FOLIA 122

Annales Universitatis Paedagogicae Cracoviensis

Studia Mathematica XI (2012)

Jan Górowski, Adam Łomnicki

Congruences characterizing twin primes

Abstract. Inspired by P.A. Clement's results in [2], we give new necessary and sufficient conditions for two prime numbers to be twin primes.

Let n be a positive integer. A pair $(n, n+2)$ is called a *twin primes pair* (or twin primes for short) if n and $n+2$ are prime numbers.

In this paper we give four congruence relations which characterize twin primes. Some basic facts and properties of congruence relations used here can be found in [8]. The set of all prime numbers will be denoted $\mathbb{P}$.

In 1946 as stated in [2] or 1949 as it is related in [8] P.A. Clement proved the following characterization.

Theorem 1
Let $n \geq 2$. A pair $(n, n+2)$ is a twin primes pair if and only if

$$4((n-1)!+1)+n \equiv 0 \bmod n(n+2).$$

The proof of this theorem can be found in [2] or [6]. Other characterizations of twin primes may be found in [1], [3] and [4]. The next results come from [5].

Theorem 2
If $n \in \mathbb{N}$ and $n > 1$ then

$$2n+1 \in \mathbb{P} \Longleftrightarrow (n!)^2 + (-1)^n \equiv 0 \bmod (2n+1).$$

Theorem 3
A positive integer $n > 1$ is a prime number if and only if

$$((n-2)!!)^2 + (-1)^{[\frac{n}{2}]} \equiv 0 \bmod n.$$

Let us recall that $0!! = 1$, $1!! = 1$ and $n!! = n(n-2)!!$ for any integer $n \geq 2$. In the sequel instead of $(n!)^2$ we will write $n!^2$, similarly $(n)!!^2$ will denote $((n)!!)^2$.

AMS (2000) Subject Classification: 11A41, 11A07.

Theorem 4
A positive integer $n > 1$ is a prime number if and only if

$$(n-1)!!^2 + (-1)^{[\frac{n}{2}]} \equiv 0 \bmod n.$$

The following theorem is called the Leibniz's theorem.

Theorem 5 ([7], p.214)
A positive integer $n > 1$ is a prime number if and only if $(n-2)! - 1 \equiv 0 \bmod n$.

We start by proving the following

Theorem 6
Let $n > 0$ be an integer, then $(2n+1, 2n+3)$ is a twin primes pair if and only if

$$2(n!^2 + (-1)^n) + 5(-1)^n(2n+1) \equiv 0 \bmod (2n+1)(2n+3). \tag{1}$$

Proof. Let $n > 0$ be an integer such that (1) holds true. Then

$$2(n!^2 + (-1)^n) \equiv 0 \bmod (2n+1) \quad \text{and} \quad n!^2 + (-1)^n \equiv 0 \bmod (2n+1).$$

This and Theorem 2 imply that $2n+1 \in \mathbb{P}$. Moreover,

$$2(n!^2 + (-1)^n) + 5(-1)^n(2n+1+2-2) \equiv 0 \bmod (2n+3),$$

thus

$$2(n!^2 + (-1)^n) - 10(-1)^n \equiv 0 \bmod (2n+3). \tag{2}$$

Since $1 = 2n+3-2(n+1)$ we have $\gcd(n+1, 2n+3) = 1$ for $n \in \mathbb{N}$, therefore (2) is equivalent to

$$\begin{aligned}
2((n+1)!^2 + (-1)^n(n+1)^2) - 10(-1)^n(n+1)^2 &\equiv 0 \bmod (2n+3),\\
2((n+1)!^2 + (-1)^{n+1}) - 2(-1)^{n+1}&\\
+ 2(-1)^n(n+1)^2 - 10(-1)^n(n+1)^2 &\equiv 0 \bmod (2n+3),\\
2((n+1)!^2 + (-1)^{n+1}) &\equiv 0 \bmod (2n+3)
\end{aligned}$$

and finally to

$$(n+1)!^2 + (-1)^{n+1} \equiv 0 \bmod (2n+3). \tag{3}$$

Condition (3) and Theorem 2 now yield $2n+3 \in \mathbb{P}$.

Conversely, assume that $2n+1, 2n+3 \in \mathbb{P}$, where $n > 0$ is an integer. By Theorem 2 we obtain (3) which is equivalent (see first part of this proof) to (2). Hence in view of $-2 \equiv 2n+1 \bmod (2n+3)$ we get

$$2(n!^2 + (-1)^n) + 5(-1)^n(2n+1) \equiv 0 \bmod (2n+3),$$

which in virtue of Theorem 2 and the fact that $\gcd(2n+1, 2n+3) = 1$ for $n \in \mathbb{N}$ gives

$$2(n!^2 + (-1)^n) + 5(-1)^n(2n+1) \equiv 0 \bmod (2n+1)(2n+3).$$

This completes the proof.

