Catalan numbers, primes, and twin primes

Elem. Math. 63 (2008) 153 – 164
0013-6018/08/040153-12

Elemente der Mathematik

Catalan numbers, primes, and twin primes

Christian Aebi and Grant Cairns

Christian Aebi studied mathematics at the University of Geneva. After his studies he worked for many years as a high school teacher. His main field of interest is the study of the development of number theory and algebra, in particular between the 17th and 19th century.

Grant Cairns studied engineering and science at the University of Queensland, Australia. He received his Ph.D. at the University of Montpellier, France. After stays at the University of Geneva and the University of Waterloo, Canada, he took a position at La Trobe University in Melbourne in 1988.

1 Introduction

Originally Catalan numbers were revealed for the first time in a letter from Euler to Goldbach in 1751 when counting the number of triangulations of a convex polygon (for a brief history see [6]). Today they are usually defined by $C_n = \frac{1}{n+1}\binom{2n}{n}$ and can be characterized recursively by

$$C_n = \frac{2(2n-1)}{n+1}C_{n-1} \quad \text{or} \quad C_n = C_{n-1}C_0 + C_{n-2}C_1 + \ldots + C_1C_{n-2} + C_0C_{n-1},$$

In dem nachfolgenden Beitrag führen uns die beiden Autoren in interessante Zusammenhänge zwischen Primzahlen bzw. Primzahlzwillingen und Catalanschen Zahlen ein. Dazu erinnern wir daran, dass die n-te Catalansche Zahl durch $C_n = \frac{1}{n+1}\binom{2n}{n}$ gegeben ist. Bekanntlich gilt nun für eine ungerade Primzahl p nach dem kleinen Fermatschen Satz $2^p \equiv 2 \mod p$. Hiervon gilt allerdings nicht die Umkehrung; deshalb wird eine natürliche Zahl n, welche $2^n \equiv 2 \mod n$ erfüllt, Pseudoprimzahl genannt. Der Zusammenhang zwischen Catalanschen Zahlen und Primzahlen besteht in dem offenbar wenig bekannten Ergebnis, dass für eine Primzahl p die Beziehung $(-1)^{(p-1)/2}C_{(p-1)/2} \equiv 2 \mod p$ gilt. Wiederum ist die Umkehrung hiervon im Allgemeinen nicht richtig, und man wird entsprechend zum Begriff der Catalanschen Pseudoprimzahl geführt. In Analogie zu den beiden genannten Kriterien stellen die Autoren schliesslich zwei notwendige, aber nicht hinreichende Kriterien für Primzahlzwillinge vor.

with $C_0 = 1$. Their appearances occur in a dazzling variety of combinatorial settings where they are used to enumerate various kinds of geometric and algebraic objects (see Richard Stanley's collection [29, Chap. 6]; an online Addendum is continuously updated). Quite a lot is known about the divisibility of the Catalan numbers; see [2, 10]. They are obviously closely related to the middle binomial numbers and not surprisingly, there is a considerable literature on their divisibility too; see [13, 5, 19, 15, 17, 16].

The aim of this paper is to observe a connection between Catalan numbers, primes and twin primes.

2 Primes

"There are few better known or more easily understood problems in pure mathematics than the question of rapidly determining whether a given integer is prime" [18]. A classic primality criterion is Wilson's theorem, which says (see [24, Ch. 11]):

Wilson's theorem. *A natural number p is prime if and only if* $(p-1)! \equiv -1 \pmod{p}$.

Wilson's theorem is a very striking result, and yet it is quite impractical as a primality check. "The trouble with Wilson's theorem is that it is more beautiful than useful" [26]. In some texts, it is used to prove Fermat's little theorem, a particular case of which is:

Theorem 1. *If p is prime, then* $2^p \equiv 2 \pmod{p}$.

A fascinating account of the history of proofs of Wilson's and Fermat's theorems is given in [11, Chap. 3]. Although Theorem 1 is a useful basic primality test, its converse is false; for example, $2^{341} \equiv 2 \pmod{341}$, but 341 is not prime; such numbers are called *pseudoprimes*. Some other pseudoprimes are: 561, 645, 1105, 1387, and 1729, just to stop on a famous number.

In a similar vein, we have:

Theorem 2. *If p is an odd prime, then* $(-1)^{\frac{p-1}{2}} \cdot C_{\frac{p-1}{2}} \equiv 2 \pmod{p}$.

It seems surprising that the above connection does not seem to have been previously explicitly observed, especially since Catalan numbers are the subject of such interest (sometimes known as *Catalan disease*) and there have been so many proofs of Wilson's theorem, including proofs by Catalan himself [11, Chap. 3]. We give two proofs of Theorem 2.

