VALUES OF THE EULER AND CARMICHAEL FUNCTIONS WHICH ARE SUMS OF THREE SQUARES

Paul Pollack[1]
Department of Mathematics, University of Illinois, Urbana, Illinois 61801, USA
pppollac@illinois.edu

Received: 6/23/10, Accepted: 12/23/10, Published: 1/31/11

Abstract

Let φ denote Euler's totient function. The frequency with which $\varphi(n)$ is a perfect square has been investigated by Banks, Friedlander, Pomerance, and Shparlinski, while the frequency with which $\varphi(n)$ is a sum of two squares has been studied by Banks, Luca, Saidak, and Shparlinski. Here we look at the corresponding three-squares question. We show that $\varphi(n)$ is a sum of three squares precisely seven-eighths of the time. We also investigate the analogous problem with φ replaced by Carmichael's λ-function. We prove that the set of n for which $\lambda(n)$ is a sum of three squares has lower density > 0 and upper density < 1.

1. Introduction

Let $\varphi(n)$ denote Euler's totient function, defined as the size of the unit group $(\mathbf{Z}/n\mathbf{Z})^{\times}$. A theorem of Banks et al. [2, pp. 40, 43] asserts that for any $\epsilon > 0$ and all large x,

$$x^{0.7038} \leq \#\{n \leq x : \varphi(n) = \square\} \leq \frac{x}{L(x)^{1-\epsilon}}, \tag{1}$$

where

$$L(x) = \exp(\sqrt{\log x \log\log\log x}).$$

We write "$\square$" here and below to denote a generic member of the set $\{n^2 : n = 0, 1, 2, 3, \dots\}$ of perfect squares. The same authors present a heuristic argument that the left-hand side of (1) can be replaced with $x^{1-\epsilon}$. An investigation into the corresponding question for sums of two squares appeared the following year, where it was shown [4, p. 124, eq. (1)] that

$$\#\{n \leq x : \varphi(n) = \square + \square\} \asymp \frac{x}{(\log x)^{\frac{3}{2}}}. \tag{2}$$

[1]The author is supported by an NSF postdoctoral research fellowship.

(Recall that "$F \asymp G$" means that the ratio F/G is bounded between two positive constants.) This may be compared with the theorem of Landau [11] that as $x \to \infty$,

$$\#\{n \le x : n = \Box + \Box\} \sim \left(\frac{1}{\sqrt{2}} \prod_{\substack{p \equiv 3 \pmod 4 \\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} \right) \frac{x}{(\log x)^{1/2}}.$$

See [15] for an extended discussion of Landau's theorem and its generalizations, and see [20, pp. 183–185] for what seems to be the most elementary proof.

What about sums of three squares? (By a theorem of Lagrange, every positive integer is a sum of four squares, so this is the last interesting case.) The natural numbers which are sums of three squares are characterized by a theorem of Legendre: $n = \Box + \Box + \Box$ precisely when n is *not* of the form $4^k(8l + 7)$, where k and l are nonnegative integers (see, e.g., [21, Appendix to Chapter IV]). A straightforward consequence of this characterization is that about 5/6 of all natural numbers up to x are expressible as a sum of three squares, once x is large. The error term in this approximation is easily seen to be $O(\log x)$, but as discussed in [22] and [17], it displays somewhat complicated pointwise and average behavior. Our first result is the determination of the density of n for which $\varphi(n) = \Box + \Box + \Box$.

Theorem 1. *The set of n for which $\varphi(n)$ is a sum of three squares has asymptotic density 7/8. More precisely, for $x \ge 2$, we have*

$$\#\{n \le x : \varphi(n) = \Box + \Box + \Box\} = \frac{7}{8}x + O\left(\frac{x}{(\log x)^{3/10}}\right). \tag{3}$$

It seems amusing that for $k = 1, 2$, and 3, the odds that $\varphi(n)$ is a sum of k squares are alternately higher, then lower, then higher, than the corresponding odds that n is a sum of k squares. One can anticipate a possible objection to these comparisons: Since $\varphi(n)$ is even for $n > 2$, we should compare $\varphi(n)$ only with even m. An even number m is a sum of three squares with probability 11/12, and so $\varphi(n)$ is *less* likely to be a sum of three squares than its even brethren. This is all true, but we can respond as follows: $\varphi(n)$ is almost always a multiple of 4 (since almost every n has at least two different odd prime divisors), and a multiple of 4 is a sum of three squares with probability 5/6. Our hypothetical detractor can then counter by suggesting we consider multiples of 8 (where the probability is again 11/12), to which we counter with multiples of 16 (where it is 5/6), etc. In any case, the objection highlights the importance of the highest power of 2 dividing $\varphi(n)$, which will feature prominently in the proof of Theorem 1 below.

What happens if we replace φ with a cognate arithmetic function? Candidates here include the sum of divisors function $\sigma(n)$ and Carmichael's function $\lambda(n)$, defined as the exponent of the group $(\mathbf{Z}/n\mathbf{Z})^\times$. The estimates (1) and (2) remain valid with σ (see [2, pp. 31, 43] and [4, Theorem 2]), and it is straightforward to prove that Theorem 1 also holds for σ. (See the remarks following the proof of the Theorem 3, which is a generalization of Theorem 1.) One can also show that (1) and (2) hold with φ replaced by λ (see [2, Theorem 6.3 and §7] and [3]). For sums of three squares, we can prove the following:

Theorem 2. *We have*

$$\begin{aligned} 0 &< \liminf_{x\to\infty} \frac{1}{x}\#\{n \le x : \lambda(n) = \square + \square + \square\} \\ &\le \limsup_{x\to\infty} \frac{1}{x}\#\{n \le x : \lambda(n) = \square + \square + \square\} \\ &< 1. \end{aligned}$$

Perhaps surprisingly, we conjecture that Theorem 1 does *not* hold for λ. In fact, we believe that the lim inf and lim sup in Theorem 2 do not coincide, so that the set of n for which $\lambda(n) = \square + \square + \square$ does not possess an asymptotic density.

