MATH. SCAND. 67 (1990), 167–176.

SOPHIE GERMAIN'S PRINCIPLE AND LUCAS NUMBERS

ANASTASIOS SIMALARIDES

Abstract.

A criterion for the first case of Fermat's Last Theorem is given, which involves the Lucas numbers $v_n = \omega_1^n + \omega_2^n$, where $\omega_1 = \frac{1-\sqrt{5}}{2}$ and $\omega_2 = \frac{1+\sqrt{5}}{2}$. This criterion improves some previous results of Krasner and Dénes.

Introduction.

The first case of Fermat's Last Theorem is said to be true for the odd prime p, if

$$x^p + y^p + z^p = 0, \ (p, xyz) = 1, \tag{1}$$

has no solution in integers. Sophie Germain [10] proved that (1) is impossible in integers if $2p + 1$ is a prime. Her theorem was subsequently improved by Legendre [10] Dickson [3], [4] and Dénes [2]. Dénes's result reads:

(1) *is impossible in integers provided that* $cp + 1$ *is a prime, for some* c *with* $(3, c) = 1$ *and* $c \leqq 100$ *or* $c = 110$.

In 1940 Krasner [9] proved:

(1) *is impossible in integers provided that there exists a prime* q, $q = 1 + cp$, $(3, c) = 1$, $2^c \not\equiv 1 \pmod{q}$, $q > 3^{c/4}$. This result is "asymptotically" sharper than the above ones. However Krasner's theorem supersedes that of Dénes only when $p > 3^{25}/100$.

Combining Germain's principle with sophisticated analytic techniques Adleman, Fouvry and Heath-Brown [1], [5] proved that the first case of Fermat's Last Theorem is true for infinitely many prime exponents. Moreover Powell [12] and Ribenboim [13] extended Germain's method to a wide class of diophantine equations.

Recently Granville [7] established the impossibility of (1), in case $6p + 1$ is a prime, under certain additional hypotheses.

The author in this thesis [15] obtained an improvement of Krasner's theorem for the case of sufficiently large exponents, by invoking an inequality due to Siegel [14].

Received August 7, 1989, in revised form November 7, 1989

Here a new criterion is given by the use of a different method:

THEOREM 1. (1) *has no solution in integers provided that there exists a prime* q *with the following properties:*

(i) $q = 1 + cp$; (ii) $(3, c) = 1$; (iii) $c \equiv 0 \pmod 4$ *or* $2^c \not\equiv 1 \pmod q$;

(iv) $v_{\frac{c}{2}} \not\equiv 1 + (-1)^{c/2}$ *and* $-v_{\frac{c}{2}} \not\equiv 1 + (-1)^{c/2} \pmod q$;

(v) $q > \theta^{c/4}$, *where* $\theta = \frac{9}{2}e^{-881/1458} = 2.45917269\ldots$.

Here $v_n = \omega_1^n + \omega_2^n$, $\left(\omega_1 = \dfrac{1-\sqrt{5}}{2}, \omega_2 = \dfrac{1+\sqrt{5}}{2}\right)$, *is the* n-th *Lucas number.*

Before giving the proof of Theorem 1 we derive some of its corollaries. The inequalities

$$0 < |\pm v_{\frac{c}{2}} + 1 + (-1)^{c/2}| < 3 + \left(\frac{1+\sqrt{5}}{2}\right)^{c/2} > \theta^{c/4},$$

yield the following improvement of Krasner's theorem, namely

COROLLARY 1. (1) *has no solution in integers provided that there exists a prime* q, $q = 1 + cp$; $(3, c) = 1$; $c \equiv 0 \pmod 4$ *or* $2^c \not\equiv 1 \pmod q$; $q > 3 + \left(\dfrac{1+\sqrt{5}}{2}\right)^{c/2} = 3 + (2.618\ldots)^{c/4}$.

We will use Theorem 1 to improve Denes's theorem. For this let L be the greatest known number N with the following property: The first case of Fermat's Last Theorem is true for every prime $\leqq N$. At present $L = 714591416091389$ by Granville's result [8]. We need the following technical lemma, which goes back to Krasner [9].