Proof 1 of Theorem 2. Suppose that p is an odd prime. Modulo p, one has $p - i \equiv -i$, for all i. Hence $(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2$ and so

$$C_{\frac{p-1}{2}} = \frac{1}{\frac{p+1}{2}} \binom{p-1}{\frac{p-1}{2}} = \frac{2}{p+1} \frac{(p-1)!}{\left(\left(\frac{p-1}{2}\right)!\right)^2} \equiv \frac{2(-1)^{\frac{p-1}{2}}}{p+1} \equiv 2(-1)^{\frac{p-1}{2}}.$$

□

Before giving the next proof, first recall the following elementary facts (part (a) was observed by Leibniz [11, p. 59], part (b) was observed as early as 1830 [11, p. 67] and appears for example in [1, Ex. 3.3.15]):

Lemma 1. *If p is prime and $0 < i < p$, then we have:*

(a) $\binom{p}{i} \equiv 0 \pmod{p}$,

(b) $(-1)^i \binom{p-1}{i} \equiv 1 \pmod{p}$,

(c) $(-1)^{i+1} \cdot \frac{1}{p} \cdot \binom{p}{i} \equiv \frac{1}{i} \pmod{p}$, *where $\frac{1}{i}$ denotes the multiplicative inverse of i modulo p.*

Proof. Part (a) is obvious, but that will not stop us giving a proof in Section 4.

(b) The binomial theorem gives $\binom{p-1}{i} = \binom{p}{i} - \binom{p-1}{i-1}$. It follows that

$$\binom{p-1}{i} = \binom{p}{i} - \binom{p}{i-1} + \binom{p}{i-2} - \ldots + (-1)^i \equiv (-1)^i,$$

using (a). Part (c) follows from (b) since $\frac{i}{p}\binom{p}{i} = \binom{p-1}{i-1}$. □

Proof 2 of Theorem 2. By Lemma 1(b), we have

$$(-1)^{\frac{p-1}{2}} \cdot C_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \cdot \frac{2}{p+1}\binom{p-1}{\frac{p-1}{2}} \equiv 2.$$

□

Notice that the above proofs are completely elementary; they do not even use Wilson's theorem. Like Theorem 1, Theorem 2 gives a necessary condition for p to be prime, and like Theorem 1, its converse is false; for example, $C_{2953} \equiv -2 \pmod{5907}$, but 5907 is not prime (being equal to $3 \cdot 11 \cdot 179$). We will call such numbers *Catalan pseudoprimes*. Comparing Theorems 1 and 2, notice that although the computation of the Catalan numbers is quite involved [7], $C_{\frac{p-1}{2}}$ is considerably smaller than 2^p. Moreover, Catalan pseudoprimes seem to be far less common than standard pseudoprimes. Indeed, searching for Catalan pseudoprimes with a computer can be quite discouraging. A more theoretical approach consists in trying to identify Catalan pseudoprimes of a given form, the simplest of all being p^2, where p is prime. In that case the natural question arises as to whether they would also be standard pseudoprimes. The affirmative answer here below is even more precise.

Proposition 1. *If p is an odd prime, then the following numbers are equal modulo p^2:*

(a) $\frac{1}{2} \cdot C_{\frac{p^2-1}{2}}$, (b) $(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}}$, (c) $2^p - 1$, (d) $2^{p^2} - 1$,

(e) $1 + 2p\left(1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2}\right)$, *where $\frac{1}{i}$ denotes the inverse of i modulo p.*

Proof. First note that if $1 \leq i < p^2$ and i is not a multiple of p, then i has an inverse modulo p^2, and $\frac{p^2-i}{i} \equiv -1$. Thus

$$\frac{1}{2} \cdot C_{\frac{p^2-1}{2}} = \frac{1}{p^2+1}\binom{p^2-1}{\frac{p^2-1}{2}} \equiv \binom{p^2-1}{\frac{p^2-1}{2}} = \frac{p^2-1}{1} \cdot \frac{p^2-2}{2} \cdot \frac{p^2-3}{3} \cdots \frac{\frac{p^2+1}{2}}{\frac{p^2-1}{2}}$$

$$\equiv (-1)^{\frac{p^2-p}{2}} \cdot \frac{p^2-p}{p} \cdot \frac{p^2-2p}{2p} \cdot \frac{p^2-3p}{3p} \cdots \frac{p^2-\frac{p-1}{2}p}{\frac{p-1}{2}p}$$

$$= (-1)^{\frac{p^2-p}{2}} \cdot \frac{p-1}{1} \cdot \frac{p-2}{2} \cdot \frac{p-3}{3} \cdots \frac{\frac{p+1}{2}}{\frac{p-1}{2}}$$

$$= (-1)^{\frac{p^2-p}{2}} \cdot \binom{p-1}{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \cdot \binom{p-1}{\frac{p-1}{2}}.$$