1.1. Notation

We write $\omega(n) := \sum_{p\mid n} 1$ for the number of distinct prime factors of n and $\Omega(n) := \sum_{p^\ell \mid n} 1$ for the number of prime factors of n counted with multiplicity. $P(n)$ denotes the largest prime factor of n, with the understanding that $P(1) = 1$. We write $d \parallel n$ (read "d exactly divides n") if d divides n and $\gcd(d, n/d) = 1$. Throughout the paper, the letters p and q are reserved for primes. For each prime p and each natural number n, we write $v_p(n)$ for the *p-adic order of n*; thus, $v_p(n) = 0$ if $p \nmid n$, and if $p \mid n$, then $v_p(n)$ is the unique positive integer for which $p^{v_p(n)} \parallel n$.

The Bachmann–Landau o and O-symbols (see [1, p. 401], [12, §12]), as well as Vinogradov's $\ll$ and $\gg$ symbols, appear with their usual meanings. For $x > 0$, we set $\log_1 x = \max\{\log x, 1\}$, and we let $\log_k$ denote the kth iterate of $\log_1$.

2. Euler's Function

2.1. Proof of Theorem 1

For each natural number m, define $u(m)$ (the *odd part* of m) by the relation $m = 2^{v_2(m)}u(m)$. Note that v_2 is completely additive while u is completely multiplicative.

Let G denote the group $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/8\mathbf{Z})^\times$. We let θ denote the map from $\mathbf{N}$ to G defined by

$$n \mapsto (v_2(\varphi(n)) \bmod 2, u(\varphi(n)) \bmod 8).$$

Then θ is a G-valued multiplicative function, in the sense that $\theta(mn) = \theta(m)\theta(n)$ whenever m and n are coprime. By Legendre's theorem,

$$\varphi(n) = \square + \square + \square \iff \theta(n) \ne (0 \bmod 2, 7 \bmod 8).$$

To prove Theorem 1, we show that as n runs over the natural numbers, the elements $\theta(n) \in G$ become equidistributed.

Our starting point is a pretty theorem of Wirsing [24] from probabilistic number theory, which confirmed a conjecture of Erdős and Wintner.

Theorem A. *Let f be a real-valued multiplicative function satisfying $-1 \leq f(n) \leq 1$ for all $n \in \mathbf{N}$. If the series*

$$\sum_p \frac{1-f(p)}{p}$$

diverges, then f has mean value zero.

Theorem A is enough to obtain Theorem 1 without the error term. To justify the error expression, we use the following effective version due to Hall and Tenenbaum [9] (see also [23, Theorem 7, p. 345]):

Theorem B. *Suppose that f is a real-valued multiplicative function with $-1 \leq f(n) \leq 1$ for all $n \in \mathbf{N}$. Let ϕ_0 be the unique solution on $(0, 2\pi)$ of the equation $\sin(\phi_0) + (\pi - \phi_0)\cos(\phi_0) = \frac{1}{2}\pi$, and put $L = \cos\phi_0 \approx 0.32867$. Then for $x \geq 1$,*

$$\frac{1}{x}\sum_{n \leq x} f(n) \ll \exp\left(-L \sum_{p \leq x} \frac{1-f(p)}{p}\right),$$

where the implied constant is absolute.

Proof of Theorem 1. Let $\hat{G}$ denote the character group of G. Since G has exponent 2, each $\chi \in \hat{G}$ assumes values in $\{1, -1\}$. Given $\chi \in \hat{G}$, we "lift" χ to $\mathbf{N}$ by setting $\chi(n) = \chi(\theta(n))$ for each $n \in \mathbf{N}$. (By abuse of notation, we use the same symbol for the function on $\mathbf{N}$ and the function on G.) Then χ is a multiplicative function taking values in $\{-1, 1\}$. By the orthogonality relations, to prove Theorem 1, it will suffice to show that

$$\sum_{n \leq x} \chi(n) \ll \frac{x}{(\log x)^{3/10}} \tag{4}$$

for each nontrivial χ.

We have $\hat{G} \cong \widehat{(\mathbf{Z}/2\mathbf{Z})} \times \widehat{(\mathbf{Z}/8\mathbf{Z})^{\times}}$. Moreover, the isomorphism shows that for each nontrivial χ, there is a $\zeta \in \{-1, 1\}$ and a Dirichlet character $\tilde{\chi}$ to the modulus 8, with

$$\chi(n) = \zeta^{v_2(\varphi(n))}\tilde{\chi}(u(\varphi(n)))$$

for all natural numbers n. Since χ is nontrivial, either $\zeta \neq 1$ or $\tilde{\chi}$ is not the trivial character mod 8.

