MATHEMATICS OF COMPUTATION
VOLUME 37, NUMBER 156
OCTOBER, 1981

Primes Differing by a Fixed Integer

By W. G. Leavitt and Albert A. Mullin

Abstract. It is shown that the equation $(*)$ $(n-1)^2 - \sigma(n)\phi(n) = m^2$ is always solvable by $n = p_1 p_2$ where p_1, p_2 are primes differing by the integer m. This is called the "Standard" solution of $(*)$ and an m for which this is the only solution is called a "*-number". While there are an infinite number of non *-numbers there are many (almost certainly infinitely many) *-numbers, including $m = 2$ (the twin prime case). A procedure for calculating all non *-numbers less than a given bound L is devised and a table is given for $L = 1000$.

The prime numbers p_1, p_2 are said to form a pair of "twin primes" if $p_1 - p_2 = 2$. Using $\sigma(n)$, the sum of the divisors of n (including n itself), and $\phi(n)$, the number of numbers less than n and relatively prime to n, S. A. Sergusov [1] has recently announced two criteria for an integer to be the product of twin primes. They are: n is the product of twin primes if and only if either $\sigma(n) = n + 1 + 2\sqrt{n+1}$ or $\phi(n) = n + 1 - 2\sqrt{n+1}$. Combining these two results gives the sufficiency for:

THEOREM 1. *The integer n is the product of twin primes if and only if*

$$(n-1)^2 - \sigma(n)\phi(n) = 4. \tag{1}$$

Proof of the Necessity. For primes $p_1 < p_2 < \cdots < p_k$, suppose (1) is satisfied when $n = \prod_1^k p_i^{n_i}$. Then (1) can be written

$$2\prod_1^k p_i^{n_i} + 3 = \prod_1^k p_i^{2n_i} - \prod_1^k \left(p_i^{2n_i} - p_i^{n_i - 1}\right). \tag{2}$$

Since (2) would reduce for $k = 1$ to $2p^n + 3 = p^{n-1}$, it is clear that $k \geqslant 2$. Then note that if $p_1 = 2$, the left side of (2) is odd whereas the right side is even, and so $p_1 \geqslant 3$. Also from (2) it follows that if $p_1 = 3$, then $n_1 = 2$ or 1, and in all other cases $n_i = 1$.

Now if $k \geqslant 3$, it is easy to show that the right-hand side of (2) is greater than $p_3\prod_1^k p_i^{n_i}$ and so exceeds the left-hand side, and if $k = 2$ with $p_1 = 3$ and $n_1 = 2$, the right side is $3p_2^2 + 78$ which again is always greater than the left-hand side.

In the only remaining case $k = 2$ and $n_1 = n_2 = 1$, so (2) reduces to $2p_1p_2 + 3 = p_1^2 + p_2^2 - 1$, that is $(p_1 - p_2)^2 = 4$, and we conclude that $n = p_1p_2$ with $p_1 - p_2 = 2$.

We now generalize (1) to

$$(n-1)^2 - \sigma(n)\phi(n) = m^2 \tag{$*$}$$

for any integer m. It is easy to check that

THEOREM 2. *If $n = p_1p_2$ with p_1, p_2 primes such that $p_1 - p_2 = m$, then n satisfies* $(*)$.

Received December 4, 1980.
1980 *Mathematics Subject Classification.* Primary 10B99; Secondary 10A99.

0025-5718/81/0000-0173/$02.25

We will call the n of Theorem 2 the *standard* solution of $(*)$, and we will say that m is a $*$-*number* if $(*)$ has only the standard solution, that is if $(*)$ characterizes those n which are products of two primes differing by the fixed integer m. Thus Theorem 1 states that 2 is a $*$-number.