LEMMA 1. *Let* α *be a real number,* $1 < \alpha \leqq 3$ *and let* $n \geqq 3$ *be an integer. We denote by* $c_1(\alpha, n)$, $c_2(\alpha, n)$, $c_3(\alpha, n)$ *the greatest positive roots of the equations* $1 + xn = \alpha^{x/4}$, $1 + xn = 1 + \alpha^{x/4}$, $1 + xn = 3 + \alpha^{x/4}$ *respectively. Then*

$$1 + cn > \begin{cases} \alpha^{c/4}, & \text{if } c < c_1(\alpha, n) \\ 1 + \alpha^{c/4}, & \text{if } c < c_2(\alpha, n) \\ 3 + \alpha^{c/4}, & \text{if } c < c_3(\alpha, n) \end{cases}$$

The numbers $c_1(\alpha, n)$, $c_2(\alpha, n)$, $c_3(\alpha, n)$ *are the limits of the sequences* x_k, y_k, z_k *defined by the recursive formulae* $1 + nx_k = \alpha^{x_{k+1}/4}$, $1 + ny_k = 1 + \alpha^{y_{k+1}/4}$, $1 + nz_k = 3 + \alpha^{z_{k+1}/4}$, *respectively, with* $x_0 = y_0 = z_0 = \dfrac{4}{\log\alpha}\log n$. *Evidently* $c_1(\alpha, n)$, $c_2(\alpha, n)$, $c_3(\alpha, n) > \dfrac{4}{\log\alpha}\log n$.

We can always assume that $p > L$; this implies that

$$c_i(\alpha, p) \geqq c_i(\alpha, L), \text{ for } i = 1, 2, 3.$$

Also Lemma 1 implies

$$1 + cp > \begin{cases} \theta^{c/4} & \text{if } c < c_1(\theta, p) \\ 1 + 2^{c/2} & \text{if } c < c_2(4, p) \\ 3 + \omega_2^{c/2} & \text{if } c < c_3(\omega_2^2, p) \end{cases}$$

In view of these inequalities Theorem 1 leads to:

THEOREM 2. (1) *has no solution in integers provided that:*

(I) $q = cp + 1$ *is a prime for some* c, *with* $(3, c) = 1$ *and* $c < c_1(\theta, L)$.

(II) $2^c \not\equiv 1 \pmod{q}$ *if* $c \not\equiv 0 \pmod 4$, $c_2(4, L) \leqq c < c_1(\theta, L)$ *and* $p > L$.

(III) $\pm v_{\frac{c}{2}} \not\equiv 1 + (-1)^{c/2} \pmod{q}$ *if* $c_3(\omega_2^2, L) \leqq c < c_1(\theta, L)$ *and* $p > L$.

Applying Theorem 2 for $L = 714591416091389$ we obtain the following improvement of Denes's result:

COROLLARY 2. (1) *has no solution in integers provided that* $cp + 1$ *is a prime for some* c, *with* $(3, c) = 1$ *and* $c \leqq 174$.

PROOF. Since $c_1(\theta, 714591416091389) = 175.0007\ldots$, $c_2(4, 714591416091389) = 112.31\ldots$, $c_3(\omega_2^2, 714591416091389) = 163.44\ldots$, hypothesis (I) of Theorem 2 is satisfied. Hyphotesis (II) is also satisfied, since the number $2^u - 1$ does not have any prime divisor of the form $1 + ul$ with l prime and $l > 714591416091389$ for $u = 116, 118, 122, 124, 128, 130, 134, 136, 140, 142, 146, 148, 152, 154, 158, 160, 164, 166, 170, 172$, ([11] gives references for factorisation tables of these numbers). Now since

$v_{82} - 2 = 137083915467899401 = 370248451^2$,

$v_{82} + 2 = 137083915467899405 = 5 \cdot 2789 \cdot 9830327391029$,

$v_{86} - 2 = 939587134549734841 = 969323029^2$,

$v_{86} + 2 = 939587134549734845 = 5 \cdot 433494437^2$,

it follows that the prime divisors of $\pm v_{\frac{u}{2}} + 1 + (-1)^{u/2}$ for $u = 164$ or 172 are $\leqq 1 + u \cdot 714591416091389$. By the well known factorisation tables of Lucas numbers ([11]) it follows that the numbers v_{83} and v_{85} do not have any prime factor of the form $1 + ul$, where l is a prime > 714501416091389, for $u = 166$ or 170 respectively. Consequently hypothesis (III) of Theorem 2 is satisfied. This ends the proof of Corollary 2.

