MATH. SCAND. 63 (1988), 117–135

GENERALIZATIONS OF FURTWÄNGLER'S CRITERIA FOR FERMAT'S LAST THEOREM AND SOME RELATED RESULTS

K. INKERI

1. Introduction and history.

1. In a recent paper Azuhata [1] has proved among other things, the following result.

THEOREM 1. *If there exist relatively prime integers x, y, z such that*

$$x^{l^n} + y^{l^n} + z^{l^n} = 0, \tag{1}$$

where l is an odd prime and n a positive integer, then a prime p satisfies the congruence

$$p^{l-1} \equiv 1 \pmod{l^{2n}} \tag{2}$$

in each of the following four cases:

(i) $p|x, \quad l \nmid x,$

(ii) $p|x-y, \quad l \nmid x^2 - y^2,$

(iii) $p|x^2 - yz, \quad l \nmid xy + yz + zx,$

(iv) $p|x^2 + yz, \quad l \nmid x(y-z)(x^2 + yz).$

For $n = 1$ the cases (i) and (ii) state the well-known first and second theorem of Furtwängler (iii) and (iv) Donnell's two theorems (see [12] or [6]). The primary proofs of all these theorems are based on Eisenstein's reciprocity law.

In (iii) the latter condition may be replaced by $l \nmid x^2 - yz$ or $l \nmid x^2 + xy + y^2$ or also may be, according to Pollaczek [11], omitted. In his proof of Theorem 1 Azuhata applies some results (particularly Stickelberger's relation) of the theory of the cyclotomic field $\mathbf{Q}(\zeta_m)$ $(m = l^n)$, where ζ_m is a primitive mth root of unity. Applying only the theory of the field $\mathbf{Q}(\zeta_l)$, a similar theorem

Received April 8, 1987.

has been proved in [6], in which, however, there is at the place (2) the weaker congruence

$$p^{l-1} \equiv 1 \pmod{l^{n+1}}. \tag{3}$$

The treatment for the verification of this theorem implies new proofs for Furtwängler's (and also Donnell's) theorems, the background of which is of the slenderest possible.

Moriya [10] had already earlier proved the cases (i) and (ii) of the latter result by making use of a rather deep result, namely of a generalization by Hasse [2] of Eisenstein's reciprocity law. Hellegouarch [3], [4] has made a attempt to verify in a similar way the cases (i) and (ii) of Theorem 1, but (on account of an omission) only Moriya's result has been attained. By the way, it could be a very interesting task to prove Theorem 1 by Hasse's result.

In order to derive some formulae concerning the so-called singular integers, the theory of the field $\mathbf{Q}(\zeta_m)$ has been appealed to in [7], as in [1]. As an application a generalization of Furtwängler's first theorem has been treated. (The fact of taking a stand in advance that d in the condition (16) in [7] could be divisible by l, a presumption which is not true, has proved to be an obstacle, preventing the author from seeing that case (i) of Theorem 1 follows from this condition on a few lines; see [1, Lemma 2].)

Making use of the ideas of the papers [6], [7] we will prove in Sections 7–11 some theorems and corollaries related to Theorem 1. The most general of these results seems to be Theorem 4, which e.g. contains as a corollary Theorem 1 and may give new cases in addition to the above four.

Particularly Furtwängler's theorems have had many applications in the research concerning Fermat's last theorem. For instance, the very important criteria of Wieferich and Mirimanoff follow from these theorems and it seems that this way presupposes the most concise background for proving these criteria (cf. [6] and also [7]).

2. Preliminaries.

2. We denote by r a positive primitive root modulo $m = l^n$ and by r_i the smallest positive residue of r^i modulo m. So $r^i \equiv r_i \pmod{m}$, $1 \leqq r_i \leqq m-1$. Let

$$q_i = \frac{1}{m}(rr_i - r_{i+1}), \quad Q(\sigma) = \sum_{i=0}^{\varphi-1} q_{-i}\sigma^i, \tag{4}$$

where $\varphi = \varphi(m) = l^{n-1}(l-1)$ (Euler function) and $\sigma = (\zeta_m : \zeta_m^r)$ a substitution

generating $\mathrm{Gal}(\boldsymbol{K}/\mathbb{Q})$ ($\boldsymbol{K} = \mathbb{Q}(\zeta_m)$). It is easily seen that the coefficients q_i are nonnegative integers. Let $\boldsymbol{D}$ be the ring of algebraic integers in $\boldsymbol{K}$.

Stickelberger's well-known relation (see e.g. [8] or [13] is the source of the results in question. Here the following related tool will be the basis of our considerations.

LEMMA 1. *Let α be an integer of $\boldsymbol{D}$ prime to $\lambda = 1-\zeta_m$ such that the prime ideal factors of the ideal (α) are of first degree. If α satisfies the condition*

$$(\alpha) = A^a, \tag{5}$$

where A is an ideal in $\boldsymbol{D}$ and a a positive rational integer, then

$$\alpha^{Q(\sigma)} = \pm \zeta_m^f \beta^a, \tag{6}$$

where the left-hand side is a symbolic power in the usual sense, f a rational integer and β belongs to $\boldsymbol{D}$.

In [7] we have presented for this lemma the sketch of a proof. Now we will detail it, keeping the treatment as elementary as possible. It seems that the background of our results will thus become apparent.

We consider any prime ideal Q of first degree and different from (λ). Let q be the prime belonging to Q, g a primitive root mod q and $q-1 = mm'$, where m' is an even integer. As usual, let $\operatorname{ind} h$ be defined by

$$g^{\operatorname{ind} h} \equiv h \pmod q, \quad 0 \leqq \operatorname{ind} h \leqq q-2,$$

when $q \nmid h$.

3. To begin with, we deduce some properties of Gauss sum (Lagrangian resolvent)

$$(\zeta, \eta) = \sum_{h=1}^{q-1} \zeta^{\operatorname{ind} h} \eta^h,$$

where η is a primitive qth root of unity and ζ a mth root of unity (later also primitive).

