An Extension of a Result of Gauss to Finite Groups: A Linear Algebraic Approach

M. R. Pournaki*

Abstract

Let n be a positive integer and a be an integer. Gauss proved that $\sum_{d|n} \mu(n/d)a^d \equiv 0 \pmod{n}$, where μ is the Möbius function. This result generalizes both Fermat's little theorem and Euler's theorem. In this paper, a generalization of this result to finite groups is proved by methods of (multi-) linear algebra.

Keywords: Finite group, Congruence, Arithmetic function, Tensor product of vector spaces.

2000 Mathematics Subject Classification: Primary 20A05, 11A07, 11A25; Secondary 15A69.

1 Introduction

Fermat's little theorem states that if p is a prime number, then

$$a^p \equiv a \pmod{p} \tag{1}$$

holds true for any integer a. One may ask what happens when p is not a prime. The answer to this question seems little known to mathematicians, even to number theorists. The reason for this seems to be its absence from most of the standard reference books. The missing result which is essentially due to Gauss is a beautiful one (see [2]): If n is any positive integer, then

$$\sum_{d|n} \mu(n/d)a^d \equiv 0 \pmod{n} \tag{2}$$

holds true for any integer a, where μ is the *Möbius function* defined by $\mu(1) = 1$; $\mu(m) = 0$, if m is not square-free; and $\mu(m) = (-1)^r$, if $m = p_1 \ldots p_r$, where p_i's are distinct primes.

Congruence (2) is a generalization of congruence (1); the left hand side of congruence (2) comes down to $a^n - a$ if n is a prime number.

The history of congruence (2) is chronicled in Dickson [1, pp. 84-86]. — In his

*This research was in part supported by a grant from IPM.

early draft of the planned eighth chapter of the *Disquisitiones Arithmeticae*, probably written in 1797 and never published in his lifetime – see the second volume of Gauss's Collected Works (Göttingen 1863), pp. 212-240 –, C. F. Gauss treated congruences of polynomials with integer coefficients, modulo a prime number and an irreducible polynomial. In other words, he developed a theory of what we would treat today as general finite fields, or, equivalently, of residue fields of rings of cyclotomic integers. Warming up for this task, he counted the number of polynomials of a given degree modulo p by grouping them according to the degrees of their irreducible (modulo p) factors. As a consequence, he saw (loc. cit., p. 222, §347) that the left hand side of (2), for a prime number p instead of a, equals n times the number of irreducible (modulo p) polynomials of degree n. In particular, this left hand side is divisible by n. Gauss deduced a few variants of Fermat's little theorem from this fact, admiring in passing the many diverse ways in which these theorems could be obtained.

According to Dickson, it was not until 1880-83 that four independent proofs of (2) for all a were published by Kantor, Weyr, Lucas, and Pellet (for precise references see [1]; see also [5]). In 1872, Petersen [3] proved Fermat's little theorem (1) by using a combinatorial method, and Thue [6] in 1910 published a proof of congruence (2) by generalizing this idea. His proof is neatly summarized in [1, p. 82]. Thue uses congruence (2) to prove Euler's generalization of congruence (1), which states

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \tag{3}$$

for relatively prime a, n, where $\varphi(n) = n\prod_{p|n}(1 - 1/p)$ is *Euler's totient function*. Szele [5] gives three proofs of congruence (2); his proofs are similar to those of Dickson, Thue, and Grandi, in 1895, 1910, and 1882, respectively. Finally, in 1986, Smyth [4] gives a coloring proof of a generalization of congruence (2).

2 The Main Theorem

As mentioned above, congruence (2) is a generalization of Fermat's little theorem (1) and Euler's theorem (3). In this paper, we prove the following generalization of congruence (2) to finite groups:

Main Theorem *Let G be a finite group of order n and let $\mathbb{C}^\times$ be the multiplicative group of non-zero complex numbers. If $f : G \longrightarrow \mathbb{C}^\times$ is a group homomorphism,* *then*

$$\sum_{g\in G} f(g)a^{n/o(g)} \equiv 0 \pmod{n} \tag{4}$$

holds true for any integer a, where $o(g)$ denotes the order of g.

With every choice of the finite group G and the homomorphism $f: G \longrightarrow \mathbb{C}^\times$ in the above general result, we get a polynomial expression in a that is guaranteed to be divisible by $|G|$ for every integer a. Let us check that the Main Theorem really is a generalization of congruence (2):

Corollary 2.1 *Let n be a positive integer and let a be an integer. Then*

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

holds true, where μ is the Möbius function.

