A remark on Fermat's last theorem.


H. J. A. Duparc en A. van Wijngaarden.
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
\[ x^p + y^p = z^p \] (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: \(z^p > 10^{5.2 \times 10^8}\).
In this note it is shown that in case I by using the same lower bound \(p \geq 253747889\) of D. H. and EMMA LEHMER ²) the following sharper result can be derived:
Case I: \(z > 10^{6 \times 10^4}; \quad z^p > 10^{1.5 \times 10^{18}}\).

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
\[ x^p + y^p + z^p = 0. \] (2.1)
With the restriction of case I \((p \nmid xyz)\) one has:
\(X, Y, Z\) are integers, \(p \nmid XYZ\).
LANDAU ³) proves
where \(A, B\) and \(C\) are integers and
\[ X + A = Y + B \equiv Z + C \equiv 0 \pmod{p}; \]
\[ X^{p-1} = Y^{p-1} \equiv Z^{p-1} \equiv 1 \pmod{p}. \]
Hence

\[ A + B + C = -(X + Y + Z) = -(X^p + Y^p + Z^p) = 0 \pmod{p^3}. \]

Further 4)

\[-2CC' = A^p + B^p - C^p; \quad (C, C') = 1; \quad C' = 1 \pmod{p^3}.\]

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

i) \( q_1 \mid C, \ q_2 \mid A + B. \) From \( q_1 \mid A^p + B^p \) a simple argument learns \( q_1 \equiv 1 \pmod{p^3}, \) hence \( q_1^2 \equiv 1 \pmod{p^3}. \) Moreover using the first theorem of Furtwängler 3) the prime factor \( q_1 \) of C, hence of Z satisfies

\[ q_1 = q_1^2 = 1 \pmod{p^3}. \]

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

\[ (A + B, \ \frac{A^p + B^p}{A + B}) = (A + B, \ \frac{A^{p-1}}{A + B}) = 1 \quad \text{for otherwise} \]

either \( p \mid AB \mid XY \) or \( (A, B) = 1 \) 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

\[ C_1 = 1 \pmod{p^3}; \quad C = C_2 \pmod{p^3}; \quad C_2 \mid A + B + C. \quad (2.2) \]

Similarly

\[ A = A_2 \pmod{p^3}; \quad B = B_2 \pmod{p^3} \quad (2.3) \]

and

\[ A_2 \mid A + B + C; \quad B_2 \mid A + B + C. \quad (2.4) \]

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
\[ a + b - c \equiv a_2 + b_2 - c_2 \equiv 0 \pmod{\delta^2} \]

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
\[ a + b - c \equiv 0 \pmod{6 \cdot \delta^2}. \] (2.7)

Finally in virtue of (2.2) and (2.3) one obtains
\[ a = a_2 + a_3 \delta^2, \; b = b_2 + b_3 \delta^2, \; c = c_2 + c_3 \delta^2, \] (2.8)

where \( a_2, b_2 \) and \( c_2 \) are integers and in virtue of (2.5) one has
\[ a_2 b_2 c_2 \mid a + b - c. \] (2.9)

3. Putting \( \frac{a}{c} = a, \frac{b}{c} = \beta \) from (1.1) and (2.6) one obtains
\[ (-a^p + \beta^p + 1)^p + (a^p - \beta^p + 1)^p = (a^p + \beta^p + 1)^p, \]
\[ 0 < a < \beta < 1; \; a^p + \beta^p < 1. \] (3.1)

Using after a suggestion of C. G. Lekkerkerker for \( 0 < u < v \) the relation
\[ \beta(v-u)u^{v-1} < v^p - u^p < \beta(v-u)v^{p-1} \]
one has
\[ 2pa^p(1-a^p + \beta^p)p^{-1} < (a^p - \beta^p + 1)^p < 2pa^p(1 + 2\beta^p)^p, \]

hence
\[ a^p < (a^p - \beta^p + 1)^p < 2pa^p(1 + 2\beta^p)^p, \]

thus
\[ a < a^p - \beta^p + 1 < (1 + 2\beta^p)^{\frac{p}{2}}. \]

Consequently one finds the result
\[ 1 - \beta^p < a(1 + 2\beta^p)^{\frac{p}{2}} \] (3.2)

and
\[ 2(1 - \beta^p) > a-a^p + 1 - \beta^p > a, \]

thus
\[ 1 - \beta^p > \frac{1}{2}a. \] (3.3)