Clearly, $(1, \eta) = -1$. Assume now $\zeta \neq 1$. We consider the product

$$(\zeta, \eta)(\zeta^t, \eta) = \sum_{k=1}^{q-1} \sum_{h=1}^{q-1} \zeta^{\operatorname{ind} h + t \operatorname{ind} k} \eta^{h+k}.$$

For fixed k,h can be replaced by jk, where j is determined by $jk \equiv h \pmod q$, $1 \leqq j \leqq q-1$. Here j runs with h through the numbers $1, 2, \ldots, q-1$. Hence the double sum may be written as

$$\sum_{j=1}^{q-1} \zeta^{\operatorname{ind} j} \sum_{k=1}^{q-1} \zeta^{(t+1)\operatorname{ind} k} \eta^{k(j+1)} \tag{7}$$

(i) $m|t+1$, that is, $t \equiv -1 \pmod m$. Now the sum becomes

$$\sum_{j=1}^{q-1} \zeta^{\operatorname{ind} j}\left(\sum_{k=0}^{q-1} \eta^{k(j+1)}-1\right)=\zeta^{\operatorname{ind}(q-1)} q-\sum_{j=1}^{q-1} \zeta^{\operatorname{ind} j}=q,$$

since $\operatorname{ind}(q-1)=\frac{1}{2}(q-1) \equiv 0 \pmod m$ and by $\zeta \neq 1$,

$$\sum_{j=1}^{q-1} \zeta^{\operatorname{ind} j}=\sum_{i=0}^{q-2} \zeta^{i}=0.$$

Thus we have shown that

$$(\zeta,\eta)(\zeta^{-1},\eta)=q \quad \text{and} \quad (\zeta,\eta) \neq 0. \tag{8}$$

(ii) $m \nmid t+1$. Assume ζ is a primitive mth root of unity. Since $\zeta^{t+1} \neq 1$ and therefore

$$\sum_{k=1}^{q-1} \zeta^{(t+1)\operatorname{ind} k}=0,$$

the sum (7) can be written in the form

$$\sum_{j=1}^{q-2} \zeta^{\operatorname{ind} j-(t+1)\operatorname{ind}(j+1)} \sum_{k=1}^{q-1} \zeta^{(t+1)\operatorname{ind} k(j+1)} \eta^{k(j+1)}.$$

Here the last sum is equal to (ζ^{t+1},η) for each j in question, as $k(j+1)$ runs with k through the complete set of reduced residues $(\bmod q)$. Consequently, we have

$$(\zeta,\eta)(\zeta^{t},\eta)=\alpha_t(\zeta)(\zeta^{t+1},\eta), \tag{9}$$

where

$$\alpha_t(\zeta)=\sum_{j=1}^{q-2} \zeta^{\operatorname{ind} j-(t+1)\operatorname{ind}(j+1)} \tag{10}$$

is a number of $\boldsymbol{D}$.

Taking in (9), $t=1,2,\ldots,i-1 \leqq m-2$ and multiplying these relations, we obtain

$$(\zeta,\eta)^{i}=(\zeta^{i},\eta)\alpha_1(\zeta)\ldots\alpha_{i-1}(\zeta), \tag{11}$$

because $(\zeta^{t},\eta) \neq 0$. Taking here $i=m-1$ and observing (8), it follows that

$$(\zeta,\eta)^{m}=q\alpha_1(\zeta)\ldots\alpha_{m-2}(\zeta)=\omega(\zeta) \tag{12}$$

with $\omega=\omega(\zeta)$ belonging to $\boldsymbol{D}$.

From (12), $\omega(\zeta^r) = (\zeta^r, \eta)^m$. Now, by (11), we find easily

$$\omega^{r-\sigma} = \left(\frac{(\zeta,\eta)^r}{(\zeta^r,\eta)}\right)^m = \gamma^m, \tag{13}$$

where γ belongs to $\boldsymbol{D}$. If $\bar{\omega}$ denotes the complex conjugate and $\psi = \frac{1}{2}\varphi$, then from (8) and (12) we see immediately that

$$\omega\bar{\omega} = \omega^{1+\sigma^\psi} = q^m. \tag{14}$$

4. After these preliminary considerations we are now going to prove relation (6). Since $q \equiv 1 \pmod m$, then all prime ideal factors of the principal ideal (q) are of first degree and

$$(q) = \prod_{i=0}^{\varphi-1} Q^{\sigma^i},$$

where Q is any prime factor of (q).

There is a prime factor Q of (q) such that

$$\zeta \equiv g^{-m'} \pmod Q. \tag{15}$$

To see this, notice that

$$g^{q-1} - 1 = \prod_{a=0}^{m-1} (g^{m'} - \zeta^a) \equiv 0 \pmod Q$$

for any prime factor Q of (q). If now $Q \mid g^{m'} - \zeta^a$, then $\not\forall\ a$, as otherwise

$$g^{l^{n-1}m'} \equiv 1 \pmod Q \quad \text{and also } \pmod q,$$

contrary to the definition of g. Therefore, there is an integer i such that $ar^i \equiv -1 \pmod m$. Obviously, the prime Q^{σ^i} satisfies the condition (15).

We show now that every $\alpha_t(\zeta)$ in (12) is nondivisible by the prime Q satisfying (15). Observing the presentation (10) of $\alpha_t(\zeta)$ in terms of ζ we see from (15) that

$$\alpha_t(\zeta) \equiv \alpha_t(g^{-m'}) \equiv \sum_{j=1}^{q-2} g^{u \operatorname{ind} j + v \operatorname{ind}(j+1)} \equiv \sum_{j=1}^{q-1} j^u (j+1)^v \pmod Q,$$

where $u = q-1-m'$, $v = m'(t+1)$. By binomial theorem the last sum becomes

$$\sum_{h=0}^{v} \binom{v}{h} \sum_{j=1}^{q-1} j^{h+u}.$$

Furthermore, here the last sum is congruent to -1 or 0 modulo q according

as $h+u$, that is $h-m'$, is divisible by $q-1$ or not. But

$$-(q-1) < -m' \leqq h-m' < v \leqq m'(m-1) < q-1$$

and so $q-1 \mid h-m'$ iff $h=m'$. Now we can write

$$\alpha_t(\zeta) \equiv \left(\frac{v}{m'}\right) \not\equiv 0 \pmod{Q},$$

since $m' < v < q$.

