Canad. Math. Bull. Vol. 67 (2), 2024, pp. 304–317
http://dx.doi.org/10.4153/S0008439523000723

On theorems of Fermat, Wilson, and Gegenbauer

Heng Huat Chan, Song Heng Chan, Teoh Guan Chua, and Cheng Yeaw Ku

Abstract. In this article, we give generalizations of the well-known Fermat's Little Theorem, Wilson's theorem, and the little-known Gegenbauer's theorem.

1 Introduction

The well-known Fermat's Little Theorem states that for any prime p and any integer a,

$$a^p \equiv a \pmod{p}. \tag{1.1}$$

Wilson's theorem, on the other hand, states that for any prime p,

$$(p-1)! \equiv -1 \pmod{p}. \tag{1.2}$$

Around 1956, Moser [13] discovered the congruence

$$(p-1)!a^p + (p-1)^2 a \equiv 0 \pmod{p}. \tag{1.3}$$

By setting $a = 1$ in (1.3), one obtained (1.2), and using (1.2) in (1.3), we deduced (1.1). On the other hand, (1.3) follows immediately from (1.2) and (1.1). Moser's congruence (1.3) was mentioned in the book of Sierpinski [20, pp. 216 – 217]. Sierpinski appeared to have mistaken that Moser discovered

$$(p-1)!a + a^p \equiv 0 \pmod{p} \tag{1.4}$$

when it should have been (1.3).

About 30 years later, Moser's brother, William Moser [14], found a generalization of Moser's congruence (1.3) given by

$$\sum_{d|n} \varphi^2(d) \left(\frac{n}{d}\right)! d^{n/d} a^{n/d} \equiv 0 \pmod{n^2}, \tag{1.5}$$

Received by the editors August 11, 2023; revised August 31, 2023; accepted September 7, 2023.
Published online on Cambridge Core September 12, 2023.
AMS subject classification: **11A07**, **11A25**.
Keywords: Fermat's theorem, Wilson's theorem, Frobenius–Burnside theorem, Gegenbauer's theorem.

where

$$\varphi(n) = \sum_{\substack{1\le k\le n\\ \gcd(k,n)=1}}^{n} 1.$$

When n is a prime p, (1.5) reduces to (1.3). Since the special case of (1.5) is discovered by L. Moser and (1.5) is discovered by his brother, we will name (1.5) the Moser–Moser congruence. The Moser–Moser congruence is a generalization of (1.3), while (1.4) is its analog. In this article, we will derive new generalizations of (1.3) and (1.4).

In 2006, a special case of (1.5) with the value $a = 1$, namely,

$$\sum_{d|n} \varphi^2(d)\left(\frac{n}{d}\right)!d^{n/d} \equiv 0 \pmod{n^2}, \tag{1.6}$$

was rediscovered by Evans [9] as a generalization of (1.2). It turns out that Evans' proof of (1.6), which is different from Moser's proof, can be modified to derive (1.5).

The proofs of Evans and Moser of (1.5) are different. Evans used the action of the group $\mathbf{Z}/n\mathbf{Z}$ on the set of Hamilton cycles with n vertices, whereas Moser used the action of the group $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ on the set of line permutations of $\{1, 2, \ldots, n\}$. In this article, we will present a third proof of (1.6). We will then deduce the Moser–Moser congruence (1.5), which is (1.6) with an extra factor of $a^{n/d}$, from L. Gegenbauer's theorem [10] is given as follows.

Theorem 1.1 *Let n and a be positive integers. Let $F : \mathbf{Z}^+ \to \mathbf{Z}$. Suppose $F(n) \neq \mu(n)$, where μ is defined in Section 4 (see Definition 4.1). If*

$$\sum_{d|n} F(d) \equiv 0 \pmod{n},$$

then

$$\sum_{d|n} F(d)a^{n/d} \equiv 0 \pmod{n}.$$

Although

$$\sum_{d|n} \mu(d)a^{n/d} \equiv 0 \pmod{n} \tag{1.7}$$

is true, it does not follow from Theorem 1.1 and the fact [3, Theorem 2.1] that

$$\sum_{d|n} \mu(d) = 0,$$

for $n > 1$. This is because (1.7) is used in the proof of Theorem 1.1 and (1.7) needs to be proved separately as what Gegenbauer did in his article.

In the next section, we state the Frobenius–Burnside theorem, a fundamental tool used in proving many congruences such as (1.5) and (1.7). In Section 3, we give a new proof of the Moser–Moser congruence (1.5) using the Frobenius–Burnside. In Section 4, we give a new proof of an interesting result of András [1, p. 267, Remark 2] (see

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

Theorem 4.3) and give a brief history of (1.7) and its analogue. In Section 5, we give a generalization of (1.5). In the final section, we prove a generalization of Theorem 1.1.

