ACTA ARITHMETICA
142.2 (2010)

Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients

by

JOHN B. COSGRAVE (Dublin) and KARL DILCHER (Halifax)

1. Introduction. One of the most remarkable congruences for binomial coefficients, due to Gauss (1828), is related to the representation of an odd prime p as a sum of two squares. It is a well-known theorem of Fermat that p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$, and that the representation is unique up to sign and order of the summands. Let us now fix p and a such that

$$p \equiv 1 \pmod 4, \quad p = a^2 + b^2, \quad a \equiv 1 \pmod 4. \tag{1.1}$$

The theorem of Gauss can now be stated as follows.

THEOREM 1 (Gauss). *Let the prime p and the integer a be as in* (1.1). *Then*

$$\binom{(p-1)/2}{(p-1)/4} \equiv 2a \pmod p. \tag{1.2}$$

For a proof and generalizations of this result see, e.g., [2, p. 268]. Beukers [3] first conjectured an extension to a congruence (mod p^2), and this was first proved by Chowla, Dwork, and Evans [4].

THEOREM 2 (Chowla, Dwork, Evans). *Let p and a be as in* (1.1). *Then*

$$\binom{(p-1)/2}{(p-1)/4} \equiv \left(1 + \tfrac{1}{2}pq_p(2)\right)\left(2a - \frac{p}{2a}\right) \pmod{p^2}. \tag{1.3}$$

Here $q_p(m)$ is the *Fermat quotient to base m* ($p \nmid m$), defined for odd primes p by

$$q_p(m) := \frac{m^{p-1} - 1}{p}. \tag{1.4}$$

2010 *Mathematics Subject Classification*: Primary 11B65; Secondary 11S80, 05A10.
Key words and phrases: Wilson's theorem, Gauss' theorem, factorials, congruences, p-adic gamma function, Catalan numbers.

DOI: 10.4064/aa142-2-1

Congruences such as (1.3) have been very useful in large-scale computations to search for Wilson primes; see [6] or [7]. While the congruences (1.2) and (1.3) have been extended to numerous other binomial coefficients (see [2]), it is one of the purposes of this paper to extend them to a congruence modulo p^3.

THEOREM 3. *Let p and a be as in* (1.1). *Then*

$$\binom{(p-1)/2}{(p-1)/4} \equiv \left(2a - \frac{p}{2a} - \frac{p^2}{8a^3}\right) \times \left(1 + \tfrac{1}{2}pq_p(2) + \tfrac{1}{8}p^2(2E_{p-3} - q_p(2)^2)\right) \pmod{p^3}. \tag{1.5}$$

Here E_n denotes the nth Euler number, defined in (4.4). The second main result, Theorem 7, of which Theorem 3 is a consequence, concerns quotients of what we call Gauss factorials. These quotients resemble binomial coefficients, and we will prove congruences modulo arbitrarily high powers of p. This will be done in Sections 2 and 3, and in Section 4 we derive Theorem 3 from the results of Section 2.

In much the same way as just outlined one can derive (mod p^3) congruences also for numerous other binomial coefficients. Here we will restrict ourselves to the following important classical case. In analogy to (1.1) we fix an odd prime p and integers r, s such that

$$p \equiv 1 \pmod 6, \quad 4p = r^2 + 3s^2, \quad r \equiv 1 \pmod 3, \quad s \equiv 0 \pmod 3. \tag{1.6}$$

The integer r is then uniquely determined. The following congruence, analogous to Gauss' Theorem 1, is due to Jacobi (1837); see [2, p. 291] for remarks and references.

THEOREM 4 (Jacobi). *Let p and r be as in* (1.6). *Then*

$$\binom{2(p-1)/3}{(p-1)/3} \equiv -r \pmod{p}. \tag{1.7}$$

In analogy to Theorem 2, this congruence has also been extended, apparently independently by Evans and Yeung; see [2, p. 293] for remarks and references.

THEOREM 5 (Evans; Yeung). *Let p and r be as in* (1.6). *Then*

$$\binom{2(p-1)/3}{(p-1)/3} \equiv -r + \frac{p}{r} \pmod{p^2}. \tag{1.8}$$

For the usefulness of this congruence, see [6] or [7]. We are now ready to state the following extension.

THEOREM 6. *Let p and r be as in* (1.6). *Then*

$$\binom{2(p-1)/3}{(p-1)/3} \equiv \left(-r + \frac{p}{r} + \frac{p^2}{r^3}\right)\left(1 + \tfrac{1}{6}p^2 B_{p-2}\left(\tfrac{1}{3}\right)\right) \pmod{p^3}. \tag{1.9}$$

Here $B_n(x)$ is the nth Bernoulli polynomial; for a definition see (5.5). The proof of this result, in Section 5, is analogous to the development in Sections 2–4. We conclude this paper with several remarks in Section 6.

2. Gauss factorials and the p-adic gamma function. We found it convenient to introduce the following notation. For positive integers N and n let $N_n!$ denote the product of all integers up to N that are relatively prime to n, i.e.,

$$N_n! = \prod_{\substack{1\le j\le N\\ \gcd(j,n)=1}} j. \tag{2.1}$$

In a previous paper [5] we called these products *Gauss factorials*, a terminology suggested by the theorem of Gauss which states that for any integer $n \ge 2$ we have

$$(n-1)_n! \equiv \begin{cases} -1 \pmod{n} & \text{for } n = 2, 4, p^\alpha, \text{ or } 2p^\alpha,\\ 1 \pmod{n} & \text{otherwise,}\end{cases} \tag{2.2}$$

where p is an odd prime and α is a positive integer. Note that the first case in (2.2) indicates exactly those n that have primitive roots. For references, see [8, p. 65].