5. From (12) and (14) we infer that

$$(\omega) = Q^{a_0 + a_1\sigma + \ldots + a_{\varphi-1}\sigma^{\varphi-1}}, \quad 1 \leqq a_i \leqq m,$$

where $a_0 = 1$ by virtue of the above. In order to determine the other coefficients a_i $(i = 1,\ldots,\varphi-1)$ observe that $\omega^r = \omega^\sigma \gamma^m$ (see (13)). This implies that only the conjugates of Q may be the prime factors of (γ) and therefore

$$ra_i \equiv a_{i-1} \pmod{m} \quad (i = 1,2,\ldots,\varphi-1). \tag{16}$$

Recall that r_i is the smallest positive integer such that $r^i \equiv r_i \pmod{m}$. Clearly, $r_0 = 1 = a_0$. By induction we conclude from (16) that always $a_i = r_{-i}$. If, namely, $a_{i-1} = r_{-i+1}$, then by (16), $a_i \equiv r^{-1}r^{-i+1} \equiv r^{-i} \equiv r_{-i} \pmod{m}$ and hence $a_i = r_{-i}$, as both these numbers belong to the interval $(1, m-1)$. Thus we have shown that

$$(\omega) = Q^{R(\sigma)} \quad \text{with} \quad R(\sigma) = r_0 + r_{-1}\sigma + \ldots + r_{-\varphi+1}\sigma^{\varphi-1}. \tag{17}$$

Raising the relations (13), (14), and (17) to the symbolic $\sigma^i (i = 1,\ldots,\varphi-1)$ power we conclude that every conjugate of Q and also of ω satisfies the relations of the same forms. Furthermore, we see that $R(\sigma)$ is independent of q and so the same properties are valid for every prime ideal $Q(\neq(\lambda))$ of first degree.

For A in (5) we can write $A = Q_1 Q_2 \ldots$, where every Q_i denotes a prime ideal of first degree (and different from (λ)). Raising (5) to the $R(\sigma)$ power, yields, by (17),

$$\alpha^{R(\sigma)} = \varepsilon(\omega_1 \omega_2 \ldots)^a,$$

where ε is a unit in $\boldsymbol{D}$ and every $\omega = \omega_i$ satisfies the conditions (13) and (14). We wish to specify ε. Raising the above equation to the $1+\sigma^\psi$ and observing that $R(\sigma)(1+\sigma^\varphi)$ may be replaced by $m\sum_{i=0}^{\varphi-1}\sigma^i$, we find

$$N(\alpha)^m = \varepsilon\bar{\varepsilon}(q_1 q_2 \ldots)^{am},$$

where $N(\alpha)$ is the norm of α in $\boldsymbol{K}$. From this it can be seen that $\varepsilon\bar{\varepsilon}$ is rational and positive. So this unit must be necessarily unity. Also $|\varepsilon^{\sigma^i}| = 1$, i.e. the absolute values of all the conjugates of ε are equal to 1. Then it follows

immediately (see e.g. [5, Satz 48]) that $\varepsilon = \pm\zeta^e$. Therefore

$$\alpha^{R(\sigma)} = \pm\zeta^e\delta^a$$

with $\delta = \omega_1\omega_2 \ldots$. Finally, raising to the $r-\sigma$ power and observing (13), we obtain

$$\alpha^{mQ(\sigma)} = (\pm\beta^a)^m,$$

and, further, taking the mth root of each side, we obtain (6). This completes the proof of Lemma 1.

3. Theorems and their proofs.

6. We still introduce some lemmas for later use. Let

$$Q(u,v) = \frac{u^l+v^l}{u+v} \quad \text{with} \quad u+v \neq 0,\ (u,v) = 1.$$

It is well-known (cf. e.g. [9, Sätze 1042, 1043]) that $l^2 \nmid Q(u,v)$ and $\gcd(u+v, Q(u,v)) = l$ or 1 according as $u^l + v^l$ is divisible by l or not.

By these facts we can easily prove the following.

LEMMA 2. *Let*

$$Q_0(u,v) = u+v, \quad Q_m(u,v) = Q(u^{l^{m-1}}, v^{l^{m-1}}) \quad (m \geqq 1).$$

If $l \nmid u+v$, then the numbers $Q_m(u,v)$ $(m = 0, 1, \ldots)$ are pairwise relatively prime integers, and if $l \mid u+v$, then the same holds for the numbers

$$\frac{1}{l}\, Q_m(u,v).$$

In the latter case $l^2 \nmid Q_m(u,v)$ for $m = 1, 2, \ldots$ and so, if $l^g \| u^{l^n} + v^{l^n}$, then $g \geqq n+1$ and $l^{g-n} \| u+v$.

PROOF. By the above this holds for $m = 0, 1$. Suppose that Lemma 2 has been verified for $m = 0, 1, \ldots, n-1$ $(n > 1)$.

Now $(u^{l^{n-1}} + v^{l^{n-1}},\ Q_n(u,v))$ equals 1 or l according as $l \nmid u+v$ or $l \mid u+v$, and $l^2 \nmid Q_n$ also by virtue of the above. But

$$u^{l^{n-1}} + v^{l^{n-1}} = \prod_{m=0}^{n-1} Q_m(u,v)\ .$$

and we may conclude that respectively $(Q_s, Q_t) = 1$ or l for $0 \leqq s < t \leqq n$. Lema 2 follows immediately.

LEMMA 3. *If an integer a belonging to the exponent f modulo l^s ($s \geqq 1$) satifies the condition*

$$a^f \equiv 1 \pmod{l^{s+1}},$$

then $f \mid l-1$ and a belongs to f also modulo l^t for $t = 1, 2, \ldots, s+1$.