So (a) = (b). The claim (b) = (e) can be deduced directly from [20, Theorem 133]. We supply a proof for completeness. We have

$$(-1)^{\frac{p-1}{2}} \cdot \binom{p-1}{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \cdot \frac{p-1}{1} \cdot \frac{p-2}{2} \cdot \frac{p-3}{3} \cdots \frac{p-\frac{p-1}{2}}{\frac{p-1}{2}}$$

$$= \frac{1-p}{1} \cdot \frac{2-p}{2} \cdot \frac{3-p}{3} \cdots \frac{\frac{p-1}{2}-p}{\frac{p-1}{2}}.$$

So, expanding in powers of p,

$$(-1)^{\frac{p-1}{2}} \cdot \binom{p-1}{\frac{p-1}{2}} \equiv 1 - p\Big(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{\frac{p-1}{2}}\Big)$$

$$\equiv 1 - 2p\Big(\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \ldots + \frac{1}{p-1}\Big) \pmod{p^2}.$$

Modulo p, each inverse $\frac{1}{i}$ equals a unique number j with $1 \le j < p$. Thus one has the following fact observed by Cauchy [11, Chap. III]:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} = 1 + 2 + 3 + \ldots + (p-1) = p\frac{p-1}{2} \equiv 0 \pmod{p}. \quad (1)$$

Hence

$$(-1)^{\frac{p-1}{2}} \cdot \binom{p-1}{\frac{p-1}{2}} \equiv 1 + 2p\Big(1 + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{p-2}\Big) \pmod{p^2}.$$

Thus (b) = (e). The equation (e) = (c) was apparently proved by Sylvester [28, Chap. 8A]; it follows from [20, Theorem 132], but once again we supply a proof for completeness. Using Lemma 1(c) and (1), we have modulo p^2,

$$2^p = (1+1)^p = \sum_{j=0}^{p} \binom{p}{j}$$

$$\equiv 2 + p\Big[\Big(\frac{1}{1} + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{p-2}\Big) - \Big(\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \ldots + \frac{1}{p-1}\Big)\Big]$$

$$\equiv 2 + 2p\Big(\frac{1}{1} + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{p-2}\Big) \pmod{p^2}.$$

This gives (e) = (c). Finally, by Theorem 1, $2^p \equiv 2 \pmod{p}$, so modulo p^2, we have $2^p = 2 + xp$, for some $x \in \{0, 1, \ldots, p-1\}$. Thus

$$2^{p^2} = (2^p)^p = (2+xp)^p \equiv 2^p \pmod{p^2}.$$

Hence (c) = (d). □

Recall that if p is prime and $2^p \equiv 2$ modulo p^2, then p is a *Wieferich prime*. 1093 and 3511 are the only known Wieferich primes; there are no other Wieferich primes less than 1.25×10^{15} [21], but at present it is not known whether there are only finitely many Wieferich primes. Wieferich showed in 1909 that if the Fermat equation $x^p + y^p = z^p$ had a solution for an odd prime p not dividing xyz, then the smallest such p is necessarily a Wieferich prime [27]. Notice that the above proposition has the following corollary:

Corollary 1. *If p is prime, then the following are equivalent:*

(a) *p is a Wieferich prime,*

(b) *p^2 is a pseudoprime,*

(c) *p^2 is a Catalan pseudoprime.*

So $1194649 = 1093^2$ and $12327121 = 3511^2$ are examples of Catalan pseudoprimes. Much rarer than standard pseudoprimes, 5907, 1093^2 and 3511^2 are the only Catalan pseudoprimes we are currently aware of.

Remark 1. Notice that by Theorems 1 and 2, when p is prime, $(-1)^{\frac{p-1}{2}} \cdot C_{\frac{p-1}{2}} \equiv 2^p \pmod{p}$. Proposition 1 gives a stronger version of this. Indeed, from Proposition 1 we obtain

$$(-1)^{\frac{p-1}{2}} \cdot C_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \frac{2}{p+1}\binom{p-1}{\frac{p-1}{2}} \equiv \frac{2}{p+1}(2^p - 1) \equiv 2(1-p)(2^p-1) \pmod{p^2}.$$

We remark in passing that an even stronger statement can be deduced from a result of Frank Morley [23]: if $p > 3$ is prime, then

$$(-1)^{\frac{p-1}{2}} \cdot C_{\frac{p-1}{2}} \equiv (1 - p + p^2)2^{2p-1} \pmod{p^3}.$$

For related information, see [14, Lecture 2].

