#A53 INTEGERS 9 (2009), 611-716

SQUARES IN $(1^2 + m^2) \cdots (n^2 + m^2)$

Pak Tung Ho
Department of Mathematics, Purdue University, West Lafayette, IN
pho@math.purdue.edu

Received: 7/10/08, Revised: 2/11/09, Accepted: 9/11/09, Published: 12/23/09

Abstract

Recently, Cilleruelo proved that the product $\prod_{k=1}^{n}(k^2+1)$ is a square only for $n = 3$. In this note, using similar techniques, we prove that for the positive integer m whose divisors are of the form of $4q + 1$, the product $\prod_{k=1}^{n}(k^2 + m^2)$ is not a square for n sufficiently large. As a corollary, we prove that for $m = 5, 13, 17$, $\prod_{k=1}^{n}(k^2 + m^2)$ is not a square for all n.

1. Introduction

In [2], Cilleruelo proved that $\prod_{k=1}^{n}(k^2+1)$ is a square only for $n = 3$. In particular, he proved that $\prod_{k=1}^{n}(k^2 + 1)$ is not a square for n large enough. Using similar techniques, we prove the following result.

Theorem 1. *Let m be a positive integer such that its divisors are of the form of $4q + 1$ and $N = \max(m, 10^8)$. Then $P_m(n) = \prod_{k=1}^{n}(k^2 + m^2)$ is not a square for $n \geq N$.*

As corollaries, we prove the following results.

Corollary 2. $P_5(n) = \prod_{k=1}^{n}(k^2 + 5^2)$ *is not a square for all n.*

Corollary 3. $P_{13}(n) = \prod_{k=1}^{n}(k^2 + 13^2)$ *is not a square for all n.*

Corollary 4. $P_{17}(n) = \prod_{k=1}^{n}(k^2 + 17^2)$ *is not a square for all n.*

As an easy consequence, we deduce that for $m = 5, 13, 17$ the sequence

$$x_m(n) := \tan\left(\sum_{k=1}^{n} \arctan(k/m)\right) \tag{1}$$

does not vanish for all n. To see this, note that $\sum_{k=1}^{n} \arctan(k/m)$ is the argument of the Gaussian integer $\prod_{k=1}^{n}(m + k\sqrt{-1}) = r + s\sqrt{-1}$. Hence, if $x_m(n) = 0$, then $s = 0$ which implies that $P_m(n) = \prod_{k=1}^{n}(k^2+m^2) = r^2$. This contradicts Corollaries 2, 3 and 4. This result is similar to the main result of [1], which states that $x_1(n)$ does not vanish for $n \geq 4$.

2. Results

Proof of Theorem 1. Throughout the proof, p denotes a prime. If $P_m(n)$ were square, then $p|P_m(n)$ would imply that $p^2|P_m(n)$. If $p^2|P_m(n)$, then there are two possibilities both of which imply $p < 2n$:

- $p^2|k^2 + m^2$ for some $k \leq n$, which implies that $p \leq \sqrt{k^2+m^2} < 2n$ since $n \geq N \geq m$.
- $p|k^2 + m^2$ and $p|j^2 + m^2$ for some $j < k \leq n$. This implies that $p|(k^2 - j^2) = (k-j)(k+j)$, which infers that $p|k-j$ or $p|k+j$. This also gives $p < 2n$.

In either case, we have $p < 2n$. Therefore we can write

$$P_m(n) = \prod_{p<2n} p^{\alpha_p}.$$

Writing

$$n! = \prod_{p\leq n} p^{\beta_p},$$

the inequality $P_m(n) > (n!)^2$ yields

$$\sum_{p\leq n} \beta_p \log p < \sum_{p<2n} \frac{\alpha_p}{2} \log p. \tag{2}$$

Now we estimate α_p and β_p. Since all divisors of m are of the form of $4q+1$, m is odd. This implies that

$$k^2 + m^2 \equiv \begin{cases} 0 \pmod 2, & \text{if } k \equiv 1 \pmod 2; \\ 1 \pmod 2, & \text{if } k \equiv 0 \pmod 2. \end{cases}$$

Hence,

$$\alpha_2 \leq \lceil \frac{n}{2} \rceil,$$

It is well known that if an odd prime p divides k^2+m^2, then $p \equiv 1 \pmod 4$ when $(k,m) = 1$. Also, if $(k,m) \neq 1$, by our assumption that all divisors of m are of the form of $4q+1$, we also have $p \equiv 1 \pmod 4$. In this case, if $p \nmid m^2$, then each interval of length p^j contains two solutions of $x^2 + m^2 \equiv 0 \pmod{p^j}$; and if $p^j|m^2$, then each interval of length p^j contains at most one solution of $x^2 + m^2 \equiv 0 \pmod{p^j}$. It follows that

$$\alpha_p = \sum_{j\leq \frac{\log(n^2+m^2)}{\log p}} \#\{k \leq n : p^j|k^2+m^2\} \leq \sum_{j\leq \frac{\log(n^2+m^2)}{\log p}} 2\lceil \frac{n}{p^j} \rceil. \tag{3}$$

