# A NOTE ON PRODUCTS OF PRIMES THAT DIFFER BY A FIXED INTEGER

AMITABHA TRIPATHI

Abstract. Let $d$ be a fixed even integer. We characterize positive integers $n$ that are products of two primes that differ by $d$. These characterizations are in terms of Euler's $\phi$ function and the sum of divisors function $\sigma$, and generalize some known results in the case $d = 2$.

Prime numbers are indispensable in the study of Number Theory and Euclid's proof on the infinitude of primes is still considered a masterpiece. Twin primes are consecutive pairs of odd integers that are both prime numbers. Twin primes have attracted a lot of attention, especially since the enunciation of the *Twin Prime Conjecture* which asserts that there are infinitely many pairs $p$, $p+2$ such that both $p$ and $p+2$ are primes.

Arithmetical functions are functions defined on the set of positive integers. Two of the most studied arithmetical functions are Euler's function $\phi$, given by $\phi(n) := |\{a : 1 \leq a \leq n, \gcd(a,n) = 1\}|$, and the sum of divisors function $\sigma$, given by $\sigma(n) := \sum_{d|n} d$. For $n > 1$, it is easy to see that $\sigma(n) \geq n+1$ and that $\phi(n) \leq n-1$, with equality in either case precisely when $n$ is prime. Both these functions are *multipicative*, that is, each meets the condition $f(mn) = f(m)f(n)$ whenever $m$, $n$ are coprime positive integers.

The purpose of this article is to characterize $\phi(n)$ and $\sigma(n)$ for those $n$ that are products of primes that differ by a fixed even integer. The case when the difference is two was dealt with by Sergusov [2], who showed that $n$ is a product of twin primes is equivalent to each of the two statements $\sigma(n) = n + 1 + 2\sqrt{n+1}$, $\phi(n) = n + 1 - 2\sqrt{n+1}$, and by Leavitt and Mullin [1], who showed the equivalence to $\sigma(n)\phi(n) = (n+1)(n-3)$. It turns out that one of the equivalences due to Sergusov is not quite correct, viz., whereas whenever $n$ is a product of twin primes it is true that $\sigma(n) = n + 1 + 2\sqrt{n+1}$, the converse holds not only for those $n$ that are a product of twin primes but also for $n = 8$. We give a simpler proof of all these equivalences, adding the equivalent statement $\sigma(n) - \phi(n) = 4\sqrt{n+1}$ and correcting the result of Sergusov. Clearly, the equivalent conditions imply $\sigma(n) + \phi(n) = 2(n+1)$; we show conversely that $n$ is only a product of two distinct primes, not necessarily differing by two. We close this note by generalizing the results to the characterization of positive integers that are products of two primes that differ by a fixed even integer.

**Theorem 1.** *Consider the following statements:*

(1) $n = p(p+2)$, *where* $p$, $p+2$ *is a pair of twin primes;*
(2) $\sigma(n) = n + 1 + 2\sqrt{n+1}$;
(3) $\phi(n) = n + 1 - 2\sqrt{n+1}$;
(4) $\sigma(n) - \phi(n) = 4\sqrt{n+1}$;
(5) $\sigma(n)\phi(n) = (n+1)(n-3)$.

*Statements (1), (3), (4) and (5) are equivalent, and (1) implies (2) whereas (2) implies either (1) or* $n = 8$.

*Proof.* We first show that (1) implies each of the other four statements. Suppose $n = p(p+2)$, where $p$, $p+2$ are both prime.

(1) $\Rightarrow$ (2):
Since $n+1 = (p+1)^2$, $\sigma(n) = n+1+p+(p+2) = n+1+2(p+1) = n+1+2\sqrt{n+1}$.

(1) $\Rightarrow$ (3):
Again since $n+1 = (p+1)^2$, $\phi(n) = (p-1)(p+1) = (p+1)^2 - 2(p+1) = n+1-2\sqrt{n+1}$.

(1) $\Rightarrow$ (4) and (1) $\Rightarrow$ (5) directly follow from the first two implications. They are also easy to derive from the formulas $\sigma(n) = (p+1)(p+3)$ and $\phi(n) = (p-1)(p+1)$.

Conversely, we show that each of the last four statements imply the first, with the exception that the second statement also holds when $n = 8$.

