Supercongruences for the Catalan-Larcombe-French numbers

Frazer Jarvis
Department of Pure Mathematics
University of Sheffield, Sheffield S3 7RH, U.K.
a.f.jarvis@shef.ac.uk

Helena A. Verrill
Department of Mathematics
Louisiana State University, Baton Rouge, Louisiana 70803-4918, USA
verrill@math.lsu.edu

November 30, 2009

Abstract

In this short note, we develop the Stienstra-Beukers theory of supercongruences in the setting of the Catalan-Larcombe-French sequence. We also give some applications to other sequences.

AMS Subject Classification: 11B83, 11B65, 11F30, 33E05

1 Introduction

The Catalan-Larcombe-French numbers P_n for $n \geq 0$ were first defined by Catalan in [4, Section 9, p. 195], in terms of the "Segner numbers". Catalan stated that the P_n could be defined by the recurrence relation:

$$n^2 P_n - 8(3n^2 - 3n + 1)P_{n-1} + 128(n-1)^2 P_{n-2} = 0 \qquad (1)$$

for $n \geq 2$, with the initial values given by $P_0 = 1$, $P_1 = 8$.

Larcombe and French [12] give a detailed account of properties of the P_n, and obtained [12, Equations (23) and (35)] the following formulas for these numbers:

$$P_n = 2^n \sum_{i=0}^{\lfloor n/2 \rfloor} (-4)^i \binom{2(n-i)}{n-i}^2 \binom{n-i}{i}, \qquad (2)$$

and

$$P_n = \frac{1}{n!} \sum_{r+s=n} \binom{2r}{r}\binom{2s}{s} \frac{(2r)!(2s)!}{r!s!} = \sum_{r+s=n} \binom{2r}{r}^2 \binom{2s}{s}^2 \Big/ \binom{n}{r}. \qquad (3)$$

for $n \geq 0$. These numbers occur in the theory of elliptic integrals [12], and there are relations to the arithmetic-geometric-mean [10]. The first few P_n are $1, 8, 80, 896, 10816, 137728$. This is sequence A053175 in Sloane's database [15].

Throughout this paper, p will denote an odd prime.

In an earlier paper [11, Theorem 7, p.16], the first author proved the following:

Proposition 1.1. *If we write $n = a_d a_{d-1} \dots a_0$ in base p, then*

$$P_n \equiv P_{a_d} P_{a_{d-1}} \dots P_{a_0} \pmod{p}.$$

This implies, for example, that no P_n is ever divisible by 3 (as none of P_0, P_1 or P_2 are), or that P_n is divisible by 5 if and only if n has a 2 in its base 5 representation. Surprisingly, the stronger result that the 5-adic valuation $v_5(P_n)$ (i.e., the power of 5 dividing P_n) is equal to the number of 2s in this base 5 representation also seems to be true, but we have no explanation for this.

Further, it was observed empirically in [11, Conjectures 3 and 4, p.19] that

Claim 1.2. *Suppose that p is an odd prime, and that $0 \le n \le p-1$. Then*

1. *$p|P_n$ if and only if $p|P_{p-1-n}$.*
2. *$p|P_{\frac{p-1}{2}}$ if and only if $p \equiv 5 \pmod{8}$ or $p \equiv 7 \pmod{8}$.*

In this article, we prove Claim 1.2 (Corollaries 2.2 and 2.3 and Remark 2.4) and furthermore, we prove the following

Theorem 1.3. $P_{mp^r} \equiv P_{mp^{r-1}} \pmod{p^r}$.

In fact, the proofs of the results in the claim are mostly entirely elementary, and follow from the symmetry of the recurrence relation modulo p when n is replaced with $p-1-n$, as we explain briefly in Section 2 below. In Section 4 we use the theory developed by Stienstra-Beukers [16] and others to prove the mod p^r congruences. In Section 5, we show how to also obtain these congruences using results of Granville.

We thank the anonymous referee for valuable comments on the first draft of this paper.

2 Symmetry of the recurrence relation

2.1 Symmetries for the Catalan-Larcombe-French sequence

As stated in the Introduction, the P_n may be defined by the recurrence relation

$$n^2 P_n - 8(3n^2 - 3n + 1)P_{n-1} + 128(n-1)^2 P_{n-2} = 0$$

for $n \ge 2$, with the initial values given by $P_0 = 1$, $P_1 = 8$. In this section we will regard this as defining a sequence $P_0, P_1, \dots, P_{p-1}$ modulo p. (Of course, we cannot determine P_p modulo p from this relation owing to the coefficient of p^2 when we put $n = p$. However, Proposition 1.1 already tells us that $P_p \equiv P_1 \pmod{p}$, as p is written 10 in base p.)

First shift the variable:

$$(n+1)^2 P_{n+1} - 8(3n^2 + 3n + 1)P_n + 128n^2 P_{n-1} = 0$$

This recurrence relation has a lot of symmetry when regarded modulo a prime number p. Indeed, let us write $m = p - 1 - n$, and reduce modulo p. Then

$$m^2 P_{p-m} - 8(3m^2 + 3m + 1)P_{p-1-m} + 128(m + 1)^2 P_{p-2-m} \equiv 0 \pmod{p}.$$

Multiply throughout by 128^m:

$$128^m m^2 P_{p-m} - 128^m 8(3m^2+3m+1)P_{p-1-m} + 128^m 128(m+1)^2 P_{p-2-m} \equiv 0 \pmod{p},$$

and put $Q_m = 128^m P_{p-1-m}$. Then

$$128m^2 Q_{m-1} - 8(3m^2 + 3m + 1)Q_m + (m + 1)^2 Q_{m+1} \equiv 0 \pmod{p}.$$

We conclude that (Q_n) satisfies the same recurrence relation as (P_n) (at least, modulo p).

