FOLIA 128

Annales Universitatis Paedagogicae Cracoviensis

Studia Mathematica XII (2013)

Flavio Torasso

Simultaneous primality of the integers n and $2n-d$

Abstract. A necessary and sufficient condition for the simultaneous primality of integers n and $2n-d$ is given by means of congruences $\bmod\, n(2n-d)$ that hold if and only if they form a prime pair. These are used to obtain explicit primality criteria for some values of d, after computation of a finite number of exceptions that appear when n is lower than a fixed quantity depending only on d.

Many primality criteria for pairs of primes originates by the well known converse of Wilson's theorem: n is a prime if and only if $(n-1)! \equiv -1 \bmod n$.

Using it and focusing on twin primes, Clement proved in 1949 [2] that n and $n+2$ are both primes if and only if $4((n-1)!+1)+n \equiv 0 \bmod n(n+2)$. Dence and Dence [3] later improved previous results proving that n and $n+2$ are both primes if and only if $2(\frac{n-1}{2})!^2 \equiv \pm(5n+2) \bmod n(n+2)$.

A new characterization of twin primes was recently given by Górowski and Łomnicki [6]: they proved that $2n+1$ and $2n+3$ are both primes if and only if $12((2n-1)!-1)-5(2n+1) \equiv 0 \bmod (2n+1)(2n+3)$.

Other forms of prime pairs appear to be less studied. In 1905, again starting from Wilson's theorem, Carmichael [1] proved that p and $2p-1$ are simultaneously primes if and only if $(p-1)!^4 \equiv 1 \bmod p(2p-1)$.

The aim of this work is to extend Carmichael's result to generic pairs of odd primes p and $2p-d$ by suitable variations on the original proof of Wilson's theorem. Using elementary methods, we start by proving the following theorem.

Theorem 1
Let $n > d$ and $A = (\frac{d-1}{2})!^2$. Let moreover $2n-d > A$, then $(n, 2n-d)$ is an odd prime pair if and only if

$$Ad\Big(n - \frac{d+1}{2}\Big)!^2 \equiv 2n\big(A(-1)^{\frac{d+1}{2}} - 1\big) + d \bmod n(2n-d).$$

Proof. A necessary and sufficient condition for an integer p to be a prime is the following congruence holding true:

$$(p-x)!(x-1)! \equiv (-1)^x \bmod p. \tag{1}$$

AMS (2000) Subject Classification: 11A51.

According to Dickson [4, page 64], this was first proved in 1783 by Genty [5]. For $x = \frac{p+1}{2}$, the latter expression is

$$\Big(\frac{p-1}{2}\Big)!^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p, \tag{2}$$

a result already obtained in 1771 by Lagrange [8].

Choosing $p = n$, $x = \frac{d+1}{2}$ in (1) and squaring both sides of the congruence, we obtain

$$A\Big(n - \frac{d+1}{2}\Big)!^2 \equiv 1 \bmod n, \tag{3}$$

while choosing $p = 2n - d$ in (2), we get

$$\Big(n - \frac{d+1}{2}\Big)!^2 \equiv (-1)^{\frac{2n-d+1}{2}} \bmod 2n - d$$

or

$$\Big(n - \frac{d+1}{2}\Big)!^2 \equiv (-1)^{\frac{d+1}{2}} \bmod 2n - d. \tag{4}$$

Therefore integers n and $2n - d$ are simultaneously primes if and only if both congruences (3) and (4) hold.

The combined necessary and sufficient condition for $(n, 2n - d)$ to be a prime pair is preserved even if we multiply both sides of these congruences by d, obtaining

$$Ad\Big(n - \frac{d+1}{2}\Big)!^2 \equiv d \bmod n \tag{5}$$

and

$$d\Big(n - \frac{d+1}{2}\Big)!^2 \equiv d(-1)^{\frac{d+1}{2}} \bmod 2n - d. \tag{6}$$

In (6) the condition is indeed satisfied also when $2n-d$ is a composite number (whose factors are less than $\frac{2n-d-1}{2}$): the left-hand side of (6) is then divisible by $2n - d$ but the right-hand side is not, because $2n - d$ can not divide d, as d is less than n.

The left-hand sides of (5) and (6) now differ only by a factor A. Fixing $2n-d > A$, we can then multiply both sides of (6) by A, without missing the condition for primality, because A is not divisible by $2n - d$. So we obtain

$$Ad\Big(n - \frac{d+1}{2}\Big)!^2 \equiv Ad(-1)^{\frac{d+1}{2}} \bmod 2n - d, \tag{7}$$

a congruence that continues to be a necessary and sufficient condition for the primality of $2n - d$.