(2) $\Rightarrow$ (1) or $n = 8$:
The assumption implies $n$ is composite. Since $2\sqrt{n+1}$ is a positive integer, we may write $4(n+1) = b^2$, so that $b$ must be even. With $b = 2a$, we have $n = (a+1)(a-1)$. Since $a = 2$ implies $n = 3$, it follows that $n$ has *at least* the distinct factors $n, a+1, a-1, 1$, whose sum is $n+1+2a = n+1+2\sqrt{n+1} = \sigma(n)$. Thus $n$ has exactly the four factors listed above, so that either the factors $a \pm 1$ of $n$ are both *primes* or $n = p^3$ for some prime $p$ and $a+1 = (a-1)^2 = p^2$. The latter case leads to $a = 3$ and $n = 8$.

(3) $\Rightarrow$ (1):
The assumption rules out the cases $n = 1, 2, 3$. So $\phi(n)$ must be *even*, and $n$ *odd*. Again with $n+1 = a^2$, $n = (a+1)(a-1)$ is a product of consecutive *odd* integers. Since these factors must be coprime, $a(a-2) = n+1-2\sqrt{n+1} = \phi(n) = \phi(a+1)\phi(a-1)$ and $a > 2$. Since $\phi(m) \leq m-1$ with equality if and only if $m$ is *prime*, it follows that each of the factors $a \pm 1$ of $n$ is prime.

(4) $\Rightarrow$ (1):
The assumption rules out the cases $n = 2, 4$. If $n$ is even, then $n$ has $1, 2, \frac{n}{2}, n$ as factors and none of the even positive integers less than $n$ are coprime to $n$. Therefore $\sigma(n) \geq \frac{3}{2}n+3$ while $\phi(n) \leq \frac{n}{2}$. The assumption now implies $4\sqrt{n+1} \geq n+3$ which is possible only for $n \leq 10$. Since none of these values satisfy the assumption, we may assume that $n$ is odd. Again with $n+1 = a^2$, $n = (a+1)(a-1)$ is a product of consecutive odd integers, so that $a+1$ and $a-1$ must be coprime. Now $4a = \sigma(n) - \phi(n) = \sigma(a+1)\sigma(a-1) - \phi(a+1)\phi(a-1) \geq (a+2)a - a(a-2) = 4a$. It follows that $\sigma(a+1) = a+2$, $\sigma(a-1) = a$, $\phi(a+1) = a$ and $\phi(a-1) = a-2$, so that $a \pm 1$ are both primes in this case.

(5) $\Rightarrow$ (1):
Suppose $\sigma(n)\phi(n) = (n+1)(n-3)$. Then $n \geq 4$, and odd since $\phi(n)$ is even. The assumption rules out all values of $n$ less than 10, so we may assume that $n > 10$. If $p$ is a prime such that $p^2 \mid n$, then $p \mid \phi(n)$ and so $p = 3$. Thus $n$ is *squarefree* except possibly for the factor $3^2$. If $27 \mid n$, then $9 \mid \phi(n)$ whereas $9 \nmid (n+1)(n-3)$, leading to a contradiction. So, if $3^m \mid n$, then $m \leq 2$ and since $n > 10$, $n$ must have *at least* one prime factor greater than 3. Any

prime factor $p$ of $n$ distinct from 3 contributes $p^2-1$ to the factor $\sigma(p)\phi(p)$ of $\sigma(n)\phi(n)$. So if $9 \mid n$, then $9 \mid \sigma(n)\phi(n)$ but not $(n+1)(n-3) = n^2-2n-3$. It follows that $n$ is a product of distinct primes.

Write $n = \prod_{i=1}^{k} p_i$; then $\sigma(n)\phi(n) = \prod_{i=1}^{k} (p_i^2-1)$. Now $(a^2-1)(b^2-1) < (ab)^2-1$ if $a, b > 1$. If $k > 2$,

$$\sigma(n)\phi(n) \leq \left\{ \left(\prod_{i=1}^{k-1} p_i\right)^2 - 1 \right\} (p_k^2-1) \leq (ab)^2 - 2ab - 3,$$

with $a = \prod_{i=1}^{k-1} p_i$, $b = p_k$, and $|a-b| \geq 2$ since $a$ and $b$ are odd and distinct. Thus $k \leq 2$. If $n$ were prime, $\sigma(n)\phi(n) = n^2-1$. Finally, with $n = pq$, where $p, q$ are distinct primes, the equation $n^2-2n-3 = (p^2-1)(q^2-1)$ simplifies to $|p-q| = 2$. This completes the proof. □

From Theorem 1 it follows that $\sigma(n)+\phi(n) = 2(n+1)$ whenever $n$ is a product of twin primes. The converse, however, does not hold. In fact, the condition on the sum implies only that $n$ is a product of two distinct primes.