In this article, several congruences such as (1.5) are stated modulo n^2, whereas Theorems such as Theorem 1.1 hold modulo n. We emphasize that in all our examples, we derive

$$\frac{1}{n}\sum_{d|n} F(d) \equiv 0 \pmod{n}$$

using theorems such as Theorem 1.1 and conclude that

$$\sum_{d|n} F(d) \equiv 0 \pmod{n^2}.$$

We now summarize our contributions. In this article, we present a new proof of the Moser–Moser congruence with the help of Theorem 1.1. Surprisingly, this theorem has remained relatively obscure despite its significance. We have also found the origin of (1.6). We have identified an error in Sierpinski's book, where he mistakenly attributed (1.4) instead of (1.3) to L. Moser. Additionally, we have unveiled a comprehensive generalization that encompasses both (1.3) and (1.4) (see Section 5). By using Theorem 4.3 and Theorem 6.1, we derived many new congruences from well-established ones, such as Moreau's congruence.

We would like to thank the anonymous referee for his/her invaluable insights and the references [4, 23]. These references establish crucial connections between our work and Dold sequences. Notably, one can see a link between our generalization of the Gegenbauer theorem (Theorem 6.1) and [23, Theorem 7]. This connection becomes apparent when we recognize that the function $G(n)$ defined in Theorem 6.1 is Dold sequences, leading to the conclusion that Theorem 8 follows from the equivalence of the statements in [23, Theorem 7]. This connection also shows that many of the examples discussed in this article are, therefore, examples of Dold sequences. Some of the sequences contained in (6.4) and in (6.6) might pose challenges for direct verification as Dold sequences under alternative circumstances. Finally, as highlighted by the referee, several previous works, including [1, 23], have overlooked the significance of the Gegenbauer theorem (Theorem 1.1). Our article serves to rectify this gap in the mathematical discourse.

2 The Frobenius–Burnside theorem

Let $(G, \circ)$ be a group with identity 1_G, and let X be a nonempty set. A left action of the group G on X is a function

$$\bullet : G \times X \to X,$$

which we write $g \bullet x$ instead of $\bullet(g, x)$, with the following properties that for all $a, b \in G$ and $x \in X$:

(1) $a \bullet (b \bullet x) = (a \circ b) \bullet x$,
(2) $1_G \bullet x = x$.

We say that G acts on X via $\bullet$.

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

Given a group G acting (via $\bullet$) on a nonempty set X, we define a relation $\sim$ as follows:

$$u \sim x \text{ if and only if there exists a } g \in G \text{ such that } g \bullet x = u.$$

The relation $\sim$ is an equivalence relation on X. This implies that X is a disjoint union of equivalence classes $\mathcal{O}_x$, which are also called G-orbits, where

$$\mathcal{O}_x := \{u \in X | u \sim x\}.$$

When X is a finite set, the number of distinct G-orbits in X is given by the following theorem.

Theorem 2.1 (The Frobenius–Burnside theorem) *Let G be a group acting on a finite set X, and let*

$$\mathrm{Fix}(g) = \{x \in X | g \bullet x = x\}.$$

The number of disjoint G-orbits N in X is given by

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|,$$

where $|S|$ denotes the number of elements in the set S.

We emphasize that in the proof of Theorem 2.1, one has to show that if

$$\mathrm{Stab}_G(x) = \{g \in G | g \bullet x = x\},$$

then

$$|\mathcal{O}_x| = \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

This shows immediately that

$$|\mathcal{O}_x| \text{ divides } |G|. \tag{2.1}$$

For a complete proof of the Frobenius–Burnside theorem, see [17, Chapter 5].

3 A new proof of the Moser–Moser congruence

For any positive integer n, let S_n denote the set of bijections on

$$\{1, 2, \ldots, n-1, n\}.$$

For $g \in S_n$, let

$$g = \tau_1 \tau_2 \cdots \tau_r$$

be the complete factorization (which is unique up to the arrangement of the cycles) of g into disjoint cycles. If τ_j is a cycle with length λ_j, then we say that g has cycle type

$$(\lambda_1, \lambda_2, \ldots, \lambda_r).$$

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

If g has a_j cycles of length j, we say that g has cycle structure

$$\langle 1^{a_1} 2^{a_2} \cdots n^{a_n} \rangle.$$

For example, if

$$g = (1\,2)(3\,4)(5\,6)(7\,8\,9),$$

then the cycle type and cycle structure of g are $(3, 2, 2, 2)$ and $\langle 1^0 2^3 3^1 \rangle$, respectively.

