# 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) $=$

$3^{58}\cdot 5^{12}\cdot 7^{17}\cdot 11^{4}\cdot 13^{3}\cdot 17^{5}\cdot 19\cdot 23^{3}\cdot 31^{9}\cdot 41\cdot 43^{2}\cdot 47\cdot 73^{4}\cdot 89^{3}\cdot 127^{6}\cdot$
$151^{2}\cdot 241\cdot 257^{2}\cdot 337\cdot 601\cdot 683\cdot 1801\cdot 8191^{2}\cdot 131071^{2}\cdot 178481\cdot 524287.$

Likewise we factorize gcd ($\det G_h^{I_1}(2)$, $\det G_h^{I_2}(2)$) for all $3 \le h \le 56 = (113-1)/2$, and list the prime factors $3,5,7,\ldots$, for any one $q$ of which we verify $2^{q-1} \not\equiv 1 \pmod{q^2}$. This means that $x^q + y^q + z^q = 0$, $(xyz, q) = 1$ has no solution, and thus $\det G_h^{I_1}(2)$ or $\det G_h^{I_2}(2) \not\equiv 0 \pmod{p}$. If $2^{a-1} = 1 + kp$ for some $k \in \boldsymbol{Z}$, then using the Wieferich criterion we have $1 \equiv (2^{a-1})^{p-1} \equiv 1 + (p-1)kp \pmod{p^2}$. So we have $2^{a-1} \equiv 1 \pmod{p^2}$. How ever it is easily shown that this never happens for, say, any $a \le 200$, by using Lehmer's computation [4]. Therefore we have $2^{a-1} \not\equiv 1 \pmod{p}$. Now we can use the theorem and we get $a^{p-1} \equiv 1 \pmod{p^2}$.

**2. The case** $|A| = 6$. When $A$ has six elements, Pollaczek [5] and Gunderson [3] proved

(1) $$t(t-1)(t+1)(t^2+t+1)(t^2+1)(t^2-t+1) \not\equiv 0 \pmod{p}.$$

Before computing $\det G_h^I(X)$ we can obtain some factors of $\det G_h^I(X)$. For example, when $h = 53$, $X^{26} - 1$ divides $g_{53}^{52,n}(X) - g_{53}^{26,n}(X)$. This fact is explained by the following lemma [2, Lemma 28]:

**Lemma.** *Let $l \mid m$. Then $X^l - 1$ divides*

(2) $$g_h^{m,n}(X) - g_h^{l,n}(X).$$

*Let $k \mid m$, $l \mid m$ and $e \equiv l \pmod{k}$. Then $(X^k - 1)(X^l - 1)$ divides*

(3) $$(X^e - 1)g_h^{m,n}(X) - (X^l - 1)g_h^{k,n}(X) + (X^l - X^e)g_h^{l,n}(X)$$

*and*

(4) $$(1 - X^{k-e})g_h^{m,n}(X) - (X^{l+k-e} - X^{k-e})g_h^{k,n}(X) + (X^{l+k-e} - 1)g_h^{l,n}(X).$$

Let $m = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of $m$ such that $p_1 < p_2 < \cdots < p_r$. When $r = 1$, we use (2) as $l = m/p_1$. When $r > 1$, we use (3) or (4) as $l = m/p_1$, $k = m/p_2$, $0 < e < k$. Namely we define $f_h^{m,n}(X)$ as follows:

$$f_h^{m,n}(X) = \begin{cases} 1 & \text{if } m = 1, \\ (2)/(X^l - 1) & \text{if } r = 1, \\ (3)/(X^l - 1)(X^k - 1) & \text{if } r > 1 \text{ and } e \le k - e, \\ (4)/(X^l - 1)(X^k - 1) & \text{if } r > 1 \text{ and } e > k - e. \end{cases}$$

Clearly, the degree of $f_h^{m,n}(X)$ is at most $d(m)$ where

$$d(m) = \begin{cases} 0 & \text{if } m = 1, \\ m - 1 - l & \text{if } r = 1, \\ m - 1 - l - \max(k - e, e) & \text{if } r > 1. \end{cases}$$

We use the matrix $F_h(X) = (f_h^{m,n}(X))_{1 \le m < 2h, 1 \le n < h, (m,h)=(n,h)=1}$ instead of $G_h(X)$. We define $F_h^I(X)$ similarly as $G_h^I(X)$.

The theorem in §0 is also correct if we replace $G_h^I(t)$ by $F_h^I(t)$ ([2, Theorem 5]).

