

CONGRUENCES FOR PARTIAL SUMS OF THE GENERATING SERIES FOR $\binom{3k}{k}$

SANDRO MATTAREI AND ROBERTO TAURASO

ABSTRACT. We produce congruences modulo a prime $p > 3$ for sums $\sum_k \binom{3k}{k} x^k$ over ranges $0 \leq k < q$ and $0 \leq k < q/3$, where q is a power of p . Here x equals either $c^2/(1-c)^3$, or $4s^2/(27(s^2-1))$, where c and s are indeterminates. In the former case we deal more generally with shifted binomial coefficients $\binom{3k+e}{k}$. Our method derives such congruences directly from closed forms for the corresponding series.

1. INTRODUCTION

There is a growing literature on congruences modulo a prime, or sometimes modulo a power of a prime, for sums involving binomial coefficients. In several cases such sums are truncated versions of power series for which a closed form is known. Similarities of the finite congruences with those closed forms are often highlighted without making explicit connections. In [4] the authors initiated a systematic derivation of congruences directly from closed forms for the corresponding series, focussing on various sums involving *central binomial coefficients* $\binom{2k}{k}$. In that case the paradigm was the congruence

$$\sum_{0 \leq k < q/2} \binom{2k}{k} x^k \equiv (1-4x)^{(q-1)/2} \pmod{p},$$

for any power q of an odd prime p , which is not hard to prove directly but may conveniently be deduced from the well-known identity $\sum_{k=0}^{\infty} \binom{2k}{k} x^k = (1-4x)^{-1/2}$ via a procedure that one may call *truncation and reduction modulo p* . A range of variations was systematically investigated, and substitution of rational, or more generally algebraic numbers, for x yielded various interesting numerical congruences, such as $\sum_{0 \leq k < p} \binom{2k}{k} k^{-3} \equiv 2B_{p-3}/3 \pmod{p}$, where $p > 3$ is a prime and B_{p-3} is a Bernoulli number.

In this paper we investigate certain sums involving binomial coefficients of the form $\binom{3k}{k}$. More generally, one may consider the power series $y = \sum_{k=0}^{\infty} \binom{rk}{k} x^k$. Because that series satisfies

$$(1) \quad (y-1)((r-1)y+1)^{r-1} - r^r xy^r = 0,$$

an equation of degree r in y , the existence of a closed form for the series depends on being able to ‘solve’ that equation. In Section 2 we apply an artifice to decrease

2020 *Mathematics Subject Classification.* Primary 11A07; secondary 05A10, 05A15.

Key words and phrases. Congruences, generating functions, binomial coefficients.

the degree of the equation by one. This consists in parametrizing one special solution of Equation (1), different from the one we are interested in, thus allowing the left-hand side of the equation to factorize, with our series y being a root of the remaining factor of degree $r - 1$. We carry this out for the more general series $\sum_{k=0}^{\infty} \binom{r+k+e}{k} x^k$, where e is a nonnegative integer.

When $r = 3$ this allows the series, once written in terms of an accessory indeterminate c , where $x = c^2/(1 - c)^3$, to have a closed form involving only one square root extraction, which is Equation (7) below. A further accessory indeterminate β , related to c by $c = \beta(1 - \beta)$, allows one to avoid explicit square root extraction and express the closed form as a rational function of β . This device, which was already employed in [4], facilitates the subsequent truncation process. Our main result here is Theorem 3, in Section 3, which states congruences for certain finite sums $\sum \binom{3k+e}{k} x^k$ in terms of rational functions of β . The proof of Theorem 3 occupies Section 4. For example, a special instance of Theorem 3 is the congruence

$$2(2 + c)(1 - c)^{q-1} \sum_{0 \leq k < q/3} \binom{3k}{k} x^k \equiv 1 + 3(1 - 4c)^{(q-1)/2} + 2c^q \pmod{p}$$

in the polynomial ring $\mathbb{Z}[c]$, where $x = c^2/(1 - c)^3$. Together with a congruence for the analogous sum over the longer range $0 \leq k < 2q/3$, this is stated in Corollary 4, which is the special case $e = 0$ of Theorem 3. In Section 5 we present some applications of Corollary 4. In particular, Theorem 5 characterizes the values of $a \in \mathbb{F}_q$, the field of q elements, such that $\sum_{0 \leq k < q/3} \binom{3k}{k} a^k \equiv 0 \pmod{p}$.

Cardano's formula offers a different approach to solving Equation (1) when $r = 3$. That yields a closed form for $y = \sum_{k=0}^{\infty} \binom{3k}{k} x^k$, to which one may then apply the machinery of truncation and reduction modulo p and obtain corresponding congruences for the truncated sums. We implement that approach in Section 6, in terms of an accessory indeterminate s , where $x = 4s^2/(27(s^2 - 1))$. That substitution has the simplifying effect of turning the discriminant of the cubic equation into a perfect square. In particular, in terms of s we obtain

$$2(1 - s^2)^{(2q-3+\varepsilon)/6} \sum_{0 \leq k < q/3} \binom{3k}{k} x^k \equiv (1 + s)^{(2q+\varepsilon)/3} + (1 - s)^{(2q+\varepsilon)/3} \pmod{p},$$

where $p > 3$ and $\varepsilon = \left(\frac{q}{3}\right)$ denotes a Legendre symbol.

In our final Section 7 we illustrate how a number of numerical congruences can be obtained by evaluating our polynomial congruences at rational values of the indeterminate, or even irrational but p -integral algebraic values. An example is $\sum_{0 \leq k < q/3} \binom{3k}{k} 3^{-k} \equiv \varepsilon F_{2(2q+\varepsilon)/3} \pmod{p}$, in terms of Fibonacci numbers.

2. THE POWER SERIES $\sum_{k=0}^{\infty} \binom{r+k+e}{k} x^k$

In this section we collect some information on the generating function of the binomial coefficients $\binom{r+k+e}{k}$ as a function of k . For r a positive integer, the power

series

$$(2) \quad \mathcal{B}_r(x) = \sum_{k=0}^{\infty} \frac{1}{rk+1} \binom{rk+1}{k} x^k = \sum_{k=0}^{\infty} \frac{1}{(r-1)k+1} \binom{rk}{k} x^k$$

was called the *generalized binomial series* in [1, Equation (5.58)]. Note that $\mathcal{B}_1(x) = 1/(1-x)$. According to [5, Example 6.2.6], $\mathcal{B}_r(x)$ satisfies

$$(3) \quad \mathcal{B}_r(x) = 1 + x\mathcal{B}_r(x)^r,$$

which can be proved using Lagrange inversion. More generally, for $e > 0$ Lagrange inversion produces

$$(4) \quad \mathcal{B}_r(x)^e = \sum_{k=0}^{\infty} \frac{e}{rk+e} \binom{rk+e}{k} x^k,$$

which is [1, Equation (5.60)]. One may also obtain Equation (4) inductively from Equation (2) using the Rothe-Hagen convolution identity [1, Equation (5.63)]. The series in Equation (4) is the ordinary generating function of the Fuss-Catalan numbers, a generalization of the Catalan numbers introduced by Nicolaus Fuss in the late eighteenth century. Differentiating Equations (3) and (4), and then eliminating the derivative of $\mathcal{B}_r(x)$, one finds

$$(5) \quad \frac{\mathcal{B}_r(x)^e}{1-r+r\mathcal{B}_r(x)^{-1}} = \sum_{k=0}^{\infty} \binom{rk+e}{k} x^k,$$

which is [1, Equation (5.61)]. Although this derivation is only valid for $e > 0$, Equation (5) holds for $e = 0$ as well, as one can see by differentiating the second expression for $\mathcal{B}_r(x)$ given in Equation (2) instead of Equation (4).