Departing from (1.3) we were able to prove the congruence

$$\frac{\left(\frac{p^2-1}{2}\right)_p!}{\left(\left(\frac{p^2-1}{4}\right)_p!\right)^2} \equiv 2a - \frac{p}{2a} \pmod{p^2}, \tag{2.3}$$

with p and a as in (1.1). The proof is similar to (but easier than) that of Theorem 3. Based on numerical experiments, using the computer algebra system Maple [14], it was easy to conjecture

$$\frac{\left(\frac{p^3-1}{2}\right)_p!}{\left(\left(\frac{p^3-1}{4}\right)_p!\right)^2} \equiv 2a - \frac{p}{2a} - \frac{p^2}{8a^3} \pmod{p^3}. \tag{2.4}$$

In this section and the next we are going to prove this, and in fact the following general congruence.

Theorem 7. *Let p and a be as in (1.1) and let $\alpha \ge 2$ be an integer. Then*

$$\begin{aligned}\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} &\equiv 2a - C_0\,\frac{p}{2a} - C_1\,\frac{p^2}{8a^3} - \cdots - C_{\alpha-2}\,\frac{p^{\alpha-1}}{(2a)^{2\alpha-1}}\\ &= 2a - 2a\sum_{j=1}^{\alpha-1}\frac{1}{j}\binom{2j-2}{j-1}\left(\frac{p}{4a^2}\right)^j \pmod{p^\alpha},\end{aligned} \tag{2.5}$$

where $C_n := \frac{1}{n+1}\binom{2n}{n}$ is the nth Catalan number, which is always an integer.

If the summation on the right is considered 0 for $\alpha = 1$, then Gauss' Theorem 1 can also be seen as a special case of (2.5).

As in the proofs of Theorem 2 and its generalizations in [4] and [2], the p-adic gamma function and its connection with Jacobi sums will be useful here. Following the exposition in [2, p. 277], we fix an odd prime p and define a function F on the nonnegative integers by $F(0) := 1$ and

$$F(n) := (-1)^n \prod_{\substack{0<j<n \\ p\nmid j}} j \qquad (n \geq 1), \tag{2.6}$$

with (2.6) interpreted so that $F(1) = -1$. Let now $\mathbb{Q}_p$ denote the p-adic completion of $\mathbb{Q}$, and $\mathbb{Z}_p$ the ring of p-adic integers in $\mathbb{Q}_p$. The p-adic gamma function is then defined by

$$\Gamma_p(z) = \lim_{n \to z} F(n) \qquad (z \in \mathbb{Z}_p), \tag{2.7}$$

where n runs through any sequence of positive integers p-adically approaching z. For the existence of this limit and for other properties see, e.g., [2, p. 277] or [12, pp. 40 ff.]. Among the properties we require here is the fact that for any positive integer n,

$$z_1 \equiv z_2 \pmod{p^n} \quad \text{implies} \quad \Gamma_p(z_1) \equiv \Gamma_p(z_2) \pmod{p^n}. \tag{2.8}$$

The *Jacobi sum* over the finite field $\mathbb{F}_p$ is defined as follows. If χ and ψ are characters on $\mathbb{F}_p$, then the Jacobi sum $J(\chi, \psi)$ is defined by

$$J(\chi, \psi) = \sum_a \chi(a)\psi(1-a),$$

where a runs through the elements of $\mathbb{F}_p$. See, e.g., [2, Sect. 2.1] for a somewhat more general definition.

The following properties are used in this paper. First, let $p = 4f + 1$ be a prime and let g be a primitive root modulo p. Define the integers a_4 and b_4 by

$$p = a_4^2 + b_4^2, \qquad a_4 \equiv -\left(\frac{2}{p}\right) \pmod 4, \qquad b_4 \equiv a_4 g^{(p-1)/4} \pmod p, \tag{2.9}$$

where $\left(\frac{2}{p}\right)$ is the Legendre symbol. For a fixed g the integers a_4, b_4 are uniquely determined and differ from a and b in (1.1) only (possibly) in sign. Next, let χ be a character (mod p) of order 4 such that $\chi(g) = i$. Then from Table 3.2.1 in [2] we have

$$J(\chi, \chi) = (-1)^f (a_4 + ib_4), \tag{2.10}$$

$$J(\chi^3, \chi^3) = (-1)^f (a_4 - ib_4). \tag{2.11}$$

Furthermore, let P be a prime ideal in the ring of integers $\mathbb{Z}[i]$ dividing the prime p. Then it follows from Theorem 2.1.14 in [2, p. 66] that

$$J(\chi,\chi) \equiv 0 \pmod{P}. \tag{2.12}$$

Finally, the connection between Jacobi sums and the p-adic gamma function is a consequence of the deep Gross–Koblitz formula for Gauss sums. There is no need to go into details here; instead we just quote a special case of identity (9.3.7) in [2, p. 278], namely

$$J(\chi^3,\chi^3) = \frac{\Gamma_p(1-1/2)}{\Gamma_p(1-1/4)^2}. \tag{2.13}$$

3. Proof of Theorem 7. With the above definitions and preparations we are now in a position to prove Theorem 7. Continuing to use the ideas in [2, Ch. 9], we apply (2.8) to (2.13) and obtain

$$J(\chi^3,\chi^3) \equiv \frac{\Gamma_p(1+(p^\alpha-1)/2)}{\Gamma_p(1+(p^\alpha-1)/4)^2} \pmod{p^\alpha}. \tag{3.1}$$