Proof of Theorem 1.

Assume that (1) holds true for some integers x, y, z. We will show that this leads to a contradiction.

LEMMA 1. $(q, xyz) = 1$.

PROOF. From (1) it follows that $p \geqq 31$. So, assuming $c \geqq p$, it follows by the hypothesis (v) of the theorem that $c^2 \geqq \theta^{c/4}$ and $c \geqq 31$, which is absurd. Therefore

$$c < p. \tag{2}$$

Now assuming $(q, xyz) > 1$ it follows by Furtwängler's theorem [6] that $q^{p-1} \equiv 1 \pmod{p^2}$, which contradicts (2). This proves the lemma.

We turn back to the proof of the theorem. By Lemma 1 it follows that $x^{q-1} \equiv y^{q-1} \equiv z^{q-1} \equiv 1 \pmod q$ and so

$$x^p \equiv \zeta^{a_1},\ y^p \equiv \zeta^{a_2},\ z^p \equiv \zeta^{a_3} (\operatorname{mod} \mathfrak{q}),\ (\zeta = e^{2\pi i/c}),$$

where a_1, a_2, a_3 are integers and $\mathfrak{q}$ is a prime ideal divisor of q in $Q(\zeta)$. Consequently

$$1 + \zeta^a + \zeta^b \equiv 0 (\operatorname{mod} \mathfrak{q}), \tag{3}$$

where $0 \leqq a \leqq b < c$. By Legendre's criterion [10] it follows that

$$c \geqq 16. \tag{4}$$

We distinguish two cases 1) and 2):

1) $a = 0$ or $b = 0$ or $a = b$; then

$$2^c \equiv 1 (\operatorname{mod} q), \tag{5}$$

which contradicts hyphothesis (iii) in case the incongruence $2^c \not\equiv 1 (\operatorname{mod} q)$ holds by hyphothesis. In case $c \equiv 0 \pmod 4$ we distinguish the subcases $c \not\equiv 0 \pmod 8$ and $c \equiv 0 \pmod 8$. In the first subcase, congruence (5) leads to

$$(2^{\frac{c}{4}} - 1)(2^{\frac{c}{4}} + 1)(2^{\frac{c}{4}} - 2^{\frac{c+4}{8}} + 1)(2^{\frac{c}{4}} + 2^{\frac{c+4}{8}} + 1) \equiv 0 \qquad (\operatorname{mod} q)$$

(Aurifeuillian factorisation), which implies $q \leqq 2^{c/4} + 2^{(c+4)/8} + 1$. The last inequality contradicts, (in view of (4)), hyphothesis (v) because

$$\theta^{c/4} > 2^{c/4} + 2^{(c+4)/8} + 1, \text{ for } c \geqq 16.$$

In the second subcase we have $c = 2^k n$, with $k \geqq 3$, n odd. By (5) it follows that

$$(2^{\frac{c}{4}} - 1)(2^{\frac{c}{4}} + 1)(2^{\frac{c}{2}} + 1) \equiv 0 \qquad (\operatorname{mod} q).$$

Hence $2^{c/2} + 1 \equiv 0 (\operatorname{mod} q)$ because $\theta^{c/4} > 2^{c/4} + 1$.
Since $q \equiv 1 \pmod 8$, 2 is a quadratic residue mod q, say $2 \equiv t^2 (\operatorname{mod} q)$. Then

$$2^{\frac{c}{2}} + 1 \equiv t^c + 1 = (t^n)^{2^k} + 1 = F_{2^{k+1}}(t^n) \equiv 0 (\operatorname{mod} q),$$

where $F_m(x)$ denotes the mth cyclotomic polynomial. Since $(q, t) = 1$ it follows that $q \equiv 1 \pmod{2^{k+1}}$, which contradicts the fact that n is odd.

2) $0 < a < b < c$.