**Theorem 2.** *$n$ is a product of two distinct primes if and only if $\sigma(n)+\phi(n) = 2(n+1)$.*

*Proof.* If $n = pq$ is a product of distinct primes, then $\sigma(n)+\phi(n) = (p+1)(q+1)+(p-1)(q-1) = 2(pq+1) = 2(n+1)$. Conversely, suppose

$$2n+2 = \sigma(n)+\phi(n) = \sum_{d|n} d\left(1+\mu(\tfrac{n}{d})\right).$$

Since the term corresponding to $d = n$ contributes $2n$ to the sum, the contribution from the proper divisors of $n$ must be 2. Since each term is nonnegative and there cannot be two terms contributing 1 each, there is exactly one term equal to 2 (so $d = 1$ or 2) and all others equal 0 (so $\mu(\frac{n}{d}) = -1$). But $d = 2$ implies both $\mu(\frac{n}{2}) = 0$ and $\mu(n) = -1$, which is impossible. Thus $d = 1$ and $\mu(n) = 1$, so that $n$ must be a product of two prime factors. This completes the proof of our claim. □

It is interesting to note that the results of Theorem 1 can be extended to positive integers that are products of two primes differing by a fixed even integer $d$, although the proofs are a little more involved since these involve an arbitrary even integer. However, the generalization does not carry over to statement (5) of Theorem 1.

**Theorem 3.** *Consider the following statements:*

(1) $n = p(p+d)$, *where $p$, $p+d$ are odd primes;*
(2) $\sigma(n) = n+1+2\sqrt{n+(\frac{d}{2})^2}$ *for some $d \in 2\mathbb{N}$;*
(3) $\phi(n) = n+1-2\sqrt{n+(\frac{d}{2})^2}$ *for some $d \in 2\mathbb{N}$;*
(4) $\sigma(n)-\phi(n) = 4\sqrt{n+(\frac{d}{2})^2}$ *for some $d \in 2\mathbb{N}$.*

*Statements (1), (3) and (4) are equivalent, and (1) implies (2) whereas (2) implies either (1) or $n = p^3$ if $d = p(p-1)$ for some prime $p$ or $\sigma(n) = 2(n+1)$ if $d = n-1$ for some odd $n$.*

*Proof.* It is easy to verify that the first statement implies each of the other three. We prove each of the three implications (2) $\Rightarrow$ $\big[$(1) or $n = p^3$ if $d = p(p-1)$ for some prime $p$ or $\phi(n) = 2(n+1)$ if $d = n-1$ for some odd $n$ $\big]$, (3) $\Rightarrow$ (1) and (4) $\Rightarrow$ (1).

Throughout this proof, we write $a := \sqrt{n + (\frac{d}{2})^2}$. Then $n > 1$, and since $n = (a+\frac{d}{2})(a-\frac{d}{2})$ is a product of two integers of the same parity, $n \not\equiv 2 \pmod 4$. Moreover, $a - \frac{d}{2} = 1$ implies $2a = n + 1$ and $d = n - 1$. We use these observations in our proof.

(2) $\Rightarrow$ $\big[$ (1) or $n = p^3$ if $d = p(p-1)$ for some prime $p$ or $\sigma(n) = 2(n+1)$ if $d = n-1$ for some odd $n$ $\big]$:
If $a - \frac{d}{2} = 1$, (2) reduces to $\sigma(n) = n + 1 + 2a = 2(n+1)$ for some *odd* $n$ since $n = d + 1$. If $a - \frac{d}{2} > 1$, then $n$ has *exactly* the four distinct factors $n, a + \frac{d}{2}, a - \frac{d}{2}, 1$. Hence, either the factors $a \pm \frac{d}{2}$ of $n$ are both *primes* or $n = p^3$ for some prime $p$ and $a + \frac{d}{2} = (a - \frac{d}{2})^2 = p^2$. In the first case, $n$ is a product of two primes that differ by $d$. In the second case, we have $a(d + 1 - a) = \frac{d}{2}(\frac{d}{2} - 1)$. Since $a > \frac{d}{2}$ and $a(d + 1 - a) \geq 0$, we may write $a = \frac{d}{2} + t$ with $1 \leq t \leq \frac{d}{2} + 1$. Substituting in $a(d+1-a) = \frac{d}{2}(\frac{d}{2} - 1)$ gives $d = t(t-1)$, $a = \frac{d}{2} + t = \frac{1}{2}t(t+1)$ and $p = a - \frac{d}{2} = t$. So in the second case we have $n = p^3$ if $d = p(p-1)$ for some prime $p$.

