Volume VII, No. 1, February 1985 février

COMPTES RENDUS MATHEMATIQUES

DE L'ACADEMIE DES SCIENCES

MATHEMATICAL REPORTS

OF THE ACADEMY OF SCIENCE

The Royal Society of Canada
La Société royale du Canada

THE SET OF EXPONENTS, FOR WHICH FERMAT'S LAST THEOREM IS TRUE, HAS DENSITY ONE

Andrew Granville

Presented by Paulo Ribenboim, F.R.S.C.

ABSTRACT. We use Filaseta's theorem, which is a corollary of Faltings' theorem, to establish the proposition in the title.

1. In this paper we shall examine Fermat's equation

$$(1)_n \qquad X^n + Y^n = Z^n$$

with positive integer exponents $n > 2$.

Faltings [2] has established that for every exponent $n > 3$, $(1)_n$ has only finitely many solutions in pairwise coprime integers x, y, z. Filaseta [3] has used Faltings' theorem to show that, for each integer $r \geq 3$, there exists an integer $N(r)$, such that if $m > N(r)$ and $n = mr$ then $(1)_n$ has only trivial solutions. We note that $N(r)$ is not effectively computable.

We will use Filaseta's theorem and an elementary lemma on set densities to establish that

$$\lim_{N \to \infty} \frac{\#\{n \in \mathbb{N} \mid 1 \leq n \leq N \text{ and } (1)_n \text{ has only trivial solutions}\}}{N} = 1 .$$

This improves on the result of Ankeny and Erdös [1] who established this theorem, though with the extra condition that n is coprime to x, y and z.

Finally, we shall note that our theorem holds true for any Fermat curve $aX^n + bY^n = cZ^n$, with a, b, c non-zero integers, where, for the case $\pm a \pm b = c$ we define $(\pm 1, \pm 1, 1)$ to also be a 'trivial' solution.

2. For completeness, we present the proof of Filaseta's theorem.

Theorem 1. If $r \geq 3$ then there exists a positive integer $N(r)$ such that if $m > N(r)$ then the equation $X^{mr} + Y^{mr} = Z^{mr}$ has only the trivial solution (x,y,z) with $xyz = 0$.

Proof: If $r = 3$ the equation has only the trivial solution, as was shown by Euler. If $r > 3$, then by Faltings' theorem, there exists only finitely many triples of non-zero coprime integers (x,y,z) such that $x^r + y^r = z^r$; we note that $|z| = \max\{|x|, |y|, |z|\} > 1$. So there exists a positive integer $L(r)$ such that $|z| < L(r)$ for all solutions (x,y,z) as above.

If $m > N(r) = \left[\frac{\log L(r)}{\log 2}\right] + 1$ and if (a,b,c) is a non-trivial solution in coprime integers of $X^{rm} + Y^{rm} = Z^{rm}$ then $|c| \geq 2$, (a^m, b^m, c^m) is a non-trivial solution in coprime integers of $X^r + Y^r = Z^r$, hence $|c^m| \geq 2^m > L(r) > |c^m|$, which is a contradiction.

Now we prove a lemma about densities. Let P be a set of $(k \geq 1)$ prime numbers, let N be a positive integer and

$$S_{p,N} = \{n \in \mathbb{N} \mid 1 \leq n \leq N \text{ and there exists } p \in P \text{ such that } p \mid n\}.$$

Lemma. With the above notation

$$\frac{\#(S_{p,N})}{N} \geq 1 - \prod_{p \in P}\left(1 - \frac{1}{p}\right) - \frac{2^k}{N}$$

Proof: Let $Q = \prod_{p \in P} p$. Then

$$\#(S_{p,N}) = \sum_{p \in P} \left[\frac{N}{p}\right] - \sum_{\substack{p_1, p_2 \in P \\ p_1 \neq p_2}} \left[\frac{N}{p_1 p_2}\right] + \ldots + (-1)^{k+1} \left[\frac{N}{Q}\right]$$

$$= - \sum_{\substack{d|Q \\ d \neq 1}} \mu(d) \left[\frac{N}{d}\right] = N - \sum_{d|Q} \mu(d) \left[\frac{N}{d}\right].$$

But

$$\left| \sum_{d|Q} \mu(d) \left[\frac{N}{d}\right] - \sum_{d|Q} \mu(d) \left[\frac{N}{d}\right] \right| = \left| \sum_{d|Q} \mu(d) \left(\frac{N}{d} - \left[\frac{N}{d}\right]\right) \right|$$

$$\leq \sum_{d\ Q} 1 = 2^k.$$ Therefore

$$\#(S_{p,N}) \geq N - \sum_{d|Q} \mu(d) \frac{N}{d} - 2^k =$$

$$N \left(1 - \sum_{d|Q} \frac{\mu(d)}{d}\right) - 2^k = N \left\{1 - \prod_{p \in P} \left(1 - \frac{1}{p}\right)\right\} - 2^k.$$