Since $\zeta^{c/2} + 1 = 0$ the resultant $R(a, b)$ of the polynomials $1 + t^a + t^b$, $t^{c/2} + 1$ satisfies the congruence

$$R(a, b) \equiv 0 \pmod q. \tag{6}$$

In explicit form

$$\begin{aligned} R(a,b) &= \prod_{i=1}^{c/2} [1 + \zeta^{(2i-1)a} + \zeta^{(2i-1)b}] \\ &= \prod_{i=1}^{c_1} \left[3 + 2\cos\frac{2\pi a}{c}(2i-1) + 2\cos\frac{2\pi b}{c}(2i-1) \right. \\ &\qquad \left. + 2\cos\frac{2\pi(a-b)}{c}(2i-1) \right] d \end{aligned}$$

where

$$c_1 = \begin{cases} \dfrac{c}{4} & \text{if } c \equiv 0 \pmod 4 \\ \dfrac{c}{4} - \dfrac{1}{2} & \text{if } c \not\equiv 0 \pmod 4 \end{cases} \quad \text{and } d = \begin{cases} 1 & \text{if } c \equiv 0 \pmod 4 \\ 1 + (-1)^a + (-1)^b & \text{if } c \not\equiv 0 \pmod 4. \end{cases}$$

By (ii) if follows that $R(a, b) \neq 0$. Introducing the abbreviation

$$A_i = \cos\frac{2\pi a}{c}(2i-1) + \cos\frac{2\pi b}{c}(2i-1) + \cos\frac{2\pi(a-b)}{c}(2i-1),$$

we obtain

$$\begin{aligned} \log|R(a,b)| &= \sum_{i=1}^{c_1} \log(3 + 2A_i) + \log|d| \\ &= c_1 \log\tfrac{9}{2} + \sum_{i=1}^{c_1} \log(1 + \tfrac{1}{3}(-1 + \tfrac{4}{3}A_i)) + \log|d|, \end{aligned}$$

where evidently $-1 < \frac{1}{3}(-1 + \frac{4}{3}A_i) \leqq 1$. Since

$$\log(1 + X) \leqq X - \frac{X^2}{2} + \frac{X^3}{3}, \text{ for } -1 < X \leqq 1,$$

it follows that

$$\log(1 + \tfrac{1}{3}(-1 + \tfrac{4}{3}A_i)) \leqq -\tfrac{65}{162} + \tfrac{52}{81}A_i - \tfrac{40}{243}A_i^2 + \tfrac{64}{2187}A_i^3.$$

Consequently

$$(7)\quad \log|R(a,b)| \leqq c_1 \log\tfrac{9}{2} - \tfrac{65}{162}c_2 + \tfrac{52}{81}\cdot\sum_{i=1}^{c_1} A_i - \tfrac{40}{243}\cdot\sum_{i=1}^{c_1} A_i^2 + \tfrac{64}{2187}\cdot\sum_{i=1}^{c_1} A_i^3 + \log|d|$$

Given two real variables X and Y we have

$$[\cos X + \cos Y + \cos(X-Y)]^2 = \tfrac{3}{2} + \cos X + \cos Y + \cos(X-Y) + \tfrac{1}{2}\cos 2X + \tfrac{1}{2}\cos 2Y + \tfrac{1}{2}\cos 2(X-Y) + \cos(X+Y) + \cos(X-2Y) + \cos(2X-Y);$$

$$[\cos X + \cos Y + \cos(X-Y)]^3 = \tfrac{3}{2} + \tfrac{15}{4}\cos X + \tfrac{15}{4}\cos Y + \tfrac{15}{4}\cos(X-Y) + \tfrac{3}{2}\cos 2X + \tfrac{3}{2}\cos 2Y + \tfrac{3}{2}\cos 2(X-Y) + \tfrac{3}{2}\cos(X+Y) + \tfrac{3}{2}\cos(2X-Y) + \tfrac{3}{2}\cos(X-2Y) + \tfrac{1}{4}\cos 3X + \tfrac{1}{4}\cos 3Y + \tfrac{1}{4}\cos 3(X-Y) + \tfrac{3}{4}\cos(X+2Y) + \tfrac{3}{4}\cos(2X+Y) + \tfrac{3}{4}\cos(3X-Y) + \tfrac{3}{4}\cos(3X-2Y) + \tfrac{3}{4}\cos(2X-3Y) + \tfrac{3}{4}\cos(X-3Y);$$