(3) $\Rightarrow$ (1):
The assumption implies that $\phi(n)$ is *even* and $n$ is *odd*, and rules out the case $a - \frac{d}{2} = 1$. Rewrite (3) as

$$\big(a - 1 + \tfrac{d}{2}\big)\big(a - 1 - \tfrac{d}{2}\big) = n + 1 - 2\sqrt{n + (\tfrac{d}{2})^2} = \phi(n) = \phi\big((a + \tfrac{d}{2})(a - \tfrac{d}{2})\big).$$

Any prime $p$ dividing both $a + \frac{d}{2}$ and $a - \frac{d}{2}$ must also divide $\phi(n)$ (since $p^2 \mid n$) but divide neither $a - 1 + \frac{d}{2}$ nor $a - 1 - \frac{d}{2}$. Therefore $\gcd(a + \frac{d}{2}, a - \frac{d}{2}) = 1$, and we have $(a - 1 + \frac{d}{2})(a - 1 - \frac{d}{2}) = \phi(a + \frac{d}{2})\phi(a - \frac{d}{2})$. This is possible only if $\phi(a + \frac{d}{2}) = a + \frac{d}{2} - 1$ and $\phi(a - \frac{d}{2}) = a - \frac{d}{2} - 1$, so that each of the factors $a \pm \frac{d}{2}$ of $n$ is prime.

(4) $\Rightarrow$ (1):
If $\gcd(a + \frac{d}{2}, a - \frac{d}{2}) = 1$, then

$$\begin{aligned} 4a &= \sigma(n) - \phi(n) = \sigma(a + \tfrac{d}{2})\sigma(a - \tfrac{d}{2}) - \phi(a + \tfrac{d}{2})\phi(a - \tfrac{d}{2}) \\ &\geq (a + \tfrac{d}{2} + 1)(a - \tfrac{d}{2} + 1) - (a + \tfrac{d}{2} - 1)(a - \tfrac{d}{2} - 1) = 4a. \end{aligned}$$

This implies $\sigma(a \pm \frac{d}{2}) = a \pm \frac{d}{2} + 1$ and $\phi(a \pm \frac{d}{2}) = a \pm \frac{d}{2} - 1$, and so $a \pm \frac{d}{2}$ are both primes. In particular, this proves the implication when $a - \frac{d}{2} = 1$ and so we may henceforth assume that $a - \frac{d}{2} > 1$.

Suppose first that $n = p^m$ for some prime $p$; clearly, $m > 1$ since $\sigma(p) - \phi(p) = 2$. If $p = 2$ or $p \mid \frac{d}{2}$, then since $p \mid \phi(n)$, we have the contradiction $p \mid \sigma(p^m) = 1 + p + p^2 + \cdots + p^m$. Hence, $p$ must be odd and $p \nmid \frac{d}{2}$. Let $p^m + (\frac{d}{2})^2 = a^2$ for some integer $a$, $p \nmid a$. Then $p^m = (a + \frac{d}{2})(a - \frac{d}{2})$, so that $a + \frac{d}{2} = p^r$, $a - \frac{d}{2} = p^s$ for some $r > s > 0$ with $r + s = m$, and $a = \frac{1}{2}(p^r + p^s)$. But now the equation $\sigma(p^m) - \phi(p^m) = 4a = 2(p^r + p^s)$ is impossible since $p$ does not divide the left hand side but divides the right hand side. So we may suppose that $n$ has *at least* two distinct prime factors.

If $n$ has more than two prime factors and if $p, q$ are the two smallest prime factors of $n$, with $p < q$, then $\sigma(n) > n + \frac{n}{p} + \frac{n}{q} + p + q$ and $\phi(n) < n\big(1 - \frac{1}{p}\big)\big(1 - \frac{1}{q}\big) = n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq}$. Moreover, $a \leq \frac{1}{2}\big(\frac{n}{p} + p\big)$ since $a - \frac{d}{2} > 1$ and $2a = x + y$ with $xy = n$, $x \geq y > 1$ is maximum at $x = \frac{n}{p}$, $y = p$. But this leads to the contradiction $2\left(\frac{n}{p}+p\right) \geq 4a = \sigma(n)-\phi(n) > 2\left(\frac{n}{p}+p\right)$. Hence $n$ has *exactly* two distinct prime factors.