Remark 2. As we saw above, Theorem 2 is a trivial consequence of Lemma 1. Although the converse of Theorem 2 is false, the converse of Lemma 1 is true, as was observed by Leibniz [11, p. 91]: a natural number p is prime if and only if $\binom{p}{i}$ is divisible by p for all $0 < i < p$. Indeed, if n is composite, and q is a prime divisor of n, then $\binom{n}{q}$ is not divisible by n, as one can see by writing

$$\frac{1}{n}\binom{n}{q} = \frac{(n-1)(n-2)\ldots(n-q+1)}{q!}$$

and noting that since q divides n, q does not divide any of the terms in the numerator.

3 Twin primes

There is a twin prime version of Wilson's theorem, known as Clement's theorem [8], that says:

Clement's theorem. *The natural numbers p, $p+2$ are both prime if and only if*

$$4(p-1)! + p + 4 \equiv 0 \pmod{p(p+2)}.$$

Clement's theorem has been rediscovered and generalized by a number of people [25, 4]. In fact, it was discovered by Zahlen a few years before Clement [30]. An alternate expression is given in [9]. There is an obvious "Fermat" version of Clement's theorem, which we have not noticed in the literature:

Theorem 3. *If the natural numbers p, $p+2$ are both prime, then* $2^{p+2} \equiv 3p + 8 \pmod{p(p+2)}$.

Proof. Suppose that p, $p+2$ are both prime. We are required to show that $2^{p+2} \equiv 3p+8 \pmod{p}$ and $2^{p+2} \equiv 3p+8 \pmod{p+2}$. Modulo p, Theorem 1 gives

$$2^{p+2} \equiv 8 \equiv 3p + 8 \qquad \pmod{p},$$

while modulo $p+2$, Theorem 1 gives

$$2^{p+2} \equiv 2 \equiv 3(p+2) + 2 = 3p + 8 \qquad \pmod{p+2},$$

as required. □

The converse to Theorem 3 is false. For example, for $p = 561$, one has $2^{p+2} \equiv 3p + 8 \pmod{p(p+2)}$, but while 561 is prime, 563 is a pseudoprime. Another example is $p = 4369$, where p and $p+2$ are both pseudoprimes.

Nevertheless, in the same way that Fermat's little theorem has a generalization of the form: "p is prime if and only if for every prime $q < p$, $q^{p-1} \equiv 1 \pmod{p}$", Theorem 3 can also be generalized to:

Theorem 4. *The natural numbers p and $p+2$ are both prime, if and only if for all primes $q < p$,* $2q^{p+1} \equiv p(q^2-1) + 2q^2 \pmod{p(p+2)}$.

Theorem 4 can be established in the same way we proved Theorem 3, with the help of little Fermat's extension.

Returning to Catalan numbers, there is a recent twin-prime criterion that is not entirely unrelated to the Catalan numbers [12]. In a different direction, the following observation is directly analogous to Clement's theorem and Theorem 3:

Theorem 5. *If the natural numbers p, $p+2$ are both prime, then*

$$8(-1)^{\frac{p-1}{2}} C_{\frac{p-1}{2}} \equiv 7p + 16 \qquad \pmod{p(p+2)}.$$

Proof. Suppose that p, $p+2$ are both prime. Modulo p, Theorem 2 gives

$$8(-1)^{\frac{p-1}{2}} C_{\frac{p-1}{2}} \equiv 8 \cdot 2 \equiv 7p + 16 \equiv 0 \pmod{p}.$$

One has $C_{\frac{p-1}{2}} = \frac{p+3}{4p} C_{\frac{p+1}{2}}$. So, modulo $p+2$, Theorem 2 gives

$$8(-1)^{\frac{p-1}{2}} C_{\frac{p-1}{2}} = -\frac{p+3}{p} 2(-1)^{\frac{p+1}{2}} C_{\frac{p+1}{2}} \equiv -4\frac{p+3}{p} \equiv 2 \equiv 7p+16 \pmod{p+2},$$

which completes the proof. □

We do not have a counter-example to the converse of Theorem 5; the only Catalan pseudoprimes we currently know are 5907, 1194649 and 12327121, and none of the numbers 5907 ± 2, 1194649 ± 2, 12327121 ± 2 is prime.

Remark 3. Using Lemma 1 and Remark 2, it is not difficult to establish the following: the natural numbers p, $p+2$ are both prime if and only if

$$(-1)^{i+1}\binom{p}{i} \equiv \frac{i+1}{2} p \pmod{p(p+2)}, \qquad \text{for all } 0 < i < p.$$

4 A door ajar?

The connection between primes and Catalan numbers opens the door (however narrowly) to possible connections between primes and various combinatorial problems. There are precedents for this sort of thing. There is a geometric proof of Fermat's little theorem; see [3, Ch. 3.2]. Here is one way of seeing it. Consider the possible black-white colourings of the vertices of a regular p-gon. There are 2^p such colourings. The cyclic group $\mathbb{Z}_p$ acts by rotation on the polygon and hence on the set of colourings. There are two colourings fixed by this action (all black and all white), and for p prime, the $\mathbb{Z}_p$-action is free on the set of the $2^p - 2$ other colourings. Thus $2^p - 2 \equiv 0 \pmod{p}$, which proves Theorem 1.