The following lemma is well known [5, p. 244].

Lemma 3.1 *Let $g \in S_n$ with cycle structure $\langle 1^{a_1} 2^{a_2} \cdots n^{a_n} \rangle$, and let*

$$\mathcal{C}(g) = \{x \in S_n | g^{-1} x g = x\}$$

be the centralizer of g in S_n. Then

$$|\mathcal{C}(g)| = (1^{a_1} 2^{a_2} \cdots n^{a_n}) a_1! a_2! \cdots a_n! = \prod_{j=1}^{n} j^{a_j} a_j!.$$

We will use Lemma 3.1 to derive the following lemma.

Lemma 3.2 *Suppose $g, h \in S_n$. Let $F(g, h) = \{x \in S_n | g^{-1} x h = x\}$. Then $F(g, h)$ is nonempty if and only if g and h have the same cycle type, or equivalently, g and h are conjugate to each other in S_n. Moreover, if $F(g, h)$ is nonempty, then*

$$|F(g, h)| = \prod_{j=1}^{n} j^{a_j} a_j!,$$

where $\langle 1^{a_1} 2^{a_2} \cdots n^{a_n} \rangle$ is the cycle structure of g (and h).

Proof If g and h are conjugates, then $h = y^{-1} g y$ for some $y \in S_n$ and therefore $y \in F(g, h)$ and $F(g, h)$ is nonempty. If $F(g, h)$ is nonempty, then there exists $y \in F(g, h)$ such that $g^{-1} y h = y$ or $g = y^{-1} h y$, and so g and h are conjugates.

Suppose $h = y^{-1} g y$ for some $y \in S_n$. We claim that if $z \in C(g)$, then $zy \in F(g, h)$. We need only to check that

$$g^{-1} z y h = z g^{-1} y h = z y$$

since $g^{-1} z = z g^{-1}$. Define a map

$$\theta : \mathcal{C}(g) \to F(g, h)$$

by $\theta(z) = zy$, which is valid since $zy \in F(g, h)$. Clearly, θ is injective since $zy = z'y$ implies that $z = z'$.

Next, for $x \in F(g, h)$, note that $g^{-1} x h = x$, or $x h x^{-1} = g$. Let $z = x y^{-1}$. Then

$$z g z^{-1} = x(y^{-1} g y) x^{-1} = x h x^{-1} = g,$$

and therefore $z \in C(g)$. It is clear that $\theta(z) = \theta(x y^{-1}) = x y^{-1} y = x$ and so θ is surjective. The second assertion now follows from Lemma 3.1. ∎

We are now ready to give a new proof of (1.6).

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

Proof of (1.6) Let C_n be the subgroup of S_n generated by the n-cycle $(1\ 2\ \cdots\ n)$. Consider the action $G = C_n \times C_n$ on $X = S_n$ given by $(g,h) \bullet x = g^{-1}xh$. Indeed, this is a group action since

$$\begin{aligned}[(g_1,h_1)\cdot(g_2,h_2)] \bullet x &= (g_1g_2, h_1h_2) \bullet x = (g_1g_2)^{-1}x(h_1h_2) \\ &= g_2^{-1}(g_1^{-1}xh_1)h_2 = (g_2,h_2) \bullet [(g_1,h_1) \bullet x].\end{aligned}$$

By Theorem 2.1, the number of orbits N arising from G acting on S_n is

$$N = \frac{1}{n^2} \sum_{(g,h)\in G} |\mathrm{Fix}((g,h))|. \tag{3.1}$$

Note that $\mathrm{Fix}((g,h)) = F(g,h)$ where $F(g,h)$ is the set defined in Lemma 3.2.

For an element $g \in G$, we will use $o(g)$ to denote the order of g in G. We have seen that $F(g,h)$ is nonempty if and only if g and h are conjugate to each other. In other words, $F(g,h)$ is nonempty if and only if $o(g) = o(h)$. Furthermore, $o(g)|n$. Therefore, we may rewrite (3.1) as

$$N = \frac{1}{n^2} \sum_{d|n} \sum_{\substack{(g,h)\in G \\ o(g)=o(h)=d}} |F(g,h)|. \tag{3.2}$$

Next, it is known that if $o(g) = d$ in C_n, then g has cycle type $c(g) = (d, d, \ldots, d)$, where there are n/d copies of d in $c(g)$. By Lemma 3.2, we conclude that

$$|F(g,h)| = (n/d)!d^{n/d}$$

and rewrite (3.2) as

$$N = \frac{1}{n^2} \sum_{d|n} \varphi^2(d) d^{n/d} (n/d)!,$$

since there are precisely $\varphi^2(d)$ elements $(g,h) \in G$ with $o(g) = o(h)$. The congruence (1.6) now follows immediately. ∎

This new proof of (1.6) explains the presence of $(n/d)!d^{n/d}$ and $\varphi^2(d)$ in (1.6).