Let $\Phi_m(X)$ be the $m$-th cyclotomic polynomial. When $\det F_h^I(X)$ is calculated. we devide $\det F_h^I(X)$ by $X$ and $\Phi_m(X)$, $1 \le m < 2h$, as far as possible. Let $C_h^I(X)$ be the product of all possible such factors. Then we get $Q_h^I(X) = \det F_h^I(X) / C_h^I(X)$. For example when $h = 53$,

$I_1 = (1,2,3,4,6,5,8,10,12,7,9,14,18,15,16,20,24,11,22,30,13,21,26,28,36,$

42,17,32,34,40,48,19,27,38,54,25,33,44,50,60,23,46,66,39,45,52, 56,72,35,78,29,58)

$I_2 = (\ldots, 29,70)$, $I_3 = (\ldots, 58,84)$, $I_4 = (\ldots, 29,70)$, $I_5 = (\ldots, 58,84)$.

$I_i$ have been chosen as follows: Let $S_h = \{m\,;\, (m, h) = 1,\ 1 \le m \le 2h - 1\}$. We number $m \in S_h$ such that $d(m_j) < d(m_{j+1})$ or $d(m_j) = d(m_{j+1})$, $m_j < m_{j+1}$. Then

$I_1 = \{m_1, m_2, \ldots, m_{\varphi(h)-2}, m_{\varphi(h)-1}, m_{\varphi(h)}\}$,

$I_2 = \{\ldots, m_{\varphi(h)-2}, m_{\varphi(h)-1}, m_{\varphi(h)+1}\}$, $I_3 = \{\ldots, m_{\varphi(h)-2}, m_{\varphi(h)-1}, m_{\varphi(h)+2}\}$,

$I_4 = \{\ldots, m_{\varphi(h)-2}, m_{\varphi(h)}, m_{\varphi(h)+1}\}$, $I_5 = \{\ldots, m_{\varphi(h)-2}, m_{\varphi(h)}, m_{\varphi(h)+2}\}$.

Then we have

$$\begin{aligned} C_{53}^{I}(X) :\ & X^{17}\Phi_1(X)^{37}\Phi_2(X)^{38}\Phi_3(X)^4\Phi_4(X)^6\Phi_6(X)^8\Phi_{12}(X) \text{ for } I = I_1 \\ & X^{16}\Phi_1(X)^{37}\Phi_2(X)^{38}\Phi_3(X)^3\Phi_4(X)^6\Phi_6(X)^7\Phi_{10}(X)\Phi_{12}(X) \text{ for } I = I_2 \\ & X^{17}\Phi_1(X)^{37}\Phi_2(X)^{38}\Phi_3(X)^3\Phi_4(X)^7\Phi_6(X)^7\Phi_{10}(X)\Phi_{12}(X) \text{ for } I = I_3 \\ & X^{15}\Phi_1(X)^{35}\Phi_2(X)^{36}\Phi_3(X)^4\Phi_4(X)^6\Phi_6(X)^8\Phi_{12}(X)^2 \text{ for } I = I_4 \\ & X^{16}\Phi_1(X)^{35}\Phi_2(X)^{36}\Phi_3(X)^4\Phi_4(X)^7\Phi_6(X)^8\Phi_{12}(X)^2 \text{ for } I = I_5. \end{aligned}$$

Degrees of $Q_{53}^{I}(X)$ : 528 for $I = I_1, I_5$, 530 for $I = I_2$, 526 for $I = I_3$, 532 for $I = I_4$. Let $R_h(I_i, I_j)$ be the resultant of $Q_h^{I_i}(X)$ and $Q_h^{I_j}(X)$. Then

$$\begin{aligned} & R_{53}(I_1, I_2) = (28087 \text{ digits number}), \text{ but} \\ & \gcd(R_{53}(I_1, I_2), R_{53}(I_2, I_3), R_{53}(I_4, I_5)) \\ & = 320410393 = 4889 \cdot 65537. \end{aligned}$$

Let $q$ be a prime factor of the above gcd. We can verify $2^{q-1} \not\equiv 1 \pmod{q^2}$. Therefore $q \ne p$ and for any $t \in A$ we have $Q_{53}^{I_i}(t) \not\equiv 0 \pmod p$ for some $I_i (i = 1, \ldots, 5)$. A list of results of factorization of gcd of $R_h(I_i, I_j)$ is appended below.