Suppose first that $\tilde{\chi}$ is trivial, so that $\zeta = -1$. In this case, $\chi(n) = (-1)^{v_2(\varphi(n))}$. Then $\chi(p) = -1$ whenever $p \equiv 3 \pmod 4$, so that

$$\sum_{p \le x} \frac{1-\chi(p)}{p} \ge 2 \sum_{\substack{p \le x \\ p \equiv 3 \pmod 4}} \frac{1}{p} \sim \log\log x,$$

where the asymptotic relation holds as $x \to \infty$. Here we use a form of Dirichlet's theorem on primes in progressions (see, e.g., [5, p. 57]): Whenever a and m are coprime natural numbers,

$$\sum_{\substack{p \le x \\ p \equiv a \pmod m}} \frac{1}{p} \sim \frac{1}{\varphi(m)} \log\log x \qquad \text{as } x \to \infty. \tag{5}$$

The estimate (4) for this χ now follows from Theorem B. In fact, we can replace the exponent $3/10$ on the right-hand side of (4) with any constant smaller than L.

Suppose now that $\tilde{\chi}$ is nontrivial. Fix a large natural number K, and decompose

$$\begin{aligned}\sum_{p \le x} \frac{\chi(p)}{p} &= \frac{\chi(2)}{2} + \sum_{1 \le k \le K} \zeta^k \sum_{\substack{b \bmod 8 \\ \gcd(b,8)=1}} \tilde{\chi}(b) \sum_{\substack{p \le x \\ v_2(p-1)=k \\ u(p-1) \equiv b \pmod 8}} \frac{1}{p} + \sum_{\substack{p \le x \\ v_2(p-1) \ge K+1}} \frac{\chi(p)}{p} \\ &= \frac{\chi(2)}{2} + \sum\nolimits_1 + \sum\nolimits_2 .\end{aligned}$$

We estimate the triple sum $\sum_1$ using (5): For fixed k and b, the condition on p in $\sum_1$ says precisely that $p \equiv 2^k b + 1 \pmod{2^{k+3}}$. So the sum over p is asymptotic (as $x \to \infty$) to $\frac{1}{2^{k+2}} \log\log x$. Notice that the coefficient of $\log\log x$ exhibits no dependence on b. Since $\sum \tilde{\chi}(b)$ vanishes when b runs over a system of coprime residues modulo 8, it follows that $\sum_1 = o(\log\log x)$ as $x \to \infty$. Also,

$$\limsup_{x \to \infty} \frac{1}{\log\log x} \left|\sum\nolimits_2\right| \le \limsup_{x \to \infty} \frac{1}{\log\log x} \sum_{\substack{p \le x \\ v_2(p-1) > K}} \frac{1}{p} = \frac{1}{2^K},$$

by (5) with $m = 2^{K+1}$ and $a = 1$. Since K was arbitrary, these estimates show that $\sum_{p \le x} \chi(p)/p = o(\log\log x)$. But $\sum_{p \le x} \frac{1}{p} \sim \log\log x$ (by (5) with $a = m = 1$), and so we deduce that

$$\sum_{p \le x} \frac{1-\chi(p)}{p} \sim \log\log x$$

as $x \to \infty$. Now (4) follows from Theorem B, as above. □

2.2. A Generalization

A similar argument allows us to prove a more general equidistribution result: Let $\mathcal{Q}$ be a finite, nonempty set of primes, and redefine $u(n)$ as the part of n coprime to $\prod_{q\in\mathcal{Q}} q$, so that

$$n = u(n) \prod_{q\in\mathcal{Q}} q^{v_q(n)}.$$

Suppose that to each $q \in \mathcal{Q}$ is associated a positive integer m_q. Finally, assume that we are also given a positive integer l, and put

$$M := \prod_{q\in\mathcal{Q}} q^l. \tag{6}$$

We now introduce the group

$$G := \left(\prod_{q\in\mathcal{Q}} (\mathbf{Z}/m_q\mathbf{Z})\right) \times (\mathbf{Z}/M\mathbf{Z})^\times,$$

and we define $\theta\colon \mathbf{N} \to G$ by

$$n \mapsto \left((v_q(\varphi(n)) \bmod m_q)_{q\in\mathcal{Q}}, u(\varphi(n)) \bmod M\right).$$

Theorem 3. *As n ranges over $\mathbf{N}$, the elements $\theta(n)$ become equidistributed in G. In other words, for each $g \in G$, the set $\theta^{-1}(g)$ has asymptotic density $|G|^{-1} = (\varphi(M)\prod_{q\in\mathcal{Q}} m_q)^{-1}$.*

Remarks

1. We recover the density statement of Theorem 1 by taking $\mathcal{Q} = \{2\}$, $m_2 = 2$, and $l = 3$.

2. Since l may be taken arbitrarily large, it follows that the equidistribution statement of Theorem 3 holds for any M supported on the primes in $\mathcal{Q}$, not only those of the particular form (6).

3. The restriction to moduli M supported on primes in $\mathcal{Q}$ is a natural one. Indeed, if M' is a fixed integer coprime to $\prod_{q\in\mathcal{Q}} q$, then $M' \mid u(\varphi(n))$ for almost all natural numbers n. A somewhat stronger claim appears as [14, Lemma 2].