Since the arguments of Γ_p are now integers, we have

$$J(\chi^3,\chi^3) \equiv \frac{F(1+(p^\alpha-1)/2)}{F(1+(p^\alpha-1)/4)^2} \pmod{p^\alpha},$$

and finally, comparing (2.6) with (2.1),

$$J(\chi^3,\chi^3) \equiv -\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} \pmod{p^\alpha}. \tag{3.2}$$

Here we have used the fact that $1+(p^\alpha-1)/2 \equiv 1 \pmod{2}$, which accounts for the minus sign in (3.2).

With a view to evaluating the right-hand side of (2.11), we note that (2.10) with (2.12) gives

$$(a_4+ib_4)^\alpha \equiv 0 \pmod{P^\alpha}. \tag{3.3}$$

Since this holds for any prime ideal P dividing the prime p, we may conclude that this congruence holds also modulo p^α. We now expand the left-hand side of (3.3) and separate real and imaginary parts, to obtain

$$-ib_4\sum_{j=0}^{\lfloor(\alpha-1)/2\rfloor}\binom{\alpha}{2j+1}(-1)^j a_4^{\alpha-2j-1}b_4^{2j} \equiv \sum_{j=0}^{\lfloor\alpha/2\rfloor}\binom{\alpha}{2j}(-1)^j a_4^{\alpha-2j}b_4^{2j} \pmod{p^\alpha}. \tag{3.4}$$

Because of the relationship $b_4^2 = p - a_4^2$, the first sum, S_1, in (3.4) becomes

$$S_1 = a_4^{\alpha-1} \sum_{j=0}^{\lfloor(\alpha-1)/2\rfloor} \sum_{k=0}^{j} \binom{\alpha}{2j+1}\binom{j}{k}\left(\frac{-p}{a_4^2}\right)^{j-k}.$$

Setting $\nu := j-k$ and noting that $\binom{j}{k} = \binom{j}{j-k} = \binom{j}{\nu}$, we get

$$S_1 = a_4^{\alpha-1} \sum_{\nu=0}^{\lfloor(\alpha-1)/2\rfloor} \left(\frac{-p}{a_4^2}\right)^{\nu} \sum_{j=\nu}^{\lfloor(\alpha-1)/2\rfloor} \binom{\alpha}{2j+1}\binom{j}{\nu}.$$

The inner sum has an explicit evaluation as $2^{\alpha-1-2\nu}\binom{\alpha-1-\nu}{\nu}$; see identity (3.121) in [10]. Hence

$$S_1 = (2a_4)^{\alpha-1} \sum_{\nu=0}^{\lfloor(\alpha-1)/2\rfloor} \binom{\alpha-1-\nu}{\nu}\left(\frac{-p}{4a_4^2}\right)^{\nu}. \tag{3.5}$$

Similarly, if S_2 is the second sum in (3.4), we get

$$\begin{aligned} S_2 &= a_4^{\alpha} \sum_{j=0}^{\lfloor\alpha/2\rfloor} \sum_{k=0}^{j} \binom{\alpha}{2j}\binom{j}{k}\left(\frac{-p}{a_4^2}\right)^{j-k} \\ &= a_4^{\alpha} \sum_{\nu=0}^{\lfloor(\alpha-1)/2\rfloor} \left(\frac{-p}{a_4^2}\right)^{\nu} \sum_{j=\nu}^{\lfloor\alpha/2\rfloor} \binom{\alpha}{2j}\binom{j}{\nu}. \end{aligned}$$

Using the identity (3.120) in [10] to evaluate the inner sum, we obtain

$$S_2 = \frac{1}{2}(2a_4)^{\alpha} \sum_{\nu=0}^{\lfloor\alpha/2\rfloor} \binom{\alpha-\nu}{\nu}\frac{\alpha}{\alpha-\nu}\left(\frac{-p}{4a_4^2}\right)^{\nu}. \tag{3.6}$$

To simplify notation, we set

$$y := \frac{-p}{4a_4^2}.$$

We now claim that

$$-ib_4 \equiv \frac{S_2}{S_1} \equiv a_4 + 2a_4 \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1} y^j \pmod{p^{\alpha}}. \tag{3.7}$$