Lemma 2.1. *$P_{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ and $16P_{p-2} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$.*

Proof. In expression (3)

$$P_n = \frac{1}{n!} \sum_{r+s=n} \binom{2r}{r}\binom{2s}{s} \frac{(2r)!(2s)!}{r!s!},$$

put $n = p - 1$; all the terms except that with $r = s = \frac{p-1}{2}$ are clearly divisible by p. So

$$\begin{aligned} P_{p-1} &\equiv \frac{1}{(p-1)!}\binom{p-1}{\frac{p-1}{2}}^2 \frac{[(p-1)!]^2}{[(\frac{p-1}{2})!]^2} \\ &\equiv \frac{[(p-1)!]^3}{[(\frac{p-1}{2})!]^6} \pmod{p}. \end{aligned}$$

By Wilson's Theorem, $(p - 1)! \equiv -1 \pmod{p}$, and it is easy to see that $[(\frac{p-1}{2})!]^2 \equiv -(-1)^{\frac{p-1}{2}}$. This gives the result for P_{p-1}.

To get the result for P_{p-2}, we use the recurrence relation

$$(n + 1)^2 P_{n+1} - 8(3n^2 + 3n + 1)P_n + 128n^2 P_{n-1} = 0;$$

put $n = p - 1$ and reduce mod p:

$$-8P_{p-1} + 128P_{p-2} \equiv 0 \pmod{p},$$

which gives the value in the statement. □

Corollary 2.2.

$$128^n P_{p-1-n} \equiv (-1)^{\frac{p-1}{2}} P_n \pmod{p} \tag{4}$$

for all n such that $0 \le n \le p - 1$. In particular, $p|P_n$ if and only if $p|P_{p-1-n}$.

Proof. By definition of the Q_n and Lemma 2.1 it follows that $Q_0 = P_{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$, and $Q_1 = 128P_{p-2} \equiv (-1)^{\frac{p-1}{2}} 8 \pmod{p}$. Consequently, mod p, the values of Q_0 and Q_1 are identical to those of P_0 and P_1, except for the scaling factor of $(-1)^{\frac{p-1}{2}}$. Since (Q_n) and (P_n) also satisfy the same recurrence relation, we conclude that $Q_n \equiv (-1)^{\frac{p-1}{2}} P_n \pmod{p}$ for all n such that $0 \le n \le p - 1$. Substituting in the definition of Q_n, we deduce (4). □

Corollary 2.3. *If $p \equiv 5 \pmod 8$ or $p \equiv 7 \pmod 8$, then $p | P_{\frac{p-1}{2}}$.*

Proof. The central point of the symmetry (4) is when $n = \frac{p-1}{2}$. In this case, Corollary 2.2 gives:

$$128^{\frac{p-1}{2}} P_{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} P_{\frac{p-1}{2}} \pmod p.$$

So if $P_{\frac{p-1}{2}} \not\equiv 0 \pmod p$ then $(-128)^{\frac{p-1}{2}} \equiv 1 \pmod p$. This occurs when $(\frac{-128}{p}) = (\frac{-2}{p}) = 1$, so -2 is a quadratic residue, which means that $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$. The contrapositive gives the result. □

Remark 2.4. Using much more sophisticated techniques, Beukers and Stienstra [16] prove that if $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$, so that $p = a^2 + 2b^2$ for some a and b, then

$$P_{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} 4a^2 \pmod p.$$

In particular, $P_{\frac{p-1}{2}} \not\equiv 0 \pmod p$. Thus the converse to Corollary 2.3 also holds.

2.2 Symmetries for other sequences

Recall that in [11], it is noted that $P_{\frac{p-1}{2}}$ is divisible by p if and only if the *Franel number* $f_{\frac{p-1}{2}}$ is divisible by p (indeed, they are congruent modulo p). Here, $f_n = \sum_{r=0}^{n} \binom{n}{r}^3$.

Corollary 2.5. *Suppose that p is an odd prime. Then*

$$\sum_{r=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{r}^3 \equiv 0 \pmod p \iff p \equiv 5 \pmod 8 \text{ or } p \equiv 7 \pmod 8.$$

Of course, the method of proof of Corollary 2.2 also applies to other similar recurrence relations, and it turns out that the Franel numbers furnish another example. As was proven by Cusick [6], the Franel numbers also satisfy a recurrence relation:

$$(n+1)^2 f_{n+1} = (7n^2 + 7n + 2) f_n + 8n^2 f_{n-1},$$

with $f_0 = 1$, $f_1 = 2$. In exactly the same way as above, one can prove

Lemma 2.6. *$f_n \equiv (-8)^n f_{p-1-n} \pmod p$ for all n such that $0 \le n \le p-1$. In particular, $p | f_n$ if and only if $p | f_{p-1-n}$.*