Equation (5) shows that each formal power series $y_{r,e}(x) = \sum_{k=0}^{\infty} \binom{rk+e}{k} x^k \in \mathbb{Q}[[x]]$ is algebraic, because so is $\mathcal{B}_r(x)$ according to Equation (3). This means that $y_{r,e}(x)$ belongs to a finite-degree extension field of the field $\mathbb{Q}((x))$ of formal Laurent series. In fact, $\mathcal{B}_r(x)$ is algebraic of degree r , with minimal polynomial $z^r - zx^{-1} + x^{-1}$ obtained from Equation (2). That is indeed the minimal polynomial of $\mathcal{B}_r(x)$, because it is irreducible over $\mathbb{Q}((x))$, by an appropriate application of Eisenstein's irreducibility criterion. Since $y_{r,e}(x)$ belongs to the extension field of $\mathbb{Q}((x))$ generated by $\mathcal{B}_r(x)$, is also algebraic, of degree not exceeding r . Consequently, $y_{r,e}(x)$ satisfies an equation of degree r analogous to Equation (3). Such an equation is awkward when worked out in general, and we will have no need for that in this paper, except for the special case $e = 0$, which is easy to deduce from Equation (5) and Equation (3): the power series $y = y_{r,0}(x) = \sum_{k=0}^{\infty} \binom{rk}{k} x^k$ satisfies

$$(y-1)((r-1)y+1)^{r-1} - r^r xy^r = 0,$$

which is Equation (1) in the Introduction. This equation can also be found in [5, Example 6.2.7].

In principle, a closed form for the series $y_{r,e}(x)$ in terms of radicals and rational expressions may be obtained for $r \leq 4$ by solving the corresponding equation of degree r using radicals. This is straightforward for $r = 2$ and leads to familiar closed forms. For $r = 3$ one may use Cardano's formula, but that is more easily

done through an artifice which renders the discriminant (almost) a perfect square, and we devote Section 6 to that approach in the special case $e = 0$.

Here we discuss a different artifice, which allows one to pass from degree r to one less in the general case. In order to characterize $\mathcal{B}_r(x)$ among the roots of Equation (3), it is more convenient to work with its reciprocal. The power series $w = w(x) = 1/\mathcal{B}_r(x)$ is the only solution of the equation $w^r - w^{r-1} + x = 0$ such that $w(0) = 1$. If we set $x = -c^{r-1}/(c-1)^r$, then the resulting equation has $w = c/(c-1)$ among its roots, and its left-hand side factorizes as

$$w^r - w^{r-1} - \frac{c^{r-1}}{(c-1)^r} = \left(w - \frac{c}{c-1}\right) \left(w^{r-1} + \sum_{i=0}^{r-2} \frac{c^i}{(c-1)^{i+1}} w^{r-2-i}\right).$$

Consequently, the series $w = 1/\mathcal{B}_r(-c^{r-1}/(c-1)^r)$ is the only solution of the equation

$$(6) \quad w^{r-1} + \sum_{i=0}^{r-2} \frac{c^i}{(c-1)^{i+1}} w^{r-2-i} = 0$$

satisfying $w(0) = 1$. Our gain in passing from the indeterminate x to c lies in this equation having degree one less than the original equation $w^r - w^{r-1} + x = 0$.

In particular, when $r = 2$ Equation (6) reads $w + 1/(c-1)$, and hence $\mathcal{B}_2(-c/(c-1)^2) = 1 - c$. Equation (5) then gives us

$$\sum_{k=0}^{\infty} \binom{2k+e}{k} \left(\frac{-c}{(c-1)^2}\right)^k = \frac{(1-c)^{e+1}}{1+c}.$$

Here c can easily be obtained from x , as $c = 1 - (1 - \sqrt{1-4x})/(2x)$, which leads to the better-known equation

$$\sum_{k=0}^{\infty} \binom{2k+e}{k} x^k = \frac{1}{\sqrt{1-4x}} \left(\frac{1 - \sqrt{1-4x}}{2x}\right)^e,$$

see [9, Equation (2.47)].

When $r = 3$ we find that $w = w(c) = 1/\mathcal{B}_3(-c^2/(c-1)^3)$ is the only solution of the quadratic equation

$$w^2 + \frac{1}{c-1}w + \frac{c}{(c-1)^2} = 0$$

that satisfies $w(0) = 1 = 1/\mathcal{B}_3(0)$. Imposing this condition we find

$$\mathcal{B}_3(c^2/(1-c)^3) = \frac{2(1-c)}{1 + \sqrt{1-4c}}.$$

It is now convenient to set $\beta = (1 - \sqrt{1-4c})/2$. Noting that $\beta(1-\beta) = c$ we find

$$\mathcal{B}_3(c^2/(1-c)^3) = \frac{1 - \beta(1-\beta)}{1-\beta} = \frac{1 + \beta^3}{1 - \beta^2}.$$

Equation (5) then gives us

$$(7) \quad \sum_{k=0}^{\infty} \binom{3k+e}{k} \left(\frac{c^2}{(1-c)^3} \right)^k = \frac{1}{(1+\beta)(1-2\beta)} \frac{(1-\beta+\beta^2)^{e+1}}{(1-\beta)^e}.$$

In the next sections we will derive from this equation a congruence modulo a prime p for certain finite sums, obtained by truncating the series at appropriate places. For comparison, with the same notation we have

$$\sum_{k=0}^{\infty} \binom{2k+e}{k} c^k = \frac{1}{(1-2\beta)(1-\beta)^e},$$

which was used as a starting point for deducing congruences in the proof of [4, Theorem 5].

3. CONGRUENCES FOR FINITE SUMS $\sum_k \binom{rk+e}{k} x^k$ MODULO A PRIME

Our first goal in this paper is an evaluation, in closed form and as polynomial congruences modulo a prime, of finite sums $\sum_k \binom{rk+e}{k} x^k$ over certain ranges. We start with describing certain natural ranges for evaluations modulo a prime coming from Lucas' theorem, for the more general sums $\sum_k \binom{rk+e}{k} x^k$, which are refinements of the basic natural range $0 \leq k < q$, where q is a power of p . Recall Lucas' theorem [2]: if q is a power of a prime p , and we write any integer a in its unique form $a = a' + a''q$ with $0 \leq a'' < q$, then $\binom{a}{b} \equiv \binom{a'}{b'} \binom{a''}{b''} \pmod{p}$.

Lemma 1. *Let r be a positive integer, let q be a power of a prime p , and let $0 \leq e < q$. Then the binomial coefficient $\binom{rk+e}{k}$ for $0 \leq k < q$ is a multiple of p unless $k \in A(r, m, e)$ for some $0 < m \leq r$, where*

$$A(r, m, e) = \left\{ k \in \mathbb{Z} : \frac{(m-1)q - e}{r-1} \leq k < \frac{mq - e}{r} \right\}.$$

Proof. Because $\binom{rk+e}{k} \equiv \binom{rk+e-mq}{k} \pmod{p}$ for any integer m according to Lucas' Theorem, $\binom{rk+e}{k} \equiv 0 \pmod{p}$ holds if $0 \leq rk + e - mq < k$ for some integer m , which means $(mq - e)/r \leq k < (mq - e)/(r-1)$. These are the complementary intervals to the intervals $A(r, m, e)$ within the range $0 \leq k < q$. $\square$

Thus, when considering finite sums $\sum_k \binom{rk+e}{k} x^k$ modulo a prime p , and q is any power of p , the range $0 \leq k < q$ splits naturally into r separate ranges, possibly including empty ones such as $A(r, r, 0)$. Consequently, it is natural to look for evaluations modulo p of the partial sums

$$\sum_{0 \leq k < (mq-e)/r} \binom{rk+e}{k} x^k,$$

for $0 < m \leq r$, or on the subintervals $A(r, m, e)$ in which this range decomposes naturally according to Lemma 1.