By (3.5) and (3.6) this is equivalent to

$$\frac{\sum_{\nu=0}^{\lfloor\alpha/2\rfloor}\binom{\alpha-\nu}{\nu}\frac{\alpha}{\alpha-\nu}\,y^{\nu}}{\sum_{\nu=0}^{\lfloor(\alpha-1)/2\rfloor}\binom{\alpha-1-\nu}{\nu}y^{\nu}} \equiv 1 + 2\sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1} y^j \pmod{p^{\alpha}}$$

or

$$\sum_{\nu=0}^{\lfloor\alpha/2\rfloor}\left[\binom{\alpha-\nu}{\nu}\frac{\alpha}{\alpha-\nu}-\binom{\alpha-1-\nu}{\nu}\right]y^{\nu}$$
$$\equiv 2\Bigl(\sum_{j=1}^{\alpha-1}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}y^{j}\Bigr)\Bigl(\sum_{\nu=0}^{\lfloor(\alpha-1)/2\rfloor}\binom{\alpha-1-\nu}{\nu}y^{\nu}\Bigr)$$
$$\equiv 2\sum_{j=1}^{\alpha-1}\sum_{\nu=0}^{\lfloor(\alpha-1)/2\rfloor}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\binom{\alpha-1-\nu}{\nu}y^{j+\nu}\pmod{p^{\alpha}}.$$

It is easy to verify that

$$\binom{\alpha-\nu}{\nu}\frac{\alpha}{\alpha-\nu}-\binom{\alpha-1-\nu}{\nu}=2\binom{\alpha-1-\nu}{\nu-1},$$

which simplifies the left-hand term in the above congruence. For the right-most term we set $k := j+\nu$ and change the order of summation. Then the congruence above is equivalent to

$$\sum_{\nu=0}^{\lfloor\alpha/2\rfloor}\binom{\alpha-1-\nu}{\nu-1}y^{\nu} \equiv \sum_{k=1}^{\alpha-1}\Bigl(\sum_{j=1}^{k}\frac{(-1)^{j-1}}{j}\binom{2j-2}{j-1}\binom{\alpha-1+j-k}{k-j}\Bigr)y^{k}\pmod{p^{\alpha}}. \tag{3.8}$$

We have therefore proved our claim (3.7) if we can show that the coefficients of the powers of y on both sides of (3.8) are identical up to power $\alpha-1$. But this is an immediate consequence of the identity

$$\sum_{j\ge 0}\frac{(-1)^{j}}{j+1}\binom{2j}{j}\binom{n+j}{n-m-j}=\binom{n-1}{n-m} \tag{3.9}$$

as can be seen by setting $n=\alpha-k$ and $n-m=k-1$ in (3.9). This identity can be found, in slightly changed form, in [11, pp. 183 ff.].

To complete the proof of Theorem 7, we note that (3.7) with (2.11) and (3.2) immediately gives (2.5). It only remains to verify that $-(-1)^{f}a_4=a$. But this follows from (2.9) and the 2nd complementary law of quadratic reciprocity. Indeed, recall that $f=(p-1)/4$; then (as is also shown in [2, p. 108])

$$a_4\equiv-\left(\frac{2}{p}\right)\equiv-(-1)^{\frac{p^2-1}{8}}=-(-1)^{\frac{p-1}{4}\frac{p+1}{2}}=-(-1)^{f}\pmod 4,$$

where we have used the fact that $(p+1)/2\equiv 1\pmod 2$. Hence $-(-1)^{f}a_4\equiv 1\pmod 4$, and thus $-(-1)^{f}a_4=a$ by (1.1). The proof is now complete. ∎

4. Proof of Theorem 3. In order to derive Theorem 3 from Theorem 7 we need a number of auxiliary results on congruences for certain finite sums. We begin by listing three easy congruences.

LEMMA 1. *For all primes $p \geq 5$ we have*

$$\sum_{j=1}^{p-1} \frac{1}{j} \equiv 0 \pmod{p^2}, \tag{4.1}$$

$$\sum_{j=1}^{(p-1)/2} \frac{1}{j} \equiv -2q_p(2) \pmod{p}, \tag{4.2}$$

$$\sum_{j=1}^{\lfloor (p-1)/4 \rfloor} \frac{1}{j} \equiv -3q_p(2) \pmod{p}. \tag{4.3}$$

The congruence (4.2) also holds for $p = 3$. Congruences of this type were obtained by several authors in the early 1900s, with the most extensive and general treatment in a paper by Emma Lehmer [13]. The congruences (41) and (43) in that paper, which are given modulo p^2, immediately reduce to (4.2) and (4.3), respectively, when taken modulo p, and (4.1) follows as a special case from a congruence in [13, p. 353].

While Lemma 1 would be sufficient to obtain (2.3) from (1.3) and vice versa, for the proof of Theorem 3 we need to extend these congruences. For the following lemma we need the Euler numbers E_n which can be defined by the generating function

$$\frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n \qquad (|t| < \pi). \tag{4.4}$$

The Euler numbers are integers, and the first few are $E_0 = 1$, $E_2 = -1$, $E_4 = 5$, $E_6 = -61$, and $E_{2j+1} = 0$ for $j \geq 0$. For further properties see, e.g., [1, Ch. 23].

LEMMA 2. *For all primes $p \geq 5$ we have*

$$\sum_{j=1}^{p-1} \frac{1}{j^2} \equiv 0 \pmod{p}, \tag{4.5}$$

$$\sum_{j=1}^{(p-1)/2} \frac{1}{j} \equiv -2q_p(2) + pq_p(2)^2 \pmod{p^2}, \tag{4.6}$$

and for $p \equiv 1 \pmod{4}$,

$$\sum_{j=1}^{(p-1)/4} \frac{1}{j} \equiv -3q_p(2) + \tfrac{3}{2}pq_p(2)^2 - pE_{p-3} \pmod{p^2}. \tag{4.7}$$

The congruence (4.5) is a special case of a more general one in [13, p. 353]. (4.6) and (4.7) follow from congruences in [16, p. 290].