Indeed, this follows from a similar symmetry argument, once we verify this for $n = 0$ and $n = 1$:

$$f_{p-1} = \left(\binom{p-1}{0}^3 + \binom{p-1}{1}^3 \right) + \cdots + \binom{p-1}{p-1}^3$$

and any two consecutive terms in the sum is the sum of two cubes, and is therefore divisible by the sum of the two numbers. In particular,

$$\binom{p-1}{r}^3 + \binom{p-1}{r+1}^3$$

is divisible by

$$\binom{p-1}{r} + \binom{p-1}{r+1} = \binom{p}{r+1},$$

which is divisible by p. There are an odd number of terms in the sum; pairing terms off just leaves one term mod p, $f_{p-1} \equiv \binom{p-1}{p-1}^3$, say, so $f_{p-1} \equiv 1 \equiv f_0 \pmod p$. Reducing the recurrence relation mod p, we get $f_{p-1} + 4f_{p-2} \equiv 0 \pmod p$, so that $(-8)f_{p-2} \equiv 2 \equiv f_1 \pmod p$. The result then follows with a similar argument to Corollary 2.2.

Other series in Table 7 of Stienstra and Beukers [16] can also be treated in the same way. We summarise the results:

Lemma 2.7. *1. Define* $a_n = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}$ *so that*

$$(n+1)^2 a_{n+1} = (11n^2 + 11n + 3)a_n + n^2 a_{n-1}.$$

Then for any prime p*, and* $0 \le n \le p-1$*,*

$$a_n \equiv (-1)^n a_{p-1-n} \pmod p.$$

2. Define $b_n = \sum_{k=0}^n \binom{n}{k}^2 \binom{2k}{k}$ *so that*

$$(n+1)^2 b_{n+1} = (10n^2 + 10n + 3)b_n - 9n^2 b_{n-1}.$$

Then for any prime $p > 3$*, and* $0 \le n \le p-1$*,*

$$b_n \equiv \left(\frac{-3}{p}\right) 9^n b_{p-1-n} \pmod p.$$

3 The Picard-Fuchs equation

To say more about the P_n, we will apply the theory of Beukers and others; we wish to view the numbers P_n as the coefficients for a generating function which satisfies a certain differential equation. We then want to interpret this differential equation as a Picard-Fuchs equation for a pencil of elliptic curves.

Lemma 3.1. *The function* $\mathbf{P}(x) = \sum_{n=0}^\infty P_n x^n$ *is a solution to the second order differential equation*

$$(1-16x)(1-8x)x\frac{d^2y}{dx^2} + (384x^2 - 48x + 1)\frac{dy}{dx} - 8(1-16x)y = 0. \tag{5}$$

Proof. This follows easily from the recurrence relation for the numbers P_n. □

Remark 3.2. An alternative proof of Lemma 3.1 can be obtained by writing the generating function $\mathbf{P}(x)$ in terms of a certain elliptic integral $K(c)$ given in [3], §1.5, and using the differential equation for $K(c)$ given in [3].

We now wish to view (5) as a Picard-Fuchs equation for a pencil of elliptic curves. It turns out that a very similar equation has already appeared in a paper of the second author [17]. Indeed, on line 6, Table 6 of [17], we see that the equation

$$t(4t-1)(8t-1)f'' + (96t^2 - 24t + 1)f' + 4(8t-1)f = 0 \tag{6}$$

is the Picard-Fuchs differential equation for the family of elliptic curves with level 8 structure, with choice of uniformizing parameter

$$t(\tau) = \frac{\eta(\tau)^4\eta(4\tau)^2\eta(8\tau)^4}{\eta(2\tau)^{10}}, \tag{7}$$

a weight 0 modular function for $\Gamma_0(8)$, where η is the Dedekind eta function, defined by

$$\eta(\tau) = q^{1/24}\prod_{n\geq 1}(1-q^n),$$

and $q = \exp(2\pi i\tau)$.

The Picard-Fuchs equation is the equation satisfied by the period of this family of curves, and this is given by the weight 1 modular form of $\Gamma_0(4)$, given by

$$f(\tau) = \frac{\eta(2\tau)^{10}}{\eta(\tau)^4\eta(4\tau)^4}. \tag{8}$$

In view of the above discussion, we have the following

Theorem 3.3. *Let f and t be defined by*

$$\begin{aligned}
t(\tau) &= \frac{1}{2}\frac{\eta(\tau)^4\eta(4\tau)^2\eta(8\tau)^4}{\eta(2\tau)^{10}} \\
&= \tfrac{1}{2}q - 2q^2 + 6q^3 - 16q^4 + 39q^5 - 88q^6 + 188q^7 - 384q^8 + \tfrac{1509}{2}q^9 - 1436q^{10} + \cdots \\
f(\tau) &= \frac{\eta(2\tau)^{10}}{\eta(\tau)^4\eta(4\tau)^4} \\
&= 1 + 4q + 4q^2 + 4q^4 + 8q^5 + 4q^8 + 4q^9 + 8q^{10} + 8q^{13} + \cdots .
\end{aligned}$$

Then in a neighbourhood of $\tau = i\infty$, we have

$$\sum_{n\geq 0} P_n t(\tau)^n = f(\tau).$$

Proof. This follows from the results given in [17], and from the fact that equation (5) given in Lemma 3.1 can be obtained from (6) by setting $y = f$ and $t = 2x$. □

4 Supercongruences via the method of Stienstra-Beukers

Work on the Picard-Fuchs equation by Stienstra and Beukers [16] led to higher congruences ("supercongruences") for various quantities defined by similar recurrence relations. We wish to explore whether there are similar supercongruences for the P_n from this general theory.