When $r = 2$ the ranges of Lemma 1 read $0 \leq k < (q-e)/2$ and $q-e \leq k < q-e/2$. Finite sums $\sum_k \binom{2k+e}{k} x^k$ over each of those two intervals were evaluated, in closed form modulo p , in [4, Theorem 45]. Because we will rely on that result

to deal with the case $r = 3$, and because the latter will require a slightly different approach, we provide a new proof of [4, Theorem 45] by way of introduction to our new approach. The main novelty is that we can prove the desired congruence over the first interval $0 \leq k < (q - e)/2$ without having to consider both intervals together, as we did in the original proof. Here we prefer to use the letter c for the indeterminate in place of x , because the former bears the same relationship to the indeterminate β as that in place when we will deal with sums $\sum_k \binom{3k+e}{k} x^k$ later.

Theorem 2 (Part of Theorem 5 of [4]). *Let q be a power of an odd prime p , let $1 \leq m \leq 2$, and let $0 \leq e \leq q$. In the polynomial ring $\mathbb{Z}[\beta]$, setting $c = \beta(1 - \beta)$ and $\alpha = 1 - \beta$, we have*

$$\sum_{0 \leq k < (mq-e)/2} \binom{2k+e}{k} c^k \equiv \frac{\alpha^{mq-e} - \beta^{mq-e}}{\alpha - \beta} \pmod{p}.$$

Proof. We will first prove the case $m = 1$, and then deduce the case $n = 2$ from that. We start from the identity

$$\sum_{k=0}^{\infty} \binom{2k+e}{k} c^k = \frac{1}{(1-2\beta)(1-\beta)^e},$$

which takes place in the power series ring $\mathbb{Q}[[\beta]]$, where $c = \beta(1 - \beta)$. However, because all coefficients are integers it actually takes place in $\mathbb{Z}[[\beta]]$. Consequently,

$$\sum_{0 \leq k < (q-e)/2} \binom{2k+e}{k} c^k \equiv \frac{1}{(1-2\beta)(1-\beta)^e} \pmod{(\beta^{q-e}, p)}$$

in $\mathbb{Z}[[\beta]]$, where (β^{q-e}, p) denotes the ideal of $\mathbb{Z}[[\beta]]$ generated by β^{q-e} and p . In fact, $\binom{2k+e}{k} \equiv 0 \pmod{p}$ for $(q - e)/2 \leq k < q - e$ according to Lemma 1, and $\sum_{k \geq q-e} \binom{2k+e}{k} c^k \equiv 0 \pmod{\beta^{q-e}}$. Because $(1 - \beta)^q \equiv 1 - \beta^q \pmod{p}$ we also have

$$\frac{(1 - \beta)^{q-e} - \beta^{q-e}}{1 - 2\beta} \equiv \frac{1}{(1 - 2\beta)(1 - \beta)^e} \pmod{(\beta^{q-e}, p)}.$$

The left-hand sides of the previous two congruences are polynomials of degree less than $q - e$, and hence so is their difference. However, when the difference is viewed as a polynomial in $\mathbb{F}_p[\beta]$, we have just shown that it is a multiple of β^{q-e} . Consequently the difference must be zero in $\mathbb{F}_p[\beta]$, and the desired conclusion follows for $m = 1$:

$$\sum_{0 \leq k < (q-e)/2} \binom{2k+e}{k} c^k \equiv \frac{(1 - \beta)^{q-e} - \beta^{q-e}}{1 - 2\beta} = \frac{\alpha^{q-e} - \beta^{q-e}}{\alpha - \beta} \pmod{p}.$$

Now we may deduce the case $m = 2$ from the case $m = 1$. Using Lucas' theorem and the basic binomial coefficient identity $\binom{n}{k} = \binom{n}{n-k}$ we find

$$\begin{aligned} \sum_{q-e \leq k < q-e/2} \binom{2k+e}{k} c^k &= c^{q-e} \sum_{0 \leq k < e/2} \binom{2k+2q-e}{k+q-e} c^k \\ &\equiv c^{q-e} \sum_{0 \leq k < e/2} \binom{2k+q-e}{k+q-e} c^k \pmod{p} \\ &= c^{q-e} \sum_{0 \leq k < e/2} \binom{2k+q-e}{k} c^k. \end{aligned}$$

Now the case $m = 1$ with $q - e$ in place of e yields

$$\sum_{q-e \leq k < q-e/2} \binom{2k+e}{k} c^k \equiv \frac{\alpha^q \beta^{q-e} - \alpha^{q-e} \beta^q}{\alpha - \beta} \pmod{p},$$

and adding this to the sum over the range $0 \leq k < (q - e)/2$ we easily reach the desired conclusion. $\square$

After having reviewed the case $r = 2$, we move on to the case $r = 3$, which is the one of main interest in this paper. According to Lemma 1, we are interested in evaluating sums $\sum_k \binom{3k+e}{k} x^k$ modulo p , for $0 \leq e < q$, over each of the three finite ranges

$$0 \leq k < (q - e)/3, \quad (q - e)/2 \leq k < (2q - e)/3, \quad q - e/2 \leq k < q - e/3.$$

Theorem 3. *Let q be a power of an odd prime p , let $1 \leq m \leq 3$, and let $0 \leq e < q$. In the polynomial ring $\mathbb{Z}[\beta]$, setting $c = \beta(1 - \beta)$, $\alpha = 1 - \beta$, and $x = c^2/(1 - c)^3$, we have*

$$\begin{aligned} &2(2 + c)(1 - c)^{mq-1-e} \sum_{0 \leq k < (mq-e)/3} \binom{3k+e}{k} x^k \\ &\equiv (\alpha^{mq-e} + \beta^{mq-e}) + 3 \frac{\alpha^{mq-e} - \beta^{mq-e}}{\alpha - \beta} - 2(-c)^{mq-e} \pmod{p}. \end{aligned}$$

We will prove Theorem 3 in Section 4. Here we explicitly state the special case $e = 0$ as a corollary, because the formulas then simplify and take place in the polynomial ring $\mathbb{Z}[c]$, without the explicit involvement of the indeterminate β .