Proof. Let $G = \langle x\rangle$ be a cyclic group of order n and let $f: G \longrightarrow \mathbb{C}^\times$ be the homomorphism sending x to $\exp(2\pi i/n)$. We find, writing (l, n) for the greatest common divisor of l and n:

$$\begin{aligned}
\sum_{g\in G} f(g)a^{n/o(g)} &= \sum_{l=1}^{n} \exp(2\pi i\tfrac{l}{n})a^{n/o(x^l)} \\
&= \sum_{l=1}^{n} \exp(2\pi i\tfrac{l}{n})a^{(l,n)} \\
&= \sum_{d|n} \Big(\sum_{\substack{l\,=\,1\\(l,\,n)\,=\,d}}^{n} \exp(2\pi i\tfrac{l}{n})\Big)a^d \\
&= \sum_{d|n} \Big(\sum_{\substack{l'\,=\,1\\(l',\,n/d)\,=\,1}}^{n/d} \exp(2\pi i\tfrac{l'd}{n})\Big)a^d \\
&= \sum_{d|n} \mu(n/d)a^d.
\end{aligned}$$

Here the last identity follows from the general fact that $\mu(N)$ equals the sum over all primitive N-th roots of unity. (A very classical proof of this fact is obtained by repeating C. F. Gauss's reasoning in §81 of the *Disquisitiones Arithmeticae*, where the same relation is established for $N = p - 1$, and for the primitive roots of unity which are the generators of the multiplicative group of the integers modulo p. — To be sure, the "Möbius function" was only called like this, with a reference to a 1832 paper of Möbius, by Mertens in 1875, i.e., 74 years after the appearance of Gauss's seminal book.)

Now, by the Main Theorem, $\sum_{g\in G} f(g)a^{n/o(g)}$ is divisible by n, so the above equalities imply that $\sum_{d|n} \mu(n/d)a^d$ is divisible by n, and thus the corollary follows. $\square$

We can also obtain some generalizations of Fermat's little theorem (1) by reducing congruence (4) to special cases. For example, if, in congruence (4), we consider $f(g) = 1$, for all $g \in G$, then we find that

$$\sum_{g\in G} a^{n/o(g)} \equiv 0 \pmod{n} \tag{5}$$

holds true for any integer a, and any group G of order n. In the special case where G is cyclic of prime order p, G contains one element of order 1 and $p-1$ elements of order p, thus congruence (5) yields $0 \equiv a^p + (p-1)a \equiv a^p - a \pmod{p}$, for all integers a.

Applying congruence (5) to the case where G is cyclic of order n, we obtain the following corollary which generalizes Fermat's little theorem (1).

Corollary 2.2 *Let n be a positive integer and let a be an integer. Then*

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

holds true, where φ is the Euler's totient function.

Proof. Let $G = \langle x \rangle$ be a cyclic group of order n. We have

$$\begin{aligned}
\sum_{g\in G} a^{n/o(g)} &= \sum_{l=1}^{n} a^{n/o(x^l)} \\
&= \sum_{l=1}^{n} a^{(l,n)} \\
&= \sum_{d|n} \Big(\sum_{\substack{l=1 \\ (l,n)=d}}^{n} 1 \Big) a^d \\
&= \sum_{d|n} \varphi(n/d)a^d.
\end{aligned}$$

On the other hand, by congruence (5), $\sum_{g\in G} a^{n/o(g)}$ is divisible by n, so the above equalities imply that $\sum_{d|n} \varphi(n/d)a^d$ is divisible by n as well, and thus the corollary follows. $\square$

Let us now explain how (a generalization of) the Main Theorem may be deduced from the representation theory of finite groups. — Let G be an arbitrary finite group acting (on the right) faithfully on an arbitrary finite set S. For each group element $g \in G$, write $c(g)$ for the number of orbits of $\langle g\rangle$ on S. Note that $c(g)$ is the total number of cycles, including trivial "1-cycles", when the permutation of S induced by g is written in cycle notation. Thus, for example, if G is the symmetric group on 5 letters in the natural action on five digits, and g is the element $(1\ 2)(3\ 4)$ of order 2, then $c(g) = 3$. An important example occurs when $S = G$, with the finite group G acting on itself by right multiplication. In this case, one has $c(g) = n/o(g)$, where $n = |G|$ — this is the *regular* action.

Now look at the set M of all maps from S into a finite set A, where $|A| = a$. (It can be useful to think of the members of A as "colors" and the members of M as colorings of the points in S.) The group G then acts on the set M as follows: Let $g \in G$ and $m \in M$. Then $m \cdot g$ is the new member of M defined by the formula $(m \cdot g)(x) = m(x \cdot g^{-1})$ for all $x \in S$. (It is routine to check that $(m\cdot g)\cdot h = m\cdot(gh)$ for $g, h \in G$, and so this really does define an action.)

Given $g \in G$, write $\pi(g)$ for the number of members of M that are fixed by g, so that π is the *permutation character* of the action of G on M. How can we compute $\pi(g)$? It is easy to see that a coloring m is fixed by g if and only if all of the points in each orbit of $\langle g\rangle$ in its action on S are assigned the same color. It follows from this that $\pi(g) = a^{c(g)}$. In particular, in the regular action of a group G of order n, we have $\pi(g) = a^{n/o(g)}$.