and trivially

$$[\cos X + \cos Y + \cos(X-Y)]^1 = \cos X + \cos Y + \cos(X-Y).$$

Writing the above formulas as

$$(8)\qquad [\cos X + \cos Y + \cos(X-Y)]^n = \sum_{r,s} c_{r,s}^{(n)} \cos(rX + sY),\ n = 1,2,3$$

we obtain

$$(9)\qquad \sum_{i=1}^{c_1} A_i^n = \sum_{r,s} c_{r,s}^{(n)} \sum_{i=1}^{c_1} \cos\frac{2\pi(ra+sb)}{c}(2i-1),\ n = 1,2,3.$$

Since for an integer $m \geqq 1$,

$$\sum_{i=1}^{m} \cos(2i-1)\kappa\pi = \begin{cases} m(-1)^\kappa & \text{if } \kappa \text{ is an integer} \\ \dfrac{\sin 2m\kappa\pi}{2\sin\kappa\pi} & \text{if } \kappa \text{ is not an integer} \end{cases}$$

it follows that

$$(10)\quad \sum_{i=1}^{c_1} \cos\frac{2\pi(ra+sb)}{c}(2i-1) = \begin{cases} c_1(-1)^{2(ra+sb)/c} \text{ if } ra+sb \equiv 0\left(\operatorname{mod}\dfrac{c}{2}\right) \\ 0 \text{ if } ra+sb \not\equiv 0\left(\operatorname{mod}\dfrac{c}{2}\right) \text{ and } c \equiv 0 (\operatorname{mod} 4) \\ -\tfrac{1}{2}\cos(ra+sb)\pi \text{ if } ra+sb \not\equiv 0\left(\operatorname{mod}\dfrac{c}{2}\right) \\ \text{and } c \not\equiv 0(\operatorname{mod} 4). \end{cases}$$

LEMMA 2. *Let (a, b) be a solution of*

$$(11) \qquad 1 + \zeta^A + \zeta^B \equiv 0 (\mathrm{mod}\, \mathfrak{q}),\ 0 < A < B < c.$$

Then the following hold true:
(I) $(a, b) = (b_1 - a_1, c - a_1)$ *and* $(a, b) = (c - b_2, c - b_2 + a_2)$, *where* (a_1, b_1) *and* (a_2, b_2) *are solutions of* (11).
(II) $ra + sb \not\equiv 0\left(\mathrm{mod}\, \frac{c}{2}\right)$ *for all indices* r, s $(r, s) \neq (0, 0)$, *which appear in* (8) *for* $n = 1, 2, 3$.

PROOF The pairs $(b - a, c - a)$, $(c - b, c - b + a)$ are together with (a, b) solutions of (11). Therefore putting $(a_1, b_1) = (c - b, c - b + a)$, $(a_2, b_2) = (b - a, c - a)$ we obtain $(a, b) = (b_1 - a_1, c - a_1)$ and $(a, b) = (c - b_2, c - b_2 + a_2)$. This proves part (I) of the lemma.

We now come to part (II). At first we prove that

$$(12) \qquad \begin{matrix} 2a \not\equiv 0 & 2b \not\equiv 0 & 2(a - b) \not\equiv 0 & a + b \not\equiv 0 \\ 3a \not\equiv 0 & 3b \not\equiv 0 & 3(a - b) \not\equiv 0 & 3a - b \not\equiv 0 \\ & & & a - 3b \not\equiv 0 \end{matrix} \left(\mathrm{mod}\, \frac{c}{2}\right).$$