Corollary 4. *For any power q of an odd prime p , in the polynomial ring $\mathbb{Z}[c]$, where $x = c^2/(1 - c)^3$, we have*

$$2(2 + c)(1 - c)^{q-1} \sum_{0 \leq k < q/3} \binom{3k}{k} x^k \equiv 1 + 3(1 - 4c)^{(q-1)/2} + 2c^q \pmod{p},$$

and

$$2(2 + c)(1 - c)^{2q-1} \sum_{0 \leq k < 2q/3} \binom{3k}{k} x^k \equiv 1 + 3(1 - 4c)^{(q-1)/2} - 2c^q - 2c^{2q} \pmod{p}.$$

Proof. When $e = 0$, for $m = 1$ the right-hand side of the congruence of Theorem 3 reads

$$(\alpha^q + \beta^q) + 3 \frac{\alpha^q - \beta^q}{\alpha - \beta} - 2(-c)^q \equiv 1 + 3(\alpha - \beta)^{q-1} + 2c^q \pmod{p},$$

and the conclusion follows because $(\alpha - \beta)^2 = (1 - 2\beta)^2 = 1 - 4\beta + 4\beta^2 = 1 - 4c$. For $m = 2$ the desired conclusion follows similarly because $\alpha^{2q} + \beta^{2q} = (\alpha^q + \beta^q)^2 - 2\alpha^q\beta^q \equiv 1 - 2c^q \pmod{p}$ and $\alpha^{2q} - \beta^{2q} = (\alpha^q + \beta^q)(\alpha^q - \beta^q) \equiv (\alpha - \beta)^q \pmod{p}$. Of course when $e = 0$ we do not get anything new for $m = 3$. $\square$

According to Corollary 4 the sums over the two ranges are related by the congruence

$$\sum_{0 \leq k < q/3} \binom{3k}{k} x^k - (1 - c^q) \sum_{0 \leq k < 2q/3} \binom{3k}{k} x^k \equiv c^q \frac{(2 + c)^{q-1}}{(1 - c)^{q-1}} \pmod{p}.$$

Theorem 3 and Corollary 4 remain trivially valid also when $p = 2$, but provide no information on the corresponding sums. According to Lucas' theorem, the binomial coefficient $\binom{3k}{k}$ is odd precisely when the binary expansion of k contains no adjacent digits equal to 1. A well-known combinatorial characterization of the Fibonacci numbers then implies $\sum_{0 \leq k < 2^r} \binom{3k}{k} \equiv F_{r+2} \pmod{2}$. We will not pursue the case $p = 2$ further in this paper.

4. PROOF OF THEOREM 3

We will deduce the desired congruences from the closed form for the corresponding series, which we gave in Equation (7). Because $1 - \beta + \beta^2 = 1 - c$ and $(2 - \beta)(1 + \beta) = 2 + c$ we may rewrite that identity in the form

$$\sum_{k=0}^{\infty} \binom{3k+e}{k} \left(\frac{c^2}{(1-c)^3} \right)^k = \frac{1-c}{2(2+c)} \left(1 + \frac{3}{1-2\beta} \right) \frac{(1-c)^e}{(1-\beta)^e}.$$

We start with the case $m = 1$. In order to clear denominators of the left-hand side of the above identity in the first range $0 \leq k < q/3$ that we are interested in, we multiply both sides by $(1 - c)^{q-1-e}$. After further multiplying both sides by $2(2 + c)$ we find

$$(8) \quad 2(2 + c) \sum_{k=0}^{\infty} \binom{3k+e}{k} c^{2k} (1 - c)^{q-1-e-3k} = \frac{(1 - c)^q}{(1 - \beta)^e} \left(1 + \frac{3}{1 - 2\beta} \right),$$

to be viewed as an identity in the power series ring $\mathbb{Q}[[\beta]]$, and actually $\mathbb{Z}[[\beta]]$. Now we produce congruences, in turn, for each side of Equation (8).

According to Lemma 1 for $r = 3$, the binomial coefficient $\binom{3k+e}{k}$ is a multiple of p for $(q - e)/3 \leq k < (q - e)/2$. Consequently, the left-hand side of Equation (8)

satisfies

$$\begin{aligned}
 (9) \quad & 2(2+c) \sum_{k=0}^{\infty} \binom{3k+e}{k} c^{2k} (1-c)^{q-1-e-3k} \\
 & \equiv 2(2+c) \sum_{0 \leq k < (q-e)/3} \binom{3k+e}{k} c^{2k} (1-c)^{q-1-e-3k} \pmod{(c^{q-e}, p)}.
 \end{aligned}$$

The right-hand side of this congruence is a polynomial in c , of degree $q-e$ and leading term $-2(-c)^{q-e}$.

Before we consider the right-hand side of Equation (8), note that for $m \in \{1, 2, 3\}$ we have

$$1 - mc^q = 1 - m\beta^q + m\beta^{2q} \equiv (1 - \beta^q)^m \equiv \alpha^{mq} \pmod{(\beta^{mq}, p)},$$

where we have set $\alpha = 1 - \beta$. Consequently,

$$(10) \quad \frac{1 - mc^q}{(1 - \beta)^e} \equiv \alpha^{mq-e} \pm \beta^{mq-e} \pmod{(\beta^{mq-e}, p)}.$$

In particular, the right-hand side of Equation (8) satisfies

$$(11) \quad \frac{(1-c)^q}{(1-\beta)^e} \left(1 + \frac{3}{1-2\beta}\right) \equiv (\alpha^{q-e} + \beta^{q-e}) + 3 \frac{\alpha^{q-e} - \beta^{q-e}}{\alpha - \beta} \pmod{(\beta^{q-e}, p)}.$$

Combining Equations (9) and (11) we obtain

$$\begin{aligned}
 (12) \quad & 2(2+c) \sum_{0 \leq k < (q-e)/3} \binom{3k+e}{k} c^{2k} (1-c)^{q-1-e-3k} \\
 & \equiv (\alpha^{q-e} + \beta^{q-e}) + 3 \frac{\alpha^{q-e} - \beta^{q-e}}{\alpha - \beta} \pmod{(\beta^{q-e}, p)}.
 \end{aligned}$$

The right-hand side of this congruence is invariant under interchanging β with $\alpha = 1 - \beta$, and hence can be written as a polynomial in their elementary symmetric polynomials $\alpha + \beta = 1$ and $\alpha\beta = c$. Hence the right-hand side of Equation (12) is actually a polynomial in $c = \beta(1 - \beta)$. Because β and $1 - \beta$ are coprime, it follows that the congruence actually holds modulo (c^{q-e}, p) . Also, because the right-hand side of Equation (12) has degree at most $q-e$ as a polynomial in β , it has degree at most $(q-e)/2$ as a polynomial in c , and hence less than $q-e$. The desired congruence modulo p follows because the left-hand side of Equation (12) has leading term $-2(-c)^{q-e}$, as noted earlier.

Now we deal with the case $m = 2$, where the finite sum is over the range $0 \leq k < (2q-e)/3$. We proceed in a similar fashion, but in order to clear denominators over the longer range we first need to multiply both sides of Equation (8) by a further factor $(1-c)^q$. Because $\binom{3k+e}{k}$ is a multiple of p for $(2q-e)/3 \leq k < (2q-e)/2$,

the left-hand side of Equation (8) multiplied by $(1 - c)^q$ satisfies

$$(13) \quad \begin{aligned} & 2(2 + c) \sum_{k=0}^{\infty} \binom{3k + e}{k} c^{2k} (1 - c)^{2q-1-e-3k} \\ & \equiv 2(2 + c) \sum_{0 \leq k < (2q-e)/3} \binom{3k + e}{k} c^{2k} (1 - c)^{2q-1-e-3k} \pmod{(c^{2q-e}, p)}. \end{aligned}$$

As a polynomial in c the right-hand side of this congruence has degree $2q - e$ and leading term $2(-c)^{2q-e}$.

The right-hand side of Equation (8) also needs to be multiplied by $(1 - c)^q$, and then the result contains the factor $(1 - c)^{2q} \equiv 1 - 2c^q \pmod{c^{2q}}$. Using Equation (10) for $m = 2$ we find that the right-hand side of Equation (8) multiplied by $(1 - c)^q$ satisfies

$$\frac{(1 - c)^{2q}}{(1 - \beta)^e} \left(1 + \frac{3}{1 - 2\beta} \right) \equiv (\alpha^{2q-e} + \beta^{2q-e}) + 3 \frac{\alpha^{2q-e} - \beta^{2q-e}}{\alpha - \beta} \pmod{(\beta^{2q-e}, p)}.$$

Combining this congruence with Equation (13) we find a version of the desired conclusion as a congruence modulo (β^{2q-e}, p) . Arguing as we did for the case $m = 1$, we observe how symmetry makes the congruence hold modulo (c^{2q-e}, p) . Finally, keeping track of the leading term we obtain the desired conclusion for $m = 2$.

