Article 4 INTEGERS 11A (2011)

Proceedings of Integers Conference 2009

POWER TOTIENTS WITH ALMOST PRIMES

William D. Banks[1]
Department of Mathematics, University of Missouri, Columbia, Missouri
bankswd@missouri.edu

Florian Luca
Instituto de Matemáticas, Universidad Nacional Autónoma de México, Morelia, Michoacán, México
fluca@matmor.unam.mx

Received: 11/11/09, Accepted: 2/14/10, Published: 3/9/11

Abstract

A natural number n is called a *k-almost prime* if n has precisely k prime factors, counted with multiplicity. For any fixed $k \geqslant 2$, let $\mathcal{F}_k(X)$ be the number of k-th powers $m^k \leqslant X$ such that $\phi(n) = m^k$ for some squarefree k-almost prime n, where $\phi(\cdot)$ is the Euler function. We show that the lower bound $\mathcal{F}_k(X) \gg X^{1/k}/(\log X)^{2k}$ holds, where the implied constant is absolute and the lower bound is uniform over a certain range of k relative to X. In particular, our results imply that there are infinitely many pairs (p, q) of distinct primes such that $(p-1)(q-1)$ is a perfect square.

Dedicated to Carl Pomerance on the occasion of his 65th birthday

1. Introduction

A longstanding conjecture in number theory asserts the existence of infinitely many primes of the form $m^2 + 1$. Although the problem is intractable at present, there have been a number of partial steps in the direction of this result. For instance, thanks to Brun, one knows that the number of integers $m^2 + 1 \leqslant X$ that are prime is at most $O(x^{1/2}/\log x)$. In the opposite direction, Iwaniec [6] has shown that $m^2 + 1$ is the product of at most two primes infinitely often.

For any prime p, we clearly have

$$p = m^2 + 1 \qquad \Longleftrightarrow \qquad \phi(p) = m^2,$$

[1] Corresponding author

where $\phi(\cdot)$ is the Euler function, and hence the m^2+1 conjecture can be reformulated as the assertion that the set

$$\mathcal{S}_2 = \{n \in \mathbb{N} \;:\; \phi(n) \text{ is a perfect square}\}$$

contains infinitely many primes. Motivated by this observation, the set $\mathcal{S}_2$ was first studied by Banks, Friedlander, Pomerance and Shparlinski [3]; they showed that

$$\big|\{n \leqslant x \;:\; n \in \mathcal{S}_2\}\big| \geqslant x^{0.7038}$$

for all sufficiently large values of x.

Although we cannot prove that $\mathcal{S}_2$ contains infinitely many primes, it is interesting to ask whether other thin sets of integers enjoy an infinite intersection with $\mathcal{S}_2$. Recently, Banks [2] showed that $\mathcal{S}_2$ contains infinitely many Carmichael numbers, and he asked whether $\mathcal{S}_2$ contains infinitely many integers with at most two prime factors. In this note, we give an affirmative answer to this question by showing that there exist infinitely many pairs (p, q) of distinct primes such that $\phi(pq) = (p-1)(q-1)$ is a perfect square.

Recall that a natural number n is called a *k-almost prime* if n has precisely k prime factors, counted with multiplicity. Our main result is the following:

Theorem. *For each $k \geqslant 2$, let $\mathcal{F}_k(X)$ be the number of k-th powers $m^k \leqslant X$ such that $\phi(n) = m^k$ for some squarefree k-almost prime n. There is a constant X_0 such that the bound*

$$\mathcal{F}_k(X) \geqslant \frac{4X^{1/k}}{9e(\log X)^{2k}} \qquad \textit{holds for} \qquad 2 \leqslant k \leqslant \sqrt{\frac{\log X}{12 \log\log X}}$$

whenever $X \geqslant X_0$.

2. Notation and Outline of Proof

In what follows, the letters p and q always denote prime numbers. As is customary, we use $\pi(x)$ to denote the number of primes $p \leqslant x$ and $\pi(x; d, a)$ the number of such primes in the arithmetic progression $a \bmod d$.

Below, any constants implied by the symbols O, $\ll$, $\gg$ and $\asymp$ are absolute. In particular, the notation $x \gg 1$ means that x exceeds some positive absolute constant.