Assuming $2a \equiv 0\left(\mathrm{mod}\, \frac{c}{2}\right)$, we obtain $a = \frac{c}{4}$ or $\frac{c}{2}$ or $\frac{3c}{4}$. In the second case we have $1 + \zeta^a + \zeta^b = 1 + \zeta^{c/2} + \zeta^b = \zeta^b$, which contradicts (3) since ζ^b is a unit. In cases $a = c/4$ or $3c/4$ we have $\zeta^a = i^k$ $(k = 1$ or $3, i = \sqrt{-1})$. Then by (3) it follows that $(1 + i^k)^c \equiv 1 (\mathrm{mod}\, \mathfrak{q})$ and so $[(1 + i^k)^{c/4}]^4 \equiv 1 (\mathrm{mod}\, \mathfrak{q})$. This implies

$$(1 + i^k)^{c/4} \equiv i^m (\mathrm{mod}\, \mathfrak{q}), \text{ where } m \in \{1, 2, 3, 4\}.$$

Denoting by N_c the norm in $Q(e^{2\pi i/c})$ we obtain

$$N_4((1 + i^k)^{c/4} - i^m) \equiv 0 (\mathrm{mod}\, q),$$

which contradicts (v) because

$$0 < N_4((1 + i^k)^{c/4} - i^m) = |(1 + i)^{c/4} - i^m|^2 \leqq [(\sqrt{2})^{c/4} + 1]^2 < \theta^{c/4}, \text{ for } c \geqq 16.$$

Consequently $2a \not\equiv 0\left(\mathrm{mod}\, \frac{c}{2}\right)$. In the same way follow the relations $2b \not\equiv 0$, $2(a - b) \not\equiv 0\left(\mathrm{mod}\, \frac{c}{2}\right)$. The relations $3a \not\equiv 0$, $3b \not\equiv 0$, $3(a - b) \not\equiv 0\left(\mathrm{mod}\, \frac{c}{2}\right)$ are immediate in view of hyphothesis (ii). Assuming $a + b \equiv 0\left(\mathrm{mod}\, \frac{c}{2}\right)$ we obtain $\zeta^b = \pm \zeta^a$. We distinguish two cases (A) and (B):
(A) $\zeta^b = \zeta^{-a}$. Then $1 + \zeta^a + \zeta^b = 1 + \zeta^a + \zeta^{-a}$; hence $1 + \zeta^a + \zeta^{2a} \equiv 0 (\mathrm{mod}\, q)$, which is absurd, since the left member is a unit.

(B) $\zeta^b = -\zeta^{-a}$. Then $1 + \zeta^a + \zeta^b = 1 + \zeta^a - \zeta^{-a}$. Therefore $-1 + \zeta^a + \zeta^{2a} \equiv 0 \pmod q$. Hence the polynomials $t^2 + t - 1$ and

(13) $$t^{c/2} + (-1)^m, \text{ where } m = 1 \text{ or } 2,$$

have a common root mod q. Thus

(14) $$R = R(t^2 + t - 1, t^{c/2} + (-1)^m) \equiv 0 \pmod q.$$

The roots of $t^2 + t - 1$ are $-\omega_1$ and $-\omega_2$, and

$$R = [(-\omega_1)^{\frac{c}{2}} + (-1)^m]\cdot[(-\omega_2)^{\frac{c}{2}} + (-1)^m]$$

$$= 1 + v_{\frac{c}{2}}\cdot(-1)^{m+\frac{c}{2}} \neq 0.$$

Thus our congruence (14) contradicts the hyphothesis (iv) of the theorem. Consequently $a + b \not\equiv 0\left(\bmod \frac{c}{2}\right)$. Assuming $3a - b \equiv 0\left(\bmod \frac{c}{2}\right)$ we obtain $\zeta^{3a} = \pm\zeta^b$. We distinguish again two cases (C) and (D).

(C) $\zeta^{3a} = \zeta^b$. Then the polynomials $t^3 + t + 1$and (13) have a common root mod q; hence

(15) $$R = R(t^3 + t + 1, t^{c/2} + (-1)^m) \equiv 0 \pmod q.$$

The roots of the polynomial $t^3 + t + 1$ are
$\rho_1 = -0.68232776\ldots$, $\rho_2 = 0.34116388\ldots + (1.161541365\ldots)i$, $\bar\rho_2$. Hence

$$0 < |R| \leqq (|\rho_1|^{c/2} + 1)(|\rho_2|^{c/2} + 1)^2 < (0.68233^{\frac{c}{2}} + 1)(1.2107^{\frac{c}{2}} + 1)^2 < \theta^{\frac{c}{4}}.$$

Congruence (15) contradicts the hyphothesis (v) of the theorem.