This section is motivated by the articles of Evans [9] and András [1]. We are led to these articles because of our interest in generalizing Petersen's proof of Wilson's theorem [15] found in Andrews' book [2, Section 3.3].

4 Some facts about arithmetic functions and András' theorem

An arithmetic function f is a function from the set of positive integers to the set of complex numbers. One of the most important arithmetic functions is the Möbius function defined as follows.

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

Definition 4.1 Let $\mu(1) = 1$ and for $n = \prod_{k=1}^{m} p_k^{\alpha_k}$, let

$$\mu(n) = \begin{cases} (-1)^m, & \text{if } \alpha_k = 1, 1 \le k \le m, \\ 0, & \text{otherwise.} \end{cases}$$

The Dirichlet product of two arithmetic functions is a binary operation defined as follows.

Definition 4.2 Let f and g be two arithmetical functions. We define the *Dirichlet product* of f and g, denoted by $f * g$, as

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

From now on, we will use $f * g(n)$ to represent $(f * g)(n)$, removing the use of brackets. We will record a few facts regarding several arithmetic functions that we need for this article.

Lemma 4.1 *For any $n \in \mathbf{Z}^+$, let $u(n) = 1$, $\mathcal{N}(n) = n$, and $I(n) = [1/n]$, where $[\cdot]$ is the greatest integer function. Then:*

(1) $u * \mu(n) = I(n)$,
(2) $\mu * \mathcal{N}(n) = \varphi(n)$,
(3) $\mu\mathcal{N} * \mathcal{N}(n) = I(n)$.

The proofs of Lemma 4.1(a)–(c) can be found in Apostol's book [3, Theorem 2.1], [3, Theorem 2.3], and [3, Theorem 2.17], respectively.

Lemma 4.2 *Let f and g be two arithmetic functions. Then*

$$f(n) = g * u(n)$$

if and only if

$$g(n) = f * \mu(n).$$

The proof of Lemma 4.2 can be found in [3, Theorem 2.9].

Around 2011, András [1] revisited Evans' work and discovered the following interesting result.

Theorem 4.3 *Let $F(n)$ be an arithmetic function. Then*

$$\sum_{d|n} \varphi(d) F(n/d) \equiv 0 \pmod{n} \tag{4.1}$$

if and only if

$$\sum_{d|n} \mu(d) F(n/d) \equiv 0 \pmod{n}. \tag{4.2}$$

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

András has a complete proof of the above, but (4.1) implies (4.2) was not presented in his article. We now give our proof of Theorem 4.3 using Lemma 4.1.

Proof Suppose (4.1) holds. Then there exists an integer-valued arithmetic function G such that

$$\varphi * F(n) = \mathcal{N}(n)G(n).$$

This implies that

$$\mu\mathcal{N} * \varphi * F(n) = \mu\mathcal{N} * \mathcal{N}(n)G(n). \tag{4.3}$$

Applying Lemma 4.1(b) followed by Lemma 4.1(c), we may rewrite the left-hand side of (4.3) as

$$\mu\mathcal{N} * \varphi * F(n) = \mu\mathcal{N} * \mathcal{N} * \mu * F(n) = I * \mu * F(n) = \mu * F(n).$$

The right-hand side of (4.3) is

$$\mu\mathcal{N} * \mathcal{N}G(n) = \sum_{d|n} \mu(d) d \frac{n}{d} G\left(\frac{n}{d}\right) = n \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) \equiv 0 \pmod{n}.$$

Therefore, (4.2) holds.

Next, suppose (4.2) holds. Then

$$\mu * F(n) = \mathcal{N}(n)G(n)$$

for some integer-valued arithmetic function G. This implies that

$$\mathcal{N} * \mu * F(n) = \mathcal{N} * \mathcal{N}G(n). \tag{4.4}$$

Using Lemma 4.1(b), we deduce that the left-hand side of (4.4) is

$$\mathcal{N} * \mu * F(n) = \varphi * F(n),$$

whereas the right-hand side of (4.4) is

$$\mathcal{N} * \mathcal{N}G(n) = \sum_{d|n} d \frac{n}{d} G\left(\frac{n}{d}\right) = n \sum_{d|n} G(n/d) \equiv 0 \pmod{n}.$$