On the other hand,

$$\beta_p = \sum_{j \le \frac{\log n}{\log p}} \#\{k \le n : p^j | k\} = \sum_{j \le \frac{\log n}{\log p}} \lfloor \frac{n}{p^j} \rfloor. \tag{4}$$

Combining (3) and (4), we conclude that if $p \equiv 1 \pmod 4$, then

$$\begin{aligned} \frac{\alpha_p}{2} - \beta_p &\le \sum_{j \le \frac{\log(n^2+m^2)}{\log p}} \lceil \frac{n}{p^j} \rceil - \sum_{j \le \frac{\log n}{\log p}} \lfloor \frac{n}{p^j} \rfloor \\ &= \sum_{j \le \frac{\log n}{\log p}} \left(\lceil \frac{n}{p^j} \rceil - \lfloor \frac{n}{p^j} \rfloor \right) + \sum_{\frac{\log n}{\log p} < j \le \frac{\log(n^2+m^2)}{\log p}} \lceil \frac{n}{p^j} \rceil \\ &\le \sum_{j \le \frac{\log n}{\log p}} 1 + \sum_{\frac{\log n}{\log p} < j \le \frac{\log(n^2+m^2)}{\log p}} 1 \\ &= \frac{\log(n^2+m^2)}{\log p}. \end{aligned}$$

Substituting these into (2), we get

$$\begin{aligned} \sum_{p \le n} \beta_p \log p &< \sum_{p < 2n} \frac{\alpha_p}{2} \log p \\ &= \frac{\alpha_2}{2} \log 2 + \sum_{p \le n, p \equiv 1(4)} \frac{\alpha_p}{2} \log p + \sum_{n < p < 2n} \frac{\alpha_p}{2} \log p \\ &\le \frac{1}{2} \lceil \frac{n}{2} \rceil \log 2 + \sum_{p \le n, p \equiv 1(4)} \left(\beta_p + \frac{\log(n^2+m^2)}{\log p} \right) \log p \\ &\quad + \sum_{n < p < 2n} \frac{\alpha_p}{2} \log p, \end{aligned}$$

which implies that

$$\sum_{p \le n, p \equiv 3(4)} \beta_p \log p < \frac{n+1}{4} \log 2 + \log(n^2+m^2)\pi(n;1,4) + \sum_{n < p < 2n} \frac{\alpha_p}{2} \log p. \tag{5}$$

If $p > n$, then $\frac{n}{p^j} < 1$ for $j \ge 1$ and $\frac{\log(n^2+m^2)}{\log p} \le \frac{\log(2(p-1)^2)}{\log p} < 3$ since $m \le n$. Hence, from (3), $\alpha_p \le 4$. Moreover, if $p \le n$, by (4),

$$\beta_p \ge \frac{n}{p-1} - \frac{p}{p-1} - \frac{\log n}{\log p} \ge \frac{n-1}{p-1} - \frac{\log(n^2+m^2)}{\log p}.$$

We substitute it into (5) to get

$$\begin{aligned}\sum_{p\le n, p\equiv 3(4)} \frac{\log p}{p-1} &< \frac{(n+1)\log 2}{4(n-1)} + \frac{\log(n^2+m^2)}{n-1}\pi(n) + \frac{2}{n-1}\sum_{n<p<2n}\log p \\ &\le \frac{(n+1)\log 2}{4(n-1)} + \frac{\log(2n^2)}{n-1}\pi(n) + \frac{2}{n-1}\sum_{n<p<2n}\log p\end{aligned}$$

since $m \le N \le n$. Now we apply the Chebyshev inequalities $\sum_{n<p<2n}\log p \le n\log 4$ and $\pi(n) \le 2\log 4\frac{n}{\log n} + \sqrt{n}$ (see [3] for example) to obtain

$$\sum_{p\le n, p\equiv 3(4)} \frac{\log p}{p-1} < \frac{(n+1)\log 2}{4(n-1)} + \frac{\log(2n^2)}{n-1}\left(2\log 4\frac{n}{\log n} + \sqrt{n}\right) + \frac{2n\log 4}{n-1}.$$

This is a contradiction: The right hand side is less than 8.92 for $n \ge 10^8$. On the other hand, it can be checked that

$$\sum_{p\le n, p\equiv 3(4)} \frac{\log p}{p-1} > 8.92. \tag{6}$$

for $n \ge 10^8$. □

From the proof of Theorem 1, we can prove Corollaries 2, 3 and 4.

