STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

DR 14r

A remark on Fermat's last theorem.

euw Archief voor Wiskunde,3e Serie,1)1953),p 123-128).

H.J.A.Duparc en A.van Wijngaarden.

1953

Nieuw Archief voor Wiskunde (3) I, 123—128 (1953)

14

A REMARK ON FERMAT'S LAST THEOREM

BY

H. J. A. DUPARC and A. VAN WIJNGAARDEN
(Mathematical Centre, Amsterdam)

1. In a recent paper by R. OBLATH [1]) lower bounds for z^p, satisfying

$$x^p + y^p = z^p \quad (x, y, z \text{ positive integers}; \ p > 2, \text{ prime}) \qquad (1.1)$$

are given. As usual two cases are distinguished, viz.

Case I: $xyz \not\equiv 0 \pmod{p}$;

Case II: $xyz \equiv 0 \pmod{p}$.

In either case certain congruences are combined with numerical lower bounds of p to the following results

Case I: $z^p > 10^{4.5\times 10^9}$;

Case II: $z^p > 10^{3.2\times 10^6}$.

In this note it is shown that in case I by using the same lower bound $p \geqq 253747889$ of D. H. and EMMA LEHMER [2]) the following sharper result can be derived:

Case I: $z > 10^{6\times 10^9}$; $z^p > 10^{1.5\times 10^{18}}$.

2. In the following sections p denotes a prime > 7.

For sake of symmetry in (1.1) put $X = x$, $Y = y$, $Z = -z$, hence

$$X^p + Y^p + Z^p = 0. \qquad (2.1)$$

With the restriction of case I ($p \nmid xyz$) one has:

$$X, Y, Z \text{ are integers}, \ p \nmid XYZ.$$

LANDAU [3]) proves

$$2X = -A^p+B^p+C^p, \ 2Y = A^p-B^p+C^p, \ 2Z = A^p+B^p-C^p,$$

where A, B and C are integers and

$$X + A \equiv Y + B \equiv Z + C \equiv 0 \pmod{p^2};$$
$$X^{p-1} \equiv Y^{p-1} \equiv Z^{p-1} \equiv 1 \pmod{p^3}.$$

Hence

$$A+B+C \equiv -(X+Y+Z) \equiv -(X^p+Y^p+Z^p) = 0 \pmod{p^2}.$$

Further [4])

$$-2CC' = A^p + B^p - C^p;\ (C, C') = 1;\ C' \equiv 1 \pmod{p^2}.$$

There are two kinds of prime factors of C, viz.

i) $q_1 \mid C,\ q_1 \nmid A + B$. From $q_1 \mid A^p + B^p$ a simple argument learns $q_1 \equiv 1 \pmod{p}$, hence $q_1^p \equiv 1 \pmod{p^2}$. Moreover using the first theorem of FURTWANGLER [5]) the prime factor q_1 of C, hence of Z satisfies

$$q_1 \equiv q_1^p \equiv 1 \pmod{p^2}.$$

ii) $q_2 \mid C,\ q_2 \mid A + B$. If $q_2^u \mid C,\ q_2^{u+1} \nmid C$, then $q_2^u \mid A^p + B^p$. Since $\left(A + B, \dfrac{A^p + B^p}{A + B}\right) = (A + B,\ p\,A^{p-1}) = 1$ (for otherwise either $p \mid AB \mid XY$ or $(A, B) \neq 1$) one has $q_2^u \mid A + B$, hence $q_2^u \mid A + B + C$.

Then putting $C = C_1C_2$, where C_1 only contains prime factors of the first kind (q_1) and C_2 only prime factors of the second kind (q_2) one has

$$C_1 \equiv 1 \pmod{p^2},\ C \equiv C_2 \pmod{p^2},\ C_2 \mid A + B + C. \quad (2.2)$$

