Theorem 1. *Let p, q, be odd primes and $x, y \in \mathbb{Z}$ non-zero such that $x^p - y^q = 1$. Then*

$$p^{q-1} \equiv 1 \left(mod\ q^2\right), \tag{1}$$
$$q^{p-1} \equiv 1 \left(mod\ p^2\right).$$

A pair of primes as (1) is a Wieferich pair.

(Wieferich) If $x^p + y^p = z^p$, $p \nmid xyz$, then

$$2^{p-1} \equiv 1 \left(\text{mod } p^2\right).$$

Let be $q_2(p) = \frac{2^{p-1}-1}{p}$. Then

$$P[q_2(p) \equiv 0 \,(\mathrm{mod}\ p)] \approx \frac{1}{p}$$

$$\sum_{p \leq x} \frac{1}{p} \sim \log \log x$$

Wieferich primes known, 1093, 3511.

Wieferich pairs known,

$(2, 1093)$, $(3, 1006003)$, $(5, 1645333507)$,
$(83, 4871)$, $(911, 318917)$, $(2903, 18787)$.

There are no Wiefereich pairs (p, q) such that $p \equiv 1 \,(\mathrm{mod}\ q)$, $q < p < 4q^2$

(Cassels) Let $x^p - y^q = 1$, p, q odd primes, $xy \neq 0$. Then $p|y$, $q|x$ and

$$x - 1 = p^{q-1}a^q,$$
$$y + 1 = q^{p-1}b^p.$$

Substracting a^q we get

$$x = (p^{q-1} - 1)a^q + a^q + 1,$$

and so $q|a^q + 1$.

Lemma 1. *Let $a, b \in \mathbb{Z}$. If $a^q \equiv b^q \,(mod\ q)$, then $a^q \equiv b^q \left(mod\ q^2\right)$.*

Proof. $a \equiv a^q \equiv b^q \equiv b \,(\text{mod } q)$, so, for any j

$a^j b^{q-1-j} \equiv a^{q-1} \,(\text{mod } q)$ and

$$a^q - b^q = (a-b)\sum_{j=0}^{q-1} a^j b^{q-1-j} \equiv 0 \left(\text{mod } q^2\right).$$

Lemma 2. *(Rule of Lifting the Exponent) Let R be a commutative ring. q an odd prime such that R/qR without nilpotents. Then*

If $a^q \equiv b^q \,(mod\ qR)$ *then* $a^q \equiv b^q \left(mod\ q^2R\right).$

Proof. Apply binomial theorem in R to get

$$(a-b)^q \equiv a^q - b^q \,(\text{mod } qR).$$

If $a^q \equiv b^q \,(\text{mod } qR)$ then $a \equiv b \,(\text{mod } qR).$

In the conditions of Theorem 1, $q|a^q+1$ and so $q^2|a^q+1$

Lemma 3. $q^2|x \Leftrightarrow p^{q-1} \equiv 1 \left(mod\ q^2\right)$

Theorem 2. *Let p, q, be odd primes and $x, y \in \mathbb{Z}$ non-zero such that $x^p - y^q = 1$. Then*

$$q^2 | x.$$

Inkery (1990). Let $h_p = |Cl\mathbb{Q}(\zeta_p)|$. If $p \nmid h_q$ and $q \nmid h_p$, then (p, q) is Wieferich.

Mignotte, Roy, O'Neil, Schwarz, Steiner (1998)

If $x^p - y^q = 1$ is a non-trivial solution and $p \not\equiv 1 \pmod 4$ or $q \not\equiv 1 \pmod 4$, then (p, q) is a Wieferich pair.

For any non-trivial solution $x^p - y^q = 1$, we know $x - 1 = p^{q-1}a^q$. Hence

$$\frac{x^p - 1}{x - 1} = pb^q,$$

and so, since

$$1 + x + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1} = \prod_{i=1}^{p-1} \left(x - \zeta_p^i\right),$$

we have

$$p = \prod_{i=1}^{p-1} \left(1 - \zeta_p^i\right) \text{ and } \prod_{i=1}^{p-1} \left(\frac{x - \zeta_p^i}{1 - \zeta_p^i}\right) = b^q.$$

Lemma 4. *Let $p \nmid i$, $i \in \mathbb{Z}$. Then $1 - \zeta_p^i = \pi\varepsilon$, where $\pi = 1 - \zeta_p$ and $\varepsilon \in \mathbb{Z}[\zeta_p]^*$.*

Proof. ζ_p is an i-th power for any $p \nmid i$.
$(1 \equiv ri \pmod{p})$

Moreover, $x - \zeta_p^i = (x-1) + (1-\zeta_p^i)$ and so

$$v_\pi \left(\frac{x - \zeta_p^i}{1 - \zeta_p^i} \right) = 0.$$

If $\mathfrak{p}| < (x - \zeta_p^i), (x - \zeta_p^j) >$, then

$\mathfrak{p}| < \zeta_p^i, (1 - \zeta_p^{j-i}) >$, and so, $\mathfrak{p} = \pi$.