Proof of Corollary 2. It suffices to prove Corollary 2 for $1 \le n < 10^8$. It is clear that $P_5(1) = 26$ is not a square. For $n \ge 2$, since $5^2 + 2^2 = 29$, the next time that the prime 29 divides $k^2 + 5^2$ is for $29 - 2 = 27$. Hence $P_5(n)$ is not a square for $2 \le n \le 26$.

Since $26^2 + 5^2 = 701$, the next time that the prime 701 divides $k^2 + 5^2$ is for $701 - 26 = 675$. Hence $P_5(n)$ is not a square for $26 \le n \le 674$.

Since $672^2 + 5^2 = 451609$, the next time that the prime 451609 divides $k^2 + 5^2$ is for $451609 - 672 = 450937$. Hence $P_5(n)$ is not a square for $672 \le n \le 450936$.

Since $20016^2 + 5^2 = 400640281$, the next time that the prime 400640281 divides $k^2 + 5^2$ is for $400640281 - 20016 = 400620265$. Hence, $P_5(n)$ is not a square for $20016 \le n \le 400620264$. □

Proof of Corollary 3. It suffices to prove Corollary 3 for $1 \le n < 10^8$. It is clear that $P_{13}(1) = 170$ is not a square. For $n \ge 2$, since $13^2 + 2^2 = 173$, the next time that the prime 173 divides $k^2 + 13^2$ is for $173 - 2 = 171$. Hence $P_{13}(n)$ is not a square for $2 \le n \le 170$.

Since $168^2 + 13^2 = 28393$, the next time that the prime 28393 divides $k^2 + 13^2$ is for $28393 - 168 = 28225$. Hence $P_{13}(n)$ is not a square for $168 \le n \le 28224$.

Since $28218^2 + 13^2 = 796255693$, the next time that the prime 796255693 divides $k^2 + 13^2$ is for $796255693 - 28218 = 796227475$. Hence, $P_{13}(n)$ is not a square for $28218 \le n \le 796227474$. □

Proof of Corollary 4. It suffices to prove Corollary 4 for $1 \leq n < 10^8$. It is clear that $P_{17}(1) = 290$ is not a square. For $n \geq 2$, since $17^2 + 2^2 = 293$, the next time that the prime 293 divides $k^2 + 13^2$ is for $293 - 2 = 291$. Hence $P_{17}(n)$ is not a square for $2 \leq n \leq 290$.

Since $290^2 + 17^2 = 84389$, the next time that the prime 84389 divides $k^2 + 17^2$ is for $84389 - 290 = 84099$. Hence $P_{17}(n)$ is not a square for $290 \leq n \leq 84098$.

Since $20002^2 + 17^2 = 400080293$, the next time that the prime 400080293 divides $k^2 + 17^2$ is for $400080293 - 20002 = 400060291$. Hence, $P_{17}(n)$ is not a square for $20002 \leq n \leq 400060290$. □

We remark that by the same proof, one can check that $P_m(n)$ is not a square for all n for some small m. More generally, it would be interesting to find all the pairs (n, m), $n \geq 2$, $m \geq 1$ such that $\prod_{k=1}^{n}(k^2 + m)$ is a square. In view of Theorem 1, it seems that there are only finite number of such pairs. Based on extensive numerical evidence, we conjecture that the only ones are the pairs (3, 1), (3, 11), (4, 5). However, proving it seems to be a difficult problem. On the other hand, the sequence $x_m(n)$ defined in (1) satisfies the recurrence

$$x_m(n) = \frac{n + m x_m(n-1)}{m - n x_m(n-1)},$$

with the initial condition $x_m(0) = 0$. This sequence seems to have similar properties as $x_1(n)$. In particular it is an open question whether $x_1(n)$ is an integer for $n \geq 5$ (see Conjecture 1.2 in [1]). It is an interesting problem to decide whether $x_m(n)$ is an integer for $m > 1$.

Acknowledgement I would like to thank Professor Cilleruelo for answering my questions in his paper, and Stephen Kihwan Han for writing a program to check (6). I would also like to thank the referee whose constructive remarks have contributed to improving the presentation of the paper.

References

[1] T. Amdeberhan, L. Medina, V. Moll, Arithmetical properties of a sequence arising from an arctangent sum, *J. Number Theory*, **128** (2008), 1807-1846.

[2] J. Cilleruelo, Squares in $(1^2 + 1) \cdots (n^2 + 1)$, *J. Number Theory*, **128** (2008), 2488-2491.

[3] G. Hardy, E. Wright, An Introduction to the Theory of Numbers, Oxford Univ. Press, 1980.