Now from (3.2) it follows
\[ \beta > 1 - \frac{\log 2pe}{\delta}. \] (3.4)

In fact the supposition \( \beta \leq 1 - \frac{\log 2pe}{\delta} \) leads to
\[ \beta^p < \left( 1 - \frac{\log 2 \rho}{p} \right)^p < \frac{1}{2 \rho^p}, \]

thus

\[ e^{\frac{\lambda^2}{\mu^2}} < \frac{1}{2 \rho^p} < \frac{1}{1 + \frac{2 \rho^p}{p \mu}} < \frac{1 - \rho^p}{1 + \frac{2 \rho^p}{p \mu}} < a \sqrt[4]{2 \rho} < \beta \sqrt[4]{2 \rho} < c^{-\frac{1}{p}}, \]

which is impossible since \( c > 2 \).

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

Then using (3.2) one finds

\[
\frac{1 - \beta^p}{1 - \beta} \geq 1 + \beta + \beta^2 + \beta^3 + \beta^4 > \\
> 1 + 3\beta^p > \sqrt{2(1 + 2\beta^p)} > \sqrt[4]{2\rho}(1 + 2\beta^p) > \frac{1 - \beta^p}{\alpha},
\]

hence

\[ \alpha + \beta > 1. \] (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. \( m \geq \rho \). Then

\[ c > a = c - b + mp^2 > mp^2 \geq \rho^3. \] (4.1)

ii. \( 6 \leq m < \rho \). Using (2.9) one has \( a \text{, } b \text{, } c \mid m \), hence

\[ |a| \leq m < \rho, \ |b| < \rho, \ |c| < \rho. \]

Further \( 0 < b_2 + b_3p^2 \), hence \( b_3p^2 > -b_2 > -\rho \), thus \( b_3 \geq 0 \) and

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

hence

\[ c_3 = b_3 > \frac{b_2 - c_2}{p^2} > \frac{2}{\rho}, \ c_3 \geq b_3 \geq 0. \]

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)
\[ 1 - \frac{1}{\alpha} > \beta^p > 1 - \frac{\beta(c_2 - b_2)}{c_2 + c_3 \beta^2}, \]

hence
\[ a < \frac{2\beta(c_2 - b_2)}{c_2 + c_3 \beta^2}, \quad a < 2(c_2 - b_2)p < 4\beta^2, \]

which contradicts
\[ a = c - b + m \beta \leq 6\beta^2. \]

Consequently \( c_3 > b_3 \). Using (3.4) one has
\[ 1 - \frac{\log 2 \beta c}{\beta} < \alpha = \frac{b_3}{c_3} \left( 1 + \frac{b_2}{b_3 \beta^2} \right)^{-1}. \]

Thus
\[ \frac{b_3}{c_3} > \left( 1 - \frac{\log 2 \beta c}{\beta} \right) \left( 1 - \frac{1}{c_3 \beta^2} \right) \left( 1 - \frac{1}{b_3 \beta^2} \right) > \left( 1 - \frac{\log 2 \beta c}{\beta} \right) \left( 1 - \frac{1}{c_3 \beta^2} \right) \left( 1 - \frac{1}{b_3 \beta^2} \right) > 1 - \frac{\log 2 \beta c + \frac{1}{c_3} + \frac{1}{b_3}}{\beta} > 1 - \frac{3 + \log 2 \beta}{\beta}. \]

Since \( c_3 \geq b_3 + 1 \) one has
\[ c_3 > \frac{\beta}{3 + \log 2 \beta}, \]

hence
\[ c = c_2 + c_3 \beta^2 > \frac{\beta^3}{3 + \log 2 \beta} - \beta. \]

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
\[ z > \frac{1}{2} \epsilon \gamma, \quad \epsilon > \frac{\beta^3}{3 + \log 2 \beta} - \beta. \]

From \( \beta \geq 253747889 \) one finds
\[ z > 10^{6 \times 10^9}, \quad \epsilon > 10^{1.3 \times 10^{18}}. \]
REFERENCES

1) R. Orláth, Untere Schranken für Lösungen der Fermatschen Gleichung, Portugaliae Mathematica 11, 3 (1953), 129—132.
4) E. Landau, ibidem, 324, formulae (1126), (1127), (1128) and (1129).
5) E. Landau, ibidem, 315, theorem 1035.

(Received 13.8.53)