An extension of Legendre's criterion in connection with the first case of Fermat's last theorem.

By PETER DÉNES in Budapest.

The so-called LEGENDRE's criterion says that if l and $2l+1$ are odd primes, the first case of FERMAT's last theorem is true; that means that the equation

$$(1) \qquad x^l+y^l+z^l=0,$$

has no integer solution x, y, z such that $l \nmid xyz$.

FURTWÄNGLER[1]) extended LEGENDRE's criterion and proved that (1) has no integer solution x, y, z prime to l, if one of the numbres $ul+1$, $u=2, 4, 8, 10$, is a prime. In the present paper a further extension of LEGENDRE's criterion will be given, up to $u=110$.

Lemma. *If l and $p=ul+1$ are odd primes, u is a positive integer prime to l, ϱ is a primitive u^{th} root of unity, $\mathfrak{p}$ is a prime ideal factor of p in the field of the u^{th} roots of unity $k(\varrho)$ and further is*

$$(2) \qquad 1+\varrho^a+\varrho^b \not\equiv 0 \pmod{\mathfrak{p}}$$

for any value of a and b, (1) *has no integer solution x, y, z,* prime to l.

Proof. Let m denote an integer prime to p, so is

$$m^{ul} \equiv 1 \pmod{p}$$

and from this congruence follows

$$(3) \qquad m^l \equiv \varrho^c \pmod{\mathfrak{p}},$$

c a positive integer, because the prime ideal $\mathfrak{p}$ is of the first degree in $k(\varrho)$. Assuming none of the numbers x, y, z divisible be p, (1) and (3) yield the congruence

$$\varrho^{c_1}+\varrho^{c_2}+\varrho^{c_3} \equiv 0 \pmod{\mathfrak{p}},$$

which is, however, according to our assumption (2) impossible. Hence one of

[1]) PH. FURTWÄNGLER: Letzer Fermat'scher Satz und Eisenstein'sches Reziprozitätsgesetz. *Sitzungesberichte d. Akad. d. Wiss.*, Wien, Abt. IIa., **121** (1912), 589—592.

the numbers x, y, z must be divisible by p. In this case the following congruence holds:

$$p^l \equiv p \qquad (\mathrm{mod}\ l^2),$$

which must be satisfied [1]) for each divisor x, y, z. From this we get

$$(ul+1)^l \equiv 1 \equiv ul+1 \qquad (\mathrm{mod}\ l^2)$$

wherefrom $u \equiv 0 \ (\mathrm{mod}\ l)$ follows, in contradiction to our supposition that u is prime to l. This completes the proof of our lemma.

Denoting by $N_u(\omega)$ the norm of the number ω of the field $k(\varrho)$, from the congruence

$$1+\varrho^a+\varrho^b \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{p})$$

follows

$$N_u(1+\varrho^a+\varrho^b) \equiv 0 \qquad (\mathrm{mod}\ p).$$

Consequently, if the inequality

$$0 < N_u(1+\varrho^a+\varrho^b) < p \tag{4}$$

is satisfied, the incongruence (2) is true for any value of a and b. The norm of $1+\varrho^a+\varrho^b$ can only be equal zero, if

$$1+\varrho^a+\varrho^b = 0, \tag{5}$$

the only solution of which is $\varrho^a = e^{2\pi i/3}$ and $\varrho^b = e^{4\pi i/3}$. Hence, if u is prime to 3, the equation (5) cannot hold.

Further, as u is an even integer, we have

$$\begin{aligned} \Theta &= (1+\varrho^a+\varrho^b)^2(1+\varrho^{-a}+\varrho^{-b})^2 = \\ &= \left[3+2\cos a\frac{2\pi}{u}+2\cos b\frac{2\pi}{u}+2\cos(a-b)\frac{2\pi}{u}\right]^2 = \\ &= 1+8\cos(a+b)\frac{\pi}{u}\cos(a-b)\frac{\pi}{u}+8\cos^2(a-b)\frac{\pi}{u}+ \\ &\quad +64\cos^2 a\frac{\pi}{u}\cos^2 b\frac{\pi}{u}\cos^2(a-b)\frac{\pi}{u}. \end{aligned} \tag{6}$$

Denoting by Φ the following expression:

$$\begin{aligned} \Phi &= (2+\varrho^a)(2+\varrho^{-a})(2+\varrho^b)(2+\varrho^{-b}) = 1+8\cos(a+b)\frac{\pi}{u}\cos(a-b)\frac{\pi}{u}+ \\ &\quad +8+64\cos^2 a\frac{\pi}{u}\cos^2 b\frac{\pi}{u}, \end{aligned} \tag{7}$$

obviously it is

$$\Theta \leqq \Phi, \tag{8}$$

because both Θ and Φ are positive real numbers and

$$\Phi-\Theta = \left[1-\cos^2(a-b)\frac{\pi}{u}\right]\left[8+64\cos^2 a\frac{\pi}{u}\cos^2 b\frac{\pi}{u}\right] \geqq 0.$$