(D) $\zeta^{3a} = -\zeta^b$. Then the polynomial $t^3 - t - 1$ with roots $\rho_1 = 1.32471796\ldots$, $\rho_2 = -0.66235898\ldots + (0.562279515\ldots)i$, $\bar\rho_2$ and the polynomial (13) have a common root mod q. Thus

(16) $$R = R(t^3 - t - 1, t^{c/2} + (-1)^m) \equiv 0 \pmod q$$

and since

$$0 < |R| \leqq (|\rho_1|^{\frac{c}{2}} + 1)(|\rho_2|^{\frac{c}{2}} + 1)^2 < (1.33^{\frac{c}{2}} + 1)(0.87^{\frac{c}{2}} + 1)^2 < \theta^{c/4}$$

relation (16) contradicts hyphothesis (v) of the theorem. Consequently $3a - b \not\equiv 0\left(\bmod \frac{c}{2}\right)$. In exactly the same way we obtain $b - 3a \not\equiv 0\left(\bmod \frac{c}{2}\right)$.

We now establish the remaining incongruences of (II) for the expressions $a + 2b$, $2a + b$, $2a - b$, $a - 2b$, $3a - 2b$, $2a - 3b$, $2a - 3b$; part (I) of Lemma 2 and (12) yield:

$$\begin{array}{llll} a+2b \equiv b_1-3a_1 \not\equiv 0 & a-2b \equiv a_1+b_1 \not\equiv 0 \\ 2a+b \equiv a_2-3b_2 \not\equiv 0 & 3a-2b \equiv a_1-3b_1 \not\equiv 0 \\ 2a-b \equiv -a_2-b_2 \not\equiv 0 & 2a-3b \equiv 3a_2+b_2 \not\equiv 0 \end{array} \left(\bmod \frac{c}{2}\right).$$

This completes the proof of part (II) of the lemma.

We then turn to the proof of theorem. We distinguish two cases (α) and (β).
(α) $c \equiv 0 \pmod 4$; by part (II) of Lemma 2 the second equality in (10) and (9) it follows that

$$\sum_{i=1}^{c_1} A_i = 0,\ \sum_{i=1}^{c_1} A_i^2 = \tfrac{3}{2}c_1,\ \sum_{i=1}^{c_1} A_i^3 = \tfrac{3}{2}c_1.$$

Since $c_1 = \dfrac{c}{4}$, $d = 1$ relation (7) yields

$$\log|R(a,b)| \leqq \left(\log\tfrac{9}{2} - \tfrac{65}{162} - \tfrac{40}{243}\cdot\tfrac{3}{2} + \tfrac{64}{2187}\cdot\tfrac{3}{2}\right)\frac{c}{4} = (\log\theta)\frac{c}{4}, \tag{17}$$

which (by (6)) contradicts the hyphothesis (v) of the theorem.
(β) $c \not\equiv 0 \pmod 4$; by part (II) of Lemma 2, the third equality in (10) and (9) it follows that

$$\begin{aligned}\sum_{i=1}^{c_1} A_i &= -\tfrac{1}{2}\cdot\sum_{r,s} c_{r,s}^{(1)}\cos(ra+sb)\pi = -\tfrac{1}{2}[\cos a\pi + \cos b\pi + \cos(a-b)\pi] \\ &= -\tfrac{1}{2}[(-1)^a + (-1)^b + (-1)^{a-b}];\end{aligned}$$

$$\sum_{i=1}^{c_1} A_i^n = c_{0,0}^{(n)}\cdot\frac{c}{4} - \frac{1}{2}\cdot\sum_{r,s} c_{r,s}^{(n)}\cos(ra+sb)\pi = \tfrac{3}{8}c - \tfrac{1}{2}\cdot\sum_{r,s} c_{r,s}^{(n)}\cos(ra+sb)\pi$$

for $n = 2, 3$. The last equality implies in view of (8):

$$\sum_{i=1}^{c_1} A_i^n = \frac{3c}{8} - \frac{1}{2}[(-1)^a + (-1)^b + (-1)^{a-b}]^n,\ n = 2, 3.$$