PROOF. Evidently, $f \mid l^{s-1}(l-1)$ and a belongs to the exponent f modulo l^{s+1}. If it were $f = le$, then

$$a^f - 1 = (a^e - 1)(a^{e(l-1)} + \ldots + a^e + 1).$$

Here the product is divisible by l^{s+1}, but the latter factor only by l. Therefor $a^e \equiv 1 \pmod{l^s}$, contrary to the assumption. Thus $l \nmid f$ and so $f \mid l-1$.

If a belongs to f_1 modulo l, then $f_1 \mid f$ and $f = hf_1$, where h is not divisible by l. Now

$$\frac{a^f - 1}{a^{f_1} - 1} = a^{f_1(h-1)} + \ldots + 1 \equiv h \not\equiv 0 \pmod{l},$$

which implies that $a^{f_1} \equiv 1 \pmod{l^s}$. Hence $f_1 = f$ and the result follows readily.

LEMMA 4. *Let P be a prime ideal factor of (p), where p is a prime $\neq l$. If*

$$\zeta^d \equiv \alpha^{l^m} \pmod{P}, \tag{18}$$

where $l \nmid d$ and α is a number in $\mathbf{K}$ prime to P, then

$$l^{m+n} \mid N(P) - 1, \quad \text{that is} \quad p^f \equiv 1 \pmod{l^{m+n}} \tag{19}$$

and f, the degree of P, satisfies the condition $f \mid l-1$.

PROOF. Assume $l^a \| N(P)-1$ (so $a \geqq n$). Let $b = \min(a, m)$. Raising (18) to the $(N(P)-1)l^{-b}$ power we arrive by Fermat's theorem at

$$\zeta^{dl^{-b}(N(P)-1)} \equiv \alpha^{(N(P)-1)l^{m-b}} \equiv 1 \pmod{P}.$$

Since $p \neq l$, l^n must divide the exponent on the left. But $l \nmid d$ and therefore $l^{b+n} \mid N(P) - 1$ so that $a \geqq b + n$ and $b = m$. Consequently. (19) is valid, which completes the proof by the preceding lemma (cf. [5, Satz 122]).

7. As a beginning we consider the Diophantine equation

$$Q_n(u, v) = \frac{u^{l^n} + v^{l^n}}{u^{l^{n-1}} + v^{l^{n-1}}} = l^e w^{l^m}, \tag{20}$$

where l is an odd prime, m and n positive integers and e an integer $\geqq 0$. (So m has a new meaning).

Assume that the nonzero integers u, v, w with $u+v \neq 0$, $(u, v, w) = 1$, $l \nmid w$ satisfy this equation.

Now we may suppose that $l \nmid (u, v)$. Then $e = 0$ or 1 and $(u, v) = (u, w) = (v, w) = 1$. From now on, let ζ be a primitive l^nth root of unity. (Other notations are as before.)

Equation (20) may be put in the form

$$\prod_{h=0}^{\varphi-1} (u+\zeta^h v) = l^e w^{l^m} \quad (\varphi = l^{n-1}(l-1)). \tag{21}$$

(i) $e = 0$. It is easy to see that the factors on the left are pairwise relatively prime. Therefore,

$$(u+\zeta v) = A^{l^m}$$

where A is an ideal of $\boldsymbol{D}$. Moreover, the prime ideal factors of A are of first degree: if, namely, $P|A$, then $P^{\sigma^i}|(u+\zeta^{r^i}v)$ $(i = 1, \ldots, \varphi-1)$ and so these P's are distinct ideals. (An elementary verification of this fact: all the prime factors of the expression (20) are of the form kl^n+1; cf. e.g. [6, Lemma IV, p. 27].)

Lemma 1 shows now that

$$(u+\zeta v)^{Q(\sigma)} = \zeta^a \alpha^{l^m} \tag{22}$$

where α belongs to $\boldsymbol{D}$ and is prime to l.

We look for the residue of the exponent a modulo l in terms of the numbers u, v, and r. Set $b = -v(u+v)^{-1}$, where $(u+v)(u+v)^{-1} \equiv 1 \pmod{l}$. Then

$$\begin{aligned}\zeta^b(u+\zeta v) &\equiv (1-b\lambda)(u+v-\lambda v) \equiv u+v-(v+b(u+v))\lambda \\ &\equiv u+v \pmod{\lambda^2}.\end{aligned}$$

Since $N(\lambda) = l$, α is congruent to a rational integer modulo λ, and so is α^{l^m} modulo λ^2. Multiply (22) by

$$\zeta^{bQ(\sigma)} = \zeta^{bQ(r)}.$$

The relation obtained implies

$$\zeta^{a+bQ(r)} \equiv c \pmod{\lambda^2}$$

where c is an integer. Since now $\lambda | c-1$ and hence $l | c-1$, this congruence yields

$$a \equiv -bQ(r) \equiv v(u+v)^{-1}Q(r) \pmod{l}.$$

Here $Q(r) \equiv l^{-n}(r^{\varphi+1}-r) \not\equiv 0 \pmod{l}$ for $n > 1$ always and also for $n = 1$ if r is chosen as a primitive root of l^2.

From (22) it follows that

$$(u+\zeta v)^{(1-\sigma^\psi)Q(\sigma)} = \zeta^d \beta^{l^m}, \tag{23}$$

where $d \equiv 2v(u+v)^{-1}Q(r) \pmod{l}$ and β is in $\boldsymbol{K}$.