The proof of Theorem 3 is similar to the argument of the last section. The key difference is that the characters of G need no longer be real-valued, so that Wirsing's theorem may not apply. But the following result of Hall [8] is a suitable stand-in:

Theorem C. *Let $\mathcal{D}$ be a closed, convex proper subset of the closed unit disc in* $\mathbf{C}$ *which contains* 0*. Suppose that f is a complex-valued multiplicative function satisfying $|f(n)| \leq 1$ for all $n \in \mathbf{N}$ and $f(p) \in \mathcal{D}$ for all primes p. If the series*

$$\sum_{p} \frac{1 - \Re(f(p))}{p} \tag{7}$$

diverges, then f has mean value zero. In fact, letting $L(\mathcal{D})$ denote the perimeter of $\mathcal{D}$, we have

$$\frac{1}{x}\left|\sum_{n \leq x} f(n)\right| \ll \exp\left(-\frac{1}{2}\left(1 - \frac{L(\mathcal{D})}{2\pi}\right)\sum_{p \leq x} \frac{1 - \Re(f(p))}{p}\right)$$

for $x \geq 1$. The implied constant here depends only on the region $\mathcal{D}$.

For each $\chi \in \hat{G}$, we lift χ to a multiplicative function on $\mathbf{N}$ by setting $\chi(n) = \chi(\theta(n))$. We will apply Theorem C with $f = \chi$, where we take $\mathcal{D}$ as the convex hull of the $\#G$th roots of unity. Notice that for each prime p, either $f(p) = 1$ or $1 - \Re(f(p)) \geq 1 - \cos\frac{2\pi}{\#G} > 0$. (We assume here that $\#G > 1$; otherwise Theorem 3 is trivial.) So the series (7), with $f = \chi$, diverges if $\sum_{p\colon\, \chi(p) \neq 1} \frac{1}{p}$ diverges. We will show that this is true for every nontrivial χ.

Let χ be a nontrivial character. Then there are complex numbers $\{\zeta_q\}_{q \in \mathcal{Q}}$, with each $\zeta_q^{m_q} = 1$, and a Dirichlet character $\tilde{\chi}$ mod M, with

$$\chi(n) = \left(\prod_{q \in \mathcal{Q}} \zeta_q^{v_q(\varphi(n))}\right)\tilde{\chi}(u(\varphi(n)))$$

for all $n \in \mathbf{N}$. Suppose first that $\tilde{\chi}$ is not trivial, and choose an integer a coprime to M with $\tilde{\chi}(a) \neq 1$. Then $\chi(p) = \tilde{\chi}(a) \neq 1$ for all primes p satisfying

$$p \equiv 1 + a\prod_{q \in \mathcal{Q}} q^{m_q} \pmod{\prod_{q \in \mathcal{Q}} q^{m_q + l}}.$$

The sum of the reciprocals of these primes p diverges by Dirichlet's theorem. Now suppose that $\tilde{\chi}$ is trivial. Since χ is nontrivial, we must have $\zeta_q \neq 1$ for some $q \in \mathcal{Q}$, say $\zeta_{q_0} \neq 1$. But then $\chi(p) = \zeta_{q_0} \neq 1$ if

$$p \equiv \begin{cases} 1 + q \pmod{q^2} & \text{when } q = q_0, \\ 1 + q^{m_q} \pmod{q^{m_q+1}} & \text{when } q \in \mathcal{Q} \setminus \{q_0\}. \end{cases}$$

The sum of the reciprocals of these primes diverges also, again by Dirichlet's result.

Remarks

1. As in Theorem 1, the error term in the asymptotic formula of Theorem 3 may be taken as $O(x/(\log x)^c)$ for some $c > 0$ (which may depend on $\mathcal{Q}$, the m_q, and l). To see this, we have only to insert into the above argument the form of Dirichlet's result appearing in the proof of Theorem 1 and the quantitative half of Hall's Theorem C.

2. To prove that Theorems 1 and 3 are valid with σ in place of φ, it is only necessary is to replace each (implicit) occurrence of "$p-1$" in the proofs with "$p+1$". The reason this is so simple is that Theorems A–C refer only to the values of f at prime arguments, and not at proper prime powers.

3. It is clear that Theorem 3 does not hold for all positive integer-valued multiplicative functions, but a very general result of Ruzsa [19, Theorem (1.4)] implies that for any such function, each of the sets $\theta^{-1}(g)$ referred to in that theorem has an asymptotic density.

3. Carmichael's Function

While Carmichael's λ-function is not multiplicative, it is nonetheless easy to compute $\lambda(m)$ given the prime factorization of m. For any two coprime positive integers a and b, the isomorphism $(\mathbf{Z}/ab\mathbf{Z})^\times \cong (\mathbf{Z}/a\mathbf{Z})^\times \times (\mathbf{Z}/b\mathbf{Z})^\times$ yields that $\lambda(ab) = \mathrm{lcm}[\lambda(a), \lambda(b)]$. As a consequence,

$$\lambda(m) = \mathrm{lcm}\{\lambda(p^k) : p^k \parallel m\}; \tag{8}$$

moreover, for each prime power p^k,

$$\lambda(p^k) = \begin{cases} p^{k-1}(p-1) & \text{if } p \text{ is odd, or if } p = 2 \text{ but } k \in \{1, 2\}, \\ p^{k-2} & \text{if } p = 2 \text{ and } k \geq 3. \end{cases} \tag{9}$$

(For a proof of (9), see, e.g., [10, Chapter 4].) These facts will be used without further comment in the sequel.

We will treat the upper and lower bounds in Theorem 2 separately. To begin, we need a strengthening of (5) in the case $a = 1$, which can be found in [16] or [18]:

Lemma 4. *For all integers $m > 1$ and all $x \geq 3$,*

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{m}}} \frac{1}{p} = \frac{\log\log x}{\varphi(m)} + O\left(\frac{\log m}{\varphi(m)}\right), \tag{10}$$

with an O-constant uniform in both m and x.