To deal with the final case $m = 3$, where the finite sum is over the range $0 \leq k < (3q - e)/3$, we cannot proceed exactly in the same way as we have just done for $m = 1, 2$. In fact, a congruence analogous to Equation (13), with both sides multiplied by a further factor $(1 - c)^q$, and the summation at the right-hand side extended to $0 \leq k < (3q - e)/3$, does not hold modulo (c^{3q-e}, p) as we would need to carry out a similar argument, but only modulo (c^{2q}, p) . That is because $\binom{3k+e}{k}$ is not a multiple of p for $(3q - e)/3 \leq k < (3q - e)/2$, but only on the shorter range $(3q - e)/3 \leq k < q$.

To overcome this obstacle we evaluate a longer partial sum, over the range $0 \leq k < (4q - e)/3 = q + (q - e)/3$, of the left-hand side of Equation (8) multiplied by $(1 - c)^{3q}$. According to Lucas' theorem, for $q \leq k < (4q - e)/3$ we have

$$\binom{3k + e}{k} \equiv \binom{3q}{q} \binom{3(k - q) + e}{k - q} \equiv 3 \binom{3(k - q) + e}{k - q} \pmod{p},$$

and for $(4q - e)/3 \leq k < (3q - e)/2$ we have

$$\binom{3k + e}{k} \equiv \binom{4q}{q} \binom{3k - 4q + e}{k - q} \equiv 0 \pmod{p}.$$

Consequently, splitting the summation range $0 \leq k < (4q - e)/3$ into two portions $0 \leq k < (3q - e)/3$ and $q \leq k < (4q - e)/3 = q + (q - e)/3$ (with the range $(3q - e)/3 \leq k < q$ between them giving no contribution according to Lemma 1),

we find

$$\begin{aligned}
 & 2(2+c) \sum_{k=0}^{\infty} \binom{3k+e}{k} c^{2k} (1-c)^{4q-1-e-3k} \\
 & \equiv 2(2+c) \sum_{0 \leq k < (4q-e)/3} \binom{3k+e}{k} c^{2k} (1-c)^{4q-1-e-3k} \pmod{(c^{3q-e}, p)} \\
 (14) \quad & \equiv (1-c)^q 2(2+c) \sum_{0 \leq k < (3q-e)/3} \binom{3k+e}{k} c^{2k} (1-c)^{3q-1-e-3k} \\
 & + 3c^{2q} 2(2+c) \sum_{0 \leq k < (q-e)/3} \binom{3k+e}{k} c^{2k} (1-c)^{q-1-e-3k} \pmod{p}.
 \end{aligned}$$

The right-hand side of Equation (8) also needs to be multiplied by $(1-c)^{3q}$, and then the result contains the factor $(1-c)^{4q} \equiv (1-c^q)(1-3c^q) + 3(1-c^q)c^{2q} \pmod{c^{3q}}$. Using Equation (10) for $m = 3$, and Equation (11), we find

$$\begin{aligned}
 & \frac{(1-c)^{4q}}{(1-\beta)^e} \left(1 + \frac{3}{1-2\beta} \right) \\
 & \equiv (1-c)^q \left((\alpha^{3q-e} + \beta^{3q-e}) + 3 \frac{\alpha^{3q-e} - \beta^{3q-e}}{\alpha - \beta} \right) \\
 & + 3c^{2q} \left((\alpha^{q-e} + \beta^{q-e}) + 3 \frac{\alpha^{q-e} - \beta^{q-e}}{\alpha - \beta} \right) \pmod{(\beta^{3q-e}, p)}.
 \end{aligned}$$

Using our conclusion in the case $m = 1$ we find

$$\begin{aligned}
 & (1-c)^q 2(2+c) \sum_{0 \leq k < (3q-e)/3} \binom{3k+e}{k} c^{2k} (1-c)^{3q-1-e-3k} \\
 & \equiv (1-c)^q \left((\alpha^{3q-e} + \beta^{3q-e}) + 3 \frac{\alpha^{3q-e} - \beta^{3q-e}}{\alpha - \beta} \right) \pmod{(\beta^{3q-e}, p)}.
 \end{aligned}$$

Because the factor $(1-c)^q$ is coprime with the modulus β^{3q-e} , we deduce

$$\begin{aligned}
 & 2(2+c) \sum_{0 \leq k < (3q-e)/3} \binom{3k+e}{k} c^{2k} (1-c)^{3q-1-e-3k} \\
 & \equiv (\alpha^{3q-e} + \beta^{3q-e}) + 3 \frac{\alpha^{3q-e} - \beta^{3q-e}}{\alpha - \beta} \pmod{(\beta^{3q-e}, p)}.
 \end{aligned}$$

Arguing as we did in previous cases, the right-hand side is actually a polynomial in c , and hence the congruence holds modulo (c^{3q-e}, p) . As a polynomial in c the right-hand side has degree less than $3q - e$, and after accounting for the leading term of the left-hand side, which is $2(-c)^{3q-e}$, we obtain the desired conclusion for $m = 3$.

The proof of Theorem 3 is now complete.

5. EXPLOITING POLYNOMIAL CONGRUENCES

Working modulo $c^q - c$, and conveniently separating the initial term of the summation in the congruences of Corollary 4, we deduce the weaker but simpler congruences

$$(15) \quad 2(2+c) \sum_{0 < k < q/3} \binom{3k}{k} x^k \equiv -3 + 3(1-4c)^{(q-1)/2} \pmod{(c^q - c, p)},$$

and

$$(16) \quad 2(2+c)(1-c) \sum_{0 < k < q} \binom{3k}{k} x^k \equiv -3 + 3(1-4c)^{(q-1)/2} \pmod{(c^q - c, p)},$$

which take place in the polynomial ring $\mathbb{Z}[c]$, with $x = c^2/(1-c)^3$. In particular, when evaluating those sums on a p -adic integer c these congruences may be used in place of the more general Corollary 4, as $c^p \equiv c \pmod{p}$ then. In fact, the first of a set of four congruences proved in [6, Theorem 1.1] amounts to Equation (16) evaluated on a p -adic integer c , with $c \not\equiv 0, 1, -2 \pmod{p}$. Although Equations (15) and (16) give no information when $c = -2$, the corresponding value for x is also obtained for $c = 1/4$, where they give $\sum_{0 < k < q/3} \binom{3k}{k} (4/27)^k \equiv -2/3 \pmod{p}$, and $\sum_{0 < k < q} \binom{3k}{k} (4/27)^k \equiv -8/9 \pmod{p}$. The latter congruence appeared in [6, Theorem 3.1].

The fact that Equations (15) and (16) have the same right-hand side shows that the sums over the ranges $0 < k < q/3$ and $0 < k < q$ are related in a simple way when $c \in \mathbb{F}_q$. In particular, for $c \in \mathbb{F}_q \setminus \{1\}$ either sum vanishes if and only if the other one does. Our next result determines when the sum over the short range vanishes (modulo p).

Theorem 5. *Let $p > 3$ be a prime and let q be a power of p , and let $a \in \mathbb{F}_q$ with $a \neq 0, 1/9, 4/27$. Then the equality $\sum_{0 < k < q/3} \binom{3k}{k} a^k = 0$ holds if, and only if, the polynomial $a(1-z)^3 - z^2$ has three roots in $\mathbb{F}_q$.*

The special case $q = p$ of Theorem 5 is in [8, Theorem 2.1], under the additional assumption $a \neq 1/27$, which appears superfluous with our proof.