Assume that $n$ has only the prime factors $p$ and $q$, with $p < q$. If $p = 2$, then $4 \mid n$ since $n \not\equiv 2 \pmod 4$. Since we may further assume that $n > 8$, it follows that $\sigma(n) \geq n + \frac{n}{2} + \frac{n}{4} + 2 + 1 = \frac{7}{4}n + 3$ and $\phi(n) < \frac{1}{2}n$. But then $\sigma(n) - \phi(n) \geq \frac{5}{4}n + 3$, leading to the contradiction $n + 4 = 2\left(\frac{n}{2} + 2\right) \geq 4a = \sigma(n) - \phi(n) \geq \frac{5}{4}n + 3$ since $n > 8$. Hence $n$ must be odd. If $n > pq$, then $\sigma(n) > n + \frac{n}{p} + \frac{n}{q} + \frac{n}{pq}$ and $\phi(n) = n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq}$, and we again have the contradiction $2\left(\frac{n}{p} + p\right) \geq 4a = \sigma(n) - \phi(n) > 2\left(\frac{n}{p} + p\right)$. Therefore $n$ must be a product of two primes that differ by $d$, proving this implication and completing the proof of the theorem. $\square$

We close this note with a remark and two open problems. Theorem 3 implies that $\sigma(n)\phi(n) = (n-1+d)(n-1-d)$ always admits the solution $n = p(p+d)$, where $p, p+d$ are odd primes. However, there are infinitely many $d$ which admit other solutions. Those $d$ that do not admit any other solutions have been termed $\star$-numbers by Leavitt and Mullin in [1], and Theorem 1 shows that $d = 2$ is a $\star$-number. In [1] it has been shown that there are infinitely many non $\star$-numbers.

The last implication of statement (2) in Theorem 3 asks for an *odd* integer $n$ for which $\sigma(n) = 2n + 2$. Sloane's *The On-Line Encyclopedia of Integer Sequences* [3] lists only the following *nine* solutions to the equation $\sigma(n) = 2n + 2$:

$$n = 20, 104, 464, 650, 1952, 130304, 522752, 8382464, 134193152.$$

In fact, all these solutions are derived from the following observation of Firoozbakht [3].

**Observation 1.** *Let $k \geq 0$. If $2^e - (2k+1)$ is prime, then $n = 2^{e-1}\left\{2^e - (2k+1)\right\}$ satisfies the equation $\sigma(n) = 2(n+k)$.*

It is well-known that in the case $k = 0$ all even solutions are given by integers of the form given in the observation, but it is not known if this also holds for any other $k > 0$. Moreover, the existence or non existence of odd $n$ that satisfy $\sigma(n) = 2(n+k)$ for any $k \geq 0$ also appears to be unknown. Based on available data, we list these as open problems.

**Open Problem 1.** *Let $k \geq 0$. If $\sigma(n) = 2(n+k)$, then $n$ must be even.*

**Open Problem 2.** *Let $k \geq 1$. If $\sigma(n) = 2(n+k)$ and $n$ is even, then $n$ must be of the form $2^{e-1}\left\{2^e - (2k+1)\right\}$, where $2^e - (2k+1)$ is prime.*

The truth of Open Problem 1 would imply that if $\sigma(n) = n + 1 + 2\sqrt{n + (\frac{d}{2})^2}$ for some even $d$, then either $n$ is a product of two primes that differ by $d$ or $n = p^3$ for some prime $p$ if $d = p(p-1)$. Note that this is in agreement with the inference in Theorem 1 when $d = 2$.

## 1. Acknowledgement

The author wishes to thank the referee for pointing out numerous errors and making significant suggestions in an earlier version of this paper, all of which have contributed to a major improvement in the presentation of this work.

## References

[1] W. G. Leavitt and A. A. Mullin, *Primes differing by a fixed integer*, Math. Comp., **37** (1981), 581–585.
[2] I. S. A. Sergusov, *On the problem of prime-twins* (in Russian), Jaroslav. Gos. Ped. Inst. Učen. Zap. Vyp., **82** (1971), 85–86.
[3] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`, Entry *A*088831.

MSC2010: 11A05, 11A25

Department of Mathematics, Indian Institute of Technology, Hauz Khas, New Delhi – 110016, India
*E-mail address*: atripath@maths.iitd.ac.in