We then remark that $(n, 2n - d)$ is a prime pair if and only if congruences (5) and (7) simultaneously hold.

The next step requires to combine (5) and (7) into a single congruence $\bmod n(2n - d)$, that is solved by rewriting (5) and (7) in form of equations. Proceeding with (7), we obtain

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

or

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

or

$$Ad\Big(n-\frac{d+1}{2}\Big)!^2 - 2n\big(A(-1)^{\frac{d+1}{2}}-1\big) - d = r'(2n-d) \tag{8}$$

for some $r, r' \in \mathbb{N}$. Similarly from (5), we have

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

or

$$Ad\Big(n-\frac{d+1}{2}\Big)!^2 - 2n\big(A(-1)^{\frac{d+1}{2}}-1\big) - d = s'n \tag{9}$$

for some $s, s' \in \mathbb{N}$. Thus, we can infer that the quantity on the left-hand sides of (8) and (9) is divisible by the product of n and $2n-d$. Rearranging it in form of congruence, we get

$$Ad\Big(n-\frac{d+1}{2}\Big)!^2 \equiv 2n\big(A(-1)^{\frac{d+1}{2}}-1\big) + d \bmod n(2n-d),$$

as was to be shown.

Now we obtain a simpler result for the case when d is a prime.

Theorem 2

Let $A = (\frac{d-1}{2})!^2$ and d be a prime. If $2n-d > A$, then $(n, 2n-d)$ is an odd prime pair if and only if

$$A\Big(n-\frac{d+1}{2}\Big)!^2 \equiv \frac{2n}{d}\big(A(-1)^{\frac{d+1}{2}}-1\big) + 1 \bmod n(2n-d).$$

Proof. We infer from (2) that d divides $(A(-1)^{\frac{d+1}{2}}-1)$ if and only if d is a prime. Thus, it is possible to divide by d any term of the congruence found in Theorem 1 avoiding the constraint $n > d$, which is instead required in Theorem 1. Hence, Theorem 2 follows.

It is possible to improve on Theorem 1 by analysing the divisors of A relatively prime to d, as shown in the next theorem.

Theorem 3

Let $n > d$ and B be the greatest odd divisor of A satisfying $\gcd(B, d) = 1$. Let moreover $2n-d > B$, then $(n, 2n-d)$ is an odd prime pair if and only if

$$Ad\Big(n-\frac{d+1}{2}\Big)!^2 \equiv 2n\big(A(-1)^{\frac{d+1}{2}}-1\big) + d \bmod n(2n-d).$$

Proof. Starting from congruences (5) and (7) as obtained in the proof of Theorem 1, it suffices to consider the case when $n \le A$:

- congruence (7) may hold when $2n-d$ is a composite divisor of A, having prime factors which are less than $\frac{d-1}{2}$, but
- congruence (5) can not hold because, assumed $2n-d>B$, the properties of B imply that n is a composite number (indeed, $\gcd(2n-d,d)\neq 1$ forces n to be an odd composite number).

This assures that both (5) and (7) can not jointly hold and hence, the necessary and sufficient condition for the simultaneous primality of n and $2n-d$ is preserved. To complete the proof it only requires to apply the same scheme outlined in the proof of Theorem 1. Then Theorem 3 follows.

Next, we write the simplified form of Theorem 3 for the case when d is a prime.

Theorem 4
Let B be the greatest odd divisor of A satisfying $\gcd(B,d)=1$ and d be a prime. If $2n-d>B$, then $(n,2n-d)$ is an odd prime pair if and only if

$$A\Big(n-\frac{d+1}{2}\Big)!^2 \equiv \frac{2n}{d}\big(A(-1)^{\frac{d+1}{2}}-1\big)+1 \bmod n(2n-d).$$

Proof. We infer from (2) that d divides $(A(-1)^{\frac{d+1}{2}}-1)$ if and only if d is a prime. Thus, it is possible to divide by d any term of the congruence obtained in Theorem 3 avoiding the constraint $n>d$, which is instead required in Theorem 3. Hence, Theorem 4 follows.

Note that Theorem 4 improves on Theorem 2 by a factor $\frac{A}{B}=2^t$, where t is the exact power of 2 dividing A.

As showed by Legendre [9] in 1808, the exact power of a prime q dividing $x!$ is $[\frac{x}{q}]+[\frac{x}{q^2}]+[\frac{x}{q^3}]+\ldots$ and equals $\frac{x-\sigma_q(x)}{q-1}$, where $\sigma_q(x)$ is the sum of the digits appearing in the base q representation of x.

Thus, it is easy to see that $t=d+1-2\sigma_2(d)$, where $\sigma_2(d)$ is the sum of the digits in the binary representation of d.