The next lemma is implicit in the work of Li [13, proof of Theorem 3.1]. We include a proof for the sake of completeness.

Lemma 5. *Fix $H > 0$. Suppose that x is large, depending on H. Then for any integer R with $\frac{\log_3 x}{\log 2} - H \le R \le \frac{\log_3 x}{\log 2} + H$, there are $\gg x$ values of $n \le x$ satisfying $v_2(\lambda(n)) = R$. The implied constant here depends at most on H.*

Proof. We will construct $\gg x$ odd numbers $n \le x$ of the form mp, where $v_2(p-1) = R$ and

$$v_2(q-1) < R \quad \text{for all primes} \quad q \mid m. \tag{11}$$

Notice that each n constructed in this way satisfies $v_2(\lambda(n)) = \max_{p|n} v_2(p-1) = R$, as desired.

Fix a prime $p \le x^{1/2}$ satisfying $v_2(p-1) = R$. For each such p, we count the number of odd $m \le x/p$ satisfying (11). Put $y := \exp(\log x/\log\log x)$, and from all odd $m \le x/p$, remove those with a prime factor $q \equiv 1 \pmod{2^R}$ with $q \le y$. Since $y = x^{o(1)}$ and $x/p \ge x^{1/2}$, the fundamental lemma of the sieve (see [7, Theorem 7.2]) guarantees that the number of m surviving this process is

$$\gg \frac{x}{2p} \prod_{\substack{q \le y \\ q \equiv 1 \pmod{2^R}}} \left(1 - \frac{1}{q}\right) \gg \frac{x}{p} \exp\left(- \sum_{\substack{q \le y \\ q \equiv 1 \pmod{2^R}}} \frac{1}{q}\right).$$

We estimate the sum over q with (10). Since $2^R \asymp \log\log x$, we see that

$$\sum_{\substack{q \le y \\ q \equiv 1 \pmod{2^R}}} \frac{1}{q} = \frac{\log\log y}{\varphi(2^R)} + O\left(\frac{\log(2^R)}{2^R}\right) \ll 1,$$

and so the number of remaining m is $\gg x/p$. If m has not been sieved out, but m fails (11), then m has a prime divisor $q \equiv 1 \pmod{2^R}$ with $q > y$. But the number of such m is

$$\ll \frac{x}{p} \sum_{\substack{y < q \le x/p \\ q \equiv 1 \pmod{2^R}}} \frac{1}{q} = \frac{x}{p}\left(\frac{\log\log(x/p) - \log\log y}{\varphi(2^R)} + O\left(\frac{\log(2^R)}{2^R}\right)\right) \ll \frac{x}{p} \frac{\log\log\log x}{\log\log x}.$$

So for large x, the number of odd $m \le x/p$ satisfying (11) is $\gg x/p$, uniformly in p. Summing over p, we see that the number of n constructed in this way is

$$\begin{aligned} \gg x \sum_{\substack{p \le x^{1/2} \\ p \equiv 1 \pmod{2^R} \\ p \not\equiv 1 \pmod{2^{R+1}}}} \frac{1}{p} &= x\left(\frac{\log\log(x^{1/2})}{\varphi(2^R)} - \frac{\log\log(x^{1/2})}{\varphi(2^{R+1})}\right) + O\left(x\frac{\log(2^R)}{2^R}\right) \\ &= x\frac{\log\log x}{2^R} + O\left(x\frac{\log\log\log x}{\log\log x}\right) \gg x. \end{aligned}$$

Notice that there is no overcounting here, since in the decomposition $n = mp$, the prime p is the unique prime divisor of n with $v_2(p-1) = R$. $\square$

We can now prove half of Theorem 2.

Proof of the lower bound in Theorem 2. Applying Lemma 5 with $H = 1$ and R the nearest odd integer to $\log_3 x/\log 2$ (breaking ties arbitrarily), we see that there are $\gg x$ values of $n \le x$ with $v_2(\lambda(n))$ odd. But then $\lambda(n) = \square + \square + \square$ by Legendre's criterion. $\square$

The proof of the upper bound in Theorem 2 is more difficult. The strategy we will use was suggested to the author by Florian Luca and Carl Pomerance.

We begin by quoting a special case of [6, Theorem 4.1]. Let

$$E(n, x) := \sum_{\substack{p \le \log\log x \\ p \nmid \lambda(n)}} \frac{1}{p} + \sum_{\substack{p > \log\log x \\ p \mid \lambda(n)}} \frac{1}{p}. \tag{12}$$

Lemma 6. *For $x \ge 1$, we have $\sum_{n \le x} E(n, x) \ll x/\log_3 x$.*

In [6], the lemma is stated with $\varphi(n)$ in place of $\lambda(n)$, but from (8) and (9), the numbers $\varphi(n)$ and $\lambda(n)$ always share the same set of prime factors. As an immediate consequence of Lemma 6, the number of $n \le x$ with $E(n, x) > \epsilon$ is $\ll \epsilon^{-1} x/\log_3 x$.