THEOREM 3. *For a given prime p, if $2p - 1$ is also prime, then $n = p^k(2p - 1)$ satisfies $(*)$ for $m = p^k - 1$, so $m = p^k - 1$ is not a $*$-number for all $k \geqslant 2$. Similarly $(*)$ has a solution $n = p^k(2p + 1)$ for $m = p^k + 1$ whenever p and $2p + 1$ are prime.*

Proof. If $2p \pm 1$ is prime, then for $n = p^k(2p \pm 1)$ the left-hand side of $(*)$ becomes

$$(p^k(2p \pm 1) - 1)^2 - (p^{2k} - p^{k-1})(4p^2 \pm 4p) = (p^k \pm 1)^2.$$

COROLLARY. *There are an infinite number of odd non $*$-numbers and an infinite number of even non $*$-numbers.*

Proof. This is clear since we have as non $*$-numbers $2^k - 1$ and $2^k + 1$, and also $3^k - 1$ and $3^k + 1$ for all $k \geqslant 2$. Note: There are many other sequences of non $*$-numbers such as $7^k - 1$ or $11^k + 1$. Also note that except for 2 and 3 it is impossible for both $2p - 1$ and $2p + 1$ to be prime.

For primes $p_1 < p_2 < \cdots < p_k$ let

$$f = \left(\prod_1^k p_i^{n_i} - 1\right)^2 - \prod_1^k (p_i^{2n_i} - p_i^{n_i - 1}), \tag{3}$$

so that $n = \prod_1^k p_i^{n_i}$ is a solution of $(*)$ if and only if $\sqrt{f} = m$ is an integer.

The next two propositions gave some limitations on the type of solutions that $(*)$ may have.

PROPOSITION 1. *If p is a prime such that $p \nmid m$ then the Mersenne number $M_p = 2^p - 1$ is not a solution of $(*)$.*

Proof. Let $n = M_p$ be a solution of $(*)$. For a prime $q \mid M_p$, we have $2^p \equiv 1 \pmod{q}$ so $q \equiv 1 \pmod{p}$. But then any $q^{2r} - q^{r-1} \equiv 0 \pmod{p}$ and also $M_p - 1 \equiv 0 \pmod{p}$. Thus from (3) we have the contradiction $p^2 \mid f$.

PROPOSITION 2. *If $p < q$ are primes, then $n = pq^r$ is not a solution of $(*)$ for any $r \geqslant 2$ and any m.*

Proof. If $n = pq^r$ is a solution of $(*)$, then since $r \geqslant 2$ we have $(q, m) = 1$. Thus we can write $m = q^t h \pm \alpha$ for either $h = 0$ or $(h, q) = 1$ with some $t < 1$, and some $0 < \alpha \leqslant (q - 1)/2$. Thus $\alpha^2 \equiv 1 \pmod{q}$, so $\alpha^2 = 1$ and (3) becomes

$$q^{2r} - 2pq^r + (p^2 - 1)q^{r-1} = q^t h(q^t h \pm 2). \tag{4}$$

Case 1. $p = 2$, $q = 3$. Then, since $p^2 - 1 = 3$, it follows from (4) that $t = r + 1$. Thus (4) reduces to

$$3^{r+1}h^2 \pm 2h - 3^{r-1} + 1 = 0.$$

But the left side of this equation is positive for all $h \geqslant 1$ and is nonzero for $h = 0$. Thus no integral value of h satisfies (4), so m an integer is impossible.

Case 2. In all other cases, since $q > p$, we have $q \nmid (p^2 - 1)$ and so $t = r - 1$. Thus (4) becomes

$$q^{r-1}h^2 \pm 2h - q^{r+1} + 2pq + 1 - p^2 = 0.$$

Writing the left side of this equation $F(h)$ we have, $F(0) \neq 0$, and clearly $F(h)$ is an increasing function for all $h \geqslant 1$. Since $q > p$, it is evident that $F(q) > 0$. But also

$$\begin{aligned} F(q-1) &\leqslant q^{r-1}(q-1)^2 + 2(q-1) - q^{r+1} + 2pq + 1 - p^2 \\ &\leqslant q^{r-1}(3 - 2q) + p(2q - p) - 1 \\ &< q^{r-1}(3 - 2q + 2q - p) - 1 = q^{r-1}(3 - p) - 1 < 0. \end{aligned}$$

Thus $F(h)$ has no integral zeros, so again m an integer is impossible.