Therefore, (4.1) holds. ∎

András used Theorem 4.3 to deduce from (1.6) that

$$\sum_{d|n} \mu(d)\varphi(d) \left(\frac{n}{d}\right)! d^{n/d} \equiv 0 \pmod{n^2}.$$

We observe that András' congruence is also a generalization of (1.3). If we apply Theorem 4.3 to (1.5), we deduce the new congruence

$$\sum_{d|n} \mu(d)\varphi(d) \left(\frac{n}{d}\right)! d^{n/d} a^{n/d} \equiv 0 \pmod{n^2}. \tag{4.5}$$

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

Applying Theorem 4.3 one more time to (4.5), we conclude that

$$\sum_{d|n} \mu^2(d) \left(\frac{n}{d}\right)! d^{n/d} a^{n/d} \equiv 0 \pmod{n^2}. \tag{4.6}$$

Both congruences (4.5) and (4.6) are also generalizations of (1.3).

In the next section, we give a generalization of (4.5) and hence generalizations of (1.5) and (4.6) using Theorem 4.3.

With Theorem 4.3, we can now conclude that the congruences

$$\sum_{d|n} \varphi(d) a^{n/d} \equiv 0 \pmod{n} \tag{4.7}$$

and (1.7) are equivalent. Both (4.7) and (1.7) are generalizations of (1.1). We will now give a brief history of (4.7) and (1.7). Congruence (4.7) was discovered by MacMahon [11] using the following result of Moreau [12, p. 313].

Theorem 4.4 *Let n be a positive integer, and let*

$$n = \alpha_1 + \alpha_2 + \cdots + \alpha_s,$$

where $\alpha_1, \alpha_2, \ldots, \alpha_s$ are positive integers. Let $D = gcd(\alpha_1, \alpha_2, \ldots, \alpha_s)$. Then

$$\sum_{d|D} \varphi(d) \frac{(n/d)!}{(\alpha_1/d)!(\alpha_2/d)!\cdots(\alpha_s/d)!} \equiv 0 \pmod{n}.$$

The works of MacMahon and Moreau are mentioned in Riordan's book [16, p. 162, Problem 37]. The approach to these congruences in [16] involves using the Redfield–Polya theorem (see Stanley's book [21, p. 394, Theorem 7.24.4]). Another proof of (4.7) was given by Gegenbauer [10]. He used Theorem 1.1 and the identity [3, p. 26, Theorem 2.2]

$$\sum_{d|n} \varphi(d) = n \equiv 0 \pmod{n} \tag{4.8}$$

to derive (4.7).

We now discuss (1.7). Congruence (1.7) in the case when a is a prime number is probably known to C.F. Gauss. The expression

$$\frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}$$

counts the number of irreducible polynomials of degree n over the finite field of p elements (see Cox's book [6, p. 300, Theorem 11.2.4]). This means that (1.7), after applying Dirichlet's theorem of primes in arithmetic progression, is true for any integer n such that $(a, n) = 1$. According to Dickson [7, p. 84], (1.7) was first stated by Serret [19, p. 262] in 1855. One of the simplest proofs of (1.7) can be found in Szele's article [22] and Gegenbauer's article [10]. See also an exercise in Rose's book [18, p. 55, Problem 11].

Another proof of (1.7), using Theorem 2.1, relies on counting the number of orbits with exactly n elements for the group $\mathbf{Z}/n\mathbf{Z}$ acting on X, the set of all necklaces

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

obtained from beads which can be colored using a colors. Note that $|X| = a^n$. Let N_m be the number of orbits with exactly m elements. Note that by (2.1), N_m is nonempty if and only if $m|n$. Therefore,

$$a^n = \sum_{d|n} dN_d.$$

Applying Lemma 4.2, we deduce that

$$nN_n = \sum_{d|n} \mu(d) a^{n/d},$$

and (1.7) follows. For yet another proof of (1.7) using periodic points of a function, see [1, p. 268].

5 A generalization of the Moser–Moser congruence

In this section, we derive the following generalization of the Moser–Moser congruence.

Theorem 5.1 *Let n, a, and b be positive integers. Then*

$$\sum_{d|n} \varphi^2(d) \left(\frac{n}{d}\right)! d^{n/d} a^{n/d} b^d \equiv 0 \pmod{n^2}. \tag{5.1}$$

It is immediate that (1.5) is a special case of (5.1) with $b = 1$.

By Theorem 1.1, we see that congruence (5.1) follows immediately from the following.