Similarly

$$A \equiv A_2 \pmod{p^2},\ B \equiv B_2 \pmod{p^2} \quad (2.3)$$

and

$$A_2 \mid A + B + C,\ B_2 \mid A + B + C. \quad (2.4)$$

Since A, B and C are pairwise coprime, so are A_2, B_2 and C_2 hence

$$A_2B_2C_2 \mid A + B + C. \quad (2.5)$$

From $z > x$, $z > y$ it follows $A < 0$, $B < 0$ and from $x + y > 0$ it follows $C > 0$. Assuming without loss of generality $x < y$ one has $B < A$. Hence defining positive integers a, b, c and integers a_2, b_2, c_2 by

$$a + A = b + B = c - C = a_2 + A_2 = b_2 + B_2 = c_2 - C_2 = 0$$

one has

$$2x = a^p - b^p + c^p,\ 2y = -a^p + b^p + c^p,\ 2z = a^p + b^p + c^p. \quad (2.6)$$

Since $(x + y)^p > x^p + y^p = z^p$ one has $x + y > z$, $c^p > a^p + b^p$. Hence $c > b > a > 0$. Further the following congruences hold

$$a + b - c \equiv a_2 + b_2 - c_2 \equiv 0 \pmod{p^2}$$

and

$$0 = x^p + y^p - z^p \equiv x + y - z = c^p - a^p - b^p \equiv c - a - b \pmod{6}.$$

Thus

$$a + b - c \equiv 0 \pmod{6p^2}. \tag{2.7}$$

Finally in virtue of (2.2) and (2.3) one obtains

$$a = a_2 + a_3 p^2,\ b = b_2 + b_3 p^2,\ c = c_2 + c_3 p^2, \tag{2.8}$$

where a_3, b_3 and c_3 are integers and in virtue of (2.5) one has

$$a_2 b_2 c_2 \mid a + b - c. \tag{2.9}$$

3. Putting $\frac{a}{c} = \alpha$, $\frac{b}{c} = \beta$ from (1.1) and (2.6) one obtains

$$(-\alpha^p + \beta^p + 1)^p + (\alpha^p - \beta^p + 1)^p = (\alpha^p + \beta^p + 1)^p;$$

$$0 < \alpha < \beta < 1;\ \alpha^p + \beta^p < 1. \tag{3.1}$$

Using after a suggestion of C. G. Lekkerkerker for $0 < u < v$ the relation

$$p(v - u)u^{p-1} < v^p - u^p < p(v - u)v^{p-1}$$

one has

$$2p\alpha^p(1 - \alpha^p + \beta^p)^{p-1} < (\alpha^p - \beta^p + 1)^p < 2p\alpha^p(\alpha^p + \beta^p + 1)^{p-1},$$

hence

$$\alpha^p < (\alpha^p - \beta^p + 1)^p < 2p\alpha^p(1 + 2\beta^p)^p,$$

thus

$$\alpha < \alpha^p - \beta^p + 1 < (1 + 2\beta^p)\sqrt[p]{2p}.$$

Consequently one finds the result

$$1 - \beta^p < \alpha(1 + 2\beta^p)\sqrt[p]{2p} \tag{3.2}$$

and

$$2(1 - \beta^p) > \alpha - \alpha^p + 1 - \beta^p > \alpha,$$

thus

$$1 - \beta^p > \tfrac{1}{2}\alpha. \tag{3.3}$$

Now from (3.2) it follows

$$\beta > 1 - \frac{\log 2pe}{p}. \tag{3.4}$$

In fact the supposition $\beta \leq 1 - \frac{\log 2pe}{p}$ leads to

$$\beta^p < \left(1 - \frac{\log 2pe}{p}\right)^p < \frac{1}{2pe},$$

thus

$$e^{-\frac{2}{pe}} < \frac{1}{1 + \frac{2}{pe}} < \frac{1 - \frac{1}{2pe}}{1 + \frac{1}{pe}} < \frac{1 - \beta^p}{1 + 2\beta^p} < a\sqrt[p]{2p} < \beta\sqrt[p]{2p} < e^{-\frac{1}{p}},$$

which is impossible since $e > 2$.

Since $p \geq 8$ one obtains from (3.4) the relation $\beta > \frac{1}{2}$.