We will also need congruences for a number of double sums:

LEMMA 3. *For all primes $p \geq 5$ we have*

$$\sum_{1\le j<k\le p-1}\frac{1}{jk}\equiv 0 \pmod{p}, \tag{4.8}$$

$$\sum_{1\le j<k\le (p-1)/2}\frac{1}{jk}\equiv 2q_p(2)^2 \pmod{p}, \tag{4.9}$$

and for $p \equiv 1 \pmod 4$,

$$\sum_{1\le j<k\le (p-1)/4}\frac{1}{jk}\equiv \tfrac{9}{2}q_p(2)^2-2E_{p-3} \pmod{p}. \tag{4.10}$$

Proof. As special cases of congruences in [16, p. 296] we have, for $p \geq 5$,

$$\sum_{j=1}^{(p-1)/2}\frac{1}{j^2}\equiv 0 \pmod{p}, \tag{4.11}$$

and for $p \equiv 1 \pmod 4$,

$$\sum_{j=1}^{(p-1)/4}\frac{1}{j^2}\equiv 4E_{p-3} \pmod{p}. \tag{4.12}$$

Now note that for $d = 1$, 2, or 4 we have

$$\sum_{1\le j<k\le (p-1)/d}\frac{1}{jk}=\frac{1}{2}\Bigg(\sum_{j=1}^{(p-1)/d}\frac{1}{j}\Bigg)^2-\frac{1}{2}\sum_{j=1}^{(p-1)/d}\frac{1}{j^2}. \tag{4.13}$$

We then see that for $d = 1$, the congruences (4.1) and (4.5) imply (4.8). Likewise, for $d = 2$, the congruences (4.2) and (4.11) give (4.9). Finally, in the case $d = 4$, the congruences (4.3) and (4.12) imply (4.10). ∎

We are now ready to prove Theorem 3.

Proof of Theorem 3. We begin with the simple identity

$$\frac{p^3-1}{d}=\frac{p^2-1}{d}p+\frac{p-1}{d}\qquad (d=2 \text{ or } d=4);$$

this shows that with $s := (p^2-1)/d$ we have

$$\Big(\frac{p^3-1}{d}\Big)_p!=\prod_{\nu=0}^{s-1}[(\nu p+1)\cdots(\nu p+p-1)]\Big[(sp+1)\cdots\Big(sp+\frac{p-1}{d}\Big)\Big]. \tag{4.14}$$

Now for each $\nu = 0, 1, \ldots, s-1$ we have

$$(4.15)\qquad (\nu p + 1)\cdots(\nu p + p - 1) \equiv (p-1)!\Bigl[1 + \nu p\sum_{j=1}^{p-1}\frac{1}{j} + \nu^2 p^2 \sum_{1\le j<k\le p-1}\frac{1}{jk}\Bigr] \equiv (p-1)! \pmod{p^3},$$

where the second congruence follows from (4.1) and (4.8). Similarly,

$$(4.16)\qquad (sp+1)\cdots\Bigl(sp + \frac{p-1}{d}\Bigr) \equiv \Bigl(\frac{p-1}{d}\Bigr)!\Bigl[1 + sp\sum_{j=1}^{(p-1)/d}\frac{1}{j} + s^2p^2\sum_{1\le j<k\le (p-1)/d}\frac{1}{jk}\Bigr] \pmod{p^3}.$$

When $d = 2$, we use (4.6) and (4.9) to obtain

$$(sp+1)\cdots\Bigl(sp + \frac{p-1}{d}\Bigr) \equiv \Bigl(\frac{p-1}{d}\Bigr)!\,[1 + sp(-2q_p(2) + pq_p(2)^2) + s^2p^2 2q_p(2)^2] \pmod{p^3}.$$

Upon simplifying and using the fact that $s \equiv -1/2 \pmod{p^2}$ we get, together with (4.15) and (4.14),

$$(4.17)\qquad \Bigl(\frac{p^3-1}{2}\Bigr)_p! \equiv (p-1)!^{(p^2-1)/2}\Bigl(\frac{p-1}{2}\Bigr)!\,(1 + pq_p(2)) \pmod{p^3}.$$

In the case $d = 4$ we use (4.7) and (4.10) and the fact that now $s \equiv -1/4 \pmod{p^2}$. Then in complete analogy to the case $d = 2$, from (4.16) we obtain

$$(4.18)\qquad \Bigl(\frac{p^3-1}{4}\Bigr)_p! \equiv (p-1)!^{(p^2-1)/4}\Bigl(\frac{p-1}{4}\Bigr)! \times \bigl(1 + \tfrac{3}{4}pq_p(2) - \tfrac{3}{32}p^2q_p(2)^2 + \tfrac{1}{8}p^2E_{p-3}\bigr) \pmod{p^3}.$$

Next we note that

$$\frac{1}{1+pq_p(2)} \equiv 1 - pq_p(2) + p^2q_p(2)^2 \pmod{p^3},$$

and therefore upon multiplying and simplifying we get

$$\frac{\bigl(1 + \frac{3}{4}pq_p(2) - \frac{3}{32}p^2q_p(2)^2 + \frac{1}{8}p^2E_{p-3}\bigr)^2}{1+pq_p(2)} \equiv 1 + \tfrac{1}{2}pq_p(2) + \tfrac{1}{8}p^2(2E_{p-3} - q_p(2)^2) \pmod{p^3}.$$

Finally, if we divide (4.17) by the square of (4.18), this last congruence together with (2.4) gives the desired congruence (1.5). ■

5. Proof of Theorem 6. In order to prove Theorem 6, we follow the same development as in Sections 2–4. In particular, we first prove the following result which is of independent interest.