There are other elementary results that can be established in a similar manner. For example, there are $\binom{p}{i}$ colourings of the above kind in which exactly i vertices are coloured black. For p prime and $0 < i < p$, the $\mathbb{Z}_p$-action on these colourings is obviously free, so $\binom{p}{i} \equiv 0 \pmod{p}$, which proves Lemma 1(a).

Lemma 1(a) is admittedly trivial, being immediate from the definition $\binom{p}{i} = \frac{p!}{(p-i)!i!}$. However, the same idea can be used to give a more interesting result. Consider the regular mp-gon, where $m \in \mathbb{N}$. The vertices can be grouped into p lots of m consecutive vertices, which one can regard as forming the sides of a p-gon. Now consider the possible black-white colourings of i vertices of the mp-gon. The action of $\mathbb{Z}_p$ is once again free outside the fixed points. The colourings that are fixed by the action are just those colourings that are identical on each edge of the p-gon. So one has immediately:

Proposition 2. *If p is prime, then for all $m \in \mathbb{N}$*

(a) $\binom{pm}{i} \equiv 0 \pmod{p}$ *if* $i \not\equiv 0 \pmod{p}$,

(b) $\binom{pm}{pi} \equiv \binom{m}{i} \pmod{p}$ *for all* $i \in \mathbb{N}$.

From Proposition 2 we can quickly deduce Lucas' theorem [22, Section XXI]:

Lucas' theorem. *If p is prime and $0 \leq n, j < p$, then $\binom{pm+n}{pi+j} \equiv \binom{m}{i}\binom{n}{j} \pmod{p}$.*

Proof. By Proposition 2(a) we can assume that $n > 0$. Then for the case $j = 0$,

$$\binom{pm+n}{pi} = \frac{pm+n}{p(m-i)+n}\binom{pm+n-1}{pi} \equiv \binom{pm+n-1}{pi} \pmod{p},$$

and the result follows by induction on n. For $j \neq 0$,

$$\binom{pm+n}{pi+j} = \frac{pm+n}{pi+j}\binom{pm+n-1}{pi+j-1} \equiv \frac{n}{j}\binom{pm+n-1}{pi+j-1} \pmod{p},$$

and again the required is obtained by induction on n. □

5 Back to the middle binomial coefficient

For convenience, let us introduce the following notation:

$$\gamma_n := (-1)^{\frac{n-1}{2}}\binom{n-1}{\frac{n-1}{2}},$$

for odd n. Theorem 2 can be rephrased as follows: if p is an odd prime, then $\gamma_p \equiv 1 \pmod{p}$. The equation (a) = (b) of Proposition 1 can be rewritten as follows: if p is an odd prime, then $\gamma_{p^2} \equiv \gamma_p \pmod{p^2}$. One also has:

Lemma 2.

(a) *If p is an odd prime, then $\gamma_{mp} \equiv \gamma_m \pmod{p}$ for all odd $m \in \mathbb{N}$.*

(b) *If p, q are distinct odd primes, then $\gamma_{pq} \equiv \gamma_p\gamma_q \equiv \gamma_p + \gamma_q - 1 \pmod{pq}$.*

(c) *If p is an odd prime, then for all odd $n \leq p$, $\gamma_n \not\equiv 0$ and $\gamma_n \equiv 2^{2(n-1)}\gamma_{p-n+1} \pmod{p}$.*

Proof. (a) Arguing as in the proof of Lemma 1(b), one has for all i

$$(-1)^i\binom{mp-1}{i} = 1 - \binom{mp}{1} + \binom{mp}{2} - \ldots + (-1)^i\binom{mp}{i}$$

and so by Proposition 2,

$$(-1)^i\binom{mp-1}{i} \equiv 1 - \binom{m}{1} + \binom{m}{2} - \ldots + (-1)^j\binom{m}{j} \pmod{p}$$

where $j = \left\lfloor \frac{i}{p} \right\rfloor$. For $i = \frac{mp-1}{2}$ one has $\left\lfloor \frac{i}{p} \right\rfloor = \left\lfloor \frac{mp-1}{2p} \right\rfloor = \frac{m-1}{2}$. So

$$(-1)^i\binom{mp-1}{\frac{mp-1}{2}} \equiv 1 - \binom{m}{1} + \binom{m}{2} - \ldots + (-1)^{\frac{m-1}{2}}\binom{m}{\frac{m-1}{2}} = (-1)^{\frac{m-1}{2}}\binom{m-1}{\frac{m-1}{2}}.$$

That is, $\gamma_{mp} \equiv \gamma_m \pmod{p}$.