Then $$\frac{\#\left(S_{p,N}\right)}{N} \geq 1 - \prod_{p \in P} \left(1 - \frac{1}{p}\right) - \frac{2^k}{N}.$$

Now we shall indicate the main result. Let $p_1 = 2 < p_2 = 3 < p_3 < \ldots$ be the sequence of prime numbers, for each $k \geq 2$ let $P_k = \{p_2, p_3, \ldots, p_k\}$. For each prime p_j let $N(p_j)$ be the integer considered in Filaseta's theorem and for each $k \geq 2$ let $N_k = \max_{2 \leq j \leq k} \{p_j\ N(p_j)\}$.

For each integer $N \geq 1$ we also consider the sets

$S'_{P_k,N} = \{n \in \mathbb{N} \mid N_k < n \leq N$ and there exists $p_j \in P_k$ such that $p_j \mid n\}$

and $F_N = \{n \in \mathbb{N} \mid 3 \leq n \leq N$ such that equation $(1)_n$ has only trivial solutions$\}$.

We note that $S'_{P_k,N} \subseteq S_{P_k,N} \subseteq S'_{P_k,N} \cup \{1,2, \dots, N_K\}$

With above notations, we have:

<u>Theorem 2.</u> $$\lim_{N \to \infty} \frac{\#(F_N)}{N} = 1$$

<u>Proof:</u> Let $\varepsilon > 0$. Since

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right) = \frac{1}{\sum_{n=1}^{\infty} \frac{1}{n}} = 0$$

there exists $k \geq 2$ such that

$$2 \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right) + \frac{1}{p_k} < \varepsilon.$$

Let $N' = (2^{k-1} + N_k) N_k$ and $N > N'$. By Filaseta's theorem, $S'_{P_k,N} \subseteq F_N$, because if $n \in S'_{P_k,N}$ then $N_k < n \leq N$ and there exists $p_j \in P_k$ such that $p_j | n$; so $n = p_j m > N_k \geq p_j N(p_j)$ hence $m > N(p_j)$ and therefore $n = p_j m \in F_N$.

As $\#(S_{P_k,N}) - N_k \leq \#(S'_{P_k,N})$ it follows that

$$\frac{\#\left(S_{P_k,N}\right)}{N} - \frac{N_k}{N} \leq \frac{\#\left(S_{P_k,N}\right)}{N} \leq \frac{(F_N)}{N} \leq 1$$

On the other hand, by the lemma,

$$\frac{\#(S_{p_k},N)}{N} \geq 1 - \prod_{j=2}^{k}\left(1 - \frac{1}{p_j}\right) - \frac{2^{k-1}}{N} =$$

$$1 - 2\prod_{j=1}^{k}\left(1 - \frac{1}{p_j}\right) - \frac{2^{k-1}}{N}.$$

$$\text{Thus}\quad 1 - 2\prod_{j=1}^{k}\left(1 - \frac{1}{p_j}\right) - \frac{2^{k-1} + N_k}{N} \leq \frac{\#(F_N)}{N} \leq 1$$

hence if $N \geq N' \geq N_k \geq p_k$ then

$1 - \varepsilon \leq \frac{\#(F_N)}{N} \leq 1.$ This shows that $\lim_{N\to\infty} \frac{\#(F_N)}{N} = 1,$

which completes the proof of the theorem.

3. A final remark concerns the equations

$$(2)_n \qquad aX^n + bY^n = cZ^n$$

where a,b,c are non-zero integers, and solueions with $(X,Y,Z) \in (-1,0,1)$ are considered trivial.

For $n > 3$ the genus of $(2)_n$ is still greater than one, and a non-trivial soln of $(2)_n$ has at least one of $|X|, |Y|, |Z| > |$.

Hence the proof of Filaseta's theorem as well as the proof of theorem 2 still hold true for this equation and we conclude that the density of exponents n, for which $(2)_n$ has no solution (x,y,z) with $xyz \neq 0$, gcd $(x,y,z) = 1$, is equal to 1.

REFERENCES

1. Ankeny, N.C. & Erdős, P. The insolubility of classes of diophantine equations, Amer. J. Math., 76, 1954, 488-496.

2. Faltings, G. Einige Sätze zum Thema Abelsche Varietaten über Zahlkönpern. To appear in Invent. Math.

3. Filaseta, M. An application of Faltings' results to Fermat's last theorem. C.R. Math. Reports Acad. Sci. Canada, 6, 1984, 31-32.

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario, K7L 3N6

Received November 29, 1984.