THEOREM 8. *Let p and r be as in* (1.6) *and let $\alpha \geq 2$ be an integer. Then*

$$\frac{\left(\frac{2(p^\alpha-1)}{3}\right)_p!}{\left(\left(\frac{p^\alpha-1}{3}\right)_p!\right)^2} \equiv -r + C_0\,\frac{p}{r} + C_1\,\frac{p^2}{r^3} + \cdots + C_{\alpha-2}\,\frac{p^{\alpha-1}}{r^{2\alpha-1}} = -r + \sum_{j=1}^{\alpha-1} \frac{1}{j}\binom{2j-2}{j-1}\frac{p^j}{r^{2j-1}} \pmod{p^\alpha}, \tag{5.1}$$

where C_n is again the nth Catalan number.

Proof. Fix a primitive root g modulo p, and let χ be a cubic character modulo p such that $\chi(g) = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$. Then from Table 3.1.1 in [2, p. 106] we have

$$J(\chi,\chi) = \tfrac{1}{2}(r + is\sqrt{3}), \tag{5.2}$$

$$J(\chi^2,\chi^2) = \tfrac{1}{2}(r - is\sqrt{3}), \tag{5.3}$$

where r and s are as in (1.6), with the sign of s fixed by the congruence $3s \equiv (2g^{(p-1)/3} + 1)r \pmod{p}$. Furthermore, for any prime ideal P in the ring of integers of $\mathbb{Q}(\sqrt{-3})$ dividing p we find, again by Theorem 2.1.14 in [2, p. 66], that $J(\chi,\chi) \equiv 0 \pmod{P}$, and with (5.2) we get $(r+is\sqrt{3})^\alpha \equiv 0 \pmod{P^\alpha}$. As before, we may conclude that this last congruence also holds modulo p^α. We expand the left-hand side and separate real and imaginary parts:

$$-i\sqrt{3}\,s \sum_{j=0}^{\lfloor(\alpha-1)/2\rfloor} \binom{\alpha}{2j+1}(-3)^j r^{\alpha-2j-1}s^{2j} \equiv \sum_{j=0}^{\lfloor\alpha/2\rfloor}\binom{\alpha}{2j}(-3)^j r^{\alpha-2j}s^{2j} \pmod{p^\alpha}.$$

Using the relationship $3s^2 = 4p - r^2$, the left-hand sum, S_3, becomes

$$S_3 = r^{\alpha-1}\sum_{j=0}^{\lfloor(\alpha-1)/2\rfloor}\sum_{k=0}^{j}\binom{\alpha}{2j+1}\binom{j}{k}\left(\frac{-4p}{r^2}\right)^{j-k} = (2r)^{\alpha-1}\sum_{\nu=0}^{\lfloor(\alpha-1)/2\rfloor}\binom{\alpha-1-\nu}{\nu}\left(\frac{-p}{r^2}\right)^{\nu},$$

where we have used identity (3.121) in [10]. Similarly, for the right-hand sum, S_4, we get (see also (3.6))

$$S_4 = \frac{1}{2}(2r)^\alpha \sum_{\nu=0}^{\lfloor \alpha/2 \rfloor} \binom{\alpha-\nu}{\nu} \frac{\alpha}{\alpha-\nu} \left(\frac{-p}{r^2}\right)^\nu.$$

In the same way as in Section 3 we now obtain, with $z := -p/r^2$,

$$-i\sqrt{3}\, s \equiv \frac{S_4}{S_3} \equiv r + 2r \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} z^j \pmod{p^\alpha};$$

see also (3.7). Now, with (5.3) this gives

$$J(\chi^2, \chi^2) \equiv r + r \sum_{j=1}^{\alpha-1} \frac{(-1)^{j-1}}{j} \binom{2j-2}{j-1} \left(\frac{-p}{r^2}\right)^j \pmod{p^\alpha}. \tag{5.4}$$

Next, in analogy to (2.13) and (3.1), (3.2) we have

$$J(\chi^2, \chi^2) = \frac{\Gamma_p(1-2/3)}{\Gamma_p(1-1/3)^2} \equiv -\frac{\left(\frac{2(p^\alpha-1)}{3}\right)_p!}{\left(\left(\frac{p^\alpha-1}{3}\right)_p!\right)^2} \pmod{p^\alpha}.$$

Finally, this combined with (5.4) immediately gives (5.1). ∎

The proof of Theorem 6 is analogous to that of Theorem 3 in Section 4. For the next lemma, which supplements Lemmas 1–3, we need the Bernoulli polynomials $B_n(x)$, defined by the generating function

$$\frac{te^{tx}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!} \qquad (|t| < 2\pi). \tag{5.5}$$

See Section 6 for some further remarks on the numbers $B_{p-2}(1/3)$ that appear in all the congruences in the following lemma.

