The Uniform Density of Sets of Integers and Fermat's Last Theorem

Tom C. Brown and Allen R. Freedman

Citation data: T.C. Brown and A.R. Freedman, *The uniform density of sets of integers and Fermat's Last Theorem*, C.R. Math. Rep. Acad. Sci. Canad. **12** (1990), 1–6.

1 Introduction

In this note we take a "density theory" approach to the problem of measuring certain sets of integers including the set of exponents for which Fermat's Last Theorem is true. It is proved that this last set has *uniform* density equal to one. This is a slightly stronger statement than has been previously made about this set. The method is particularly simple and transparent and is applied to finding the uniform densities of other sets of integers from Number Theory.

2 Density concepts

Let B be a set of positive integers and write $B(x,y)$ for the number of elements in $B \cap [x,y]$. The lower and upper uniform densities are defined as follows. Let

$$\beta_s = \liminf_{t\to\infty} B(t+1, t+s).$$

That is, β_s is the smallest number which occurs infinitely often as the number of elements of B which lie in an interval of length s. It is not hard to show that $\lim_{s\to\infty} \beta_s/s$ exists, and this is the *lower uniform density* of B, denoted by $\underline{u}(B)$:

$$\underline{u}(B) = \lim_{s\to\infty} \frac{1}{s} \liminf_{t\to\infty} B(t+1, t+s).$$

Similarly, with

$$\beta^s = \limsup_{t\to\infty} B(t+1, t+s),$$

the *upper uniform density* of B is $\overline{u}(B) = \lim_{s\to\infty} \beta^s/s$, or

$$\overline{u}(B) = \lim_{s\to\infty} \frac{1}{s} \limsup_{t\to\infty} B(t+1, t+s).$$

If $\underline{u}(B) = \overline{u}(B) = u(B)$, then $u(B)$ is the *(natural) uniform density* of B.

With this notation the definitions of the *lower asymptotic density* $\underline{d}(B)$ and the *upper asymptotic density* $\overline{d}(B)$ are respectively

$$\underline{d}(B) = \liminf_{s\to\infty} \frac{1}{s} B(1,s),$$

and

$$\overline{d}(B) = \limsup_{s\to\infty} \frac{1}{s} B(1,s).$$

If $\underline{d}(B) = \overline{d}(B) = d(B)$, then $d(B)$ is the *(natural) asymptotic density* of B/

It's clear that

$$\underline{u}(B) \le \underline{d}(B) \le \overline{d}(B) \le \overline{u}(B)$$

for any set B, and it is easy to produce an example of a set B with $d(B) = 1$ and $\underline{u}(B) = 0$, and a set C with $d(C) = 0$ and $\overline{u}(C) = 1$. Thus the statement that a set has uniform density 1 (or uniform density 0) is in fact stronger than the corresponding statement about asymptotic density. As another example, let S be the set of square-free integers. It is well known that $d(S) = 6/\pi^2$ while it can easily be shown that $\underline{u}(S) = 0$ and $\overline{u}(S) = d(S)$.

We mention three important properties of these densities which can be proved without difficulty directly from the definitions: 1) If $A \subset B$, then $\delta(A) \le \delta(B)$ where δ stands for any of the density functions defined above. 2) For either upper density, $\bar{\delta}$, and any sets A and B, $\bar{\delta}(A \cup B) \le \bar{\delta}(A) + \bar{\delta}(B)$. 3) If B is a union of disjoint arithmetic progressions,

$$B = \bigcup_{i=1}^{n} \{a_i t + i : t = 0, 1, 2, \dots\},$$

then $u(B)$ exists and equals $\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$.

3 Three lemmas

Let $P = \{p_1 < p_2 < p_3 < \cdots\}$ be the set of prime numbers and let $N_k = \{x : x$ is not divisible by $p_1, p_2, \dots, p_k\}$. More generally, if $Q = \{q_1, q_2, \dots, q_k\}$ is a set of distinct primes, then let $N_Q = \{x : x$ is not divisible by $q_1, q_2, \dots, q_k\}$. For any set S and integer n write S_n for the set of all $x \in S$ which are divisible by n. We begin with a well known computation.

Lemma 1. $u(N_Q) = (1 - \frac{1}{q_1})(1 - \frac{1}{q_2}) \cdots (1 - \frac{1}{q_k})$.

Proof. Let $R = q_1 q_2 \cdots q_k$. Evidently, N_Q is the disjoint union of the arithmetic progressions $\bigcup_a \{Rt + a\}$ where a ranges over the $\phi(R)$ elements of $[1, R]$ which are prime to R. Hence

$$u(N_Q) = \frac{\phi(R)}{R} = (1 - \frac{1}{q_1})(1 - \frac{1}{q_2}) \cdots (1 - \frac{1}{q_k}). \qquad \square$$

Lemma 2. *Let $Q = \{q_1, q_2, q_3, \dots\}$ be a set of primes for which*

$$\sum \frac{1}{q_i} = \infty. \tag{1}$$

Let S be a set of positive integers and suppose that $u(S_q) = 0$ for each prime q in Q. Then $u(S) = 0$.