Remark. The method of Theorem 1 can be used to show that, for certain values of m, (*) has only the standard solution, so that m is a *-number. However, with increasing m the method rapidly becomes more complicated and must in any case be done one m at a time. The following propositions yield a much simpler method, namely that for any chosen limit L there is a systematic procedure by which all nonstandard solutions of (*) can be calculated for all $m \leqslant L$. Eliminating all such m then leaves those *-numbers that are $\leqslant L$.

The following are clear from (3).

PROPOSITION 3. *If $k = 1$, then $f < 0$ so (*) is impossible.*

PROPOSITION 4. *If $k \geqslant 2$, then f is odd if and only if n is even.*

PROPOSITION 5. *In all cases f is an increasing function of n_j for all j.*

Proof. We take the partial of f with respect to n_j and check directly in the case $j = 1$, $k = 2$, $n_2 = 1$ that the partial derivative is greater than $p_1^{n_1-1}\log p_1(p_1 - p_2)^2$. In all other cases we examine the effect on the partial of replacing $p_i^{2n_i} - p_i^{n_i-1}$ by $p_i^{2n_i}$ for all $i \geqslant 2$ and (when $j \geqslant 2$) replacing $2p_j^{2n_j} - p_j^{n_j-1}$ by $2p_j^{2n_j}$. It is then immediately clear that in all cases the partial derivative is positive.

PROPOSITION 6. *In the case $k = 2$ and $n_1 = 1$, f is a decreasing function of p_1 but is an increasing function of p_2. In all other cases f is an increasing function of p_j for all j.*

Proof. When $k = 2$ and $n_1 = 1$, we find that the partial derivative $f_{p_1} = 2p_2^{n_2-1}(p_1 - p_2) < 0$. To show that all other partials are positive we examine (for the cases $k \geqslant 3$ or $k = 2$ and $j \geqslant 2$) the effect of replacing in f_{p_j} the term $2n_jp_j^{2n_j-1} - (n_j - 1)p_j^{n_j-2}$ by $2n_jp_j^{2n_j-1}$ and replacing $p_i^{2n_i} - p_i^{n-1}$ by $p_i^{2n_i}$ for all $i \geqslant 2$ when $j \geqslant 2$, and for all $i \geqslant 3$ when $j = 1$ and $k \geqslant 3$. Finally in the case $k = 2$, $n_1 \geqslant 2$ we show directly that

$$f_{p_1} \geqslant p_1^{n_1-2}p_2^{n_2-1}\left[4p_1^3 + p_2^2 - 4p_1p_2\right] > p_1^{n_1-2}p_2^{n_2-1}(2p_1 - p_2)^2.$$

PROPOSITION 7. *f increases with k in the sense that if p is a prime not dividing a then $f(ap^h) > f(a)$ for all $h \geqslant 1$.*

Proof. Let $b = \sigma(a)\phi(a)$. Then

$$f(ap^h) = (ap^h - 1)^2 - b(p^{2h} - p^{h-1}) > p^{2h}f(a).$$

The Computations. In calculating nonstandard solutions $n = \prod^k p_i^{n_i}$ of $(*)$ it follows from Propositions 3 and 4 that $k \geqslant 2$ and if $k = 2$ we do not need to consider the case $n_1 = 1$. Therefore from Propositions 5–7, we can regard f as always an increasing function in all variables. Thus, for any upper limit L, there is clearly a systematic way of calculating for all $\sqrt{f} \leqslant L$, namely for each increasing k (starting with $k = 2$) and each increasing choice of the n_i (starting with $n_1 = 2$ and $n_2 = 1$) we calculate for all $p_1 < p_2 < \cdots < p_k$ in each case up until $\sqrt{f} > L$, recording all those n in which $m = \sqrt{f}$ is an integer.

Note that in the following table we have separated the solutions for odd and even m since the odd m appear to have somewhat different properties. In fact, to say m is an odd *-number is simply to say that $m + 2$ is prime and $(*)$ has the sole solution $n = 2(m + 2)$ or that $(*)$ has no solutions at all.

The following is the set of all nonstandard solutions of $(*)$ for $m \leqslant 1000$. Note that the solutions marked # are those guaranteed by Theorem 3.