Theorem 5.2 *Let n and b be positive integers. Then*

$$\sum_{d|n} \varphi^2(d) \left(\frac{n}{d}\right)! d^{n/d} b^d \equiv 0 \pmod{n^2}. \tag{5.2}$$

We should note the difference between (5.2) and (1.5). Our congruence (5.2) is a generalization of (1.4) in exactly the same manner that (1.5) is a generalization of (1.3). We have not been able to find a proof of (5.2) which involves Theorem 2.1.

Proof Let $n = \prod_{j=1}^{s} p_j^{\alpha_j}$. Our aim is to show that for $1 \le j \le s$,

$$\sum_{d|n} \mu(d)\varphi(d)\,(n/d)!\, d^{n/d} a^d \equiv 0 \pmod{p_j^{2\alpha_j}}. \tag{5.3}$$

We note that it suffices to prove (5.3) for a fixed j. Let $p = p_1$ and $\alpha = \alpha_1$. We first observe that the presence of $\mu(n)$ implies that

$$\sum_{d|n} \mu(d)\varphi(d)\,(n/d)!\, d^{n/d} a^d = \sum_{d|pp_2\cdots p_s} \mu(d)\varphi(d)\,(n/d)!\, d^{n/d} a^d.$$

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

We pair up the divisors of $pp_2\cdots p_s$ as pv and v, where $(v,p)=1$. We claim that for each such pair of divisors, the terms corresponding to them satisfy

$$\mu(pv)\varphi(pv)(p^{\alpha-1}\ell/v)!(pv)^{p^{\alpha-1}\ell/v}a^{pv}+\mu(v)\varphi(v)(p^{\alpha}\ell/v)!v^{p^{\alpha}\ell/v}a^{v}\equiv 0 \pmod{p^{2\alpha}}, \tag{5.4}$$

where ℓ is given by $\ell=n/p^{\alpha}$. Congruence (5.4) would imply (5.3). Note that from (5.4), we find that

$$\begin{aligned}&\mu(pv)\varphi(pv)(p^{\alpha-1}\ell/v)!(pv)^{p^{\alpha-1}\ell/v}a^{pv}+\mu(v)\varphi(v)(p^{\alpha}\ell/v)!v^{p^{\alpha}\ell/v}a^{v}\\&\quad=\mu(v)\varphi(v)\left(-\varphi(p)(p^{\alpha-1}\ell/v)!(pv)^{p^{\alpha-1}\ell/v}a^{pv}+(p^{\alpha}\ell/v)!v^{p^{\alpha}\ell/v}a^{v}\right).\end{aligned}$$

Let

$$S_1=(p^{\alpha}\ell/v)!v^{p^{\alpha}\ell/v}a^{v}\quad\text{and}\quad S_2=\varphi(p)(p^{\alpha-1}\ell/v)!(pv)^{p^{\alpha-1}\ell/v}a^{pv}.$$

It suffices to show that

$$S_1-S_2\equiv 0 \pmod{p^{2\alpha}}. \tag{5.5}$$

We divide our arguments into the following cases, according to the values of ℓ/v, α, and p.

Case 1: $\ell/v\geq 2$. We note that $(p^{\alpha}\ell/v)!$ contains the factors $2p^{\alpha}$ and p^{α}. Therefore, $p^{2\alpha}$ is a factor of S_1. On the other hand, we see that

$$p^{\alpha-1}\frac{\ell}{v}\geq 2^{\alpha}\geq 2\alpha.$$

Therefore, $p^{2\alpha}$ divides $p^{p^{\alpha-1}\ell/v}$, and so is a factor of S_2. Hence, (5.5) is true.

Case 2a: $\ell/v=1$ and $\alpha=1$. In this subcase, we find that

$$S_1-S_2=p!v^pa^v-(p-1)vpa^{pv}=p((p-1)!v^pa^v-(p-1)va^{pv})\equiv 0 \pmod{p^2},$$

where we have used Wilson's theorem and Fermat's Little Theorem.

Case 2b(i): $\ell/v=1$, $\alpha=2$ and $p=2$. For these values, we see that

$$S_1-S_2=4!v^4a^v-2!v^22^2a^{2v}=2^3v^2a^v(3v^2-a^v)\equiv 0 \pmod{2^4}$$

since $v^2a^v(3v^2-a^v)$ must be even.

Case 2b(ii): $\ell/v=1$, $\alpha=2$, and $p\geq 3$. We note that $(p^2)!$ contains the factors p^2, $2p$, and p. Hence, p^4 divides S_1. On the other hand, clearly, p^3 divides $(pv)^p$ and so p^4 divides S_2.

