PRIMALITY CRITERIA FOR PAIRS $\mathbf{n}$ AND $\mathbf{n+d}$

Flavio Torasso

Abstract. The existence of primality criteria for generic pairs n and $n+d$ is investigated. A congruence $\pmod{n(n+d)}$ is found, that holds if and only if $(n, n+d)$ is a prime pair, except for a finite number of exceptions that appear when n is lower than a fixed quantity only depending on d. Explicit primality criteria for $d = 2, 4, 6, 8, 10, 12$ are given and a formula predicting the number of exceptions is conjectured.

In 1949 using Wilson's theorem (n is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$), Clement [1] proved that p and $p+2$ are twin primes if and only if $4[(p-1)!+1]+p \equiv 0 \pmod{p(p+2)}$.

In 1995 Dence and Dence [2] improved Clement's result and proved that p and $p+2$ are twin primes if and only if $2[(p-1)/2]!^2 \equiv \pm(5p+2) \pmod{p(p+2)}$, the sign being "+" when $p = 4k-1$, "−" when $p = 4k+1$.

This kind of result is not restricted to only twin primes, although the cited papers focused on this topic. Dence and Dence [2] noticed that a similar formula holds for prime pairs p and $p+4$. We investigate how to extend their work to generic prime pairs p and $p+d$. Furthermore, using elementary methods, we prove the following theorem.

<u>Theorem 1</u>. Let A be the square product of the odd numbers from 1 to $d-1$, namely $A = \prod_{(i=1,3,\dots,d-3,d-1)} i^2$. When $n > A$, $(n, n+d)$ is a prime pair if and only if

$$Ad[(n-1)/2]!^2 \equiv (-1)^{(n+1)/2} A(n+d) - (-1)^{(n+d+1)/2} 2^d n \pmod{n(n+d)}.$$

<u>Proof</u>. The basic tool of our proof is the following result that gives the necessary and sufficient condition for an integer n to be a prime. That is, n is a prime if and only if

$$[(n-1)/2]!^2 \equiv \begin{cases} -1 \pmod{n} & \text{if } n = 4k+1; \\ +1 \pmod{n} & \text{if } n = 4k-1. \end{cases} \tag{1}$$

According to Dickson [3], Lagrange [4] proved this result in 1771, the same paper where he published the first proof of Wilson's theorem.

Dealing with generic prime pairs n and $n+d$ four cases arise, depending on the combination of numbers of the form $4k+1$ and $4k-1$. We prove in detail one of the four cases, choosing $n \equiv 1 \pmod{4}$ and $n+d \equiv -1 \pmod{4}$. The proofs of the other cases may be easily obtained using the same scheme.

From (1), it follows that $(n, n+d)$ is a prime pair if and only if the following congruences simultaneously hold:

$$\left(\frac{n-1}{2}\right)!^2 \equiv -1 \pmod{n} \quad \text{and}$$
$$\left(\frac{n+d-1}{2}\right)!^2 \equiv 1 \pmod{n+d}.$$

First, note that we can multiply both sides of the previous congruences by d without losing the combined necessary and sufficient condition for $(n, n+d)$ to be a prime pair. Hence,

$$d\left(\frac{n-1}{2}\right)!^2 \equiv -d \pmod{n} \quad \text{and} \tag{2}$$
$$d\left(\frac{n+d-1}{2}\right)!^2 \equiv d \pmod{n+d}. \tag{3}$$

If $n+d$ is prime then congruence (3) continues to hold as a necessary and sufficient condition for the primality of $n+d$; when $n+d$ is composite (and hence, its factors are $< (n+d-1)/2$), the left-hand side of (3) is $\equiv 0 \pmod{n+d}$ but the right-hand side is not, because d is never divisible by $n+d$.

Congruence (2) may also hold for a composite n, when d is a multiple of n, but in this case $n+d$ is forced to be composite; this assures that both (2) and (3) cannot jointly hold and hence, the necessary and sufficient condition for the simultaneous primality of n and $n+d$ is maintained.