Let $S = \{k : k \ne 6, 5 \le k,\ \Phi_k(X) \text{ divides } C_h^{I_i}(X) \text{ for some } h (3 \le h \le 56) \text{ and } I_i (1 \le i \le 5)\}$. Let $T_{k,l}$ be the resultant of $\Phi_k(X)$ and $\Phi_l(1 - X)$. Let $q$ be a prime factor of some $T_{k,l}$, $k, l \in S$. We can verify $2^{q-1} \not\equiv 1 \pmod{q^2}$. Therefore $q \ne p$ and $T_{k,l} \not\equiv 0 \pmod p$ for any $k, l \in S$. If there exists $k \in S$ and $t \in A$ such that $\Phi_k(t) \equiv 0 \pmod p$, then we have $\Phi_l(1/(1 - t)) \not\equiv 0 \pmod p$ and $\Phi_l(1 - 1/(1 - t)) \not\equiv 0 \pmod p$ for any $l \in S$, because

$$\Phi_k(t) \equiv 0 \ \Leftrightarrow \Phi_l(1 - t) \not\equiv 0 \ \Leftrightarrow \Phi_l\left(\frac{1}{1 - t}\right) \not\equiv 0$$

$$\Leftrightarrow \Phi_k\left(\frac{1}{t}\right) \equiv 0 \Leftrightarrow \Phi_l\left(1 - \frac{1}{t}\right) \not\equiv 0 \Leftrightarrow \Phi_l\left(\frac{t}{t - 1}\right) \not\equiv 0 \pmod p.$$

Therefore there exists $t \in A$ such that $\Phi_k(t) \not\equiv 0 \pmod p$ and $\Phi_k(1 - t) \not\equiv 0 \pmod p$ for any $k \in S$. Using (1), this is also valid for $k \in \{1,2,3,4,6\}$. We can factorize $T_{k,l}$ easily (see the Table III of [2] for $k, l \le 109$).

Let $U = \{a - 1\,;\, a : \text{prime},\ a \le 113\}$. Let $v_k(X) = (X^k - 1)/(X^6 - 1)$ if $k \equiv 0 \pmod 6$, $v_k(X) = X^k - 1$ otherwise. Let $V_k$ be the resultant of $v_k(X)$ and $v_k(1 - X)$. Let $q$ be a prime factor of some $V_k$, $k \in U$. We can verify $2^{q-1} \not\equiv 1 \pmod{q^2}$. Therefore $V_k \not\equiv 0 \pmod p$ and for any $t \in A$ and for any prime $a \le 113$, we have $t^{a-1} \not\equiv 1 \pmod p$ or $(1 - t)^{a-1} \not\equiv 1 \pmod p$ because of (1).

Now we can use also in this case the theorem in §0. First of all there exists $t \in A$ such that $\Phi_k(t) \not\equiv 0 \pmod p$ and $\Phi_k(1-t) \not\equiv 0 \pmod p$ for any $k \in S \cup \{1,2,3,4,6\}$. We fix $a \leq 113$. If $t^{a-1} \equiv 1 \pmod p$ then we use $1-t$ instead of $t$. So there exists $t \in A$ such that $\Phi_k(t) \not\equiv 0 \pmod p$ and $t^{a-1} \not\equiv 1 \pmod p$. For this $t$ and for any $h (3 \leq h \leq 56)$ there exists $I_i$ such that $Q_h^{I_i}(t) \not\equiv 0 \pmod p$. Hence we have $\det F_h^{I_i}(t) \not\equiv 0 \pmod p$ and finally we get $a^{p-1} \equiv 1 \pmod{p^2}$ for any $a \leq 113$. We can see some of large factors of $V_k$ for $k \in U$, in Table III of [2].

We implemented the program for the above computation in FORTRAN on a HITAC S-820/80 at Computer Centre University of Tokyo. In case $h = 53$, where $\varphi(h)$ is maximal for $3 \leq h \leq 56$, we have obtained five polynomials $Q_{53}^{I_i} (i = 1, \ldots, 5)$ within about 120 seconds.

**Table** $\gcd(R_h(I_1, I_2), R_h(I_2, I_3), R_h(I_4, I_5), R_h(I_5, I_1))$ $(h \leq 44)$
$\gcd(R_h(I_1, I_2), R_h(I_2, I_3), R_h(I_4, I_5))$ $(h \geq 45)$

For $3 \leq h \leq 10$, $h = 12$, $h = 14$, we can find $Q_h^{I_i}(t) = 1$ for some $I_i$.

