Y_1 \equiv 0 \pmod{p^{\alpha p-3}} \tag{9}$$

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

$$\begin{aligned} z - x &= \frac{y^p}{z^{p-1} + xz^{p-2} + \cdots + x^{p-1}} > \frac{y^p}{pz^{p-1}} > \frac{y^p}{p(2^{1/p}y)^{p-1}} \\ &= \frac{y}{2^{p-1/p}p} > \frac{1}{2}p^{6p-3}. \end{aligned}$$

The theorem is proved.

Acknowledgment

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

References

1. K. Inkeri, *Abschätzungen für eventuelle Lösungen der Gleichung im Fermatschen Problem*, Ann. Univ. Turku, 1953, 3–9.
2. ——, *Remarks on Fermat's equation: The very knowledge of coding*, Univ. Turku, Turku, 1987, pp. 82–87.
3. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.
4. P. Ribenboim, 13 *lectures on Fermat's last theorem*, Springer-Verlag, New York, 1979.
5. H. Vandiver, *A property of cyclotomic integers and its relation to Fermat's last theorem*, Ann. of Math. **21** (1919), 73–80.

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