Proof. Let $Q_k = \{q_1, q_2, \ldots, q_k\}$. Then, for each k,

$$S \subset N_{Q_k} \cup S_{q_1} \cup S_{q_2} \cup \cdots \cup S_{q_k}.$$

Hence,

$$\begin{aligned} \overline{u}(S) &\leq \overline{u}(N_{Q_k}) + \overline{u}(S_{q_1}) + \cdots + \overline{u}(S_{q_k}) = \overline{u}(N_{Q_k}) \\ &= (1 - \frac{1}{q_1})(1 - \frac{1}{q_2}) \cdots (1 - \frac{1}{q_k}). \end{aligned}$$

As the last product tends to zero as $k \to \infty$, the lemma is proved. □

Lemma 3. *$u(S) = 0$ if and only if there exists a set of primes Q with infinite reciprocal sum, such that for any sequence $(q_1, q_2, \ldots)$ of distinct elements of Q, $u(S_{q_1 q_2 \cdots q_k}) = 0$ for some k.*

Proof. If $u(S) = 0$, the conclusion is obvious with $Q = P$. On the other hand, if $\overline{u}(S) > 0$ and Q is any set of primes satisfying (1), then, using Lemma 2, we can find q_1 in Q such that $\overline{u}(S_{q_1}) > 0$. Again, since $(S_p)_q = S_{pq}$ for distinct primes p and q, and using Lemma 2, we can find q_2 in $Q - \{q_1\}$ such that $\overline{u}(S_{q_1 q_2}) > 0$. Continuing in this mander we construct the required infinite sequence such that $\overline{u}(S_{q_1 q_2 \cdots q_k}) > 0$ for all k. □

4 Applications

Before moving on to Fermat's last theorem we prove striking properties concerning the number of prime factors of a "typical" integer (cf. [4] Sections 22.11, 22.12).

Theorem 1. $u(P) = 0$.

Proof. Take $S = P$ in Lemma 2. Each S_p is a singleton. □

Theorem 2. *Let $G^t = \{x : x$ is the product of no more than t prime numbers (counting multiplicities)$\}$. Then $u(G^t) = 0$.*

Proof. $G^1 = P \cup \{1\}$ and so $u(G^1) = 0$. Proceeding inductively,

$$(G^{t+1})_p = pG^t \quad \text{and so} \quad u((G^{t+1})_p) = 0.$$

By Lemma 2 $u(G^{t+1}) = 0$. (Here we use $kA = \{kx : x \in A\}$ and the fact that $\overline{u}(kA) = \frac{1}{k}\overline{u}(A)$.) □

Using Lemma 3 we can prove the more difficult result presented in the next theorem.

Theorem 3. *Let $H^t = \{x : x$ has t or fewer prime divisors$\}$. Then $u(H^t) = 0$.*

Proof. Fix t, take $Q = P$, and let $q_1, q_2, \ldots, q_{t+1}$ be any $t+1$ distinct primes. Clearly, $(H^t)_{q_1 q_2 \cdots q_{t+1}}$ is empty and we may apply Lemma 3. □

Finally, we prove that the set of exponents, F, for whic Fermat's Last Theorem is *false* has uniform density zero. Faltings' Theorem [1] implies that for each odd prime p the equation $x^p + y^p = z^p$ has only *finitely many* primitive solutions, and recently Heath-Brown [5] and Granville [3] have shown independently as a corollary to Faltings' Theorem that the set T of exponents n for which $x^n + y^n = z^n$ has *no* primitive solution (and hence no solution at all in positive integers) has *natural asymptotic* density 1. Of course, the idea behind our proof is also the use of Faltings' Theorem for prime exponents p. Both Heath-Brown and Granville attribute this idea to Filaseta [2].

Theorem 4. *Let F be the set of all n such that $x^n + y^n = z^n$ has a solution. Then $u(F) = 0$.*

Proof. Fix any odd prime p. Then for each $n \geq 3$,

$$\left\{ \begin{array}{c} p \text{ divides } n \\ a^n + b^n = c^n \\ (a,b,c) = 1 \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} (a^{n/p})^p + (b^{n/p})^p = (c^{n/p})^p \\ (a^{n/p}, b^{n/p}, c^{n/p}) = 1 \end{array} \right\},$$

and so, by Faltings' Theorem, each odd prime p divides only finitely many elements of F (since $a^{n/p}$ must assume at most finitely many values with $a > 1$). Therefore F_p is finite and so, by Lemma 2, F has uniform density 0. □

It is apparently still unknown whether or not Fermat's Last Theorem is true for an infinite set of prime exponents. Filaseta proved that for any $n \geq 3$, Fermat's Last theorem is true for exponent kn for all large k. The proof of this can be gleened from the proof of Theorem 4. It is interesting to note that with this result we can easily construct a sequence of products of two primes, $q_1q_2, q_3q_4, q_5q_6, \ldots$, such that Fermat's Last Theorem is true for each member of the sequence and each prime p equals exactly one q_i.

References

[1] G. Faltings, *Endlichkeitssatze fur abelsche varietaten uber zahlkorpern*, 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] A. Granville, *The set of exponents, for which Fermat's Last Theorem is true, has density one*, C. R. Math. Rep. Acad. Sci. Canada **8** (1985), 55–60.

[4] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Oxford, 1960.

[5] D. Heath-Brown, *Fermat's Last Theorem for "almost all" exponents*, Bull. London Math. Soc. **17** (1985), 15–16.