For convenience, we first give a simple result:

Lemma 4.1. *If $t(u)$ is a polynomial in $\mathbb{Z}[u]$, then for a prime p and integer $k \geq 0$ we have*

$$t^{p^k}(u^p) \equiv t^{p^{k+1}}(u) \pmod{p^{k+1}}$$

Proof. We prove the result by induction on k.

$$t(u^p) \equiv t(u)^p \pmod{p} \tag{9}$$

i.e., the result holds for $k = 0$. Now suppose $t^{p^{k-1}}(u^p) \equiv t^{p^k}(u) \pmod{p^k}$ for some $k \geq 1$, i.e.,

$$t^{p^{k-1}}(u^p) = t^{p^k}(u) + p^k f(u)$$

for some polynomial $f(u) \in \mathbb{Z}[u]$. Taking pth powers of both sides we get

$$t^{p^k}(u^p) = (t^{p^k}(u) + p^k f(u))^p = t^{p^{k+1}}(u) + \sum_{i=1}^{p} \binom{p}{i} p^{ik} t^{p^k(p-i)}(u) f^i(u).$$

When $i = 1$, the summand is divisible by $\binom{p}{1} p^k = p^{k+1}$, and for $i > 1$, the summand is divisible by p^{ik}, with $ik \geq 2k \geq k+1$, since $k \geq 1$. Hence the result follows. □

The next result, following the method of Beukers, is a variant of [2, Proposition 3].

Proposition 4.2. *Let t be the power series*

$$t = \frac{1}{m} \sum_{n \geq 1} a_n u^{n/v},$$

convergent in a neighbourhood of $u = 0$, with m, v positive integers, $a_n \in \mathbb{Z}$ and $a_1 = 1$. Suppose that in some neighbourhood of $u = 0$ we have an equality of convergent power series given by

$$\sum_{n \geq 1} b_n t^{n-1} dt = \sum_{n \geq 1} c_n u^{n-1} du, \tag{10}$$

for some integers b_n and c_n, $n \geq 1$.

Assume p is a prime not dividing m or v. Then if

$$b_{mp^r} \equiv b_{mp^{r-1}} \pmod{p^r}, \tag{11}$$

then we also have

$$c_{mp^r} \equiv c_{mp^{r-1}} \pmod{p^r}. \tag{12}$$

Proof. By [18, Proposition 1.1] the congruence (11) is equivalent to

$$\Omega(t) - \frac{1}{p}\Omega(t^p) = d\theta(t) \tag{13}$$

where $\Omega(t) = \sum_{n \geq 1} b_n t^{n-1} dt$ and $\theta(t) \in \mathbb{Z}_p[[t]]$ (where $\mathbb{Z}_p$ denotes the p-adic integers), and (12) is equivalent to

$$\tilde{\Omega}(u) - \frac{1}{p}\tilde{\Omega}(u^p) = d\tilde{\theta}(u) \tag{14}$$

where $\tilde{\Omega}(u) = \sum_{n \geq 1} c_n u^{n-1} du$ and $\tilde{\theta}(u) \in \mathbb{Z}_p[[u]]$.

We can write Ω and $\tilde{\Omega}$ as

$$\Omega(t) = df(t) \qquad \text{and} \qquad \tilde{\Omega}(u) = d\tilde{f}(u) \tag{15}$$

where $f(t) = \sum_{n\geq 1} \frac{b_n}{n} t^n$ and $\tilde{f}(u) = \sum_{n\geq 1} \frac{c_n}{n} u^n$. By hypothesis, we have $\Omega(t(u)) = \tilde{\Omega}(u)$, i.e., $df(t(u)) = d\tilde{f}(u)$, so $\tilde{f}(u) = f(t(u)) + const.$ Now we have

$$\begin{aligned}\Omega(t^p) - \tilde{\Omega}(u^p) &= d(f(t^p(u)) - \tilde{f}(u^p)) \\ &= d(f(t^p(u)) - f(t(u^p))) \\ &= d\left[\sum_{n\geq 1} \frac{b_n}{n}\Big(t^{np}(u) - t^n(u^p)\Big)\right].\end{aligned}$$

Note that Lemma 4.1 also applies to polynomials in $\mathbb{Z}_p[u]$, and for $p \nmid m$, we have $\frac{1}{m} \in \mathbb{Z}_p$. Taking limits of sequences of polynomials, Lemma 4.1 also applies to power series in u (and fractional powers of u) and in particular to our $t(u)$. For any positive integer n, write $n = mp^k$ where $p \nmid m$. Then replacing t with t^m in Lemma 4.1, we get

$$t^{np}(u) \equiv t^n(u^p) \pmod{p^{k+1}},$$

i.e., $t^{np}(u) - t^n(u^p)$ is divisible by np in $\mathbb{Z}_p[[u]]$. Thus

$$\frac{1}{p}\Omega(t^p) - \frac{1}{p}\tilde{\Omega}(u^p) = d\tilde{\theta}_1(u). \tag{16}$$

where $\tilde{\theta}_1(u) \in \mathbb{Z}_p[[u]]$.