Case 2c: $\ell/v=1$ and $\alpha\geq 3$. We note that $(p^{\alpha})!$ contains the factors p^{α}, $p^{\alpha-1}$, and p. Hence, $p^{2\alpha}$ divides S_1. On the other hand,

$$p^{\alpha-1}\geq 2^{\alpha-1}\geq 2(\alpha-2).$$

Therefore, $p^{2\alpha-2}$ divides $p^{p^{\alpha-1}}$. Also, clearly, $p^2|p^{\alpha-1}$. Collectively, we see that $p^{2\alpha}$ divides S_2.

Thus, all cases of the congruence (5.5) are proved, and this completes the proof of the theorem. ∎

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

Once again, by Theorem 4.3, we deduce the following theorem.

Theorem 5.3 *Let n and b be positive integers. Then*

$$\sum_{d|n}\mu(d)\varphi(d)\left(\frac{n}{d}\right)!d^{n/d}b^d a^{n/d} \equiv 0 \pmod{n^2}. \tag{5.6}$$

By using Theorem 4.3 yet again, we deduce from (5.6) the following congruence:

$$\sum_{d|n}\mu^2(d)\left(\frac{n}{d}\right)!d^{n/d}b^d a^{n/d} \equiv 0 \pmod{n^2}.$$

6 Analogues of Gegenbauer's theorem

In this final section, we will derive a generalization of Gegenbauer's theorem.

Theorem 6.1 *Let n be a positive integer. Let $F : \mathbf{Z}^+ \to \mathbf{Z}$ and G be an arithmetic function. Suppose*

$$\sum_{d|n}\mu(d)G(n/d) \equiv 0 \pmod{n}. \tag{6.1}$$

If

$$\sum_{d|n}F(d) \equiv 0 \pmod{n}, \tag{6.2}$$

then

$$\sum_{d|n}F(d)G(n/d) \equiv 0 \pmod{n}.$$

The function $G(n)$ which appears in Theorem 6.1 is known as a Dold sequence [4, Definition 2.1].

Let a be a positive integer, and let

$$G(k) = \begin{cases} a^k, & \text{if } k|n, \\ 0, & \text{otherwise.} \end{cases}$$

Then since (1.7) holds, we see that Theorem 6.1 implies Theorem 1.1.

Our proof of Theorem 6.1 follows Gegenbauer's proof of Theorem 1.1. Another proof of Theorem 6.1 can be found in a recent article of Wójcik [23]. The proof given there is dependent on the equivalence of Newton sequence and Dold sequence established by Du, Huang, and Li [8].

Proof of Theorem 6.1 We write (6.1) and (6.2) as

$$\mu * G(n) = \mathcal{N}H(n)$$

and

$$F * u(n) = \mathcal{N}K(n), \tag{6.3}$$

https://doi.org/10.4153/S0008439523000723 Published online by Cambridge University Press

respectively, where $H(\ell), K(\ell) \in \mathbf{Z}$ for all $\ell \in \mathbf{Z}^+$. From (6.3) and Lemma 4.2, we deduce that

$$F(n) = \mathcal{N}K * \mu(n).$$

This implies that

$$\begin{aligned} F * G(n) &= \mathcal{N}K * \mu * G(n) = \mathcal{N}K * \mathcal{N}H(n) \\ &= \sum_{d|n} dH(d)\frac{n}{d}K\left(\frac{n}{d}\right) = nH * K(n) \equiv 0 \pmod{n}, \end{aligned}$$

and the proof of Theorem 6.1 is complete. ∎

There are already several $G(n)$ which we can choose from the congruences we discussed in the previous sections. For example, we could identify $G(n)$ from (5.6) and deduce using Theorem 6.1 that if (6.2) holds, then

$$\sum_{d|n} F(d)\varphi(d)\left(\frac{n}{d}\right)!d^{n/d}b^d \equiv 0 \pmod{n^2}. \tag{6.4}$$

We may also apply Theorem 6.1 to a variant of Theorem 4.4, which we state as follows (with φ replaced by μ via Theorem 4.3).

Theorem 6.2 *Let n be a positive integer, and let*

$$n = \alpha_1 + \alpha_2 + \cdots + \alpha_s,$$

where $\alpha_1, \alpha_2, \ldots, \alpha_s$ are positive integers. Let $D = gcd(\alpha_1, \alpha_2, \ldots, \alpha_s)$. Then

$$\sum_{d|D} \mu(d)\frac{(n/d)!}{(\alpha_1/d)!(\alpha_2/d)!\cdots(\alpha_s/d)!} \equiv 0 \pmod{n}. \tag{6.5}$$