Our approach to the proof of the theorem is as follows. Let $x = X^{1/k}$. We begin by constructing a certain set $\mathcal{Q}$ of primes close to $x^{1/(3k)}$. Next, we take $\mathcal{P}$ to be the set of primes $p \leqslant x$ such that $p - 1 = aq^k$ for some prime $q \in \mathcal{Q}$ and an integer a that is not divisible by any prime in $\mathcal{Q}$. The number $a_p = a$ is uniquely determined by p, and $a_p \ll x^{2/3}$ for all $p \in \mathcal{P}$, whereas the cardinality of $\mathcal{P}$ satisfies the lower bound $|\mathcal{P}| \gg x^{2/3+1/3k}(\log x)^{-2}$, and hence it follows that $\mathcal{P}$ has a large subset of the form $\mathcal{P}_a = \{p \in \mathcal{P} \ : \ a_p = a\}$. For every k-element subset $\{p_1, \ldots, p_k\}$ of $\mathcal{P}_a$, the number $n = p_1 \cdots p_k$ does not exceed $x^k = X$, and n is a squarefree k-almost prime for which the totient $\phi(n)$ is a k-th power. Indeed, writing $p_j = aq_j^k + 1$ with $q_j \in \mathcal{Q}$ for each j, we have

$$\phi(n) = \phi(p_1 \cdots p_k) = (p_1 - 1) \cdots (p_k - 1) = (aq_1 \cdots q_k)^k.$$

Thus, to obtain a lower bound for $\mathcal{F}_k(X)$, it suffices to count the number of k-element subsets of $\mathcal{P}$ that are contained in one of the sets $\mathcal{P}_a$.

3. Proof of the Theorem

Following Alford, Granville and Pomerance [1], let $\mathcal{B}$ be the set of numbers $B \in (0,1)$ for which there is a number $x_0(B) > 0$ and an integer $D_B \geqslant 1$ such that whenever $x \geqslant x_0(B)$, $\gcd(a,d) = 1$ and $1 \leqslant d \leqslant \min\{x^B, y/x^{1-B}\}$, one has

$$\pi(y; d, a) \geqslant \frac{\pi(y)}{2\phi(d)} \tag{1}$$

provided that d is not divisible by some member of $\mathcal{D}_B(x)$, a set consisting of at most D_B integers, each of which exceeds $\log x$. In [1, Section 2], it is shown that the interval $(0, 5/12)$ is contained in $\mathcal{B}$.

Let $B = 1/3 \in \mathcal{B}$, let $x \geqslant x_0(1/3)$, and let $k \geqslant 2$ be an integer such that

$$k \leqslant \frac{\log x}{12 \log\log x}\,. \tag{2}$$

Observe that if $x \geqslant 3$, then $k \leqslant \log x$, and we have

$$k \log k \leqslant \frac{\log x}{12}\,. \tag{3}$$

Let $\mathcal{Q}$ be the set of primes q in the range

$$x^{1/(3k)} < q \leqslant x^{1/(3k)}\,(1 + 1/k)$$

and such that $q \notin \mathcal{D}_{1/3}(x)$. Since

$$|\mathcal{Q}| = \pi\big(x^{1/(3k)}\,(1+1/k)\big) - \pi\big(x^{1/(3k)}\big) + O(1),$$

it follows that

$$|\mathcal{Q}| = \frac{c_1 x^{1/(3k)}}{\log x} \tag{4}$$

holds with some $c_1 = c_1(x,k) \in [2,4]$ provided that x is large and uniformly for all k satisfying (2). Indeed, to derive (4) we have used the estimate

$$\pi(u+v) - \pi(u) = \frac{v}{\log u}\left(1 + O\left(\frac{(\log\log u)^4}{\log u}\right)\right),$$

which is valid for any $v \geqslant u^{7/12}$ (see [4, 5]). Note that this estimate can be applied with $u = x^{1/(3k)}$ and $v = x^{1/(3k)}/k$ since the inequality $v \geqslant u^{7/12}$ is then equivalent to

$$k \log k \leqslant \frac{5\log x}{36},$$

which holds in view of (3).

Let $\mathcal{P}$ be the set of primes $p \leqslant x$ such that $q^k \mid p-1$ for some $q \in \mathcal{Q}$, and $a = (p-1)/q^k$ is not divisible by any prime in $\mathcal{Q}$. Clearly,

$$|\mathcal{P}| \geqslant \sum_{q\in\mathcal{Q}} \pi(x; q^k, 1) - \sum_{q_1,q_2\in\mathcal{Q}} \pi(x; q_1^k q_2, 1). \tag{5}$$