Next, we change (3) to an equivalent but more suitable form. Observe that

$$\begin{aligned}
&\left(\frac{n+d-1}{2}\right)! \\
&= \left(\frac{n-1}{2}\right)! \left(\frac{n+1}{2}\right) \left(\frac{n+3}{2}\right) \cdots \left(\frac{n+d-3}{2}\right) \left(\frac{n+d-1}{2}\right) \\
&= \left(\frac{n-1}{2}\right)! \prod_{(i=1,3,\dots,d-3,d-1)} \left(\frac{n+i}{2}\right)
\end{aligned}$$

so that congruence (3) can now be written as

$$d\left(\frac{n-1}{2}\right)!^2 \prod_{(i=1,3,\dots,d-3,d-1)} \left(\frac{n+i}{2}\right)^2 \equiv d \pmod{n+d}.$$

Multiplying both sides of the previous congruence by $4^{d/2}$, we obtain

$$d\left(\frac{n-1}{2}\right)!^2 4^{d/2} \prod_{(i=1,3,\dots,d-3,d-1)} \left(\frac{n+i}{2}\right)^2 \equiv 4^{d/2} d \pmod{n+d}$$

or

$$d\left(\frac{n-1}{2}\right)!^2 \prod_{(i=1,3,\dots,d-3,d-1)} 4\left(\frac{n+i}{2}\right)^2 \equiv 4^{d/2}d \pmod{n+d}. \tag{4}$$

We now observe that

$$4\left(\frac{n+i}{2}\right)^2 \equiv (d-i)^2 \pmod{n+d}.$$

Hence, each term of the product in the left-hand side of (4) is $\equiv (d-i)^2 \pmod{n+d}$ so that

$$d\left(\frac{n-1}{2}\right)!^2 \prod_{(i=1,3,\dots,d-3,d-1)} (d-i)^2 \equiv 4^{d/2}d \pmod{n+d}$$

or

$$Ad\left(\frac{n-1}{2}\right)!^2 \equiv 2^d d \pmod{n+d}. \tag{5}$$

In order to get a congruence $\pmod{n}$ whose left-hand side equals that of (5), we now multiply both sides of (2) by A, obtaining:

$$Ad\left(\frac{n-1}{2}\right)!^2 \equiv -Ad \pmod{n}. \tag{6}$$

Since $n > A$ congruence (6) continues to be a necessary and sufficient condition for the primality of n, because A is never divisible by n. Then $(n, n+d)$ is a prime pair if and only if congruences (5) and (6) simultaneously hold.

It remains only to combine congruences (5) and (6) into a single congruence $\pmod{n(n+d)}$. Rewriting (5) as an equation, we get

$$Ad\left(\frac{n-1}{2}\right)!^2 - 2^d d = r(n+d)$$

or

$$Ad\left(\frac{n-1}{2}\right)!^2 + A(n+d) - 2^d d + 2^d(n+d) = r'(n+d)$$

or

$$Ad\left(\frac{n-1}{2}\right)!^2 + A(n+d) + 2^d n = r'(n+d) \tag{7}$$

for some $r, r' \in \mathbb{N}$. Similarly from (6), we get

$$Ad\left(\frac{n-1}{2}\right)!^2 + Ad = sn$$

or

$$Ad\left(\frac{n-1}{2}\right)!^2 + An + Ad + 2^d n = s'n$$

or

$$Ad\left(\frac{n-1}{2}\right)!^2 + A(n+d) + 2^d n = s'n \tag{8}$$

for some $s, s' \in \mathbb{N}$. Thus, it is clear that the quantity on the left-hand side of (7) and (8) is divisible by the product of n and $n+d$. Hence,

$$\begin{aligned} &Ad\left(\frac{n-1}{2}\right)!^2 \equiv -A(n+d) - 2^d n \pmod{n(n+d)} \\ &\equiv (-1)^{(n+1)/2}A(n+d) - (-1)^{(n+d+1)/2}2^d n \pmod{n(n+d)}, \end{aligned}$$

as was to be shown.

Theorem 2. Let B be the greatest divisor of A satisfying $\gcd(B,d) = 1$. When $n > B$, $(n, n+d)$ is a prime pair if and only if

$$Ad[(n-1)/2]!^2 \equiv (-1)^{(n+1)/2}A(n+d) - (-1)^{(n+d+1)/2}2^d n \pmod{n(n+d)}.$$

Proof. Proceed as in the proof of Theorem 1 obtaining congruences (5) and (6). Next observe that when $n \leq A$, congruence (6) may hold for a composite n whose prime factors are $< d$, namely for a composite divisor of A. In this case, since $n > B$, n and d are not relatively prime and consequently $n+d$ is forced to be composite. This assures that both (5) and (6) cannot jointly hold and hence, the necessary and sufficient condition for the simultaneous primality of n and $n+d$ is maintained. To complete the proof, combine (5) and (6) into a single congruence $\pmod{n(n+d)}$, as in the proof of Theorem 1, and then Theorem 2 follows.