The function $G(n)$ in (6.1) can now be identified from (6.5), allowing us to deduce from Theorem 6.1 that if (6.2) holds, then

$$\sum_{d|D} F(d)\frac{(n/d)!}{(\alpha_1/d)!(\alpha_2/d)!\cdots(\alpha_s/d)!} \equiv 0 \pmod{n}. \tag{6.6}$$

We may use combinations of Theorem 1.1, (6.4), and (6.6) to derive many new congruences. For example, we have

$$\sum_{d|D} \varphi^2(d)\frac{(n/d)!}{(\alpha_1/d)!(\alpha_2/d)!\cdots(\alpha_s/d)!}\left(\frac{n}{d}\right)!d^{n/d}b^d a^{n/d} \equiv 0 \pmod{n^2}.$$

Acknowledgment We are very grateful to Professors G. E. Andrews, W. Zudilin, and Kuo-Jye Chen for their encouragement. We thank Professor P. Moree for helping us locate L. Moser's paper. We also thank Professors T. J. Evans and S. András for answering our queries with regard to their works. Finally, we thank the referee for the references [4, 23].

References

[1] S. András, *A combinatorial generalization of Wilson's theorem*. Aust. J. Combin . **49**(2011), 265–272.
[2] G. E. Andrews, *Number theory*, W. B. Saunders Company, Philadelphia, PA, 1971.
[3] T. M. Apostol, *Introduction to analytic number theory*, Undergradute Text in Mathematics, Springer, New York, 1976.
[4] J. Byszewski, G. Graff, and T. Ward, *Dold sequences, periodic points, and dynamics*. Bull. Lond. Math. Soc. **53**(2021), 1263–1298.
[5] P. J. Cameron, *Combinatorics: topics, techniques, algorithms*, Cambridge University Press, Cambridge, 1994.
[6] D. A. Cox, *Galois theory*, John Wiley & Sons, Hoboken, NJ, 2004.
[7] L. E. Dickson, *History of the theory of numbers*, Carnegie Institute of Washington, Washington, DC, 1919. Reprinted by Chelsea Publishing, New York, 1971.
[8] B. S. Du, S. S. Huang, and M. C. Li, *Newton, Fermat, and exactly realizable sequence*. J. Integer Seq. **8**(2005), Article no. 05.1.2.
[9] T. J. Evans, *On some generalizations of Fermat's, Lucas's and Wilson's theorems*. Ars Combin. **79**(2006), 189–194.
[10] L. Gegenbauer, *Überein theorem des Herrn MacMahon*. Monatsh. Math. Phys. **11**(1900), 287–288.
[11] P. A. MacMahon, *Applications of the theory of permutations on circular procession to the theory of numbers*. Proc. Lond. Math. Soc. **23**(1891–2), 305–313.
[12] C. Moreau, *Sur les permutations circulaires distincts*. Nouv. Ann. Math. **11**(1872), 309–314.
[13] L. Moser, *On the theorems of Wilson and Fermat*. Scripta Math. **22**(1956), 288.
[14] W. O. J. Moser, *A (modest) generalization of the theorems of Wilson and Fermat*. Can ad. Math. Bull. **33**(1990), 253–256.
[15] J. Petersen, *Beviser for Wilsons og Fermats Theoremer*. Tidsskrift Math. (3) **2**(1872), 64–65.
[16] J. Riordan, *Introduction to combinatorial analysis*, John Wiley & Sons, New York, 1958.
[17] D. J. S. Robinson, *Abstract algebra, an introduction with applications*. 2nd ed., De Gruyter, Berlin, 2015.
[18] H. E. Rose, *A course in number theory*. 2nd ed., Oxford University Press, Oxford, 1994.
[19] J. A. Serret, *Théorème de Fermat généralisé*. Nouv. Ann. Math. **14**(1855), 261–262.
[20] W. Sierpinski, *Elementary theory of numbers*, North-Holland Mathematical Library, 31, Polish Scientific Publishers, Warsaw, 1987.
[21] R. P. Stanley, *Enumerative c ombinatorics. Vol. 2*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1999.
[22] T. Szele, *Une généralization de la congruence de Fermat*. Mat. Tidsskr. B (1948), 57–59.
[23] K. Wójcik, *Newton sequence and Dirichlet convolution*. Integers **21**(2021), Article no. A63.

Department of Mathematics, National University of Singapore, Block S17, 10 Lower Kent Ridge Road, Singapore 119076, Singapore
e-mail: matchh@nus.edu.sg

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Singapore
e-mail: chansh@ntu.edu.sg

Department of Mathematics, Ngee Ann Secondary School, 1 Tampines Street 32, Singapore 529283, Singapore
e-mail: teohguan.chua@gmail.com

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Singapore
e-mail: cyku@ntu.edu.sg