| $h$ | factorization |
|---|---|
| 11 | $(5^2)^2$ |
| 13 | $(2^5 \cdot 3 \cdot 19^2)^2$ |
| 15 | $(2^2)^2$ |
| 16 | $(3^2 \cdot 5)^2$ |
| 17 | $(5^3 \cdot 73)^2$ |
| 18 | $7^2$ |
| 19 | $(2^{13} \cdot 3^5 \cdot 7)^2$ |
| 20 | $1$ |
| 21 | $13^4$ |
| 22 | $(2^5 \cdot 5^2 \cdot 11 \cdot 31)^2$ |
| 23 | $(2^3 \cdot 3 \cdot 7 \cdot 11^3)^4$ |
| 24 | $(3^2 \cdot 13)^2$ |
| 25 | $2^{36}$ |
| 26 | $(2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 19^2 \cdot 73 \cdot 769)^2$ |
| 27 | $1$ |
| 28 | $(2^6 \cdot 3^2 \cdot 5 \cdot 7^3 \cdot 11^2 \cdot 13^2)^2$ |
| 29 | $(2^{62} \cdot 3^3 \cdot 7^6)^2$ |
| 30 | $(2 \cdot 5)^4$ |
| 31 | $(2^7 \cdot 3^7 \cdot 5^2)^4$ |
| 32 | $(3^2 \cdot 17)^6$ |
| 33 | $(2^{13} \cdot 5)^2$ |
| 34 | $(2^{13} \cdot 3^8 \cdot 5^5 \cdot 19)^2$ |
| 35 | $(2^{21} \cdot 3^4 \cdot 13^2)^2$ |
| 36 | $(7 \cdot 13^3 \cdot 19 \cdot 31 \cdot 79)^2$ |
| 37 | $(2^{14} \cdot 3^{29} \cdot 7^6 \cdot 19^8 \cdot 37^2)^2$ |
| 38 | $(2^4 \cdot 3^{14} \cdot 7 \cdot 19^5 \cdot 73 \cdot 487)^2$ |
| 39 | $(2^6 \cdot 3^{14} \cdot 5^3 \cdot 13^2 \cdot 19^2 \cdot 37^2)^2$ |
| 40 | $(2^2 \cdot 5^2 \cdot 7 \cdot 41^2)^2$ |
| 41 | $(2^{62} \cdot 3^6 \cdot 5^9 \cdot 11^{11})^2$ |

| $h$ | factorization |
|---|---|
| 42 | $(2\cdot 3^8\cdot 5^6\cdot 7^5\cdot 13^4)^2$ |
| 43 | $(2^{17}\cdot 3^6\cdot 5^2\cdot 7^{10}\cdot 29^2\cdot 211^2)^2$ |
| 44 | $(2^8\cdot 3^8\cdot 5^4\cdot 7\cdot 11^4\cdot 23^2\cdot 29\cdot 31^6\cdot 101\cdot 641\cdot 15641)^2$ |
| 45 | $(2^{12}\cdot 3^3\cdot 5\cdot 7\cdot 11)^4$ |
| 46 | $(2^5\cdot 3^4\cdot 11^4\cdot 23^2\cdot 67\cdot 89\cdot 37181)^2$ |
| 47 | $(2^{12}\cdot 3\cdot 5^2\cdot 11\cdot 17\cdot 23^{18}\cdot 139^4)^2$ |
| 48 | $3^2\cdot 13$ |
| 49 | $(2^9\cdot 3\cdot 43^2)^2$ |
| 50 | $(3^4\cdot 11^3\cdot 23\cdot 29\cdot 31\cdot 47)^2$ |
| 51 | $(2^{33}\cdot 3^3\cdot 5^2)^4$ |
| 52 | $(2^4\cdot 3^4\cdot 5^4\cdot 7^3\cdot 13^4\cdot 19^2\cdot 73\cdot 769)^2$ |
| 53 | $4889\cdot 65537$ |
| 54 | $(7\cdot 17\cdot 19\cdot 37\cdot 73\cdot 271\cdot 307)^2$ |
| 55 | $(2^{73}\cdot 3^6\cdot 5^9\cdot 11^{11}\cdot 19)^2$ |
| 56 | $(2^8\cdot 3^3\cdot 5^5\cdot 7\cdot 11^4\cdot 13^8\cdot 43\cdot 73)^2$ |

## References

[1] Coppersmith, D.: Fermat's last theorem (case 1) and the Wieferich criterion. Math. Comp., **54**, 895–902 (1990).

[2] Granville, A., and Monagan, B.: The first case of Fermat's last theorem is true for all prime exponents up to **714,591,416,091,389**. Trans. Amer. Math. Soc., **306**, 329–359 (1987).

[3] Gunderson, N. G.: Derivation of criteria for the first case of Fermat's last theorem and the combination of these criteria to produce a new lower bound for the exponent. Thesis. Cornell University (1948).

[4] Lehmer, D. H.: On Fermat's quotient, base two. Math. Comp., **36**, 289–290 (1981).

[5] Pollaczek, F.: Über den grössen Fermat'schen Satz. Wien. Berichte. Abt. IIa, **126**, 45–59 (1917).

[6] Suzuki, J.: On the generalized Wieferich criteria for the first case of Fermat's last theorem (in preparation).