Inequality (7) yields then the estimate

$$\begin{aligned}\log|R(a,b)| \leqq{}& (\log\theta)\frac{c}{4} - \tfrac{1}{2}\log\tfrac{9}{2} + \tfrac{65}{324} - \tfrac{26}{81}[(-1)^a + (-1)^b + (-1)^{a-b}] \\ &+ \tfrac{20}{243}[(-1)^a + (-1)^b + (-1)^{a-b}]^2 \\ &- \tfrac{32}{2187}[(-1)^a + (-1)^b + (-1)^{a-b}]^3 + \log|d|.\end{aligned}$$

Hence

$$\log|R(a,b)| \leqq \begin{cases} (\log\theta)\dfrac{c}{4} - 0.070093067\ldots, & \text{if } a,b \text{ are both even} \\ (\log\theta)\dfrac{c}{4} - 0.133497321\ldots, & \text{otherwise,} \end{cases} \tag{18}$$

which (by (6)) contradicts hyphothesis (v) of the theorem. Therefore (1) is impossible and the theorem is proved.

The method of proof used here has Krasner's proof [9] as its origin. The estimates (17) and (18) improve the estimate $|R(a,b)| \leqq 3^{c/4}$ obtained by Krasner by using an inequality due to Hadamard.

NOTE. In [8] the new bound $L = 156442236847241650$, due to Tanner and Wagstaff, is announced without proof. For this bound: $c_1(\theta, L) = 199.538\ldots$, $c_2(4, L) = 128.242\ldots$, $c_3(\omega_2^2, L) = 186.274\ldots$, and so the inequality in corollary 2 can be improved to $c \leqq 198$.

REFERENCES

1. L. M. Adleman and D. R. Heath-Brown, *The first case of Fermat's last theorem*, Invent. Math. 79(1985), 409–416.
2. P. Dénes, *An extension of Legendre's criterion in connection with the first case of Fermat's last theorem*, Publ. Math. Debrecen 2 (1951), 115–120.
3. L. E. Dickson, *On the last theorem of Fermat*, Quarterly Journ. of Math. 40 (1907), 27–45.
4. L. E. Dickson, Messenger of Math. (2) 38 (1908), 14–33.
5. E. Fouvry, *Théorème de Brun-Titchmarsh: application au théorème de Fermat*, Invent. Math. 79 (1985), 383–407.
6. P. Furtwängler, *Letzter Fermatschen Satz und Eisenstein'sches Reziprozitätsgesetz*, Sitzungsber. Akad. Wiss. Wien. Abt. IIa 121 (1912), 589–592.
7. A. Granville, *Sophie Germain's Theorem for prime pairs p*, 6p + 1, J. Number Theory 27 (1987), 63–72.
8. A. Granville, *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 (1988), 329–359.
9. M. Krasner, *A propos du critère de Sophie Germain-Furtwängler pour le premier cas du théorème de Fermat*, Math. Cluj 16 (1940), 109–114.
10. A. M. Legendre, *Recherches sur quelques objects d'analyse indéterminée et particulièrement sur la théorème de Fermat*, Mem. Acad. Sci. Inst. France 6 (1823), 1–60.
11. D. H. Lehmer, *Guide to the Tables in the Theory of Numbers*, National Research Council Bulletin, Washington, 1941.
12. B. J. Powell, *Proof of the impossibility of the Fermat equation* $X^p + Y^p = Z^p$ *for special values of p and of the more general equation* $bX^n + cY^n = dZ^n$, J. Number Theory 18 (1984), 34–40.
13. P. Ribenboim, *An extension of Sophie Germain's method to a wide class of diophantine equations*, J. Reine Angew. Math. 356 (1985), 49–66.
14. C. L. Siegel, *The trace of totally positive and real algebraic integers*, Ann. of Math. 46 (1945), 302–312.
15. A. Simalarides, *Applications of the theory of the cyclotomic field to Fermat's equation and congruence*, Ph. D. Thesis, Athens University, Athens 1984.

L. KIFISSIAS 196
KIFISSIA 14562
ATHENS
GREECE