Similarly, note that Theorem 3 improves on Theorem 1 by a factor $\frac{A}{B}=2^t q_1^{t_1}q_2^{t_2}\ldots q_n^{t_n}$, where q_i are the primes dividing d and t_i are their exact powers dividing A.

The number B can be computed starting from the initial value $x=A$ and applying recursively the relation $x\to\frac{x}{\gcd(x,2d)}$ until $\gcd(x,2d)=1$.

The last theorem reformulates the previous results unconditionally respect to n, revealing a number of consequently exceptions.

Theorem 5
Let $D=d$ if d is a composite number or $D=1$ otherwise. Then $(n,2n-d)$ is a prime pair if and only if

$$AD\Big(n-\frac{d+1}{2}\Big)!^2 \equiv \frac{2n}{d}\big(A(-1)^{\frac{d+1}{2}}-1\big)D+D \bmod n(2n-d)$$

except for a finite number of pairs that are those pairs where n is a prime and $2n-d\equiv(-1)^{\frac{d-1}{2}} \bmod 4$ is a composite divisor of B and those pairs where n is a prime or 1 and $2n-d=1$.

Proof. Thanks to Theorems 3 and 4, it is sufficient to resume from congruences (5) and (7), this time restricting the analysis to the case $n \leq B$. Hence it happens that congruence (7) holds when $2n-d$ is a composite divisor of B or equals 1. Two cases arise:

– if $2n-d \not\equiv (-1)^{\frac{d-1}{2}} \bmod 4$, then n is forced to be even and (5) would consequently fail;

– in the opposite case n is odd and then (5) and (7) both hold when n is a prime or equals 1.

To complete the proof, match (5) and (7) into a single congruence $\bmod\, n(2n-d)$, and then Theorem 5 follows.

We can now use Theorem 5 to derive explicit primality criteria for some values of d. To do so it is necessary to identify and specify the exceptions foreseen by Theorem 5. Therefore we wrote a program in Pari-GP that runs over any integer b belonging to the set of composite divisor of B and checks the numbers $\frac{b+d}{2}$ for primality. Applying this procedure for any $d = 1,3,5,7,9,11,13,15,17,19$ we obtained the explicit primality criteria listed in the following corollaries. Note that for $d = 1,3$, it was also necessary a supplementary check for the two special cases due to $n = 2$, not covered by the program, for which the corresponding congruences would incorrectly fail, for the prime pair (2,3), and would incorrectly hold, for the pair (2,1).

Corollary 1
For $n > 2$, $(n, 2n-1)$ is a prime pair if and only if

$$(n-1)!^2 \equiv -4n+1 \bmod n(2n-1).$$

Corollary 2
For $n > 2$, $(n, 2n-3)$ is a prime pair if and only if

$$(n-2)!^2 \equiv 1 \bmod n(2n-3).$$

Corollary 3
Except for $n = 3$, $(n, 2n-5)$ is a prime pair if and only if

$$(2!(n-3)!)^2 \equiv -2n+1 \bmod n(2n-5).$$

Corollary 4
$(n, 2n-7)$ is a prime pair if and only if

$$(3!(n-4)!)^2 \equiv 10n+1 \bmod n(2n-7).$$

Corollary 5
Except for $n = 5$, $(n, 2n-9)$ is a prime pair if and only if

$$9(4!(n-5)!)^2 \equiv -1154n+9 \bmod n(2n-9).$$

Corollary 6
Except for $n = 13, 43$, $(n, 2n-11)$ *is a prime pair if and only if*

$$(5!(n-6)!)^2 \equiv 2618n + 1 \bmod n(2n-11).$$

Corollary 7
Except for $n = 7, 11, 19, 29, 47, 1019$, $(n, 2n-13)$ *is a prime pair if and only if*

$$(6!(n-7)!)^2 \equiv -79754n + 1 \bmod n(2n-13).$$

Corollary 8
$(n, 2n-15)$ *is a prime pair if and only if*

$$15(7!(n-8)!)^2 \equiv 50803198n + 15 \bmod n(2n-15).$$

Corollary 9
Except for $n = 13, 19, 31, 61, 103, 131, 211, 229, 271, 1021, 1993, 2371, 5521, 9931$, $(n, 2n-17)$ *is a prime pair if and only if*

$$(8!(n-9)!)^2 \equiv -191259106n + 1 \bmod n(2n-17).$$

Corollary 10
Except for $n = 17, 23, 41, 47, 83, 97, 131, 167, 293, 347, 617, 797, 1103, 1427, 1847, 5477, 16547, 22973, 53591, 114827$, $(n, 2n-19)$ *is a prime pair if and only if*

$$(9!(n-10)!)^2 \equiv 13861252042n + 1 \bmod n(2n-19).$$

The above mentioned program in Pari-GP was also used to count $E_{(d)}$, the total number of exceptions appearing in each corollary and for any further value of d from $d = 21$ up to $d = 65$, as reported in Table 1.