Proof. Suppose first that all roots of cubic polynomial $a(1-z)^3 - z^2$ belong to $\mathbb{F}_q$. They are distinct because its discriminant $a(4-27a)$ is not zero. Moreover, neither 1 nor -2 is a root. According to Equation (15), for each root $c \in \mathbb{F}_q$ of $a(1-z)^3 - z^2$ we have

$$\sum_{0 < k < q/3} \binom{3k}{k} a^k = \frac{-3 + 3(1-4c)^{(q-1)/2}}{2(2+c)} \in \left\{0, \frac{-3}{2+c}\right\},$$

because $(1-4c)^{(q-1)/2} = \pm 1$. Because the latter alternative can hold for at most one value of c , we conclude that the former alternative holds, which is the desired conclusion.

In the opposite direction, suppose $\sum_{0 < k < q/3} \binom{3k}{k} a^k = 0$, and let c satisfy $a(1-c)^3 - c^2 = 0$, with c in the algebraic closure of $\mathbb{F}_q$. Our goal is to show that $c^q = c$,

which is equivalent to $c \in \mathbb{F}_q$. The first congruence of Corollary 4 with $x = a$ yields

$$2(2+c)(1-c)^{q-1} = 1 + 3(1-4c)^{(q-1)/2} + 2c^q,$$

or, equivalently,

$$(4+2c)(1-c^q) - (1+2c^q)(1-c) = 3(1-4c)^{(q-1)/2}(1-c),$$

which simplifies to

$$1+c-2c^q = (1-4c)^{(q-1)/2}(1-c).$$

Squaring both sides and then multiplying by $1-4c$ yields

$$((1-c) - 2(c^q - c))^2(1-4c) = (1-4c^q)(1-c)^2,$$

which is equivalent to

$$4(c^q - c)(1-c)^2 - 4(c^q - c)(1-c)(1-4c) + 4(c^q - c)^2(1-4c) = 0.$$

Unless $c^q = c$, which is the desired conclusion, we deduce

$$(1-c)^2 - (1-c)(1-4c) + (c^q - c)(1-4c) = 0,$$

whence $1-c^q = (1-c)^2/(1-4c)$, and $c^q = -c(2+c)/(1-4c)$. Because $c \neq 0, 1$ we also find $c^{q-1} = -(2+c)/(1-4c)$ and $(1-c)^{q-1} = (1-c)/(1-4c)$.

At this point we use the information that $a \in \mathbb{F}_q^*$, which means $a^{q-1} = 1$, and reads $c^{2(q-1)} = (1-c)^{3(q-1)}$ in terms of c . Substituting the expressions that we just found for c^{q-1} and $(1-c)^{q-1}$ we find $(2+c)^2(1-4c) = (1-c)^3$. Noting that $(2+c)^2(1-4c) = 4(1-c)^3 - 27c^2$ we find $(1-c)^3 = 9c^2$, in contrast with our hypothesis $a \neq 1/9$. This contradiction concludes the proof. $\square$

In the rest of this section we discuss some consequences of Theorem 5. If $a \in \mathbb{F}_q$ then $a(1-z)^3 - z^2$, like any cubic polynomial in $\mathbb{F}_q[x]$, has all its roots in $\mathbb{F}_{q^2}$ or $\mathbb{F}_{q^3}$, and hence splits into linear factors over the extension field $\mathbb{F}_{q^6}$. Therefore, as an example, when $a = 1$ we find

$$(17) \quad \sum_{0 < k < q/3} \binom{3k}{k} \equiv 0 \pmod{p}$$

for $p > 3$ and $p \neq 23$, and q a power of p^6 . This is the crucial case of [6, Theorem 1.4], which was proved there in a more complicated way. Of course the hypothesis that q is a power of p^6 can be relaxed to the polynomial $(1-z)^3 - z^2$ splitting into linear factors over $\mathbb{F}_q$.

Similarly, for $p > 3$ and $p \neq 31$, and q any power of p^6 we have

$$(18) \quad \sum_{0 < k < q/3} \binom{3k}{k} (-1)^k \equiv 0 \pmod{p},$$

Combining Equations (17) and (18) we find

$$\sum_{0 < h < q/6} \binom{6h}{2h} \equiv \sum_{0 < h < q/6} \binom{6h-3}{2h-1} \equiv 0 \pmod{p}$$

for $p > 3$ and $p \notin \{23, 31\}$, and q any power of p^6 .

If $a = 4/(27 + m^2)$ with $m \in \mathbb{Q}$, then

$$\sum_{0 < k < q/3} \binom{3k}{k} a^k \equiv 0 \pmod{p},$$

whenever q is a power of p^3 and $a \in \mathbb{Z}_p$. This is because the discriminant $a(1 - 4m)$ of the polynomial $a(1 - z)^3 - z^2$ is then a perfect square (equal to $(am)^2$), and hence all roots of the polynomial viewed modulo p belong to $\mathbb{F}_{p^3}$. The special case where $q = p$ is part of [8, Theorem 2.5].

Theorem 5 can also be applied to algebraic integer values for a , such as $a = i$. With $p > 3$, imposing $i^2 \not\equiv (4/27)^2 \pmod{p}$ amounts to $5 \cdot 149 \not\equiv 0 \pmod{p}$. Consequently, if $p > 3$ and $p \notin \{5, 149\}$, the congruence

$$\sum_{0 < k < q/3} \binom{3k}{k} i^k \equiv 0 \pmod{p},$$

holds for any power q of p^6 if $p \equiv 1 \pmod{4}$, and for q a power of p^{12} if $p \equiv -1 \pmod{4}$. Together with Equations (17) and (18), under the same assumptions but including $p \notin \{23, 31\}$ we conclude

$$\sum_{0 < h < q/12} \binom{12h}{4h} \equiv 0 \pmod{p}.$$

In a similar fashion, one may take $a = \pm\omega$, where $\omega = (-1 + \sqrt{-3})/2$. For example, taking $a = \omega$, and combining with Equation (17), if $p > 3$ and $p \notin \{23, 853\}$ one concludes that

$$\sum_{0 < h < q/9} \binom{9h}{3h} \equiv 0 \pmod{p}$$

holds for q a power of p^6 if $p \equiv 1 \pmod{3}$, and for q a power of p^{12} if $p \equiv -1 \pmod{3}$.

6. A DIFFERENT APPROACH TO THE CUBIC EQUATION

Now we take a different approach to the series $y = \sum_{k=0}^{\infty} \binom{3k}{k} x^k$. According to Equation (1) it satisfies $(4 - 27x)y^3 - 3y - 1 = 0$. In principle one may obtain a closed form for this generating function by solving this equation through Cardano's formula. However, such a closed form would involve taking both a square root and a cube root, and this is not well suited to further manipulations we intend to do in order to deduce a congruence modulo a prime for a truncated version of the series.

The discriminant of $(4 - 27x)y^3 - 3y - 1$, viewed as a polynomial in y , equals $3^6 \cdot x(4 - 27x)$. We would like to substitute a rational function for x in such a way that the discriminant becomes the square of a rational function. The most elegant substitution appears to be $x = 4s^2/(27(s^2 - 1))$, which amounts to $s^2 = -27x/(4 - 27x)$, for which the discriminant becomes $-3 \cdot (12s)^2/(s^2 - 1)^2$. Note that the discriminant is only a square up to the factor -3 , but some occurrence of a square root of -3 is bound to turn up somewhere with any other choice of

a substitution, as solving the cubic equation by radicals requires the presence of a primitive cube root of unity $(-1 \pm \sqrt{-3})/2$ in the ground field. Adopting that substitution the series y acquires the following simple closed form.