Proof of the upper bound in Theorem 2. We start with a summary of our strategy: Let R be the nearest even integer to $\frac{\log_3 x}{\log 2}$, and consider pairs (m, p) with $v_2(\lambda(m)) = R$ and $v_2(p-1) \le R$. Assume also that p is coprime to m. Then with $n := mp$,

$$\lambda(n) = \frac{p-1}{d}\lambda(m), \quad \text{where} \quad d := \gcd(p-1, \lambda(m)).$$

The number $(p-1)/d$ is odd, so that $v_2(\lambda(n)) = v_2(\lambda(m)) = R$. In particular, $v_2(\lambda(n))$ is even. Using again $u(\cdot)$ to denote the odd part, we have that

$$u(\lambda(n)) = \frac{p-1}{d} u(\lambda(m)).$$

Thus, if we define $A_m \in \{1, 3, 5, 7\}$ so that

$$A_m \cdot u(\lambda(m)) \equiv 7 \pmod 8,$$

and if p is such that

$$\frac{p-1}{d} \equiv A_m \pmod 8, \tag{13}$$

then $u(\lambda(n)) \equiv 7 \pmod 8$. So by Legendre's criterion, $\lambda(n)$ is not a sum of three squares. We now show how to construct $\gg x$ such values of $n \le x$.

Since we are seeking a lower bound, we are free to impose convenient conditions on the pairs (m,p) which we consider. In order to ensure that p is coprime to m and that the representation of n in the form mp is unique (so as to avoid overcounting), we require that

$$x^{1/6} < m \le x^{1/3}$$

and that

$$\frac{1}{2}x/m < p \le x/m,$$

so that $p > \frac{1}{2}x^{2/3} > x^{1/3} \ge m$ for large x. Thus, the number of $n \le x$ for which $\lambda(n) \ne \square + \square + \square$ is bounded below by

$$\sum_{d} \sum_{\substack{x^{1/6}<m\le x^{1/3}\\ d\mid\lambda(m)\\ v_2(\lambda(m))=R}} \sum_{\substack{\frac{1}{2}x/m<p\le x/m\\ (p-1,\lambda(m))=d\\ v_2(p-1)\le R\\ \frac{p-1}{d}\equiv A_m \pmod 8}} 1.$$

To simplify the situation slightly, let us sum only over d for which $2 \parallel d$. Note that for large x, the condition $v_2(p-1) \le R$ then follows automatically from the two conditions $(p-1,\lambda(m)) = d$ and $v_2(\lambda(m)) = R$; in fact, we get that $v_2(p-1) = 1$. For technical reasons having to do with limitations in the range of uniformity of the prime number theorem in arithmetic progressions, we impose further arithmetic restrictions on m and d: We require that $E(m,x)$, defined by (12), satisfies

$$E(m,x) \le 1$$

and that the number and size of the prime factors of d are constrained,

$$\Omega(d) \le 2\log_4 x \quad \text{and} \quad P(d) \le \log\log x. \tag{14}$$

Reordering the sums, we are led to the following lower bound, valid for all large x:

$$\#\{n \le x : \lambda(n) \ne \square + \square + \square\} \ge \sum_{\substack{x^{1/6}<m\le x^{1/3}\\ v_2(\lambda(m))=R\\ E(m,x)\le 1}} \sum_{\substack{d\mid\lambda(m),\ 2\parallel d\\ P(d)\le\log\log x\\ \Omega(d)\le 2\log_4 x}} \sum_{\substack{\frac{1}{2}x/m<p\le x/m\\ \frac{p-1}{d}\equiv A_m \pmod 8\\ (p-1,\lambda(m))=d}} 1. \tag{15}$$

Instead of requiring in the final sum of (15) that $\gcd(p-1,\lambda(m)) = d$, for the sake of subsequent estimates it is expedient to impose a slightly weaker condition on p, viz.

$$\min\{v_q(p-1), v_q(\lambda(m))\} = v_q(d) \quad \text{for all} \quad q \le \log_2 x. \tag{16}$$

In other words, we require only that d be the $(\log_2 x)$-smooth part of $\gcd(p-1,\lambda(m))$. This change causes us to count some additional integers, but this does not hurt us since, as we show below, the number $A(x)$ of additional integers satisfies

$$A(x) \ll x/\log_3 x. \tag{17}$$

Indeed, suppose that p satisfies (16) but that $\gcd(p-1,\lambda(m)) \neq d$. Since $P(d) \leq \log_2 x$, it follows that there is some $q > \log_2 x$ with $q \mid \gcd(p-1,\lambda(m))$. So the contribution of these p to the right-hand side of (15) is bounded by

$$\sum_{x^{1/6}<m\leq x^{1/3}} \sum_{\substack{q>\log\log x\\ q\mid\lambda(m)}} \sum_{\substack{p\leq x/m\\ q\mid p-1}} 1 \ll \sum_{x^{1/6}<m\leq x^{1/3}} \sum_{\substack{q>\log\log x\\ q\mid\lambda(m)}} \frac{x}{mq\log x}$$
$$\ll \frac{x}{\log x} \sum_{x^{1/6}<m\leq x^{1/3}} \frac{1}{m} \sum_{\substack{q>\log\log x\\ q\mid\lambda(m)}} \frac{1}{q}.$$

(Here we have applied the Brun–Titchmarsh inequality; note that $mq \leq m^2 \leq x^{2/3}$, so that $\log\frac{x}{mq} \gg \log x$.) For $x^{1/6} \leq y \leq x^{1/3}$, we have

$$\sum_{m\leq y} \sum_{\substack{q>\log\log x\\ q\mid\lambda(m)}} \frac{1}{q} \leq \sum_{m\leq y} E(m,y) \ll \frac{y}{\log_3 y},$$

so that by Abel summation,

$$\sum_{x^{1/6}<m\leq x^{1/3}} \frac{1}{m} \sum_{\substack{q>\log\log x\\ q\mid\lambda(m)}} \frac{1}{q} \ll \frac{\log x}{\log_3 x}.$$

Collecting our estimates, we have (17). Hence, to show that the right-hand side of (15) is $\gg x$, it is enough to show that

$$\sum_{m}\sum_{d} \sum_{\substack{x/2m<p\leq x/m\\ p \text{ satisfies (13), (16)}}} 1 \gg x. \tag{18}$$

Here and below, a sum over m or d without additional subscripts indicates that the conditions of summation are the same as in (15).