ODD

m	n	m	n	m	n	m	n
3	$2^2.3$ #	37	$2^2.3^3$	163	$2^3.3^4$	511	$2^9.3$ #
5	$2^2.5$ #	49	$2^3.5^2$	179	$2.3^2.19$	513	$2^9.5$ #
7	$2^3.3$ #	55	$2^3.3^3$	185	$2^3.3.19$	577	$2.3^2.61$
9	$2^3.5$ #	61	$2^2.3.11$	249	$2^3.5^3$	639	$2.5.11^2$
13	$2^2.11$	63	$2^6.3$ #	255	$2^8.3$ #	739	$2^2.3.131$
15	$2^4.3$ #	65	$2^6.5$ #	257	$2^8.5$ #	813	$2.7.113$
17	$2^4.5$ #	99	$2.5.19$	303	$2^4.109$	877	$2.13.67$
19	$2^3.3^2$	127	$2^7.3$ #	321	$2.5.61$	897	$2^7.113$
23	$2^3.13$	129	$2^7.5$ #	357	$2^2.13.19$	921	$2^3.5.73$
23	$2.3.7$	145	$2^4.53$	413	$2^2.3^2.29$	955	$2^2.3^2.67$
31	$2^5.3$ #	157	$2^2.113$	437	$2^2.311$	993	$2^5.7.23$
33	$2^5.5$ #	159	$2^5.41$	487	$2^3.3^5$		

Note. The only values of $m \leqslant 5000$ for which $(*)$ has a solution with $k = 4$ are:

m	n
1744	3.5.7.41
3216	5.11.13.19
4516	3.5.19.41

EVEN

m	n	m	n	m	n	m	n
8	$3^2.5$ #	172	$3^2.7.11$	414	$5^2.7.13$	694	$3.5.11^2$
10	$3^2.7$ #	176	3.5.31	432	7.17.23	708	7.23.29
26	$5^2.11$ #	226	$5^3.43$	438	$19^2.79$	728	$3^6.5$ #
26	$3^3.5$ #	228	7.11.17	440	$3^2.257$	730	$3^6.7$ #
28	$3^3.7$ #	230	$11^2.71$	440	$7^3.47$	732	$17^2.181$
40	3.5.7	240	5.13.17	450	5.7.53	744	13.19.31
46	$5^2.23$	242	$3^4.47$	456	5.19.23	760	3.7.101
48	$7^2.13$ #	242	$3^5.5$ #	472	$11^2.149$	762	11.17.37
62	$7^2.23$	244	$3^5.7$ #	476	$5^3.97$	796	3.5.139
78	$7^2.31$	246	5.7.29	510	$7^2.199$	804	5.11.67
80	$3^4.5$ #	258	$7^2.103$	516	5.11.43	824	$11^2.257$
82	$3^3.29$	288	7.13.19	530	$23^2.47$ #	842	$29^2.59$ #
82	$3^4.7$ #	296	$5^2.137$	530	$3^2.5.43$	844	5.19.43
96	5.7.11	320	$11^2.101$	540	$7^3.67$	870	$11^2.271$
118	$3^2.71$	328	3.17.19	620	$3^3.11.13$	904	3.29.31
122	$11^2.23$ #	342	$7^2.11^2$	626	$5^4.11$ #	926	$5^2.419$
126	$5^3.11$ #	342	$7^3.13$ #	648	13.17.29	926	$3^2.5^2.19$
142	3.7.19	354	$5^2.163$	660	11.19.29	932	$7^3.131$
144	$11^2.37$	358	$17^2.71$	662	$13^2.191$	960	$31^2.61$ #
148	3.11.13	360	$19^2.37$ #	690	$13^2.199$	990	$23^2.199$
166	$11^2.47$	408	11.13.23	692	7.13.47	1000	$3^3.7.29$

Department of Mathematics and Statistics
University of Nebraska
Lincoln, Nebraska 68488

475-B Cook Drive
Redstone Arsenal, Alabama 35808

1. S. A. SERGUSOV, "On the problem of prime-twins," *Jaroslav. Gos. Ped. Inst. Učen. Zap.* Vyp. 82, *Anal. i Algebra*, 1971, pp. 85–86. (Russian)