Lemma 6. *In the power series ring $\mathbb{Q}[[s]]$ we have*

$$2 \sum_{k=0}^{\infty} \binom{3k}{k} \left(\frac{4s^2}{27(s^2-1)} \right)^k = (1+s)^{2/3}(1-s)^{1/3} + (1-s)^{2/3}(1+s)^{1/3}.$$

Proof. According to the case $r = 3$ of Equation (1), which reads $(4 - 27x)y^3 - 3y - 1 = 0$, after applying the substitution $x = 4s^2/(27(s^2 - 1))$ the formal series

$$y_1(s) := \sum_{k=0}^{\infty} \binom{3k}{k} \left(\frac{4s^2}{27(s^2-1)} \right)^k \in \mathbb{Q}[[s]]$$

is a root of the polynomial

$$\frac{4}{1-s^2} \cdot y^3 - 3y - 1 \in (\mathbb{Q}[[s]])[y].$$

Because $4y^3 - 3y - 1 = (y-1)(2y+1)^2$, the series $y_1(s)$ is the only root of this polynomial having constant term 1. The series

$$y_2(s) := \frac{1}{2}(1-s^2)^{1/3} \cdot ((1+s)^{1/3} + (1-s)^{1/3}) \in \mathbb{Q}[[s]]$$

has constant term 1 and is also root of the same polynomial, whence $y_1(s) = y_2(s)$ as claimed. $\square$

Now we derive corresponding congruences for the finite sums.

Theorem 7. *Set $x = 4s^2/(27(s^2 - 1))$ in the polynomial ring $\mathbb{Z}[s]$. Let q be a power of the prime $p > 3$, and set $\varepsilon = \left(\frac{q}{3}\right)$, a Legendre symbol. Thus, $\varepsilon = \pm 1$ according to whether $q \equiv \pm 1 \pmod{3}$. Then*

$$2(1-s^2)^{(2q-3+\varepsilon)/6} \sum_{0 \leq k < q/3} \binom{3k}{k} x^k \equiv (1+s)^{(2q+\varepsilon)/3} + (1-s)^{(2q+\varepsilon)/3} \pmod{p},$$

and

$$\begin{aligned} & 2(1-s^2)^{(4q-3-\varepsilon)/6} \sum_{0 \leq k < 2q/3} \binom{3k}{k} x^k \\ & \equiv (1+s)^{(q-\varepsilon)/3} (1-s^q/3) + (1-s)^{(q-\varepsilon)/3} (1+s^q/3) \pmod{p}. \end{aligned}$$

From the two congruences of Theorem 7 one obtains the polynomial congruence

$$\begin{aligned} & 3(1-s^2)^{(4q-3-\varepsilon)/6} s^{-q} \sum_{q/2 \leq k < 2q/3} \binom{3k}{k} x^k \\ & \equiv (1+s)^{(q-\varepsilon)/3} - (1-s)^{(q-\varepsilon)/3} \pmod{p}, \end{aligned}$$

where in the range $q/3 \leq k < q/2$ we have used Lemma 1 for $r = 3$.

Proof. Starting from the identity of power series in Lemma 6 we produce polynomial congruences in the usual way. We start with the shorter range, noting that $\sigma = (2q - 3 + \varepsilon)/6$ is the largest integer which is less than $q/3$.

On the one hand we have

$$\begin{aligned} & 2(1 - s^2)^\sigma \sum_{k=0}^{\infty} \binom{3k}{k} x^k \\ & \equiv 2(1 - s^2)^\sigma \sum_{0 \leq k < q/3} \binom{3k}{k} \left(\frac{4s^2}{27(s^2 - 1)} \right)^k \pmod{(s^q, p)} \\ & = 2 \sum_{0 \leq k < q/3} \binom{3k}{k} (-4s^2/27)^k (1 - s^2)^{\sigma-k}. \end{aligned}$$

This final expression is a polynomial in s , of degree at most 2σ , which is less than q . On the other hand, because $(1 \pm s)^{q/3} \equiv 1 \pmod{(s^q, p)}$, for $q \equiv 1 \pmod{3}$ we have

$$\begin{aligned} & 2(1 - s^2)^{(q-1)/3} \sum_{k=0}^{\infty} \binom{3k}{k} x^k \\ & = (1 + s)^{(q+1)/3} (1 - s)^{q/3} + (1 - s)^{(q+1)/3} (1 + s)^{q/3} \\ & \equiv (1 + s)^{(2q+1)/3} + (1 - s)^{(2q+1)/3} \pmod{(s^q, p)} \end{aligned}$$

and for $q \equiv -1 \pmod{3}$ we have

$$\begin{aligned} & 2(1 - s^2)^{(q-2)/3} \sum_{k=0}^{\infty} \binom{3k}{k} x^k \\ & = (1 + s)^{q/3} (1 - s)^{(q-1)/3} + (1 - s)^{q/3} (1 + s)^{(q-1)/3} \\ & \equiv (1 - s)^{(2q-1)/3} + (1 + s)^{(2q-1)/3} \pmod{(s^q, p)}. \end{aligned}$$

Now we prove the congruence over the longer range $0 \leq k < 2q/3$. Note that $q - 1 - \sigma = (4q - 3 - \varepsilon)/6$ is the largest integer which is less than $2q/3$.

On the one hand we have

$$\begin{aligned} & 2(1 - s^2)^{q-1-\sigma} \sum_{k=0}^{\infty} \binom{3k}{k} x^k \\ & \equiv 2(1 - s^2)^{q-1-\sigma} \sum_{0 \leq k < 2q/3} \binom{3k}{k} \left(\frac{4s^2}{27(s^2 - 1)} \right)^k \pmod{(s^{2q}, p)} \\ & = 2 \sum_{0 \leq k < 2q/3} \binom{3k}{k} (-4s^2/27)^k (1 - s^2)^{q-1-\sigma-k}. \end{aligned}$$

This last expression is a polynomial in s , of degree not exceeding $2q - 2 - 2\sigma$, which is less than $2q$. On the other hand, because $(1 \pm s)^{q/3} \equiv 1 \pm s^{q/3} \pmod{(s^{2q}, p)}$,

for $q \equiv 1 \pmod{3}$ we have

$$\begin{aligned} & 2(1-s^2)^{(2q-2)/3} \sum_{k=0}^{\infty} \binom{3k}{k} x^k \\ &= (1-s^2)^{q/3} (1+s)^{q/3} (1-s)^{(q-1)/3} + (1-s^2)^{q/3} (1-s)^{q/3} (1+s)^{(q-1)/3} \\ &\equiv (1-s)^{(q-1)/3} (1+s^q/3) + (1+s)^{(q-1)/3} (1-s^q/3) \pmod{(s^{2q}, p)}. \end{aligned}$$

and for $q \equiv -1 \pmod{3}$ we have

$$\begin{aligned} & 2(1-s^2)^{(2q-1)/3} \sum_{k=0}^{\infty} \binom{3k}{k} x^k \\ &= (1-s^2)^{q/3} (1+s)^{(q+1)/3} (1-s)^{q/3} + (1-s^2)^{q/3} (1-s)^{(q+1)/3} (1+s)^{q/3} \\ &\equiv (1+s)^{(q+1)/3} (1-s^q/3) + (1-s)^{(q+1)/3} (1+s^q/3) \pmod{(s^{2q}, p)}. \end{aligned}$$

This concludes our proof. $\square$

7. SOME NUMERICAL APPLICATIONS OF THEOREM 7

In this final section we give several numerical applications of Theorem 7 by assigning some interesting values to s . Recall that $x = 4s^2/(27(s^2-1))$. To simplify notation, all unadorned congruences in this section are meant modulo p , with $p > 3$.