Next, we show that $d\theta(t) = d\tilde{\theta}_2(u)$ for some $\tilde{\theta}_2(u) \in \mathbb{Z}_p[[u]]$. The conditions on m and v in the statement (i.e., that m and v are not divisible by p) imply that we can invert the expansion for t in terms of u to get an expansion of the form $u = \sum \alpha_n t^n$ with $\alpha_n \in \mathbb{Z}_p$ (since $a_1 = 1$). From this we have $dt^k = d(\sum \alpha_n u^n)^k = d(\sum \beta_n u^n)$ where k and β_n are integers. Since $\theta(t) \in \mathbb{Z}_p[[t]]$ is a power series in t, this means that $d\theta(t)$ can also be written as $d\tilde{\theta}_2(u)$ for some $\tilde{\theta}_2(u) \in \mathbb{Z}_p[[u]]$.

Then, by (16), assuming (13),

$$\begin{aligned}\tilde{\Omega}(u) - \frac{1}{p}\tilde{\Omega}(u^p) &= \Omega(t) - \frac{1}{p}\Omega(t^p) + d\tilde{\theta}_1(u) \\ &= d\theta(t) + d\tilde{\theta}_1(u) = d\tilde{\theta}_2(u) + d\tilde{\theta}_1(u),\end{aligned}$$

so we put $\tilde{\theta}(u) = \tilde{\theta}_1(u) + \tilde{\theta}_2(u) \in \mathbb{Z}_p[[u]]$, and (14) follows. Therefore (13) implies (14), and thus (11) implies (12), as required. □

In the application of this result, we will take $m = v = 2$ and $u = q^2$.

Lemma 4.3. *Let t and f be as in (7) and (8). Then*

$$f\frac{q\frac{dt}{dq}}{t} = 1 - 4q^2 - 4q^4 + 32q^6 - 4q^8 - 104q^{10} + 32q^{12} + 192q^{14} + \cdots$$

is an Eisenstein series of weight 3 on $\Gamma_0(8)$ (and a non-trivial character), and furthermore we have

$$f\frac{q\frac{dt}{dq}}{t}(\tau) = E(2\tau) \tag{17}$$

where

$$E(\tau) = \frac{\eta(\tau)^4\eta(2\tau)^6}{\eta(4\tau)^4} \tag{18}$$

Proof. By [18, Lemma 0.3], $\frac{q\frac{dt}{dq}}{t}$ is a holomorphic modular form of weight 2, so that $f(q)\frac{q\frac{dt}{dq}}{t}$ is a holomorphic modular form of weight 3. One can check directly that $t(\tau), f(\tau), E(2\tau)$ are modular forms for $\Gamma_0(8)$ with a certain character, using the transformation properties of η, as given for example in [1, Theorem 3.4]. We can alternatively refer to the eighth case listed in [13, Table 1, p.4852], to see that $E(\tau)$ is a Hecke eigenform of weight 3 and level 4, the sixth case in the same table to see that $f(\tau)$ is a Hecke eigenform of weight 1 and level 4, and to the last entry in [5, Table 3, line 17] to see that $t(\tau)$ is a weight 0 modular function for $\Gamma_0(8)$.

Thus $f(q)\frac{q\frac{dt}{dq}}{t}$ and $E(2\tau)$ are modular forms of weight 3 for $\Gamma_0(8)$, with some character. Since the space of weight 3 modular forms for $\Gamma_1(8)$ is finite dimensional, the equality (17) can be obtained by comparison of sufficiently many terms of the q-expansions, computed using a computer program such as PARI, for example. (One could be more precise; for example, we can show that these forms are modular forms for $\Gamma_0(8) \cap \Gamma_1(4)$, for which, using [14, Theorem 2.25], the space of weight 3 modular forms has dimension 4. One can determine a basis of Eisenstein series, also given in terms of eta products, vanishing at all but one of each of the four cusps, and show that one only needs to compare the coefficients of $1, q, q^2, q^3$ to determine the equality (17). See also the modular forms given in [7, Table 11].) □

Lemma 4.4. *Let γ_n be the sequence of integers such that $E(\tau)$ has q-expansion*

$$E(\tau) = 1 - 4\sum_{n\geq 1} \gamma_n q^n. \tag{19}$$

Then

$$\gamma_{mp^r} \equiv \gamma_{mp^{r-1}} \pmod{p^r}. \tag{20}$$

Proof. Fine [8, p. 85, Eq. (32.7)] tells us that

$$\gamma_n = \sum_{d|n, d\equiv 1 \pmod 4} d^2 - \sum_{d|n, d\equiv 3 \pmod 4} d^2.$$

Thus for a prime $p > 2$,

$$\gamma_{mp^r} - \gamma_{mp^{r-1}} = \sum_{d|m, dp^r\equiv 1 \pmod 4} (dp^r)^2 - \sum_{d|m, dp^r\equiv 3 \pmod 4} (dp^r)^2 \equiv 0 \pmod{p^r}.$$

See sequences A120030 and A002173 in Sloane's database [15] for further references on the γ_n. □

Proof of Theorem 1.3. By Theorem 3.3 we have $f(\tau) = \mathbf{P}(t(\tau))$, and by Lemma 4.3, and using the expression for $E(\tau)$ given in Lemma 4.4, we have $f\frac{dt}{t} = E(2\tau)\frac{dq}{q}$, so, setting $u = q^2$, we have

$$\sum P_n t^{n-1} dt = \mathbf{P}(t)\frac{dt}{t} = f\frac{dt}{t} = \left(1 - 4\sum_{n\geq 1}\gamma_n u^n\right)\frac{du}{2u}.$$

Now we apply Proposition 4.2 with $u = q^2$, $v = 2$ and $m = 2$. We take the b_n and c_n of (10) to be $-2\gamma_n$, where γ_n is defined by (18) and (19) (for $n \geq 1$), and the Catalan-Larcombe-French numbers P_n respectively.