(ii) $e = 1$. We see easily that now $l \nmid uv$ and all the factors of the product in (21) are divisible by λ. Thus

$$\prod_{h=0}^{\varphi-1}\left(\frac{u+\zeta^{r^h}v}{1-\zeta^{r^h}}\right) = (w)^{l^m},$$

where the principal ideals on the left-hand side are pairwise relatively prime and prime to (λ). As in the previous case we conclude that

$$\left(\frac{u+\zeta v}{1-\zeta}\right) = A^{l^m}.$$

where all the prime ideal factors of the ideal A are of first degree. Again we deduce from Lemma 1 that

$$\left(\frac{u+\zeta v}{1-\zeta}\right)^{Q(\sigma)} = \zeta^a \alpha^{l^m}, \tag{24}$$

where a is an integer and α belongs to $\boldsymbol{D}$. Clearly, $l|u+v$ so that

$$\lambda^{-1}(u+\zeta v) = \lambda^{-1}(u+v) - v \equiv -v \pmod{\lambda^2}$$

for $l^n > 3$. Now the relation (24) implies

$$\zeta^a \equiv 1 \pmod{\lambda^2},$$

whence it follows that a must be divisible by l. Since

$$(1-\zeta)^{1-\sigma^\psi} = -\zeta,$$

we obtain from (24) also now a relation of the form (23) where, however, this time $d = 2a + Q(r) \equiv Q(r) \pmod{l}$.

8. We are now going to prove the following four theorems (and also Theorem 1).

THEOREM 2. *If the nonzero integers u, v, w satisfy the equation* (20) *with $u+v \neq 0$, $(u,v,w) = 1$, $l \nmid w$, $l^n > 3$, then for a prime p*

$$p^{l-1} \equiv 1 \pmod{l^{m+n}} \tag{25}$$

in the following two cases

(i) $p|v$, $l \nmid v$;
(ii) $p|u^2 - v^2$, $l \nmid u^2 - v^2$.

PROOF. Clearly, $(u, v) = 1$ and $e = 0$ or 1 in both cases. We have shown above that

$$(u+\zeta v)^{(1-\sigma^\psi)Q(\sigma)} = \zeta^d \beta^{l^m}, \tag{26}$$

where

$$d \equiv \begin{cases} 2v(u+v)^{-1}Q(r) \pmod{l} & \text{if } e = 0 \\ Q(r) \pmod{l} & \text{if } e = 1 \end{cases}$$

and $Q(r) \equiv (r^{\varphi+1} - r)l^{-n} \not\equiv Q \pmod{l}$.

(i) Both for $e = 0$ and $e = 1$ it is obvious that $l \nmid d$. Since $p|v$, we obtain from (26) the congruence of the form (18). It is easily seen that α may be assumed prime to the ideal P. The result (25) follows at once from Lemma 4.

(ii) Now $l \nmid u+v$, $e = 0$ and $u+\zeta v \equiv u(1 \pm \zeta) \pmod{p}$. Here $(u(1 \pm \zeta), p) = (1)$, since $1-\zeta | l$, $1+\zeta$ is a unit in $\boldsymbol{D}$ and $p|u^2 - v^2$, $(u, v) = 1$. As

$$(1 \pm \zeta)^{1-\sigma^{\psi}} = \pm\zeta,$$

we have from (26) for any prime ideal factor P of (p) again

$$\zeta^{Q(r)-d} \equiv \alpha^{l^m} \pmod{P},$$

where α is a number in $\boldsymbol{K}$ prime to P, $d \equiv 2v(u+v)^{-1}Q(r) \pmod{l}$. But

$$(u+v)(1-2v(u+v)^{-1}) \equiv u - v \not\equiv 0 \pmod{l}$$

so that $l \nmid Q(r) - d$. Again, by Lemma 4, (25) holds as desired.

The following is actually a corollary of Theorem 2 (cf. [1, Theorem 1]).

THEOREM 3. *If the integers x, y, z satisfy the equation*

$$x^{l^n} + y^{l^n} + z^{l^m} = 0$$

with $(x, y, z) = 1$, then for a prime p congruence (25) *is valid in both of the cases*

(i) $p|x$, $l \nmid x$;
(ii) $p|x^2 - y^2$, $l \nmid x^2 - y^2$.

PROOF. We may assume that $l > 3$, since Fermat's last theorem is true for $l = 3$. It is evident that the trivial solutions can be omitted, in other words, we may assume that $xyz \neq 0$.

Clearly, $x + y \neq 0$ $(x, y) = 1$ and (cf. the facts associated with Lemma 2)

$$(x^{l^{n-1}} + y^{l^{n-1}}, Q_n(x, y)) = 1 \quad \text{or} \quad l, l^2 \nmid Q_n.$$

Hence

$$Q_n(x, y) = l^e z_1^{l^m},$$

where $z_1 | z$, $l \nmid z_1$, $e = 0$ or 1, $(x, y, z) = 1$. Now the result follows in both cases immediately from the preceding theorem.

Naturally Theorem 3 implies the validity of the parts (i) and (ii) of Theorem 1.

9. We are going to prove the following general theorem, which contains Theorem 1 as an easy consequence.

THEOREM 4. *Let x, y, z be nonzero integers such that*

$$x^{l^n}+y^{l^n}+z^{l^n}=0, \quad (x,y,z)=1, \tag{1}'$$

and let u_i, v_i, w_i for $i=1,2,..,k$ be these integers in some order. Denote by p a prime not equal to l. If there is a product

$$\pi=\prod_{i=1}^{k}(u_i+\zeta^{h_i}v_i)^{k_i} \quad (l\nmid h_i, k_i\neq 0),$$

which is prime to p and congruent to a rational (or, more generally, to a real) number (mod p) *and if*

$$d=\sum_{i=1}^{k}h_ik_id_i\not\equiv 0 \pmod{l} \tag{27}$$

with

$$d_i\equiv\begin{cases}-2v_iw_i^{-1}Q(r) & \text{for } l\nmid w_i(w_iw_i^{-1}\equiv 1 \pmod{l})\\ Q(r) & \text{for } l\mid w_i,\end{cases} \tag{28}$$

then congruence (2) *holds.*

PROOF. The numbers $u=u_i$, $v=v_i$ satisfy (20), where now $w\mid w_i$ and $m=n$. Since ζ^{h_i} for $l\nmid h_i$ is a primitive l^nth root of unity, we have by our presentation in section 7 and in the proof of Theorem 2

$$(u_i+\zeta^{h_i}v_i)^{(1-\sigma^\psi)Q(\sigma)}=\zeta^{h_id_i}\alpha_i^{l^n}.$$