Let us mention that condition (1) was obtained through a different method by J.B. Dence, T.P. Dence in [3]. Now we prove

Theorem 7
Let $n > 0$ be an integer, then $(2n+1, 2n+3)$ is a twin primes pair if and only if

$$8((2n-1)!!^2 + (-1)^n) + 5(-1)^n(2n+1) \equiv 0 \bmod (2n+1)(2n+3). \tag{4}$$

Proof. Fix $n > 0$ and let (4) be fulfilled. Then

$$8((2n-1)!!^2 + (-1)^n) \equiv 0 \bmod (2n+1) \quad \text{and} \quad (2n-1)!!^2 + (-1)^n \equiv 0 \bmod (2n+1),$$

which in view of Theorem 3 yields $2n+1 \in \mathbb{P}$. Furthermore, by (4) we have

$$8((2n-1)!!^2 + (-1)^n) + 5(-1)^n(2n+1) \equiv 0 \bmod (2n+3)$$

and hence

$$8((2n-1)!!^2 + (-1)^n) - 10(-1)^n \equiv 0 \bmod (2n+3). \tag{5}$$

As $\gcd(2n+1, 2n+3) = 1$ congruence (5) is equivalent to

$$(2n+1)!!^2 + (-1)^{n+1} \equiv 0 \bmod (2n+3). \tag{6}$$

Indeed, condition (5) is equivalent to each of the following:

$$\begin{aligned}
8((2n+1)!!^2 + (-1)^n(2n+1)^2) - 10(-1)^n(2n+1)^2 &\equiv 0 \bmod (2n+3),\\
8((2n+1)!!^2 + (-1)^{n+1})\qquad\qquad\qquad\qquad&\\
+\, 8(-1)^n(2n+1)^2 - 10(-1)^n(2n+1)^2 - 8(-1)^{n+1} &\equiv 0 \bmod (2n+3),\\
8((2n+1)!!^2 + (-1)^{n+1}) &\equiv 0 \bmod (2n+3),
\end{aligned}$$

which is equivalent to (6). Now congruence (6) and Theorem 3 imply that $2n+3 \in \mathbb{P}$. Conversely, suppose that $2n+1, 2n+3 \in \mathbb{P}$. By Theorem 3 we get (6) or equivalently (5). This and the condition $-2 \equiv 2n+1 \bmod (2n+3)$ give

$$8((2n-1)!!^2 + (-1)^n) + 5(-1)^n(2n+1) \equiv 0 \bmod (2n+3).$$

Now using Theorem 3 and the fact that $\gcd(2n+1, 2n+3) = 1$ for $n \in \mathbb{N}$ we get

$$8((2n-1)!!^2 + (-1)^n) + 5(-1)^n(2n+1) \equiv 0 \bmod (2n+1)(2n+3),$$

which ends the proof.

We may use Theorem 4 to prove in the similar way the following result.

Theorem 8
Let $n > 0$ be an integer, then $(2n+1, 2n+3)$ is a twin primes pair if and only if

$$(2n)!!^2 + (-1)^n(2n+1) \equiv 0 \bmod (2n+1)(2n+3).$$

Lemma 1

If $n \in \mathbb{N}$, $n > 1$ *and*

$$12((2n-1)!-1) - 5(2n+1) \equiv 0 \bmod (2n+1)(2n+3),$$

then $3 \nmid (2n+1)$ *and* $3 \nmid (2n+3)$.

Proof. Suppose that $3 \mid (2n+1)$ or $3 \mid (2n+3)$ for some integer $n \geq 2$. If $3 \mid (2n+1)$ then $2n+1 = 3k$ for some $k > 1$ such that $k \notin 2\mathbb{N}$. Therefore

$$12((3k-2)!-1) - 5 \cdot 3k \equiv 0 \bmod 3k(3k+2).$$

Hence

$$12((3k-2)!-1) \equiv 0 \bmod 3k$$

and in consequence

$$(3k-2)! - 1 \equiv 0 \bmod k.$$

However, $k \mid (3k-2)!$, thus $k \mid 1$, a contradiction, so $3 \nmid (2n+1)$.