First we suppose that none of the numbers $a, b, a-b$ is divisible by u; then, denoting by Ψ the following relation:

$$\Psi = \frac{8+64\cos^2 a\frac{\pi}{u}\cos^2 b\frac{\pi}{u}}{\Phi},$$

we have

$$\Psi = \frac{8+64\cos^2 a\frac{\pi}{u}\cos^2 b\frac{\pi}{u}}{1+8\cos^2 a\frac{\pi}{u}+8\cos^2 b\frac{\pi}{u}+64\cos^2 a\frac{\pi}{u}\cos^2 b\frac{\pi}{u}} \geqq \frac{8}{9},$$

and hence

$$\frac{\Theta}{\Phi} = 1-\Psi\left[1-\cos^2(a-b)\frac{\pi}{u}\right] \leqq 1-\frac{8}{9}\left[1-\cos^2(a-b)\frac{\pi}{u}\right],$$

or, from this,

$$\frac{\Theta}{\Phi} \leqq \frac{5}{9}+\frac{4}{9}\cos(a-b)\frac{2\pi}{u} = \frac{(2+\varrho^{a-b})(2+\varrho^{-a+b})}{3^2}. \tag{9}$$

From (6), (7), (9), we get the following inequality, if none of the numbers $a, b, a-b$ is divisible by u:

$$N_u(1+\varrho^a+\varrho^b) \leqq \frac{\{N_u(2+\varrho^a)N_u(2+\varrho^b)N_u(2+\varrho^{a-b})\}^{1/2}}{3^{\varphi(u)/2}} \tag{10}$$

where $\varphi(u)$ represents the number-theroretical function of EULER.

The first case of FERMAT's last theorem is proved [2]) for all odd primes $l<L$, $L=253\,747\,899$ and therefore, it is true, with respect to (10), if

$$\frac{[N_u(2+\varrho^c)]^{3/2}}{u\cdot 3^{\varphi(u)/2}} < L \quad\text{and}\quad \frac{N_u(2+\varrho^c)}{u} < L, \tag{11}$$

where c is chosen in the way that $N_u(2+\varrho^c) \geqq N_u(2+\varrho^d)$, d any positive integer prime to $u/2$. The numbers $u=2, 4, 8, 10, 14, 16, 20, 22, 26, 28, 32, 34, 38, 40, 44, 46, 50, 52, 56, 70$ suffice the inequalities (11), even with $c=u/4$, rendering the most inadvantageous case.

Investigating the other primes l, whether $N_u(1+\varrho^a+\varrho^b)$ is divisible by p, we may suppose $(a, b, u)=1$, as else $N_u(1+\varrho^a+\varrho^b)$ would be the power of an integer n and it would suffice to show that n is smaller than p. Is one of the numbers a, b divisible bu u, then it is sufficient to study simply $N_u(2+\varrho)$.

We take now into consideration some values of u and examine the different possible bounds of $N_u(1+\varrho^a+\varrho^b)$ with help of (10).

---

[2]) D. H. and EMMA LEHMER: On the first case of Fermat's Last Theorem. *Bull. Amer. Math. Soc.* 47 (1941), 139—142.

$u = 58$; $c = 1$.

$$N_{58}(2+\varrho) = 2^{29} - 1 < 58L + 1.$$

$$\frac{(2^{29}-1)^{3/2}}{3^{14}} < 58L + 1.$$

$u = 62$; $c = 1$.

$$N_{62}(2+\varrho) = 2^{31} - 1 < 62L + 1.$$

$$\frac{(2^{31}-2)^{3/2}}{3^{15}} < 62L + 1.$$

$u = 64$.

$$N_{64}(1+\varrho) = 2^{32} + 1 < 64L + 1.$$

In (10) only one of the numbers a, b may be even; the largest norm bound is obtained with $a = 1$ and $b = 16$:

$$\frac{(2^{32}+1)\cdot(2^2+1)^8}{3^{16}} < 64L + 1.$$

$u = 68$.

$$N_{68}(2+\varrho) = \frac{2^{34}+1}{2^2+1} < 68L + 1.$$

In (10) the largest value results with $a = 1$, $b = 17$:

$$\frac{(2^{34}+1)^{1/2}\cdot(2^{17}+1)\cdot(2^2+1)^8}{(2^2+1)^{1/2}\cdot(2+1)\cdot 3^{16}} < 68L + 1.$$

$u = 74$; $c = 1$. In this case is, however,

$$N_{74}(2+\varrho) = 2^{37} - 1 > 74L + 1.$$

Now, to be able to decide for some more values of u, whether the norm $N_u(2+\varrho)$ is divisible by a prime p of the form $p = ul + 1$, $l > L$, we make some simple transformations. $(2+\varrho)$ and its conjugated numbers are either prime to each another, or have a prime ideal divisor of u as common factor, contain therefore only prime ideals of first degree; hence, $N_u(2+\varrho)$ may only be divisible by a divisor of u and by primes of the form $ku + 1$. Let us denote by $N'_u(2+\varrho)$ the number deriving from $N_u(2+\varrho)$, having divided with the divisors of u. Denoting by T_0:

$$T_0 = \frac{N'_u(2+\varrho) - 1}{u},$$

if among the numbers

$$T_k = \frac{T_0 - k}{uk + 1} < L \qquad (k = 0, 1, \ldots, t) \tag{12}$$

there is no integer prime, $N_u(2+\varrho)$ is not divisible by a prime $p = ul + 1$, $l > L$. This follows simply, as $N'_u(2+\varrho)$ has only divisors of the form $\equiv 1 \pmod{u}$.

