FERMAT'S LAST THEOREM FOR "ALMOST ALL" EXPONENTS

D. R. HEATH-BROWN

Fermat's Last Theorem—which we shall abbreviate to FLT—is the (as yet unproved) assertion that the Diophantine equation $x^n + y^n = z^n$ has no solutions in positive integers if $n \geqslant 3$. It would suffice to deal with the case in which n is prime, and this is where the most significant work has been done. None the less it is not yet known even whether FLT is true for infinitely many prime exponents. If one considers general exponents n one sees that FLT is true at least for a proportion

$$1 - \frac{3}{4} \prod_{3 \leqslant p \leqslant 125000} \left(1 - \frac{1}{p}\right) \simeq 0{\cdot}93$$

of all n, since the cases $n = 4$ and $n = p \leqslant 125000$ ($p \neq 2$) are known to hold (Wagstaff [3]). The object of this note is to prove the following corollary to the recent work of Faltings [1] on Mordell's Conjecture.

THEOREM. FLT *is true for "almost all" exponents* n. *That is, if* $N(x)$ *is the number of* $n \leqslant x$ *for which* FLT *fails, then* $N(x) = o(x)$ *as* $x \to \infty$.

Unfortunately the proof, being based on Faltings' Theorem, is ineffective. Thus, given $\varepsilon > 0$, we can assert that x_ε exists such that $N(x) \leqslant \varepsilon x$ for $x \geqslant x_\varepsilon$, but we have no means of calculating x_ε.

According to Faltings' Theorem the equation $x^p + y^p = z^p$ has, for each $p \geqslant 3$, only a finite number of primitive solutions (i.e. solutions with $(x, y, z) = 1$). Suppose these are x_i, y_i, z_i for $1 \leqslant i \leqslant i(p)$ and define

$$B(p) = \operatorname*{Max}_i |x_i y_i z_i| .$$

Now let $u^{kp} + v^{kp} = w^{kp}$ with $(u, v, w) = 1$ and $uvw \neq 0$. Then $\{u^k, v^k, w^k\} = \{x_i, y_i, z_i\}$ for some i, whence $|uvw|^k \leqslant B(p)$. However $|uvw| \geqslant 2$, so that we must have $k \leqslant B(p)$. Thus FLT is true for all exponents $n \equiv 0 \pmod p$ such that $n > pB(p)$. This idea, of using Faltings' Theorem for a prime p, and then considering multiples of p, is due to Filaseta [2] who showed that there is an infinite sequence $n_1, n_2, \ldots$ of mutually coprime exponents for which FLT is true.

To complete the proof of the theorem we use the sieve of Eratosthenes. Let $\varepsilon > 0$ be given and choose $y = y(\varepsilon)$ such that

$$\prod_{3 \leqslant p \leqslant y} \left(1 - \frac{1}{p}\right) < \tfrac{1}{2}\varepsilon .$$

Received 15th October, 1984.

1980 *Mathematics Subject Classification:* 10B15.

Set

$$z = z(\varepsilon) = \operatorname*{Max}_{3 \leqslant p \leqslant y} pB(p)$$

and

$$P = \prod_{3 \leqslant p \leqslant y} p .$$

Thus

$$\begin{aligned} N(x) &\leqslant z + \#\{n : z < n \leqslant x, (n, P) = 1\} \\ &\leqslant z + \#\{n : n \leqslant x, (n, P) = 1\} \\ &= z + \sum_{n \leqslant x} \sum_{d \mid (n, P)} \mu(d) \\ &= z + \sum_{d \mid P} \mu(d) \left[\frac{x}{d}\right] \\ &\leqslant z + \sum_{d \mid P} \mu(d) \frac{x}{d} + \sum_{d \mid P} 1 \\ &\leqslant z + x \frac{\phi(P)}{P} + 2^y \\ &\leqslant z + \tfrac{1}{2}\varepsilon x + 2^y \\ &\leqslant \varepsilon x , \end{aligned}$$

if $x \geqslant x_\varepsilon$, and the theorem follows.

References

1. G. Faltings, 'Endlichkeitssätze für abelsche Varietäten über Zahlkörpern', *Invent. Math.*, 73 (1983), 349–366.
2. M. Filaseta, 'An application of Faltings' results to Fermat's Last Theorem', *C. R. Math. Rep. Acad. Sci. Canada*, 6 (1984), 31–32.
3. S. S. Wagstaff, 'The irregular primes to 125000', *Math. Comp.*, 32 (1977), 583–591.

Magdalen College,
Oxford OX1 4AU.