Here α_i is a number in $\boldsymbol{K}$ and d_i is determined modulo l by (28), as $u_i+v_i+w_i\equiv 0 \pmod{l}$ because of (1)' and so $(u_i+v_i)^{-1}\equiv -w_i^{-1} \pmod{l}$. Applying the above relation for $i=1,\ldots,k$ to π we obtain

$$\pi^{(1-\sigma^\psi)Q(\sigma)}=\zeta^{-d}\beta^{l^n},$$

where β is a number in $\boldsymbol{K}$ prime to p and d is determined by (27). But $\pi^{(1-\sigma^\psi)}\equiv 1 \pmod{p}$ by assumption and therefore this equation gives for any prime ideal factor P of (p)

$$\zeta^d\equiv\beta^{l^n} \pmod{P}.$$

Now the validity of congruence (2) follows, once more, from Lemma 4. The proof is complete.

As a consequence we wish to verify Theorem 1. At once it is seen that in all four cases $xyz \neq 0$.

(i) Choose $\pi = y + \zeta x$. Since $p|x$, $p \nmid yz$, and $\pi \equiv y \pmod{p}$ so that $(\pi, p) = (1)$. Now $d \equiv 2xz^{-1}Q(r)$ or $d \equiv -Q(r) \pmod{l}$ according as $l \nmid z$ or $l|z$. Thus $l \nmid d$, that is (27) is valid.

(ii) Let $\pi = (y+\zeta x)(x+\zeta y)^{-1}$. From $p|x-y$ it follows that $y+\zeta x \equiv x+\zeta y \equiv x(1+\zeta) \pmod{p}$, where $1+\zeta$ is a unit and $p \nmid x$. So π is prime to p and $\pi \equiv 1 \pmod{p}$. Furthermore, $l \nmid z$, as $l \nmid x+y$. Hence

$$d \equiv 2xz^{-1}Q(r) - 2yz^{-1}Q(r) \equiv 2z^{-1}(x-y)Q(r) \not\equiv 0 \pmod{l}.$$

(iii) Without loss of generality we may assume that $l|z$ if $l|yz$. Let now $\pi = (y+\zeta x)(x+\zeta z)^{-1}$. Noting $p|x^2 - yz$ and $(1)'$, we find that $p \nmid xyz$ and hence $(y+\zeta x, p) = (x+\zeta z, p) = (1)$. Moreover $\pi \equiv y/x \pmod{p}$. To see that also the condition (27) holds, we firstly consider the case $l \nmid yz$. Then $d \equiv -2(zy^{-1} - xz^{-1})Q(r) \pmod{l}$. But

$$yz(zy^{-1} - xz^{-1}) \equiv z^2 - xy \equiv x^2 + xy + y^2 \not\equiv 0 \pmod{l}.$$

Since $x+y+z \equiv 0 \pmod{l}$. (The last step is true according to Pollaczek [11]; notice also $xy+yz+zx \equiv -(x^2-yz) \pmod{l}$.) At any rate $l \nmid d$.

If secondly $l|yz$ and so $l|z$ because of our assumption made at the beginning, then

$$d \equiv -Q(r)(1+2zy^{-1}) \equiv -Q(r) \not\equiv 0 \pmod{l}.$$

(iv) As before we may assume that $l|z$ if $l|yz$. Choose

$$\pi = (x+\zeta z)(y+\zeta x)(y+\zeta^2 z)^{-1}.$$

Noting that $p|x^2+yz$, we see that $p \nmid xyz$ and π is prime to p. Also $(x+\zeta z)(y+\zeta x) \equiv x(y+\zeta^2 z) \pmod{p}$ so that $\pi \equiv x \pmod{p}$.

By assumption, $l \nmid x$. If $l \nmid z$, then also $l \nmid y$. Then

$$d \equiv (2zy^{-1} + 2xz^{-1} - 4zx^{-1})Q(r) \pmod{l}.$$

Using the congruence $x+y+z \equiv 0 \pmod{l}$ we may easily infer that

$$xyzd \equiv 2(y-z)(x^2+yz)Q(r) \pmod{l}.$$

By assumption we notice that $d \not\equiv 0 \pmod{l}$.

If $l|z$, then

$$d \equiv -(-2zy^{-1} + 1 + 4zx^{-1})Q(r) \equiv -Q(r) \not\equiv 0 \pmod{l}.$$

We have seen that in all these four cases the assumptions of Theorem 4 hold so that the validity of Theorem 1 follows.

4. Applications.

10. As an aplication of Theorem 1 we present the following generalization of a result of Vandiver (see [9, Satz 1046], or [12]) and one of Inkeri [6].

THEOREM 5. *Let x, y, z be integers satisfying the conditions* (1)′. *Then*

$$x^l \equiv x, \quad y^l \equiv y, \quad z^l \equiv z \pmod{l^{3n}}. \tag{29}$$

PROOF. If $xyz = 0$, then x, y, z are in some order equal to the numbers $0, 1, -1$ and therefore the congruences (29) are trivially true. We can thus assume that $xyz \neq 0$, and also, without loss of generality, that $l \nmid xy$. It follows that $y + z \neq 0$, $l \nmid y^{l^n} + z^{l^n}$. Therefore, by Lemma 2,

$$Q(y,z) = a^{l^n}, y^l + z^l = b^l, \tag{30}$$

where $a|x, b|x^{l^n - 1}$ and $y + z \equiv b \not\equiv 0 \pmod{l}$, $a^{l^n} \equiv b^{l-1} \equiv 1 \pmod{l}$ because of Fermat's theorem.