(b) Suppose that p, q are distinct odd primes. From part (a), $\gamma_{pq} \equiv \gamma_q \pmod{p}$. So, as $\gamma_p \equiv 1 \pmod{p}$, we have $\gamma_{pq} \equiv \gamma_p\gamma_q \pmod{p}$. Similarly, $\gamma_{pq} \equiv \gamma_p\gamma_q \pmod{q}$. Thus $\gamma_{pq} \equiv \gamma_p\gamma_q \pmod{pq}$. Furthermore, since $\gamma_p - 1 \equiv 0 \pmod{p}$ and $\gamma_q - 1 \equiv 0 \pmod{q}$, one has $(\gamma_p - 1)(\gamma_q - 1) \equiv 0 \pmod{pq}$, and so $\gamma_p\gamma_q \equiv \gamma_p + \gamma_q - 1 \pmod{pq}$, as required.

(c) First notice that for all odd $i > 1$

$$(-1)^{\frac{i-1}{2}}\gamma_i = \binom{i-1}{\frac{i-1}{2}} = 4\frac{i-2}{i-1}\binom{i-3}{\frac{i-3}{2}} = 4\frac{i-2}{i-1}(-1)^{\frac{i-3}{2}}\gamma_{i-2}.$$

Hence

$$\gamma_i = -4\frac{i-2}{i-1}\gamma_{i-2}. \tag{2}$$

Now we prove (c) by induction on n. For $n = 1$ it is obvious, so let $n > 1$. Using (2) first and the induction hypotheses we obtain

$$\begin{aligned}
\gamma_n &\equiv -4\frac{n-2}{n-1}2^{2(n-3)}\gamma_{p-n+3} \pmod{p} \\
&= 4\frac{n-2}{n-1}2^{2(n-3)}4\frac{p-n+1}{p-n+2}\gamma_{p-n+1} \qquad \text{(using (2) again)} \\
&= \frac{n-2}{n-1}\cdot\frac{p-n+1}{p-n+2}2^{2(n-1)}\gamma_{p-n+1} \\
&\equiv 2^{2(n-1)}\gamma_{p-n+1} \pmod{p}.
\end{aligned}$$

□

Remark 4. It is not true that $\gamma_{pqr} \equiv \gamma_p\gamma_q\gamma_r \pmod{pqr}$ for all distinct primes p, q, r. For example, $\gamma_{105} \not\equiv \gamma_3\gamma_5\gamma_7 \pmod{105}$.

Notice that from the definition, a composite number n is a Catalan pseudoprime if and only if $\gamma_n \equiv 1 \pmod{n}$. Further, one has:

Proposition 3. *If p, q are distinct odd primes, then pq is a Catalan pseudoprime if and only if $\gamma_q \equiv 1 \pmod{p}$ and $\gamma_p \equiv 1 \pmod{q}$.*

Proof. If pq is a Catalan pseudoprime, then $\gamma_{pq} \equiv 1 \pmod{pq}$. In particular, $\gamma_{pq} \equiv 1 \pmod{p}$. So by Lemma 2(a), $\gamma_p\gamma_q \equiv 1 \pmod{p}$. But as p is prime, $\gamma_p \equiv 1 \pmod{p}$. Hence $\gamma_q \equiv 1 \pmod{p}$. By the same reasoning, $\gamma_p \equiv 1 \pmod{q}$.

Conversely, if $\gamma_p \equiv 1 \pmod{q}$ and $\gamma_p \equiv 1 \pmod{q}$, then as p, q are distinct primes, $\gamma_p \equiv 1 \pmod{pq}$. Similarly, $\gamma_q \equiv 1 \pmod{pq}$ and so by Lemma 2(b), $\gamma_{pq} \equiv 1 \pmod{pq}$. □

The above considerations enable one to show that if p, q are prime with $p < q$ and either p or $q - p$ is quite small, then pq is not a Catalan pseudoprime. To give a trivial example of this, we prove:

Corollary 2. *There are no Catalan pseudoprimes of the form $p(p + 2)$, where p, $p + 2$ are twin primes.*

Proof. If p, $p+2$ are primes, then by Lemma 2(c), $\gamma_p \equiv 2^{2(p-1)}\gamma_3 \pmod{p+2}$. One has $\gamma_3 = -2$ and by Fermat's little theorem, $2^{2(p-1)} \equiv 2^{-4} \pmod{p+2}$. So $\gamma_p \equiv -2^{-3} \pmod{p+2}$. If $p(p+2)$ was a Catalan pseudoprime, then by Proposition 3 we would have $\gamma_p \equiv 1 \pmod{p+2}$ and thus $-2^{-3} \equiv 1 \pmod{p+2}$, i.e., $p+2 = 9$ contradicting the assumption that $p+2$ is prime. □

We now come to the main result of this paper, which enables one to reduce the calculation of $\gamma_n \pmod{p}$ to the case where $n < p$.