By Lemma 4.4, the congruence (20) holds for the γ_n, and so it also holds for $b_n = -2\gamma_n$, which is precisely (11). Now the desired congruence for the P_n follows from Proposition 4.2. $\square$

5 Supercongruences via Granville's method

In this section we show how the supercongruences we are interested in can be obtained in an alternative manner.

We begin by establishing some general results for congruences of binomial coefficients, following work of Granville [9]. The next result is Theorem 1 of [9].

Theorem 5.1 (Granville)**.** *Suppose that p^q is an odd prime power, and $n = m + r$. Write $n = n_d p^d + \cdots + n_0$ in base p,and let N_j be the least residue of $\lfloor \frac{n}{p^j} \rfloor$ modulo p^q for each $j \geq 0$; make corresponding definitions of m_j, M_j, r_j, R_j. Let e_j be the number of indices $i \geq j$ with $n_i < m_i$ (the number of base p carries beyond the jth digit in adding m and r). Then*

$$\frac{1}{p^{e_0}}\binom{n}{m} \equiv (-1)^{e_{q-1}} \left(\frac{(N_0!)_p}{(M_0!)_p(R_0!)_p}\right)\left(\frac{(N_1!)_p}{(M_1!)_p(R_1!)_p}\right)\cdots\left(\frac{(N_d!)_p}{(M_d!)_p(R_d!)_p}\right) \pmod{p^q}, \tag{21}$$

where $(k!)_p$ denotes the product of the integers $\leq k$ not divisible by p.

(Note that e_0 is the number of carries in the base p sum $m + r = n$, so this confirms the claims made in the course of the proof of Proposition 5.4.)

Recall that Ljunggren proved the following congruence:

$$\binom{pn}{pm} \equiv \binom{n}{m} \pmod{p^3}$$

for $p \geq 5$ and any integers n and m. In fact, Jacobsthal showed that this congruence holds modulo p^q, the power of p dividing $p^3mn(m-n)$, and that this is usually best possible: see [9] for more on this. Using Theorem 5.1, we can prove the following:

Corollary 5.2. *Notation as in Theorem 5.1. Then*

$$\frac{1}{p^{e_0}}\binom{pn}{pm} \equiv \left(\frac{((pN_0)!)_p}{((pM_0)!)_p((pR_0)!)_p}\right) \cdot \frac{1}{p^{e_0}}\binom{n}{m} \pmod{p^q}. \tag{22}$$

Proof. This simply follows on observing that there is only one additional term in the product when (21) is applied with pn and pm. $\square$

If n and m are divisible by p^q, we can deduce further results. Indeed, notice that $(p^q!)_p \equiv -1 \pmod{p^q}$, simply by pairing off a number less than p^q and not divisible by p with its multiplicative inverse modulo p^q, leaving only ± 1 which are self-inverse (as in one of the proofs of Wilson's Theorem). It follows that $((mp^q)!)_p \equiv (-1)^m \pmod{p^q}$, for much the same reason. As a corollary to this observation and Corollary 5.2, we deduce the following:

Corollary 5.3. *Let p^q be an odd prime power. Then if p^{e_0} denotes the power of p dividing the binomial coefficient $\binom{mp^r}{kp^s}$, and $r \geq s \geq q$, then*

$$\frac{1}{p^{e_0}}\binom{mp^r}{kp^s} \equiv \frac{1}{p^{e_0}}\binom{mp^{r-1}}{kp^{s-1}} \pmod{p^q}.$$

Proof. Indeed, in the previous corollary, we observe that the numerators and denominators are of the form $((kp^s)!)_p$ for various values of k, and consequently are all ± 1 modulo p^s, and therefore modulo p^q. It is easy to see that the powers of -1 cancel. □

We now return to our study of the Catalan-Larcombe-French numbers.

We recall (see (2)) that

$$P_n = 2^n \sum_{i=0}^{\lfloor n/2 \rfloor} (-4)^i \binom{2(n-i)}{n-i}^2 \binom{n-i}{i},$$

and we write

$$g(i,n) = \binom{2(n-i)}{n-i}^2 \binom{n-i}{i} = \frac{((2n-2i)!)^2}{((n-i)!)^3 i!(n-2i)!},$$

so that $P_n = 2^n \sum_{i=0}^{\lfloor n/2 \rfloor} (-4)^i g(i,n)$.