From the last congruence we obtain further $a \equiv 1 \pmod{l}$. On the other hand, since $a|x$ and $l \nmid x$,

$$a^l \equiv a \pmod{l^{2n}}$$

an account of Theorem 1, (i).

$$(a-1)(Q(a,-1)-1) \equiv 0 \pmod{l^{2n}}.$$

Here the quotient is divisible by l, whence $a \equiv 1 \pmod{l^{2n}}$ and further (e.g. by Lemma 2)

$$a^{l^n} \equiv 1 \pmod{l^{3n}}.$$

This congruence yields in connection with (30)

$$y^l + z^l \equiv y + z \pmod{l^{3n}}. \tag{31}$$

In the same way (or by symmetry) one obtains

$$x^l + z^l \equiv x + z \pmod{l^{3n}} \tag{32}$$

and also, if $l \nmid z$,

$$x^l + y^l \equiv x + y \pmod{l^{3n}}.$$

From these three congruences (29) follows immediately.

If $l|z$, only congruences (31) and (32) are at our disposal. Adding up these congruences, we have

$$x^l + y^l + 2z^l \equiv x + y + 2z \pmod{l^{3n}}.$$

Let l^h be the highest power of l dividing z. By Lemma 2 it follows from equation (1)′ that

$$l^{hl^n-n} | (x+y, x^l+y^l).$$

But $hl^n-n \geqq n(l-1)+1-n \geqq 2$ and hence $h \geqq 2$ by virtue of the last congruence. Therefore, $hl^n-n \geqq n(2l-3)+1 > 3n$ and from that congruence it still follows that

$$z^l \equiv z \pmod{l^{3n}},$$

i.e., $l^{3n} | z$. Finally, by subtracting this congruence from (31) and (32) we have the other conditions of (29). The proof is ready.

THEOREM 6. *Let x, y, z be integers satisfying (1)′. If $l | x-y$, then*

$$x \equiv y \pmod{l^{3n}}, \quad 2^{l-1} \equiv 1 \pmod{l^{4n}}. \tag{33}$$

PROOF. By the preceding theorem

$$x^{l^n} \equiv x,\ y^{l^n} \equiv y,\ z^{l^n} \equiv z \pmod{l^{3n}}. \tag{29}′$$

Hence

$$x^{l^n} - y^{l^n} \equiv x-y \pmod{l^{3n}}$$

or

$$(x-y)((x^{l^n}-y^{l^n})/(x-y)-1) \equiv 0 \pmod{l^{3n}}.$$

But here the quotient is divisible by l and so the first congruence in (33) is valid.

To prove the latter assertion in (33), we note firstly, by (1) and (29)′, $x+y \equiv -z \pmod{l^{3n}}$. Since $l^{3n} | x-y$, it follows from this and Lemma 2 that

$$2x \equiv -z \pmod{l^{3n}}, \quad x^{l^n} \equiv y^{l^n} \bmod l^{4n}).$$

These congruences combining with (1)′ give

$$2^{l^n} x^{l^n} \equiv -z^{l^n},\ 2x^{l^n} \equiv -z^{l^n} \pmod{l^{4n}},$$

whence

$$2^{l^n} \equiv 2 \pmod{l^{4n}}.$$

For brevity let $Q = (l^n-1)/(l-1)$. We have

$$2^{l^n-1}-1 = (2^{l-1}-1)(2^{(l-1)(Q-1)}+\ldots+2^{l-1}+1).$$

Since here the latter factor is congruent to Q modulo l and therefore non-divisible by l, we infer by virtue of the above congruence that also the latter assertion in (33) is valid. This finishes the proof.

11. As a consequence of Theorem 1 we have the following corollary, which is a simple generalization of a well-known result concerning the case $n = 1$.

COROLLARY 1. *If* (1) *has a solution* x, y, z *in integers such that none of the numbers* x, y, z *is divisible* (a) by $2l$, (b) *by* $3l$, *then*

$$2^{l-1} \equiv 1 \quad \textit{or} \quad 3^{l-1} \equiv 1 \pmod{l^{2n}}, \tag{34}$$

respectively.

PROOF. Clearly, $xyz \neq 0$. Without loss of generality we may also assume in both of the cases that $(x, y, z) = 1$.

(a) One of the numbers x, y, z is even and according to the assumption this number is not divisible by l. From Theorem 1 (i) the validity of the first congruence in (34) now follows.

(b) If one of x, y, z is divisible by 3, then the assertion follows as in the preceding case.

If none of x, y, z is divisible by 3, then $x^2 \equiv y^2 \equiv z^2 \equiv 1 \pmod 3$ so that each of the differences $x^2 - y^2$, $x^2 - z^2$, and $y^2 - z^2$ is divisible by 3. All these differences may not be divisible by l, for otherwise the congruences $x^2 \equiv y^2 \equiv z^2 \pmod l$ and $x + y \equiv -z \pmod l$ would give $3x^2 \equiv 0 \pmod l$, which is impossible, since for $l = 3$ the equation (1) has no solution with $xyz \neq 0$. This completes the proof.

We consider now the equation

$$x^{l^n} + y^{l^n} + z^{l^m} = 0. \tag{35}$$

COROLLARY 2. *If the integers* x, y, z *satisfy equation* (35) *with* $(x, y, z) = 1$ *and none of the numbers* $x, y, x^2 - y^2$ *is divisible* (a) *by* $2l$, (b) *by* $3l$, *then*

$$2^{l-1} \equiv 1 \pmod{l^{m+n}}, \quad 3^{l-1} \equiv 1 \pmod{l^{m+n}}, \tag{36}$$

respectively.

PROOF. We see at once that one of the numbers x, y, z is divisible by 2 and one by 3. In both of the cases this number is, according to the assumptions, nondivisible by l. Now the result follows directly from Theorem 3.

The following analogous result to this corollary holds for equation (20).

COROLLARY 3. *Under the same conditions as in Theorem* 2 *and under the additional assumption that none of the numbers* u, v *and* $u^2 - v^2$ *is divisible* (a) *by* $2l$, (b) *by* $3l$, *each of the congruences* (36), *respectively is valid.*

For equation (35) also the case $l \mid x - y$ is a matter of considerable interest.