Taking $y = x$, $d = q^k$, $a = 1$ in (1), we have

$$\pi(x; q^k, 1) \geqslant \frac{\pi(x)}{2\phi(q^k)} \geqslant \frac{c_2 x}{q^k \log x} \qquad (q \in \mathcal{Q},\ x \gg 1),$$

where $c_2 = 0.46$ (say). Using this bound together with (4), it follows that

$$\begin{aligned}\sum_{q\in\mathcal{Q}} \pi(x; q^k, 1) \geqslant \frac{c_2 x}{\log x}\sum_{q\in\mathcal{Q}}\frac{1}{q^k} &\geqslant \frac{c_2 x}{\log x}\cdot\frac{|\mathcal{Q}|}{(x^{1/(3k)})^k(1+1/k)^k} \\ &\geqslant \frac{c_1 c_2 x^{2/3+1/(3k)}}{e(\log x)^2} \end{aligned}\tag{6}$$

if x is sufficiently large. On the other hand, using the Montgomery-Vaughan large sieve estimate (see [7]) one has

$$\pi(x; q_1^k q_2, 1) \leqslant \frac{2x}{q_1^k q_2 \log(x/(q_1^k q_2))}.$$

For all primes $q_1, q_2 \in \mathcal{Q}$ we have

$$q_1^k q_2 \leqslant (1+1/k)^{k+1} x^{1/3+1/(3k)} \leqslant x^{2/3}$$

for all large x and uniformly in $k \geqslant 2$. Therefore, taking (4) into account we derive the bound

$$\begin{aligned}\sum_{q_1,q_2\in\mathcal{Q}} \pi(x; q_1^k q_2, 1) &\leqslant \frac{6x}{\log x}\sum_{q_1\in\mathcal{Q}}\frac{1}{q_1^k}\sum_{q_2\in\mathcal{Q}}\frac{1}{q_2} \\ &\leqslant \frac{6x}{\log x}\cdot\frac{c_1^2 x^{2/(3k)}}{(x^{1/(3k)})^{k+1}(\log x)^2} \\ &\leqslant \frac{96 x^{2/3+1/(3k)}}{(\log x)^3} \end{aligned}\tag{7}$$

provided that x is large. Here, we have used the fact that $c_1 \leqslant 4$. Inserting the bounds (6) and (7) into (5), and taking into account that $c_1c_2/e > 1/3$, we obtain the lower bound

$$|\mathcal{P}| \geqslant \frac{x^{2/3+1/(3k)}}{3(\log x)^2} \qquad (x \gg 1). \tag{8}$$

By construction, every prime $p \in \mathcal{P}$ has a unique expression of the form $p = a_p q_p^k + 1$, where a_p is a natural number and q_p is a prime in $\mathcal{Q}$. Let

$$\mathcal{A} = \{a \in \mathbb{N} \ : \ a = a_p \text{ for some } p \in \mathcal{P}\}.$$

Since every a_p is a positive integer that does not exceed $x^{2/3}$, we have the trivial bound

$$|\mathcal{A}| \leqslant x^{2/3}. \tag{9}$$

We also note that the inequality

$$\frac{k|\mathcal{A}|}{|\mathcal{P}|} \leqslant \frac{1}{k+1} \tag{10}$$

holds for all large x and uniformly for all k satisfying (2). Indeed, in view of (8) and (9) this inequality is implied by

$$3k(k+1)(\log x)^2 \leqslant x^{1/(3k)}.$$

Since k satisfies (2), it follows that $3k(k+1) \leqslant (\log x)^2$ for all large x, and hence it suffices to observe that the inequality $(\log x)^4 \leqslant x^{1/(3k)}$ is equivalent to (2).

For every $a \in \mathcal{A}$, let

$$\mathcal{P}_a = \{p \in \mathcal{P} \ : \ a_p = a\}.$$

For an arbitrary subset $\mathcal{S}$ of $\mathcal{P}$ satisfying the properties

(i) $|\mathcal{S}| = k$,

(ii) $\mathcal{S} \subset \mathcal{P}_a$ for some $a \in \mathcal{A}$,

we put

$$n_{\mathcal{S}} = \prod_{p \in \mathcal{S}} p.$$

Then $n_{\mathcal{S}}$ is a squarefree k-almost prime, and the totient $\phi(n_{\mathcal{S}})$ is a k-th power since

$$\phi(n_{\mathcal{S}}) = \prod_{p \in \mathcal{S}} (p-1) = \prod_{p \in \mathcal{S}} (a q_p^k) = \Big(a \prod_{p \in \mathcal{S}} q_p\Big)^k.$$

Moreover, the k-th powers constructed in this way are pairwise distinct as $\mathcal{S}$ varies over the subsets of $\mathcal{P}$ satisfying (i) and (ii) since the set $\mathcal{S}$ is uniquely determined by the number $m = \phi(n_{\mathcal{S}})^{1/k}$. Indeed, the number a is the largest divisor of m that is coprime to every element of $\mathcal{Q}$, and after factoring $m = aq_1 \cdots q_k$, one recovers the set $\mathcal{S} = \{p_j = aq_j^k + 1 \ : \ j = 1, \ldots, k\}$.