Note that Theorem 2 is equivalent to Theorem 1 when d is an exact power of 2, because in this case, $\gcd(A,d) = 1$ and then $B = A$. In any other case, $B < A$ and Theorem 2 improves on the previous result.

To compute B one may apply recursively the relation $x \to x/\gcd(x,d)$ until $\gcd(x,d) = 1$, starting from the initial value $x = A$.

Theorem 3. Except for a finite number of pairs where n is a composite divisor of B and $n+d$ is prime, $(n, n+d)$ is a prime pair if and only if

$$Ad[(n-1)/2]!^2 \equiv (-1)^{(n+1)/2}A(n+d) - (-1)^{(n+d+1)/2}2^d n \pmod{n(n+d)}.$$

Proof. As a consequence of Theorem 2, it suffices to cover the case when $n \leq B$. Proceed as in the previous proof obtaining (5) and (6). Next, observe that congruences (5) and (6) both hold when n is a composite divisor of B and $n+d$ is prime. To complete the proof, combine (5) and (6) into a single congruence $\pmod{n(n+d)}$. Theorem 3 follows.

The explicit primality criteria for $d = 2, 4, 6, 8, 10, 12$ are listed below. These are obtained using Theorem 3 and identifying the exceptions that appear when $n \leq B$. Note that for $d = 4$, we found the exception, not listed in [2], for $n = 9$.

Corollary 1. $(n, n+2)$ is a prime pair if and only if

$$2[(n-1)/2]!^2 \equiv (-1)^{(n+1)/2}(5n+2) \pmod{n(n+2)}.$$

Corollary 2. Except for $n = 9$, $(n, n+4)$ is a prime pair if and only if

$$36[(n-1)/2]!^2 \equiv (-1)^{(n+1)/2}(-7n+36) \pmod{n(n+4)}.$$

Corollary 3. Except for $n = 25$, $(n, n+6)$ is a prime pair if and only if

$$1350[(n-1)/2]!^2 \equiv (-1)^{(n+1)/2}(289n+1350) \pmod{n(n+6)}.$$

Corollary 4. Except for $n = 9, 15, 21, 35, 45, 63, 75, 105, 225, 441, 735, 1575, 2205$, $(n, n+8)$ is a prime pair if and only if

$$88200[(n-1)/2]!^2 \equiv (-1)^{(n+1)/2}(10769n+88200) \pmod{n(n+8)}.$$

Corollary 5. Except for $n = 9, 21, 27, 49, 63, 147, 189, 567, 729, 5103, 35721$, $(n, n+10)$ is a prime pair if and only if

$$8930250[(n-1)/2]!^2 \equiv (-1)^{(n+1)/2}(894049n+8930250) \pmod{n(n+10)}.$$

Corollary 6. Except for $n = 25, 35, 49, 55, 77, 245, 385, 605, 847, 1225, 2695, 3025, 13475, 21175$, $(n, n+12)$ is a prime pair if and only if

$$\begin{aligned} &1296672300[(n-1)/2]!^2 \\ &\equiv (-1)^{(n+1)/2}(108051929n+1296672300) \pmod{n(n+12)}. \end{aligned}$$

To identify the exceptions appearing in the above corollaries we wrote a program in Pari-GP that checks the numbers $b + d$ for primality when b is any composite divisor of B.

The same program was used to count the total number of exceptions, $E_{(d)}$, for any value of d from $d = 4$ up to $d = 42$. The results of this program can be found in Table 1.

Pari-GP does not allow one to count $E_{(d)}$ for $d > 42$ because the set of composite divisors of the corresponding B grows too fast. Indeed, writing B in terms of its prime factorization,

$$B = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{\omega(B)}^{\alpha_{\omega(B)}}, \tag{9}$$

we see that the total number of divisors $\nu_{(B)}$ of B is given by

$$\nu_{(B)} = \prod_{i=1}^{\omega_{(B)}} (\alpha_i + 1),$$

where $\omega_{(B)}$ is the number of distinct prime factors of B.

Hence, the number of composite divisors of B amounts to $\nu_{(B)} - \omega_{(B)} - 1$. For $d = 44$, this quantity exceeds 53×10^6.

In order to find a formula which approximates the total number of exceptions, we apply heuristic reasoning based on the probability that the numbers $b + d$ are prime.

By the Prime Number Theorem, the probability that a random number x is prime is asymptotically $1/\log x$. Hence, we can roughly estimate the number of primes over a set of randomly selected numbers by computing the integral of their associated probabilities.

