53. On the Generalized Wieferich Criteria

By Jiro SUZUKI

School of Allied Medical Sciences, Shinshu University

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1994)

Abstract: If $x^p + y^p + z^p = 0$, $(p, xyz) = 1$ has a solution, then $a^{p-1} \equiv 1 \pmod{p^2}$ for $a \leq 113$.

0. Introduction. Let p be an odd prime. Throughout this paper we assume that there exists a solution of Fermat's equation $x^p + y^p + z^p = 0$ such that $(p, xyz) = 1$. Then $a^{p-1} \equiv 1 \pmod{p^2}$ holds for $a = 2$. This is known as the Wieferich criterion. This criterion has been extended for $a \leq 31$[5], $a \leq 89$[2]. In this paper, we shall extend it up to $a \leq 113$, which implies: if we have a solution (x, y, z) such that $(p, xyz) = 1$, then we can get $p > 8.858 \times 10^{20}$[1].

Let $A = \left\{-\frac{x}{y}, -\frac{y}{x}, -\frac{y}{z}, -\frac{z}{y}, -\frac{z}{x}, -\frac{x}{z} \pmod{p}\right\}$ for a solution of $x^p + y^p + z^p = 0$, $(p, xyz) = 1$. Let t be any element of A. Then

$$A = \left\{t, \frac{1}{t}, 1 - t, \frac{1}{1-t}, \frac{t-1}{t}, \frac{t}{t-1} \pmod{p}\right\}.$$

There are two possibilities:

(a) $A = \{-1, 2, 1/2 \pmod{p}\}$

(b) A has six elements.

When $(m, h) = 1$, then for any n, there exists a unique solution u for $hu \equiv n \pmod{m}$ such that $0 < u \leq m$. Let $g_h^{m,n}(X) = X^{u-1}$ and $G_h(X)$ be the $2\varphi(h) \times \varphi(h)$ matrix $(g_h^{m,n}(X))_{1 \leq m < 2h, 1 \leq n < h, (m,h) = (n,h) = 1}$. Let I be a $\varphi(h)$-ple $(m_1, m_2, \ldots, m_{\varphi(h)})$ such that $1 \leq m_i < 2h$, $(m_i, h) = 1$, $m_i \neq m_j$ $(i \neq j)$ and $G_h^I(X)$ be the submatrix of $G_h(X)$ by choosing $m_1, m_2, \ldots, m_{\varphi(h)}$ as m. Then Pollaczek [5] proved the following theorem:

Theorem. *Suppose there exists $t \in A$ such that $t^{a-1} \not\equiv 1 \pmod{p}$. For any h with $3 \leq h \leq (a-1)/2$ if it is possible to find a $\varphi(h)$-ple I (depending on t and h) such that $G_h^I(t) \not\equiv 0 \pmod{p}$ then we have $a^{p-1} \equiv 1 \pmod{p^2}$.*

We could verify the existence of t and I for every h, $3 \leq h \leq (a-1)/2$ as referred above for all $a \leq 113$ by computation. We shall describe our method of computation in two stages. We first treat the case $|A| = 3$ in §1. Secondly, we treat the case $|A| = 6$ in §2. The case $|A| = 6$ needs large amount of computation.

1. The case $|A| = 3$. When $A = \{-1, 2, 1/2 \pmod{p}\}$, we choose 2 as t. Let $1 = m_1 < m_2 < \cdots < m_{\varphi(h)} = h - 1$, $I_1 = (m_1, m_2, \ldots, m_{\varphi(h)})$ and $I_2 = (m_1, m_2, \ldots, m_{\varphi(h)-1}, h + 1)$. For example, in the case $h = 53$, we get the following result:

$\gcd(\det G_{53}^{I_1}(2), \det G_{53}^{I_2}(2)) =$ (168 digits number) =