The sum over p in (18) can be estimated using standard results on the distribution of primes in progressions. We may interpret (13) and (16) as asserting that p falls into a certain collection of residue classes modulo M, where

$$M := 8d \prod_{\substack{2<q\leq\log\log x\\ q\mid\lambda(m)/d}} q.$$

Notice that by the prime number theorem and (14),

$$M \leq 8d \prod_{q\leq\log\log x} q \leq 8(\log\log x)^{2\log_4 x}(\log x)^{1+o(1)} < (\log x)^{3/2}$$

for large x. One checks that the number of coprime residue classes modulo M consistent with both (13) and (16) is

$$\frac{\varphi(M)}{8}\frac{1}{\varphi(d/2)}\prod_{\substack{q|\lambda(m)/d\\ 2<q\le\log\log x}}\left(1-\frac{1}{q}\right).$$

Now a moderately strong form of the prime number theorem for progressions (see, e.g., [5, Chapter 20]) gives that the sum over p in (18) is

$$\begin{aligned}\gg \left(\frac{1}{\varphi(d)}\prod_{\substack{q|\lambda(m)/d\\ q\le\log\log x}}\left(1-\frac{1}{q}\right)\right)\frac{x}{m\log x} &\ge \frac{1}{\varphi(d)}\frac{x}{m\log x}\prod_{q\le\log\log x}\left(1-\frac{1}{q}\right)\\ &\gg \frac{1}{\varphi(d)}\frac{x}{m\log x}\frac{1}{\log\log\log x}.\end{aligned}$$

Hence the triple sum on the left-hand side of (18) is

$$\gg \frac{x}{\log x}\sum_{m}\frac{1}{m}\left(\frac{1}{\log\log\log x}\sum_{d}\frac{1}{\varphi(d)}\right). \tag{19}$$

We now turn our attention to the sum over d in (19). We start by observing that

$$\sum_{d}\frac{1}{\varphi(d)} \ge \sum_{\substack{d|\lambda(m),\ 2\|d\\ P(d)\le\log\log x}}\frac{1}{\varphi(d)} - \sum_{\substack{d|\lambda(m),\ 2\|d\\ P(d)\le\log\log x\\ \Omega(d)>2\log_4 x}}\frac{1}{\varphi(d)}. \tag{20}$$

The first right-hand sum in (20) is easy to estimate: Since $\lambda(m)$ is even, we have

$$\begin{aligned}\sum_{\substack{d|\lambda(m),\ 2\|d\\ P(d)\le\log\log x}}\frac{1}{\varphi(d)} \ge \sum_{\substack{d|\lambda(m),\ 2\|d\\ P(d)\le\log\log x\\ d\text{ squarefree}}}\frac{1}{\varphi(d)} &= \frac{1}{\varphi(2)}\prod_{\substack{2<q\le\log\log x\\ q|\lambda(m)}}\left(1+\frac{1}{q-1}\right)\\ &\gg \exp\left(\sum_{\substack{q|\lambda(m)\\ q\le\log\log x}}\frac{1}{q}\right) \gg \log\log\log x,\end{aligned}$$

where we use that

$$\sum_{\substack{q|\lambda(m)\\ q\le\log\log x}}\frac{1}{q} \ge \sum_{q\le\log\log x}\frac{1}{q} - E(m,x) \ge \log_4 x + O(1).$$

(Recall that $E(m,x)\le 1$.) We now show that the second sum on the right-hand side of (20) is $o(\log_3 x)$, so that the left-hand side of (20) is $\gg \log_3 x$. Consider first the contribution of those d with $\omega(d) > \frac{3}{2}\log_4 x$. Using the multinomial theorem, we see that this contribution is bounded by

$$\sum_{\substack{d\colon P(d)\le \log\log x\\ \omega(d)>\frac{3}{2}\log_4 x}} \frac{1}{\varphi(d)} \le \sum_{k>\frac{3}{2}\log_4 x} \frac{1}{k!}\left(\sum_{q\le \log_2 x}\left(\frac{1}{\varphi(q)}+\frac{1}{\varphi(q^2)}+\dots\right)\right)^k$$
$$\le \sum_{k>\frac{3}{2}\log_4 x} \frac{1}{k!}(\log_4 x + O(1))^k < (\log_3 x)^{9/10}.$$

(To verify the last estimate in this chain, it is helpful to keep in mind the elementary inequality $k! \ge (k/e)^k$ and to observe that the sum over k is dominated by its first term.) Now consider the contribution of those d with $\omega(d) \le \frac{3}{2}\log_4 x$. Write $d = d_1 d_2$, where d_1 is the largest squarefree divisor of d. Then

$$\Omega(d_2) = \Omega(d) - \Omega(d_1) = \Omega(d) - \omega(d) > \frac{1}{2}\log_4 x.$$