Lemma 4. *For all primes $p \equiv 1 \pmod 3$ we have*

$$\sum_{j=1}^{(p-1)/3} \frac{1}{j^2} \equiv \tfrac{1}{2} B_{p-2}\left(\tfrac{1}{3}\right) \pmod{p}, \tag{5.6}$$

$$\sum_{j=1}^{2(p-1)/3} \frac{1}{j^2} \equiv -\tfrac{1}{2} B_{p-2}\left(\tfrac{1}{3}\right) \pmod{p}, \tag{5.7}$$

$$\sum_{j=1}^{(p-1)/3} \frac{1}{j} \equiv -\tfrac{3}{2} q_p(3) + \tfrac{3}{4} p q_p(3)^2 - \tfrac{1}{6} p B_{p-2}\left(\tfrac{1}{3}\right) \pmod{p^2}, \tag{5.8}$$

$$\sum_{j=1}^{2(p-1)/3} \frac{1}{j} \equiv -\tfrac{3}{2} q_p(3) + \tfrac{3}{4} p q_p(3)^2 + \tfrac{1}{3} p B_{p-2}\left(\tfrac{1}{3}\right) \pmod{p^2}, \tag{5.9}$$

$$(5.10)\qquad \sum_{1\le j<k\le (p-1)/3}\frac{1}{jk}\equiv \tfrac{9}{8}q_p(3)^2-\tfrac{1}{4}B_{p-2}\big(\tfrac{1}{3}\big)\pmod p,$$

$$(5.11)\qquad \sum_{1\le j<k\le 2(p-1)/3}\frac{1}{jk}\equiv \tfrac{9}{8}q_p(3)^2+\tfrac{1}{4}B_{p-2}\big(\tfrac{1}{3}\big)\pmod p.$$

Proof. The congruence (5.6) can be found in [16, p. 302]. Then (5.7) follows from the observation that

$$\sum_{j=1}^{2(p-1)/3}\frac{1}{j^2}=\sum_{j=1}^{p-1}\frac{1}{j^2}-\sum_{j=1}^{(p-1)/3}\frac{1}{(p-j)^2}\equiv -\sum_{j=1}^{(p-1)/3}\frac{1}{j^2}\pmod p,$$

where we have used (4.5). The congruence (5.8) was proved in [16, p. 301]. To obtain (5.9), we rewrite

$$(5.12)\qquad \sum_{j=1}^{2(p-1)/3}\frac{1}{j}=\sum_{j=1}^{p-1}\frac{1}{j}-\sum_{j=1}^{(p-1)/3}\frac{1}{p-j}\equiv -\sum_{j=1}^{(p-1)/3}\frac{1}{p-j}\pmod{p^2},$$

where we have used (4.1). Using

$$\frac{1}{j}\equiv -\frac{1}{p-j}-p\,\frac{1}{j^2}\pmod{p^2}$$

(see [13, p. 359]) and (5.6), we see that (5.12) gives (5.9). Finally, (5.10) follows from (4.13) with $d=3$, together with (5.6) and (5.8). Similarly, (5.11) follows from (4.13) with $d=3/2$, together with (5.7) and (5.9). ∎

Proof of Theorem 6. The proof is very similar to that of Theorem 3 in Section 4. First, using (4.14)–(4.16) with $d=3/2$ and noting that $s\equiv -2/3\pmod{p^2}$ in this case, we obtain, with (5.9) and (5.11),

$$(5.13)\qquad \left(\frac{2(p^3-1)}{3}\right)_p!\equiv (p-1)!^{2(p^2-1)/3}\left(\frac{2(p-1)}{3}\right)! \times\big(1+pq_p(3)-\tfrac{1}{9}p^2B_{p-2}\big(\tfrac{1}{3}\big)\big)\pmod{p^3}.$$

Similarly, with $d=3$ and thus $s\equiv -1/2\pmod{p^2}$, we obtain, with (5.8) and (5.10),

$$(5.14)\qquad \left(\frac{p^3-1}{3}\right)_p!\equiv (p-1)!^{(p^2-1)/3}\left(\frac{p-1}{3}\right)! \times\big(1+\tfrac{1}{2}pq_p(3)-\tfrac{1}{8}p^2q_p(3)^2+\tfrac{1}{36}p^2B_{p-2}\big(\tfrac{1}{3}\big)\big)\pmod{p^3}.$$

Next we note that

$$\frac{1}{1+pq_p(3)-\frac{1}{9}p^2B_{p-2}\big(\frac{1}{3}\big)}\equiv 1-pq_p(3)+p^2q_p(3)^2+\tfrac{1}{9}p^2B_{p-2}\big(\tfrac{1}{3}\big)\pmod{p^3},$$

and therefore upon multiplying and simplifying we get

$$\frac{\left(1+\frac{1}{2}pq_p(3)-\frac{1}{8}p^2q_p(3)^2+\frac{1}{36}p^2B_{p-2}\left(\frac{1}{3}\right)\right)^2}{1+pq_p(3)-\frac{1}{9}p^2B_{p-2}\left(\frac{1}{3}\right)} \equiv 1+\frac{1}{6}p^2B_{p-2}\left(\tfrac{1}{3}\right) \pmod{p^3}.$$

Finally, if we divide (5.13) by the square of (5.14) and use this last congruence, then with (5.1) we get the desired congruence (1.9). ∎

6. Further remarks

1. Numerous other congruences of the type (1.2), (1.7) and extensions of the type (1.3), (1.8) have been obtained; see [2, Ch. 9]. For all these cases our method can be used to derive analogues of Theorems 7 and 8, and of Theorems 3 and 6.