THEOREM 7. *If the nonzero integers* x, y, z *satisfy* (35) *with* $l \mid x - y$ *and*

$(x, y, z) = 1$, *then*

$$x \equiv y(\mathrm{mod}\, l^{m+n}), \quad 2^{l-1} \equiv 1(\mathrm{mod}\, l^{M}), \tag{37}$$

where $M = \max(4m, m+n)$ *for* $n \geqq m$ *and* $M = \max(4n, m+1)$ *for* $n \leqq m$. *If* $2|xy$, *then* $M = m+n$ *can be taken.*

PROOF. It follows from the assumptions that $l \nmid xyz$. Theorem 3 (i) shows that

$$x^{l-1} \equiv 1, \quad y^{l-1} \equiv 1(\mathrm{mod}\, l^{m+n}). \tag{38}$$

Hence

$$x^{l^n} \equiv x, \quad y^{l^n} \equiv y(\mathrm{mod}\, l^{m+n}),$$

from which it follows in the same way as in the proof of Theorem 6 that the first congruence in (37) is true.

The case $2|xy$ is clear from the above. The same result is valid also for $2|z$ if $n \geqq m$, as we see when writing (35) in the form

$$x^{l^n} + (y^{l^{n-m}})^{l^m} + z^{l^m} = 0$$

and applying again Theorem 3 (i).

For $n \geqq m$ equation (35) takes also the form

$$(x^{l^{n-m}})^{l^m} + (y^{l^{n-m}})^{l^m} + z^{l^m} = 0,$$

from which we find by Theorem 6 that (37) holds for $M = 4m$.

Now we can be restricted to the case $n \leqq m$. The first congruence in (37) yields

$$x^{l^n} \equiv y^{l^n}(\mathrm{mod}\, l^{m+2n}).$$

Consequently, (35) implies

$$2x^{l^n} \equiv -z^{l^m}(\mathrm{mod}\, l^{m+2n}).$$

Raising this to the $l-1$ power gives

$$2^{l-1} \equiv z^{l^m(l-1)}(\mathrm{mod}\, l^{m+2n}),$$

since by (38) $x^{l^n(l-1)} \equiv 1(\mathrm{mod}\, l^{m+2n})$. Using Euler's theorem to eliminate z, we arrive at the following comparatively weak result

$$2^{l-1} \equiv 1(\mathrm{mod}\, l^{m+1}).$$

We write (35) still in the form

$$x^{l^n} + y^{l^n} + (z^{l^{m-n}})^{l^n} = 0.$$

Remembering that $l|x-y$ we may apply Theorem 6 to give

$$2^{l-1} \equiv 1 (\mathrm{mod}\, l^{4n}).$$

Combining this with the preceding congruence yields the final result required for $n \leqq m$.

In conclusion we state without any proof the following result, which is an improvement on our theorem presented in [6]. Making use of Theorem 1 this result can be proved in the same way as we have done in the above-mentioned paper (cf. pp. 32–37).

THEOREM 8. *If equation* (1) *is solvable in integers such that* $l \nmid xyz$, *then* $p^{l-1} \equiv 1 (\mathrm{mod}\, l^{2n})$ *in the following cases*:

(a) $p = 2, 3$,
(b) $p = 5$ *and* $l \not\equiv 1, 9 (\mathrm{mod}\, 20)$,
(c) $p = 5, 7$ *and* $2^{l-1} \not\equiv 1 (\mathrm{mod}\, l^{4n})$,
(d) $p = 11$ *and* $2^{l-1} \not\equiv 1 (\mathrm{mod}\, l^{4n})$ *and in addition* $l \equiv \pm 2 (\mathrm{mod}\, 5)$.

Evidently, Corollary 1 implies the case (a).

REMARK. Some generalizations in which the numbers of the ring of the algebraic integers of the cyclotomic field $\mathbf{Q}(\zeta_l)$ or $\mathbf{Q}(\zeta_{l^n})$ have been substituted for the rational integers as the values of x, y, z in the correponding Fermat's eqution have been presented in papers [6] and [1]. Unfortunately, the factor p for instance in the conditions (i)-(iv) of Theorem 1 remains however, unchanged as a rational prime. Is it possible in this context to replace p by any prime ideal factor P of the ideal (p)? We are waiting for a solution to this really interesting question.

REFERENCES

1. T. Azuhata, *On Fermat's last theorem*, Acta Arith. 45 (1985), 19–27.
2. H. Hasse, *Das Eisensteinsche Reziprozitätsgesetz der n-ten Potenzreste*, Math. Ann. 97 (1927), 599–623.
3. Y. Hellegouarch, *Sur un théorème de Maillet*, C. R. Acad., Sci. Paris Sér. I Math. 273 (1971), 477–478.
4. Y. Hellegouarch, *Courbes elliptiques et equation de Fermat*, Thèse, Besancon, 1972.
5. D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, in *Gesammelte Abhandlungen*, Vol. I, pp. 63–362. Chelsea Publishing Company, New York, 1965.
6. K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. A I 33 (1946), 1–60.
7. K. Inkeri, *Some extensions of criteria concerning singular integers in cyclotomic fields*, Ann. Acad. Sci. Fenn. A I 49 (1948), 1–15.
8. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate Texts in Math. 84), Springer-Verlag, Berlin - Heidelberg - New York, 1982.

9. E. Landau, *Vorlesungen über Zahlentheorie*, Vol. III, Hirzel, Leipzig, 1927 and Chelsea Publishing Company, New York, 1969.
10. M. Moriya, *Über die Fermatsche Vermutung*, J. Reine Angew. Math. 169 (1933), 92–97.
11. F. Pollaczek, *Über den grossen Fermatschen Satz*, Sitzungsber. Akad. Wiss. Wien, Abt. II a, 126 (1917) 45–59.
12. P. Ribenboim, 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, Berlin - Heidelberg - New York, 1979.
13. L. C. Washington, *Introduction to cyclotomic fields* (Graduate Texts in Math. 83), Springer-Verlag, Berlin - Heidelberg - New York, 1982.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU
SF-20500 TURKU
FINLAND