Lemma 5. $\left\langle \frac{x-\zeta_p^i}{1-\zeta_p^i} \right\rangle = \mathfrak{a}^q$

Let $\theta \in \mathbb{Z}[G]$ that anihilates Cl. Then

$$\left(\frac{x - \zeta_p^i}{1 - \zeta_p^i} \right)^\theta = \varepsilon \alpha^q, \quad \varepsilon \in \mathbb{Z}[\zeta_p]^*.$$

Proof of Theorem 2.

Notation $G = Gal\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right).$

$$\begin{aligned} \tau_a \ : \ \mathbb{Q}(\zeta_p) &\to \mathbb{Q}(\zeta_p) \\ \zeta_p &\to \zeta_p^a. \end{aligned}$$

$\mathfrak{i} = \tau_{-1} \equiv$ conjugation.

$S =< \theta_i >$ Stickelberger ideal, where

$$\theta_i = \sum_{a=1}^{p-1} \left[\frac{ia}{p}\right] \tau_a^{-1},$$

$$I \subset \mathbb{Z}[G], \quad I = (1-\mathfrak{i})S.$$

Remark $(1-\mathfrak{i})\varepsilon = \varepsilon/\bar{\varepsilon}$.

The obstruction subgroup H defined by

$$\{\alpha \in \mathbb{Q}(\zeta_p)^* \ : \ q | v_{\mathfrak{r}}(\alpha), \mathfrak{r} \neq \pi\}/\mathbb{Q}(\zeta_p)^q.$$

If $\theta \in I$, then $(x - \zeta_p)^\theta = \alpha^q$, and multiplying by $(-\zeta_p^{-1})^\theta$, we get

$$(1 - \zeta_p x)^\theta = \beta^q.$$

If $\theta = \sum_{\tau \in G} n_\tau \tau$, then

$$\begin{aligned}\beta^q &= \prod_\tau \left((1 - \zeta_p x)^\tau\right)^{n_\tau} \\ &= \prod_\tau \left((1 - \tau(\zeta_p)x)\right)^{n_\tau} \equiv 1 \,(\mathrm{mod}\ q\mathbb{Z}[\zeta_p])\,.\end{aligned}$$

Lemma 6. *If $q \nmid n$, then $R = \mathbb{Z}[\zeta_n]/q\mathbb{Z}[\zeta_n]$ has no nilpotents.*

Proof. $\alpha^r = q\beta$ in $R, \Rightarrow < \alpha >^r = \mathfrak{q}_1 \ldots \mathfrak{q}_l \mathcal{I}$, where $< q >= \mathfrak{q}_1 \ldots \mathfrak{q}_l$ is not ramified. Hence $< q > \mid < \alpha >$ and so $q\beta = \alpha, \quad \beta \in \mathbb{Z}[\zeta_n]$.

By Lemma 2,

$$\prod_{\tau} \left((1-\tau(\zeta_p)x)\right)^{n_\tau} \equiv 1 \left(\mathrm{mod}\ q^2\mathbb{Z}[\zeta_p]\right),$$

and expanding the product we get

$$1 - \sum_{\tau} n_\tau \tau(\zeta_p)x \equiv 1 \left(\mathrm{mod}\ q^2\mathbb{Z}[\zeta_p]\right).$$

Hence, either $q^2|x$ or

$$\sum_{\tau} n_\tau \tau(\zeta_p) \equiv 0 \left(\mathrm{mod}\ q\mathbb{Z}[\zeta_p]\right)$$

and so $n_\tau \equiv 0 \left(\mathrm{mod}\ q\right) \forall \tau \in G, \theta \in I$.
Recall $\theta_2 = \sum_{a=1}^{p-1} \left[\frac{2a}{p}\right] \tau_a^{-1}$ and consider

$$(1-\mathfrak{i})\theta_2 = \sum_{a=\frac{p+1}{2}}^{p-1} \tau_a^{-1} - \sum_{a=1}^{(p-1)/2} \tau_a^{-1}.$$

Let H' be the subgroup of H defined by

$$\{\alpha \in H \,:\, \alpha \equiv \beta^q \left(\mathrm{mod}\ q^2\right)\}.$$

Corollary. *In conditions of Theorem 1,*

$$x - \zeta_p \in H'.$$

Theorem 3. *In the above conditions, the following are equivalent.*

i) $x - \zeta_p \in H'$.
ii) $q^2 | x$.
iii) $p^{q-1} \equiv 1 \left(mod\ q^2\right)$.

Proof. We only need to prove $i) \Rightarrow ii)$.

If $x - \zeta_p = \alpha^q + q^2\beta$, then

$$x = \alpha^q - \gamma^q + q^2\beta.$$

Hence

$$q|\alpha^q - \gamma^q.$$

By (RLE)

$$q^2|\alpha^q - \gamma^q,$$

and so

$$q^2|x \text{ in } \mathbb{Z}[\zeta_p].$$

The result follows.