2. Further extensions of Theorems 3 and 6 to congruences (mod p^4) would also be possible. However, these congruences would be increasingly complicated and would require different values of Bernoulli polynomials which would arise from higher analogues of Lemmas 1–4.

3. We can obtain the following direct consequence of Theorem 7.

COROLLARY 1. *We have the p-adic expansion*

$$J(\chi^3,\chi^3)=\frac{\Gamma_p(1-1/2)}{\Gamma_p(1-1/4)^2}=-2a+2a\sum_{j=1}^{\infty}\frac{1}{j}\binom{2j-2}{j-1}\left(\frac{p}{4a^2}\right)^j,$$

where χ is the character modulo p of order 4 *as used in* (2.11), *and p and a are as in* (1.1).

This follows directly from (3.2) and (2.5). A similar expression exists for $J(\chi,\chi)$, via (2.10) and (3.7).

Similarly, from Theorem 8 we obtain

COROLLARY 2. *We have the p-adic expansion*

$$J(\chi^2,\chi^2)=\frac{\Gamma_p(1-2/3)}{\Gamma_p(1-1/3)^2}=r-r\sum_{j=1}^{\infty}\frac{1}{j}\binom{2j-2}{j-1}\left(\frac{p}{r^2}\right)^j,$$

where χ is the cubic character modulo p, and p and r are as in (1.6).

4. The numbers $B_{p-2}\left(\frac{1}{3}\right)$ that occur in Theorem 6 and Lemma 4 are interesting in their own right. To simplify notation, set $b_n := 3^nB_n\left(\frac{1}{3}\right)$. In (5.5) we set $x=\frac{1}{3}$; then we replace t by $3t$ and $-3t$ respectively, and subtract the two resulting identities from each other. Upon simplifying the left-hand side we then obtain

$$\frac{t}{e^t+1+e^{-t}}=-\frac{2}{3}\sum_{n=0}^{\infty}b_{2n+1}\frac{t^{2n+1}}{(2n+1)!}. \tag{6.1}$$

The sequence of numbers generated by the left-hand side of (6.1) has been studied by Glaisher [9] as analogues to the Euler numbers defined in (4.4). In particular, it turns out that his so-called G-numbers G_n are related to the numbers b_n by $b_{2n+1} = (-1)^{n+1}G_n$ $(n \geq 1)$, and in addition we have $b_1 = -\frac{1}{2}$. Thus we have, for odd primes $p \geq 5$,

$$B_{p-2}\left(\tfrac{1}{3}\right) = 3^{2-p}(-1)^{(p-1)/2}G_{(p-3)/2},$$

where Glaisher's G-numbers are integers, as was shown in [9], along with numerous other properties. This connection with Glaisher's work is also mentioned in [13, p. 352]. Finally, see [15, A002111] for some properties, references, and values for these numbers.

Acknowledgments. Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006, and by the Natural Sciences and Engineering Research Council of Canada.

References

[1] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, Nat. Bureau of Standards, Washington, 1964.

[2] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[3] F. Beukers, *Arithmetical properties of Picard–Fuchs equations*, Séminaire de théorie des nombres, Paris 1982–83, M.-J. Bertin and C. Goldstein (eds.), Progr. Math. 51, Birkhäuser, Boston, 1984, 33–38.

[4] S. Chowla, B. Dwork, and R. Evans, *On the mod p^2 determination of* $\binom{(p-1)/2}{(p-1)/4}$, J. Number Theory 24 (1986), 188–196.

[5] J. B. Cosgrave and K. Dilcher, *Extensions of the Gauss–Wilson theorem*, Integers 8 (2008), #A39.

[6] R. Crandall, *Topics in Advanced Scientific Computation*, Springer, New York, 1996.

[7] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. 66 (1997), 433–449.

[8] L. E. Dickson, *History of the Theory of Numbers. Volume I: Divisibility and Primality*, Chelsea, New York, 1971.

[9] J. W. L. Glaisher, *On a set of coefficients analogous to the Eulerian numbers*, Proc. London Math. Soc. 31 (1899), 216–235.

[10] H. W. Gould, *Combinatorial Identities*, rev. ed., Gould Publications, Morgantown, WV, 1972.

[11] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, Reading, MA, 1994.

[12] N. Koblitz, *p-Adic Analysis: A Short Course on Recent Work*, London Math. Soc. Lecture Note Ser. 46, Cambridge Univ. Press, Cambridge, 1980.

[13] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. 39 (1938), 350–360.

[14] Maple, http://www.maplesoft.com/.

[15] N. J. A. Sloane, *On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences/.

[16] Z. H. Sun, *Congruences involving Bernoulli and Euler numbers*, J. Number Theory 128 (2008), 280–312.

John B. Cosgrave
79 Rowanbyrn
Blackrock, County Dublin
Ireland
E-mail: jbcosgrave@gmail.com

Karl Dilcher
Department of Mathematics and Statistics
Dalhousie University
Halifax, Nova Scotia, B3H 3J5, Canada
E-mail: dilcher@mathstat.dal.ca

Received on 7.10.2008
and in revised form on 4.8.2009 (5818)