Throughout the rest of this section, we suppose that p is an odd prime. We first prove that if $p \nmid i$, then $g(i, mp^r) \equiv 0 \pmod{p^r}$. That is, we prove the following proposition:

Proposition 5.4. *Let p be an odd prime, and let i and n be integers with $p \nmid i$. Then*

$$v_p\left(\binom{2(n-i)}{n-i}^2 \binom{n-i}{i}\right) \geq v_p(n).$$

Proof. We recall from [11, Lemma 2], that

$$v_p\left(\binom{s}{t}\right) = \frac{S_p(t) + S_p(s-t) - S_p(s)}{p-1},$$

where $S_p(s)$ denotes the sum of the digits of s written in base p. From [11, proof of Lemma 1] $S_p(t) + S_p(s-t) - S_p(s) = (p-1)c(t, s-t)$, where $c(t, s-t)$ denotes the number of "carries" in the base p sum $t + (s-t) = s$. It follows that $v_p\left(\binom{s}{t}\right)$ is exactly $c(t, s-t)$.

In the same way,

$$v_p(g(i,n)) = \frac{3S_p(n-i) + S_p(i) + S_p(n-2i) - 2S_p(2n-2i)}{p-1}$$

can also be written as $c(n-i, n-i) + c(n-i, i, n-2i)$, the total number of carries in the two sums:

$$\begin{aligned} (n-i) + (n-i) &= 2n-2i; \\ (n-i) + i + (n-2i) &= 2n-2i. \end{aligned}$$

Suppose that $p^r | n$, but that $p^{r+1} \nmid n$. Then the base p expansion of n ends with r digits 0. Since $n-2i$ and $2n-2i$ differ by n, the final r base p digits of $(n-i)+i$ are all 0, and the sum in base p $(n-i)+i = n$ will require carries in each of the last r positions (as the final base p digit of i is non-zero). □

Perhaps a short illustrative example is in order. Suppose that $n = 18$, $p = 3$ and $i = 7$. Then, in base 3:

$$n = 200, \quad i = 21, \quad n - i = 102, \quad n - 2i = 11, \quad 2n - 2i = 211.$$

The number of carries in $(n - i) + (n - i) = (2n - 2i)$ is the number of carries in $102 + 102 = 211$, which has one carry. More importantly, the other sum is $102 + 21 + 11 = 211$, and the number of carries is the same as that in the sum $102 + 21 = 200$. However, to end with two zeros will require two carries, and, in fact, there are exactly two carries. We see that $v_3(g(7, 18)) = 1 + 2 = 3$.

By the proposition, $p^r | g(i, mp^r)$ if $p \nmid i$. In other words, $g(i, mp^r) \equiv 0 \pmod{p^r}$ if $p \nmid i$. (Indeed, for future reference, the same argument as in the proof of Proposition 5.4 tells us that $p^{r-s} | g(kp^s, mp^r)$.)

We conclude that

$$\begin{aligned} P_{mp^r} &= 2^{mp^r} \sum_{i=0}^{\lfloor mp^r/2 \rfloor} (-4)^i g(i, mp^r) \\ &\equiv 2^{mp^r} \sum_{\substack{i=0 \\ p|i}}^{\lfloor mp^r/2 \rfloor} (-4)^i g(i, mp^r) \pmod{p^r} \\ &\equiv 2^{mp^r} \sum_{j=0}^{\lfloor mp^{r-1}/2 \rfloor} (-4)^{jp} g(jp, mp^r) \pmod{p^r} \\ &\equiv 2^{mp^{r-1}} \sum_{j=0}^{\lfloor mp^{r-1}/2 \rfloor} (-4)^{jp} g(jp, mp^r) \pmod{p^r}, \end{aligned}$$

the last congruence following from the Fermat-Euler Theorem: $a^{\phi(p^r)} \equiv 1 \pmod{p^r}$ for $p \nmid a$ – apply this with $a = 2^m$, and recall that $\phi(p^r) = p^r - p^{r-1}$.

The result will follow from a consideration of the terms $g(jp, mp^r)$. To analyse these terms, we will use the congruence results we established earlier, using the results of Granville [9].

We now prove the following result.

Theorem 5.5. *$g(jp, mp^r) \equiv g(j, mp^{r-1}) \pmod{p^r}$.*

Proof. Let us write $j = kp^s$, with $p \nmid k$. We have already remarked that $p^{r-s-1} | g(kp^{s+1}, mp^r)$, and also that $p^{r-s-1} | g(kp^s, mp^{r-1})$, since the number of carries in one of the sums (as in Proposition 5.4) is at least $r - s - 1$. Let e_0 denote the total number of carries, as above, so $e_0 \geq r - s - 1$. We now want to see that

$$\frac{1}{p^{e_0}} g(kp^{s+1}, mp^r) \equiv \frac{1}{p^{e_0}} g(kp^s, mp^{r-1}) \pmod{p^{s+1}}, \tag{23}$$

i.e.,

$$\frac{1}{p^{e_0}} \binom{2mp^r - 2kp^{s+1}}{mp^r - kp^{s+1}}^2 \binom{mp^r - kp^{s+1}}{kp^{s+1}} \equiv \frac{1}{p^{e_0}} \binom{2mp^{r-1} - 2kp^s}{mp^{r-1} - kp^s}^2 \binom{mp^{r-1} - kp^s}{kp^s} \pmod{p^{s+1}}. \tag{24}$$

However, this now follows as in Corollary 5.3, with $q = s + 1$. $\square$

This is not quite what we need, as we need to account for the power of -4. Luckily, this is now also manageable:

Proposition 5.6. $(-4)^{jp} g(jp, mp^r) \equiv (-4)^j g(j, mp^{r-1}) \pmod{p^r}$.