For $s = 3$ the two congruences of Theorem 7 give

$$\sum_{0 \leq k < q/3} \binom{3k}{k} \frac{1}{6^k} \equiv \begin{cases} 2^{(2q-1)/3} - 2^{(q+1)/3} & \text{if } q \equiv -1 \pmod{3}, \\ 2^{(q+2)/3} - 2^{(2q-2)/3} & \text{if } q \equiv 1 \pmod{3}, \end{cases}$$

and

$$\sum_{k=0}^{q-1} \binom{3k}{k} \frac{1}{6^k} \equiv \begin{cases} -2^{(q-2)/3} & \text{if } q \equiv -1 \pmod{3}, \\ 2^{(q-1)/3} & \text{if } q \equiv 1 \pmod{3}, \end{cases}$$

the second of which is one of the assertions of [6, Theorem 1.2].

For $s = i\sqrt{3} = 1 + 2\omega = -1 - 2\omega^{-1}$, where $\omega = \exp(2\pi i/3)$, we have $s^2 = -3$ and $(1 \pm s)^3 = -8 = (-2)^3$. Write $q \equiv b \pmod{9}$, with $b \in \{\pm 1, \pm 2, \pm 4\}$ (as we are assuming $p > 3$). When $q \equiv -1 \pmod{3}$, that is, $b \in \{-1, 2, -4\}$, we have

$$\begin{aligned} \sum_{0 \leq k < q/3} \binom{3k}{k} \frac{1}{9^k} &\equiv 2^{-(2q-1)/3} \cdot (-2\omega^{-1})^{(2q-1)/3} + (-2\omega)^{(2q-1)/3} \\ &\equiv -\omega^{-(2b-1)/3} - \omega^{(2b-1)/3} \pmod{p}, \end{aligned}$$

which is congruent to 1, 1 or -2 according as $b = -1$, $b = 2$ or $b = -4$. Together with a similar calculation for the case $q \equiv 1 \pmod{3}$, we obtain

$$(19) \quad \sum_{0 \leq k < q/3} \binom{3k}{k} \frac{1}{9^k} \equiv \begin{cases} 1 & \text{if } q \equiv \pm 1 \pmod{9}, \\ 1 & \text{if } q \equiv \pm 2 \pmod{9}, \\ -2 & \text{if } q \equiv \pm 4 \pmod{9}. \end{cases}$$

Similarly, we find

$$(20) \quad \sum_{k=0}^{q-1} \binom{3k}{k} \frac{1}{9^k} \equiv \begin{cases} 1 & \text{if } q \equiv \pm 1 \pmod{9}, \\ 0 & \text{if } q \equiv \pm 2 \pmod{9}, \\ -1 & \text{if } q \equiv \pm 4 \pmod{9}, \end{cases}$$

as in [6, Theorem 1.5]. Note that according to Lemma 6 we have $\sum_{k=0}^{\infty} \binom{3k}{k} 9^{-k} = \exp(i\pi/9) + \exp(-i\pi/9) = 2 \cos(\pi/9)$.

Remark 8. The above results explain why the assumption $a \neq 1/9$ was essential for one of the implications of Theorem 5. In fact, when $q \equiv \pm 2 \pmod{9}$ we have $\sum_{0 < k < q/3} \binom{3k}{k} 9^{-k} \equiv 0 \pmod{p}$ according to Equation (19). However, according to Equation (20), when $q \equiv \pm 2 \pmod{9}$ we also have $\sum_{0 < k < q} \binom{3k}{k} 9^{-k} \equiv -1 \pmod{p}$. Consequently, the polynomial $(1 - z)^3 - 9z^2$ has no roots in $\mathbb{F}_q$, because if any such root c existed then according to Equations (15) and (16) the sums on the shorter range would equal $1 - c$ times the sum over the longer range.

For $s = 1/\sqrt{5}$ we have $(1 \pm s) = \pm 2\phi_{\pm}/\sqrt{5}$ with $\phi_{\pm} = (1 \pm \sqrt{5})/2$. Letting $\varepsilon = (\frac{q}{3})$ as in Theorem 7, we find

$$\sum_{0 \leq k < q/3} \binom{3k}{k} \left(-\frac{1}{27}\right)^k \equiv \frac{(\phi_+)^{(2q+\varepsilon)/3} - (\phi_-)^{(2q+\varepsilon)/3}}{\sqrt{5}} = F_{(2q+\varepsilon)/3}.$$

Note that $F_{(2q+\varepsilon)/3} \equiv (\frac{q}{5}) F_{(q-\varepsilon)/3 - (\frac{q}{5})} \pmod{p}$ because $2\phi_{\pm}^p = 1 \pm (\frac{p}{5})\sqrt{5}$, see [3, p.144], for example. Taking this into account we recover the congruence in [7, Corollary 3.1]. In a similar way we obtain

$$\sum_{q/2 < k < 2q/3} \binom{3k}{k} \left(-\frac{1}{27}\right)^k \equiv \frac{(\phi_+)^{(q-\varepsilon)/3} - (\phi_-)^{(q-\varepsilon)/3}}{3\sqrt{5}} = \frac{F_{(q-\varepsilon)/3}}{3}.$$

In this case the corresponding power series converges, and according to Lemma 6

$$\sum_{k=0}^{\infty} \binom{3k}{k} \left(-\frac{1}{27}\right)^k = \frac{(\phi_+)^{1/3} + (\phi_-)^{1/3}}{\sqrt{5}} = \frac{2 \cosh(\ln(\phi_+)/3)}{\sqrt{5}}.$$

By setting $s = 2/\sqrt{5}, 3/\sqrt{5}, i/\sqrt{3}, i$ in Theorem 7 one obtains similar congruences for $x = -16/27, 1/3, 1/27, 2/27$, respectively.

REFERENCES

- [1] R. E. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics*, second ed., Addison-Wesley, New York, 1994.
- [2] È. Lucas, *Sur les congruences des nombres eulériens et les coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1878), 49–54.
- [3] S. Mattarei and R. Tauraso, *Congruences for central binomial sums and finite polylogarithms*, J. Number Theory **133** (2013), 131–157.
- [4] S. Mattarei and R. Tauraso, *From generating series to polynomial congruences*, J. Number Theory **182** (2018), 179–205.

- [5] R. P. Stanley, *Enumerative combinatorics, Vol. 2*, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, Cambridge, 1999.
- [6] Zhi-Wei Sun, *Various congruences involving binomial coefficients and higher-order Catalan numbers*, preprint, [arXiv:0909.3808v2](https://arxiv.org/abs/0909.3808v2).
- [7] Zhi-Hong Sun, *Congruences concerning Lucas sequences*, Int. J. Number Theory **10** (2014), 793–815.
- [8] Zhi-Hong Sun, *Cubic congruences and sums involving $\binom{3k}{k}$* , Int. J. Number Theory **12** (2016), 143–164.
- [9] H. S. Wilf, *Generatingfunctionology*, third ed., A K Peters, Ltd., Wellesley, MA, 2006.
Email address: `sandro.mattarei@unimib.it`

DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, UNIVERSITÀ DEGLI STUDI DI MILANO - BICOCCA, VIA COZZI 55, 20125 MILANO, ITALY

Email address: `tauraso@mat.uniroma2.it`

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI ROMA “TOR VERGATA”, VIA DELLA RICERCA SCIENTIFICA, 00133 ROMA, ITALY