We can not go beyond this limit in computing $E_{(d)}$ because the set of composite divisors of the corresponding B grows too fast and overcomes the dimension Pari-GP's algorithm can handle.

Indeed, writing $B = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{\omega_{(B)}}^{\alpha_{\omega_{(B)}}}$ in term of its prime factorization, we see that the total number of its divisors is given by $\nu_{(B)} = \prod_{i=1}^{\omega_{(B)}} (\alpha_i + 1)$, where $\omega_{(B)}$ is the number of its distinct prime factors.

The number of composite divisors of B amounts then to $\nu_{(B)} - \omega_{(B)} - 1$. For $d = 67$, this quantity exceeds 35×10^6.

A formula, depending only on d, that approximates the expected total number of exceptions, is adapted from the simplified model developed in [10] by Torasso and summarized in the following conjecture.

Conjecture 1
The expected number of exceptions in Theorem 5 (or equivalently, the number of primes over the set of numbers $\frac{b+d}{2}$*, with* b *being any divisor of* B*) is*

$$E'_{(d)} = \log\left(\frac{B^{\frac{1}{2}} + d}{2}\right)^{-1} \prod_{i=1}^{\omega_{(B)}} \left(\frac{p_i \alpha_i}{p_i - 1} + 1\right) \prod_{q|d} \frac{q}{q-1},$$

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

The numbers of exceptions $E'_{(d)}$ resulting from Conjecture 1, for any value of d from $d=3$ up to $d=65$, are listed in Table 1.

The comparison with the known data $E_{(d)}$ seems to support the conjecture well enough even if it should be noted that we can not expect a better approximation because Conjecture 1 is found on a probabilistic model that simply considers primality of different integers as independent. As explained in [7, §22.20] by Hardy and Wright, any such model is likely to be off by a factor of $2e^{-\gamma} \approx 1.12$, which can be seen as a measure of thecorrelation, and the numerical results are often off by just as much.

d	$E_{(d)}$	$E'_{(d)}$
3	0	2
5	1	1
7	0	3
9	1	1
11	2	6
13	6	8
15	0	3
17	14	17
19	20	22
21	3	3
23	81	77
25	28	23
27	28	32
29	332	338
31	512	489
33	28	24

d	$E_{(d)}$	$E'_{(d)}$
35	69	64
37	1,596	1,592
39	147	150
41	5,657	5,395
43	7,991	7,716
45	159	136
47	34,861	34,275
49	6,623	6,194
51	1,280	1,188
53	80,846	78,433
55	2,275	2,107
57	2,511	2,231
59	346,428	335,916
61	410,947	397,097
63	7,644	7,288
65	22,861	21,397

Table 1: Actual $E_{(d)}$ and conjectured $E'_{(d)}$ exceptions in Theorem 5

References

[1] R.D. Carmichael, *Six propositions on prime numbers*, Amer. Math. Monthly **12** (1905), 106–108.

[2] P.A. Clement, *Congruences for sets of primes*, Amer. Math. Monthly **56** (1949), 23–25.

[3] J.B. Dence, T.P. Dence, *A necessary and sufficient condition for twin primes*, Missouri J. Math. Sci. **7** (1995), 129–131.

[4] L.E. Dickson, *History of the theory of numbers*, Carnegie Institute of Washington, 1919, Reprinted by Chelsea Publishing, New York, 1971.

[5] L. Genty, *Mémoires sur les nombres premiers*, Histoire et mémoires de l'academie royale des sciences et inscriptions de Toulouse **3** (1788).

[6] J.W. Górowski, A. Łomnicki, *Congruences characterizing twin primes*, Ann. Univ. Paedagog. Crac. Stud. Math. **11** (2012), 95–100.

[7] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[8] J.L. Lagrange, *Démonstration d'un théoreme nouveau concernant les nombres premiers*, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres, 1771, Berlin (1773), 125–137.

[9] A.M. Legendre, *Théorie des nombres*, 1808.

[10] F. Torasso, *Primality criteria for pairs n and $n + d$*, Missouri J. Math. Sci. **20** (2008), 94–101.

Via Maestra 25/I
10034 Chivasso (TO)
Italy
E-mail: flavio.torasso@enel.com

Received: December 3, 2013; final version: December 20, 2013;
available online: January 8, 2014.