Theorem 6. *If p is an odd prime, then for all odd $n \in \mathbb{N}$,*

$$\gamma_n \equiv \begin{cases} 0; & \lfloor n/p \rfloor \text{ odd and } n \text{ not a multiple of } p, \\ \gamma_{n/p}; & \lfloor n/p \rfloor \text{ odd and } n \text{ a multiple of } p, \\ \gamma_{\lfloor n/p \rfloor + 1} \cdot \gamma_{n - p\lfloor n/p \rfloor}; & \lfloor n/p \rfloor \text{ even.} \end{cases} \pmod{p}$$

Proof. If $\lfloor n/p \rfloor$ is odd and n a multiple of p, then n has the form mp where m is odd, and Lemma 2(a) gives the required result.

If $\lfloor n/p \rfloor$ is odd and n is not a multiple of p, then n has the form $mp + 2i$ where m is odd and $0 < i < p/2$. By induction,

$$\gamma_{mp+2i} = -4\frac{mp + 2(i-1)}{mp + 2(i-1) + 1}\gamma_{mp+2(i-1)} \equiv 0 \pmod{p}.$$

and for $i = 1$, equation (2) gives:

$$\gamma_{mp+2} = -4\frac{mp}{mp+1}\gamma_{mp} \equiv 0 \pmod{p}.$$

If $\lfloor n/p \rfloor$ is even, then n has the form $mp - 2i$ where m is odd and $0 < i < p/2$. Applying equation (2) i times gives:

$$\begin{aligned} \gamma_{mp} &= (-4)^i \cdot \frac{mp-2}{mp-1} \cdot \frac{mp-4}{mp-3} \cdots \frac{mp-2i}{mp-2i+1}\gamma_{mp-2i} \\ &\equiv (-1)^i \cdot 2^{2i} \cdot \frac{2}{1} \cdot \frac{4}{3} \cdots \frac{2i}{2i-1}\gamma_{mp-2i} \pmod{p}. \end{aligned}$$

Hence, since $\gamma_{mp} \equiv \gamma_m \pmod{p}$ by Lemma 2(a), we have:

$$\gamma_{mp-2i} \equiv (-1)^i \cdot 2^{-2i}\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2i-1}{2i}\gamma_m \pmod{p}. \tag{3}$$

Notice that by definition

$$\gamma_{2i+1} = (-1)^i\binom{2i}{i} = (-1)^i\frac{(2i)!}{(i!)^2} = (-1)^i 2^{2i}\frac{1}{2}\frac{3}{4} \cdots \frac{2i-1}{2i}.$$

So, from equation (3), $\gamma_{mp-2i} \equiv 2^{-4i}\gamma_{2i+1}\gamma_m \pmod{p}$. Thus, by Lemma 2(c), $\gamma_{mp-2i} \equiv \gamma_{p-2i}\gamma_m \pmod{p}$. That is, $\gamma_n \equiv \gamma_{\lfloor n/p \rfloor + 1} \cdot \gamma_{n - p\lfloor n/p \rfloor} \pmod{p}$, as required. □

Remark 5. Theorem 6 can be alternatively deduced from Lucas' theorem. We mention also that the blocks of zeros where $\lfloor q/p \rfloor$ is odd and q is not a multiple of p, has also been observed for the Catalan numbers [2].

Using Theorem 6 and Proposition 3, our calculations show that there are no Catalan pseudoprimes less than 10^{10} of the form pq, where p, q are distinct primes.

Notice that Theorem 6(a) gives a considerable extension of Corollary 2. Indeed, if p, q are prime and $p < q < 2p$, then by Theorem 6, $\gamma_q \equiv 0 \pmod{p}$ and so pq is not a Catalan pseudoprime, by Proposition 3. The first possible case would therefore seem to be the situation where $q = 2p + 1$, but in fact there are no Catalan pseudoprimes of this form either:

Corollary 3. *There are no Catalan pseudoprimes of the form pq, where p, $q = 2p + 1$ is a Sophie Germain pair.*

Proof. Otherwise for $q = 2p + 1$, Theorem 6 gives $\gamma_q \equiv \gamma_3 \cdot \gamma_1 \equiv -2 \pmod{p}$. But Proposition 3 implies $\gamma_q \equiv 1 \pmod{p}$. Hence $p = 3$ and $q = 7$. Again by Proposition 3 we would have $\gamma_p \equiv 1 \pmod{q}$, but $\gamma_3 = -2 \not\equiv 1 \pmod{7}$. □

References

[1] Adams, W.W.; Goldstein, L.J.: *Introduction to number theory*, Prentice-Hall Inc., Englewood Cliffs, NJ, 1976.