Applying this method to the set of numbers $b + d$, we need to take into account the fact that such numbers do not behave like random and independent variables.

Indeed, each prime p dividing b, divides $1/p^{\text{th}}$ of a random set of integers but cannot divide $b+d$, because d is relatively prime to b. To attempt to adjust for this, we can then multiply the probability of $b+d$ being prime by the correction term $p/(p-1)$, for each prime p dividing b.

Thus, we count the integral of probabilities as

$$\sum_{b|B} \left(\frac{1}{\log(b+d)} \prod_{p|b} \frac{p}{p-1} \right). \tag{10}$$

Expression (10), involving a sum extended over the set of composite divisors of B, is inadequate for a rapid computation.

We proceed therefore, assuming

$$\frac{\nu_{(B)}}{\log(B^{0,5} + d)} \tag{11}$$

is a rough approximation of $\sum_{b|B} \log(b+d)^{-1}$.

The approximation of the inner product of the corrective terms has to be a little more accurate; correction terms $p_i/(p_i - 1)$ do not apply uniformly to the whole set of composite divisors of B, but only to a proportion almost equal to $(1 - \frac{1}{\alpha_i+1})$ of them, where p_i , α_i are respectively, the prime factors and their exponents appearing in the prime factorization (9) of B. Thus, we get the following simplified expression for the product of corrective terms

$$\prod_{i=1}^{\omega_{(B)}} \frac{\alpha_i \left(\frac{p_i}{p_i - 1}\right) + 1}{\alpha_i + 1}. \tag{12}$$

Combining (11) and (12), we obtain

$$\frac{1}{\log(B^{0,5}+d)}\prod_{i=1}^{\omega(B)}\left(\frac{p_i\alpha_i}{p_i-1}+1\right).$$

We still have to consider that primes q dividing d divide $1/q^{\text{th}}$ of a random set of integers, but cannot divide $b+d$ because d (and therefore any q) is relatively prime to B (and therefore relatively prime to any of its divisors b). But again, this requires us to adjust our estimate by further correction terms $q/(q-1)$, for each prime q dividing d.

Finally we can formulate the following conjecture.

Conjecture 1. The expected number $E'_{(d)}$ of exceptions in Theorem 3 (or equivalently, the number of primes over the set of numbers $b+d$, with b being any divisor of B) is

$$E'_{(d)}=\frac{1}{\log(B^{0,5}+d)}\prod_{i=1}^{\omega(B)}\left(\frac{p_i\alpha_i}{p_i-1}+1\right)\prod_{q|d}\frac{q}{q-1},$$

where p_i and α_i are respectively, the prime factors and their exponents appearing in the prime factorization of B.

The number of exceptions $E'_{(d)}$ resulting from Conjecture 1, for any value of d from $d=4$ up to $d=42$, are listed in Table 1. The comparison with the known data $E_{(d)}$ seems to support the conjecture quite well.

d	$E_{(d)}$	$E'_{(d)}$
4	1	4
6	1	4
8	13	20
10	11	16
12	14	19
14	92	84
16	388	363
18	155	147
20	636	625
22	1,832	1,759

Table 1. Actual $E_{(d)}$ and conjectured $E'_{(d)}$ exceptions in Theorem 3

d	$E_{(d)}$	$E'_{(d)}$
24	1,529	1,480
26	7,897	7,658
28	7,051	6,714
30	1,004	940
32	225,790	224,628
34	143,735	141,980
36	43,899	42,429
38	646,692	638,705
40	343,513	335,173
42	90,739	87,525

Table 1. (cont.)
Actual $E_{(d)}$ and conjectured $E'_{(d)}$ exceptions in Theorem 3

References

1. P. A. Clement, "Congruences for Sets of Primes," *American Mathematical Monthly*, 56 (1949), 23–25.
2. J. B. Dence and T. P. Dence, "A Necessary and Sufficient Condition for Twin Primes", *Missouri Journal of Mathematical Sciences*, 7 (1995), 129–131.
3. L. E. Dickson, *History of the Theory of Numbers*, Carnegie Institute of Washington, 1919. Reprinted by Chelsea Publishing, New York, 1971.
4. J. L. Lagrange, "Démonstration d'un Théoreme Nouveau Concernant les Nombres Premiers," *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres*, année 1771, Berlin (1773), 125–137. Available at http://bibliothek.bbaw.de.

Mathematics Subject Classification (2000): 11A51

Flavio Torasso
Via XXIV Maggio 12
10034 Chivasso (TO)
Italy
email: flavio.torasso@enel.it