Proof. We start by observing that if $j = kp^s$ with $p \nmid k$, then

$$\begin{aligned} g(jp, mp^r) = g(kp^{s+1}, mp^r) &\equiv g(kp^s, mp^{r-1}) \pmod{p^r} \\ &\equiv g(kp^{s-1}, mp^{r-2}) \pmod{p^{r-1}} \\ &\dots \\ &\equiv g(k, mp^{r-s+1}) \pmod{p^{r-s-1}} \\ &\equiv 0 \pmod{p^{r-s-1}} \end{aligned}$$

Consequently, $p^{r-s-1} | g(jp, mp^r)$, and again using the proposition, $p^{r-s-1} | g(j, mp^{r-1})$. Further, again by the Fermat-Euler Theorem, we have $(-4)^{p(kp^s)} = (-4)^{kp^{s+1}} \equiv (-4)^{kp^s} \pmod{p^{s+1}}$, and so $p^{s+1} | (-4)^{jp} - (-4)^j$. Then

$$\begin{aligned} &(-4)^{jp} g(jp, mp^r) - (-4)^j g(j, mp^{r-1}) \\ = \;& (-4)^{jp} g(jp, mp^r) - (-4)^{jp} g(j, mp^{r-1}) + (-4)^{jp} g(j, mp^{r-1}) - (-4)^j g(j, mp^{r-1}) \\ = \;& (-4)^{jp} \left(g(jp, mp^r) - g(j, mp^{r-1})\right) + \left((-4)^{jp} - (-4)^j\right) g(j, mp^{r-1}) \end{aligned}$$

which is divisible by p^r as required. $\square$

We can now deduce our main theorem, giving supercongruences for the Catalan-Larcombe-French numbers:

Proof of Theorem 1.3. We have already explained that

$$P_{mp^r} \equiv 2^{mp^{r-1}} \sum_{j=0}^{\lfloor mp^{r-1}/2 \rfloor} (-4)^{jp} g(jp, mp^r) \pmod{p^r},$$

and now we know that $(-4)^{jp} g(jp, mp^r) \equiv (-4)^j g(j, mp^{r-1}) \pmod{p^r}$. It follows that

$$P_{mp^r} \equiv 2^{mp^{r-1}} \sum_{j=0}^{\lfloor mp^{r-1}/2 \rfloor} (-4)^j g(j, mp^{r-1}) \pmod{p^r}.$$

But the right-hand side is one of the ways to define $P_{mp^{r-1}}$, and the result follows. $\square$

References

[1] T.M.Apostol, Modular functions and Dirichlet series in number theory. Graduate Texts in Mathematics 41, Springer-Verlag, New York-Heidelberg, 1976.

[2] F.Beukers, Another congruence for the Apéry numbers, J. Number Theory **25** (1987) 201–210

[3] J.M.Borwein, P.B.Borwein, Pi and the AGM, Wiley-Interscience (1987)

[4] E.Catalan, Sur les Nombres de Segner, Rend. Circ. Mat. Pal. **1** (1887) 190–201

[5] J.H.Conway, S.P.Norton, Monstrous moonshine. Bull. London Math. Soc. **11** (1979) 308–339

[6] T.W.Cusick, Recurrences for sums of powers of binomial coefficients, J. Combin. Theory Ser.A **52** (1989) 77–83

[7] Liqun Fang, J.W.Hoffman, B.Linowitz, A.Rupinski, H.A.Verrill, Modular forms on noncongruence subgroups and Atkin-Swinnerton-Dyer relations. arXiv:math.NT/0805.2144

[8] N.J.Fine, Basic hypergeometric series and applications. With a foreword by George E. Andrews. Mathematical Surveys and Monographs, 27. American Mathematical Society, Providence, RI, 1988. xvi+124 pp. ISBN: 0-8218-1524-5

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

[10] A.F.Jarvis, P.Larcombe, D.French, Applications of the A.G.M. of Gauss: some new properties of the Catalan-Larcombe-French sequence. Proceedings of the Thirty-Fourth Southeastern International Conference on Combinatorics, Graph Theory and Computing. Congr. Numer. **161** (2003) 151–162

[11] A.F.Jarvis, P.Larcombe, D.French, On small prime divisibility of the Catalan-Larcombe-French numbers, Indian Journal of Mathematics **47** (2005) 159–181

[12] P.Larcombe, D.French, On the 'other' Catalan Numbers: A Historical Formulation Re-examined, Congr. Numer. **143** (2000) 33–64

[13] Y.Martin, Multiplicative η-quotients, Trans. Amer. Math. Soc. **348** (1996) 4825–4856

[14] G.Shimura, Introduction to the arithmetic theory of automorphic functions. Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Princeton University Press, Princeton, NJ, 1994. xiv+271 pp. ISBN: 0-691-08092-5

[15] N.J.A.Sloane, The On-Line Encyclopedia of Integer Sequences, published electronically at www.research.att.com/∼njas/sequences/.

[16] J.Stienstra, F.Beukers, On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces, Math. Ann. **271** (1985) 271–304

[17] H.A.Verrill, Picard-Fuchs equations of some families of elliptic curves, Proceedings on Moonshine and related topics (Montréal, Québec, 1999), 253–268, CRM Proc. Lecture Notes, 30, Amer. Math. Soc., Providence, RI, 2001.

[18] H.A.Verrill, Some congruences related to modular forms, Max Planck Institut für Mathematik preprint **26** (1999)