Then using (3.2) one finds

$$\frac{1 - \beta^p}{1 - \beta} \geq 1 + \beta + \beta^2 + \beta^3 + \beta^4 >$$

$$> 1\tfrac{1}{2} + 3\beta^p > \sqrt{2}(1 + 2\beta^p) > \sqrt[p]{2p}(1 + 2\beta^p) > \frac{1 - \beta^p}{a},$$

hence

$$a + \beta > 1. \tag{3.5}$$

4. From (2.7) and (3.5) one has

$$a + b = c + mp^2, \text{ where } 6 \mid m, \ m > 0.$$

Now two cases are distinguished

i. $m \geq p$. Then

$$c > a = c - b + mp^2 > mp^2 \geq p^3. \tag{4.1}$$

ii. $6 \leq m < p$. Using (2.9) one has $a_2b_2c_2 \mid m$, hence

$$| a_2 | \leq m < p, \ | b_2 | < p, \ | c_2 | < p.$$

Further $0 < b_2 + b_3p^2$, hence $b_3p^2 > -b_2 > -p$, thus $b_3 \geq 0$ and

$$c_2 - b_2 + p^2(c_3 - b_3) = c - b > 0,$$

hence

$$c_3 - b_3 > \frac{b_2 - c_2}{p^2} > \frac{-2}{p}, \ c_3 \geq b_3 \geq 0.$$

The case $c_3 = b_3$ is excluded.

In fact suppose $c_3 = b_3$. Then $c_2 - b_2 = c - b > 0$, hence

$$\beta = \frac{b_2 + b_3p^2}{c_2 + c_3p^2} = 1 - \frac{c_2 - b_2}{c_2 + c_3p^2},$$

thus using (3.3)

$$1 - \tfrac{1}{2}a > \beta^p > 1 - \frac{p(c_2 - b_2)}{c_2 + c_3 p^2},$$

hence

$$a < \frac{2p(c_2 - b_2)}{c_2 + c_3 p}, \ a < 2(c_2 - b_2)p < 4p^2,$$

which contradicts

$$a = c - b + mp^2 > 6p^2.$$

Consequently $c_3 > b_3$. Using (3.4) one has

$$1 - \frac{\log 2pe}{p} < \beta = \frac{b_3}{c_3}\left(1 + \frac{b_2}{b_3 p^2}\right)\left(1 + \frac{c_2}{c_3 p^2}\right)^{-1}.$$

Thus

$$\frac{b_3}{c_3} > \left(1 - \frac{\log 2pe}{p}\right)\left(1 - \frac{|c_2|}{c_3 p^2}\right)\left(1 - \frac{|b_2|}{b_3 p^2}\right) >$$

$$> \left(1 - \frac{\log 2pe}{p}\right)\left(1 - \frac{1}{c_3 p}\right)\left(1 - \frac{1}{b_3 p}\right) > 1 - \frac{\log 2pe + \dfrac{1}{c_3} + \dfrac{1}{b_3}}{p}$$

$$> 1 - \frac{3 + \log 2p}{p}.$$

Since $c_3 \geq b_3 + 1$ one has

$$c_3 > \frac{p}{3 + \log 2p},$$

hence

$$c = c_2 + c_3 p^2 > \frac{p^3}{3 + \log 2p} - p.$$

Consequently comparing (4.1) and (4.2) in both cases i and ii the result (4.2) holds.

5. Using (2.6) and (4.2) one finds

$$z > \tfrac{1}{2}c^p, \ c > \frac{p^3}{3 + \log 2p} - p.$$

From $p \geq 253747889$ one finds

$z > 10^{6 \times 10^9}$, $z^p > 10^{1.5 \times 10^{18}}$.

REFERENCES

1) R. Obláth, Untere Schranken für Lösungen der Fermatschen Gleichung, Portugaliae Mathematica 11, 3 (1953), 129—132.
2) D. H. and Emma Lehmer, On the first case of Fermat's last theorem, Bull. Amer. Math. Soc. 47 (1941), 139—142.
3) E. Landau, Vorlesungen über Zahlentheorie (1927), Band 3, 324.
4) E. Landau, ibidem, 324, formulae (1126), (1127), (1128) and (1129).
5) E. Landau, ibidem, 315, theorem 1038.

(Received 13.5.'53)