Put $X = x^k$. Since $\phi(n_\mathcal{S}) \leqslant n_\mathcal{S} \leqslant X$ for every subset $\mathcal{S} \subset \mathcal{P}$ satisfying (i) and (ii), we see that $\mathcal{F}_k(X)$ is bounded below by the number of such subsets $\mathcal{S}$; therefore,

$$\mathcal{F}_k(X) \geqslant \sum_{a \in \mathcal{A}} \binom{|\mathcal{P}_a|}{k} = \sum_{a \in \mathcal{A}_0} \binom{|\mathcal{P}_a|}{k}, \tag{11}$$

where $\mathcal{A}_0$ denotes the set of $a \in \mathcal{A}$ such that $|\mathcal{P}_a| \geqslant k$. Note that $|\mathcal{A}_0|$ is nonempty for all large X, for if $\mathcal{A}_0 = \varnothing$ it follows that $|\mathcal{P}| \leqslant k|\mathcal{A}|$, which is untenable in view of (10).

Now, for fixed $k \geqslant 2$ the function

$$f_k(y) = \binom{y}{k} = \frac{y(y-1)\cdots(y-k+1)}{k!}$$

is convex as a function of $y \geqslant k$, and hence using (11) together with Jensen's inequality, we have

$$\begin{aligned} \frac{1}{|\mathcal{A}_0|}\mathcal{F}_k(X) &\geqslant \frac{1}{|\mathcal{A}_0|} \sum_{a \in \mathcal{A}_0} f_k(|\mathcal{P}_a|) \geqslant f_k\left(\frac{1}{|\mathcal{A}_0|} \sum_{a \in \mathcal{A}_0} |\mathcal{P}_a|\right) \\ &\geqslant f_k\left(\frac{1}{|\mathcal{A}_0|} \sum_{a \in \mathcal{A}} |\mathcal{P}_a| - k\left(\frac{|\mathcal{A}| - |\mathcal{A}_0|}{|\mathcal{A}_0|}\right)\right) = f_k\left(\frac{|\mathcal{P}| - k|\mathcal{A}|}{|\mathcal{A}_0|} + k\right). \end{aligned}$$

Since

$$f_k(y) = \frac{y(y-1)\cdots(y-k+1)}{k!} > \left(\frac{y-k}{k}\right)^k \qquad (y \geqslant k \geqslant 2),$$

it follows that

$$\begin{aligned} \mathcal{F}_k(X) \geqslant |\mathcal{A}_0| \left(\frac{|\mathcal{P}| - k|\mathcal{A}|}{k|\mathcal{A}_0|}\right)^k &= \frac{|\mathcal{P}|^k}{k^k |\mathcal{A}_0|^{k-1}} \left(1 - \frac{k|\mathcal{A}|}{|\mathcal{P}|}\right)^k \\ &\geqslant \frac{|\mathcal{P}|^k}{k^k |\mathcal{A}|^{k-1}} \left(1 - \frac{k|\mathcal{A}|}{|\mathcal{P}|}\right)^k. \end{aligned} \tag{12}$$

Taking into account (10) we see that

$$\left(1 - \frac{k|\mathcal{A}|}{|\mathcal{P}|}\right)^k \geqslant \left(1 - \frac{1}{k+1}\right)^k > e^{-1}.$$

Using this result in (12) along with (8) and (9) we derive that

$$\mathcal{F}_k(X) \geqslant \frac{x}{e(3k)^k (\log x)^{2k}} = \frac{X^{1/k}}{e(3/k)^k (\log X)^{2k}}\,.$$

Since $(3/2)^2 = 9/4$ and $(3/k)^k \leqslant 1$ for all $k \geqslant 3$, this proves the desired inequality for those $k \geqslant 2$ that satisfy (2). To finish the proof, we observe that for any integer k such that

$$2 \leqslant k \leqslant \sqrt{\frac{\log X}{12 \log\log X}}\,,$$

we clearly have

$$k^2 \leqslant \frac{\log X}{12 \log\log X} \leqslant \frac{k \log x}{12 \log\log x}\,.$$

Hence, (2) holds for any such k.

References

[1] W. R. Alford, A. Granville and C. Pomerance, 'There are infinitely many Carmichael numbers', *Ann. of Math. (2)* **139** (1994), no. 3, 703–722.

[2] W. D. Banks, 'Carmichael numbers with a square totient', *Canad. Math. Bull.* **52** (2009), no. 1, 3–8.

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

[4] D. R. Heath-Brown, 'The number of primes in a short interval', *J. reine angew. Math.* **389** (1988), 22–63.

[5] M. N. Huxley, On the difference between consecutive primes', *Invent. Math.* **15** (1972), 164–170.

[6] H. Iwaniec, 'Almost-primes represented by quadratic polynomials', *Invent. Math.* **47** (1978), no. 2, 171–188.

[7] H. L. Montogomery and R. C. Vaughan, 'The large sieve', *Mathematika* **20** (1973), 119–134.