[2] Alter, R.; Kubota, K.K.: Prime and prime power divisibility of Catalan numbers. *J. Combin. Theory Ser. A* 15 (1973), 243–256.

[3] Andrews, G.E.: *Number theory*. Dover Publications Inc., New York, 1994. Corrected reprint of the 1971 original [Dover, New York].

[4] Avanesov, È.T.: On a generalization of the Leibniz theorem. *Fiz.-Mat. Spis.* 8 (41) (1965), 44–45.

[5] Berend, D.; Harmse, J.E.: On some arithmetical properties of middle binomial coefficients. *Acta Arith.* 84 (1998) 1, 31–41.

[6] Bezhanishvili, G.; Leung, H.; Lodder, J.; Pengelley, D.; Ranjan, D.: Counting triangulations of a polygon. Teaching Discrete Mathematics via Primary Historical Sources Website, http://www.math.nmsu.edu/hist_projects/, New Mexico State University, downloaded 12.12.2007.

[7] Campbell, D.M.: The computation of Catalan numbers. *Math. Mag.* 57 (1984) 4, 195–208.

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

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

[10] Deutsch, E.; Sagan, B.E.: Congruences for Catalan and Motzkin numbers and related sequences. *J. Number Theory* 117 (2006) 1, 191–215.

[11] Dickson, L.E.: *History of the theory of numbers. Vol. I: Divisibility and primality.* Chelsea Publishing Co., New York, 1966.

[12] Dilcher, K.; Stolarsky, K.B.: A Pascal-type triangle characterizing twin primes. *Amer. Math. Monthly* 112 (2005) 8, 673–681.

[13] Erdős, P.: On some divisibility properties of $\binom{2n}{n}$. *Canad. Math. Bull.* 7 (1964), 513–518.

[14] Fuchs, D.; Tabachnikov, S.: *Mathematical omnibus*. Amer. Math. Soc., Providence, RI, 2007.

[15] Granville, A.: Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle. *Amer. Math. Monthly* 99 (1992) 4, 318–331.

[16] Granville, A.: *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*. Organic mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, 253–276.

[17] Granville, A.: Correction to: "Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle" [15]. *Amer. Math. Monthly* 104 (1997) 9, 848–851.

[18] Granville, A.: It is easy to determine whether a given integer is prime. *Bull. Amer. Math. Soc. (N.S.)* 42 (2005) 1, 3–38 (electronic).

[19] Granville, A.; Ramaré, O.: Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients. *Mathematika* 43 (1996) 1, 73–107.

[20] Hardy, G.H.; Wright, E.M.: *An introduction to the theory of numbers*. Fifth ed., The Clarendon Press Oxford University Press, New York, 1979.

[21] Knauer, J.; Richstein, J.: The continuing search for Wieferich primes. *Math. Comp.* 74 (2005) 251, 1559–1563 (electronic).

[22] Lucas, E.: Théorie des Fonctions Numériques Simplement Périodiques. *Amer. J. Math.* 1 (1878), 184–240, 289–321.

[23] Morley, F.: Note on the congruence $2^{4n} \equiv (-)^n (2n)!/(n!)^2$, where $2n + 1$ is a prime. *Ann. of Math.* 9 (1894/95) 1-6, 168–170.

[24] Ore, O.: *Number Theory and Its History*. McGraw-Hill Book Company, Inc., New York, 1948.

[25] Pellegrino, F.: Teorema di Wilson e numeri primi gemelli. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend.* (8) 35 (1963), 258–262.

[26] Reid, C.: *From zero to infinity*. Fifth ed., A K Peters Ltd., Wellesley, MA, 2006.

[27] Ribenboim, P.: *13 lectures on Fermat's last theorem* Springer-Verlag, New York, 1979.

[28] Ribenboim, P.: *My numbers, my friends*. Springer-Verlag, New York, 2000.

[29] Stanley, R.P.: *Enumerative combinatorics*. Vol. 2, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, Cambridge, 1999.

[30] Zahlen, J.P.: Sur un genre nouveau de critères de primalité. *Euclides (Madrid)* 6 (1946) 64, 380–387.

Christian Aebi
Collège Calvin
CH–1211 Geneva, Switzerland
e-mail: christian.aebi@edu.ge.ch

Grant Cairns
Department of Mathematics
La Trobe University
Melbourne, Australia 3086
e-mail: G.Cairns@latrobe.edu.au