If $3 \mid (2n+3)$, then $2n = 3l$ for some $l \geq 1$ such that $l \in 2\mathbb{N}$. It follows that

$$12((3l-1)!-1) - 5 \cdot (3l+1) \equiv 0 \bmod (3l+1)(3l+3).$$

Thus

$$12((3l-1)!-1) - 5(3l+1) \equiv 0 \bmod 3,$$

which gives

$$-5 \equiv 0 \bmod 3.$$

This contradiction shows that $3 \nmid (2n+3)$.

Using Lemma 1 we may proof the following

Theorem 9

Let $n \geq 1$ *be an integer, then* $(2n+1, 2n+3)$ *is a twin primes pair if and only if*

$$12((2n-1)!-1) - 5(2n+1) \equiv 0 \bmod (2n+1)(2n+3). \tag{7}$$

Proof. Notice that for $n = 1$ congruence (7) becomes $-5 \cdot 3 \equiv 0 \bmod 3 \cdot 5$ thus for $n = 1$ the assertion follows. Assume now that $n \geq 2$ is arbitrarily fixed and (7) holds true. In view of Lemma 1 we get

$$12((2n-1)!-1) - 5(2n+1) \equiv 0 \bmod (2n+1),$$

thus

$$12((2n-1)!-1) \equiv 0 \bmod (2n+1)$$

and hence

$$(2n-1)! - 1 \equiv 0 \bmod (2n+1),$$

as $\gcd(12, 2n+1) = 1$. Now using Theorem 5 we obtain $2n+1 \in \mathbb{P}$. Moreover, we know that

$$12((2n-1)!-1) - 5(2n+3-2) \equiv 0 \bmod (2n+3)$$

is equivalent to

$$12((2n-1)!-1)+10 \equiv 0 \bmod (2n+3). \tag{8}$$

Since $1\cdot(2n+3)-2n=3$ and $3 \nmid 2n+3$, we get $\gcd(2n, 2n+3) = \gcd(2n+1, 2n+3) = 1$. Thus condition (8) is equivalent to:

$$\begin{aligned} 12((2n+1)!-2n(2n+1))+10\cdot 2n(2n+1) &\equiv 0 \bmod (2n+3),\\ 12((2n+1)!-1)-4(2n+3)(n-1) &\equiv 0 \bmod (2n+3),\\ 12((2n+1)!-1) &\equiv 0 \bmod (2n+3) \end{aligned}$$

and finally to

$$((2n+1)!-1) \equiv 0 \bmod (2n+3). \tag{9}$$

By Theorem 5 we get $2n+3 \in \mathbb{P}$. Conversely, suppose that $n \geq 2$ is such that $2n+1 \in \mathbb{P}$ and $2n+3 \in \mathbb{P}$. In virtue of Theorem 5 and Lemma 1 from (9) we obtain (8), which is equivalent to

$$12((2n-1)!-1)-5(2n+1) \equiv 0 \bmod (2n+3).$$

Using again Theorem 5 and the fact that $\gcd(2k+1, 2k+3) = 1$ for $k \in \mathbb{N}$ we get (7), this completes the proof.

A simple consequence of Theorems 6 and 7, it is enough to subtract (1) from (4), is

Theorem 10
If $2n+1$, $2n+3$ are twin primes then

$$4(2n-1)!!^2 - n!^2 + 3(-1)^n \equiv 0 \bmod (2n+1)(2n+3).$$

References

[1] Ch. Aebi, G. Cairns, *Catalan numbers, primes, and twin primes*, Elem. Math. **63** (2008), 153–164.

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

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

[4] J.F. Gold, D.H. Tucker, *A characterization of twin prime pairs*, Proceedings NCUR V. (1991) vol. 1, 362–366.

[5] J. Górowski, A. Łomnicki, *Around the Wilson's theorem*, Ann. Univ. Paedagog. Crac. Stud. Did. Math. Pert. (to appear).

[6] P. Ribenboim, *The little book of big primes*, Springer Verlag, New York, 1991.

[7] W. Sierpiński, *Elementary theory of numbers*, Second edition, North-Holland Mathematical Library, 31, North-Holland Publishing Co., Amsterdam; PWN–Polish Scientific Publishers, Warsaw, 1988.

[8] S.Y. Yan, *Number Theory for Computing*, Second edition, Springer Verlag, Berlin, 2002.

Pedagogical University
Institute of Mathematics
Podchorążych 2
PL-30-084 Kraków
Poland
E-mail: jangorowski@interia.pl,
alomnicki@poczta.fm

Received: 8 July 2012; final version: 25 August 2012;
available online: 26 September 2012.