If $u=74$, (12) gives $t=0$; $T_0=\frac{2^{37}-2}{74}=3\,714\,566\,310$ and this is no prime. On the other hand is

$$\frac{(2^{37}-1)\cdot(2^{37}+1)^{1/2}}{(2+1)^{1/2}\cdot 3^{18}}<74L+1.$$

$u=76$. In (12) is again $t=0$ and $T_0=1\,466\,725\,826$ is no prime. In (10) we must substitute $a=1$ and $b=19$ and then is

$$\frac{(2^{38}+1)^{1/2}\cdot(2^{19}-1)\cdot(2^2+1)^9}{(2^2+1)^{1/2}\cdot 3^{18}}<76L+1.$$

$u=80$.

$$N_{80}(2+\varrho)=\frac{2^{40}+1}{2^8+1}<80L+1.$$

In (10) we must take $a=5$, $b=16$:

$$\frac{(2^{40}+1)^{1/2}\cdot(2^8+1)^2\cdot(2^5+1)^4}{(2^8+1)^{1/2}\cdot(2+1)^4\cdot 3^{16}}<80L+1.$$

$u=82$; $c=1$. In (12) is $t=4$. $T_0=26\,817\,356\,775$ is no prime and T_1 is no integer.

$$\frac{(2^{41}-1)^{3/2}}{3^{20}}<82L+1.$$

$u=86$; $c=1$. In (12) is $t=4$. $T_0=102\,280\,151\,421$ is divisible by 3; T_1, T_2, T_3 and T_4 are no integers.

$$\frac{(2^{43}-1)^{3/2}}{3^{21}}<86L+1.$$

$u=88$. In (12) is $t=0$. $T_0=11\,759\,482\,650$ is no prime. In (10) we take $a=1$, $b=22$:

$$\frac{(2^{44}+1)\cdot(2^2+1)^{10}}{(2^4+1)\cdot 3^{20}}<88L+1.$$

$u=92$. In (12) is $t=6$. $T_0=152\,975\,530\,821$ and $T_3=552\,258\,234$ are no primes; the other T's are no integers. In (10) we set $a=1$ and $b=23$:

$$\frac{(2^{46}+1)^{1/2}\cdot(2^{46}-1)^{1/2}\cdot(2^2+1)^{11}}{(2^2+1)^{1/2}\cdot 3^{22}}<92L+1.$$

$u=94$; $c=1$. In (12) is $t=63$, $T_0=1\,497\,207\,322\,929$, $T_{25}=636\,838\,504$, $T_{48}=331\,754\,337$ are not primes; the other T's are not integers.

$$\frac{(2^{47}-1)^{3/2}}{3^{46}}<94L+1.$$

$u=98$. In (12) is $t=1$. $T_0=45\,231\,395\,904$ is no prime, T_1 is no integer. In (10) we set $a=1$, $b=14$

$$\frac{(2^{49}-1)\cdot(2^7+1)^3}{(2^7-1)\cdot(2+1)^3\cdot 3^{21}}<98L+1.$$

$u = 100.$

$$N_{100}(2+\varrho) = \frac{2^{50}+1}{2^{10}+1} = 1\,098\,438\,933\,505.$$

$$N'_{100}(2+\varrho) = 219\,687\,786\,701.$$

In (12) is $t = 0$ and $T_0 = 2\,196\,877\,867$. This is, however, no prime[3]):

$$T_0 = 23 \cdot 41 \cdot 2329669.$$

In (10) we set $a = 1$ and $b = 25$:

$$\frac{(2^{50}+1)^{1/2} \cdot (2^{50}-1)^{1/2} \cdot (2^2+1)^{10}}{(2^{10}+1)^{1/2} \cdot (2^{10}-1)^{1/2} \cdot 3^{20}} < 100L + 1.$$

$u = 110$. In (12) is $t = 0$ and $T_0 = 5\,161\,519\,113$ is no prime. In (10) we set $a = 1, b = 22$:

$$\frac{2^{55}-1) \cdot (2^5+1)^5}{(2^{11}-1) \cdot (2+1)^5 \cdot 3^{20}} < 110L + 1.$$

We can summarize our results in the following

Theorem. If l is an odd prime and one of the numbers $ul + 1$, $u = 2$, 4, 8, 10, 14, 16, 20, 22, 26, 28, 32, 34, 38, 40, 44, 46, 50, 52, 56, 58, 62, 64, 68, 70, 74, 76, 80, 82, 86, 88, 92, 94, 98, 100, 110, is a prime, the equation

$$x^l + y^l + z^l = 0,$$

has no integer solution x, y, z such that $l \nmid xyz$.

(*Received May 15, 1951.*)

[3]) I wish to thank here to Tibor Bakos who had determined the prime divisors of the above number.