Put $e := d_2 \prod_{q\mid d_2} q$. Then e is a squarefull divisor of d, and clearly

$$e \ge 2^{\Omega(e)} \ge 2^{\Omega(d_2)} > 2^{\frac{1}{2}\log_4 x}.$$

Moreover, e is coprime to $d' := d/e$, and so $\varphi(d) = \varphi(e)\varphi(d')$. So the contribution from these d to the second sum on the right of (20) is

$$\ll \sum_{\substack{e \text{ squarefull}\\ e>2^{(\log_4 x)/2}}} \frac{1}{\varphi(e)} \sum_{\substack{d'\mid\lambda(m)\\ P(d')\le \log_2 x\\ d' \text{ squarefree}}} \frac{1}{\varphi(d')} \le \sum_{\substack{e \text{ squarefull}\\ e>2^{(\log_4 x)/2}}} \frac{1}{\varphi(e)} \prod_{q\le \log_2 x}\left(1+\frac{1}{q-1}\right)$$
$$\ll \log_3 x \sum_{\substack{e \text{ squarefull}\\ e>2^{(\log_4 x)/2}}} \frac{1}{\varphi(e)}.$$

The final sum over e is the tail of a convergent series, since

$$\sum_{e \text{ squarefull}} \frac{1}{\varphi(e)} = \prod_q \left(1+\frac{1}{\varphi(q^2)}+\frac{1}{\varphi(q^3)}+\dots\right) < \infty.$$

So those d with $\omega(d) \le \frac{3}{2}\log_4 x$ also contribute $o(\log_3 x)$, as desired.

Referring back to (19), we now have a lower bound which is

$$\gg \frac{x}{\log x} \sum_{\substack{x^{1/6}<m\le x^{1/3}\\ v_2(\lambda(m))=R\\ E(m,x)\le 1}} \frac{1}{m}.$$

For $x^{1/6} \le y \le x^{1/3}$, there are $\gg y$ values of $m \le y$ with $v_2(\lambda(m)) = R$, by Lemma 5. (We use here that $\log_3$ is very slowly varying, so that $|\frac{\log_3 y}{\log 2} - R| \le 1.1$, say, for all such y.) Requiring $E(m, x) \le 1$ excludes only $o(y)$ of these m. (Indeed, if $E(m, x) > 1$, then $E(m, y) \ge 1/2$, and there are only $o(y)$ of these m in $[1, y]$ by Lemma 6.) The estimate $\sum \frac{1}{m} \gg \log x$ now follows by partial summation. Inserting this above shows that there are $\gg x$ values of $n \le x$ for which $\lambda(n)$ is not a sum of three squares. $\square$

Acknowledgements It is my pleasure to thank Carl Pomerance and Florian Luca for their suggestions and encouragement. I am particularly grateful to Professor Pomerance for pointing out the relevance of [13]. This work was done during a visit to Dartmouth College. I am indebted to the faculty and staff of the mathematics department for their extraordinary hospitality. Finally, I would like to thank the anonymous referee for several helpful suggestions based on a careful reading of the manuscript.

References

[1] P. Bachmann, *Zahlentheorie, Bd. 2: Die analytische Zahlentheorie*, B. G. Teubner, Leipzig, 1894.

[2] W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Multiplicative structure of values of the Euler function*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 29–47.

[3] W. D. Banks and A. M. Güloğlu, *Values of the Carmichael function equal to a sum of two squares*, Turkish J. Math. **33** (2009), 9–16.

[4] W. D. Banks, F. Luca, F. Saidak, and I. E. Shparlinski, *Values of arithmetical functions equal to a sum of two squares*, Q. J. Math. **56** (2005), 123–139.

[5] H. Davenport, *Multiplicative number theory*, second ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 1980.

[6] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 165–204.

[7] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, vol. 4, Academic Press, London-New York, 1974.

[8] R. R. Hall, *A sharp inequality of Halász type for the mean value of a multiplicative arithmetic function*, Mathematika **42** (1995), 144–157.

[9] R. R. Hall and G. Tenenbaum, *Effective mean value estimates for complex multiplicative functions*, Math. Proc. Cambridge Philos. Soc. **110** (1991), 337–351.

[10] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[11] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. **13** (1908), 305–312.

[12] ———, *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände*, 2nd ed., Chelsea Publishing Co., New York, 1953.

[13] S. Li, *On the number of elements with maximal order in the multiplicative group modulo n*, Acta Arith. **86** (1998), 113–132.

[14] F. Luca and C. Pomerance, *On some problems of Mąkowski-Schinzel and Erdős concerning the arithmetical functions ϕ and σ*, Colloq. Math. **92** (2002), 111–130.

[15] P. Moree and J. Cazaran, *On a claim of Ramanujan in his first letter to Hardy*, Exposition. Math. **17** (1999), 289–311.

[16] K. K. Norton, *On the number of restricted prime factors of an integer. I*, Illinois J. Math. **20** (1976), 681–705.

[17] A. H. Osbaldestin and P. Shiu, *A correlated digital sum problem associated with sums of three squares*, Bull. London Math. Soc. **21** (1989), 369–374.

[18] C. Pomerance, *On the distribution of amicable numbers*, J. Reine Angew. Math. **293/294** (1977), 217–222.

[19] I. Z. Ruzsa, *General multiplicative functions*, Acta Arith. **32** (1977), 313–347.

[20] A. Selberg, *Collected papers. Vol. II*, Springer-Verlag, Berlin, 1991.

[21] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 1973.

[22] P. Shiu, *Counting sums of three squares*, Bull. London Math. Soc. **20** (1988), 203–208.

[23] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.

[24] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen. II*, Acta Math. Acad. Sci. Hungar. **18** (1967), 411–467.