Now the permutation character π is actually a character of G. It is possible, therefore, to write π as a non-negative integer linear combination of the irreducible characters of G. If χ is one of these irreducible characters, then it follows from the orthogonality relations for irreducible characters that the coefficient of χ in the permutation character π is exactly $(1/n)\sum_{g\in G}\chi(g)\pi(g)$, where $n = |G|$. In particular, $\sum_{g\in G}\chi(g)\pi(g)$ is a positive integer multiple of n for each choice of irreducible character χ. We see now that

$$\sum_{g\in G}\chi(g)a^{c(g)} = \sum_{g\in G}\chi(g)\pi(g) \equiv 0 \pmod{n}.$$

Now a group homomorphism f from G into the multiplicative group $\mathbb{C}^{\times}$ is also an irreducible character. In particular, we see that our Main Theorem is exactly the case of the general fact described here when the action is regular and the irreducible character is one-dimensional.

Therefore, most of the ideas of this paper are known, even in a more general form. But perhaps they are not as well known as they might be. In the next section we present a proof of the Main Theorem in a simpler language, using (multi-) linear algebra. We refer the reader to [2] for yet another approach.

3 Proof of the Main Theorem via Linear Algebra

We continue the paper by proving the Main Theorem. Without loss of generality, we may suppose $G = \{1, \ldots, n\}$. In the sequel, we will be using G as an index set freely, writing simply "ij" for the composition of the group elements i and j. Firstly, we suppose a is a positive integer. Let V be an a-dimensional vector space over the complex field $\mathbb{C}$ and $\overset{n}{\otimes} V$ be the n-th tensor power of V. Write $v_1 \otimes \ldots \otimes v_n$ for the decomposable tensor product of the indicated vectors. For each $i \in G$, define $A_i : \overset{n}{\times} V \longrightarrow \overset{n}{\otimes} V$ by

$$A_i(v_1, \ \ldots, \ v_n) = v_{i1} \otimes \ldots \otimes v_{in}.$$

It can be easily seen that A_i is an n-linear function, so by the universal property of the tensor product, there exists a unique linear transformation $T_i : \overset{n}{\otimes} V \longrightarrow \overset{n}{\otimes} V$ which is completely determined by the rule

$$T_i(v_1 \otimes \ldots \otimes v_n) = v_{i1} \otimes \ldots \otimes v_{in}.$$

The following lemma can be obtained by a straightforward computation.

Lemma 3.1 *For each $i, j \in G$, $T_i T_j = T_{ij}$.*

We now construct a linear transformation $T : \overset{n}{\otimes} V \longrightarrow \overset{n}{\otimes} V$ by averaging:

$$T = \frac{1}{n} \sum_{i \in G} f(i) T_i.$$

Lemma 3.2 *T is an idempotent. In particular, the trace* tr T *of T is a non-negative integer.*

Proof.

$$\begin{aligned} T^2 &= \big(\tfrac{1}{n}\sum_{i\in G} f(i)T_i\big)\big(\tfrac{1}{n}\sum_{j\in G} f(j)T_j\big) \\ &= \tfrac{1}{n^2}\sum_{i\in G}\big(\sum_{j\in G} f(i)f(j)T_iT_j\big) \\ &= \tfrac{1}{n^2}\sum_{i\in G}\big(\sum_{j\in G} f(ij)T_{ij}\big) \\ &= \tfrac{1}{n^2}\sum_{i\in G}\big(\sum_{j\in G} f(j)T_j\big) \\ &= \tfrac{1}{n}\sum_{j\in G} f(j)T_j \\ &= T. \end{aligned}$$

The trace of an idempotent is the dimension of its image, and therefore in particular a non-negative integer. □

We now compute the trace of T. The following lemma will be useful for this purpose. We put $\Gamma_a^n = \overset{n}{\times}\{1,\ \ldots,\ a\}$.

Lemma 3.3 *For each $i \in G$, the number of $(\gamma_1,\ \ldots,\ \gamma_n) \in \Gamma_a^n$ for which $(\gamma_1,\ \ldots,\ \gamma_n) = (\gamma_{i1},\ \ldots,\ \gamma_{in})$ is equal to $a^{n/o(i)}$.*

Proof. Suppose $\langle i\rangle j_1,\ \ldots,\ \langle i\rangle j_s$ are the distinct right cosets of $\langle i\rangle$ in the group G, where $s = [G : \langle i\rangle] = n/o(i)$. It is easy to see that $(\gamma_1,\ \ldots,\ \gamma_n) = (\gamma_{i1},\ \ldots,\ \gamma_{in})$ if and only if

$$\gamma_{ij_t} = \ldots = \gamma_{i^{o(i)}j_t},$$

for all $1 \le t \le s$. Therefore, the number of $(\gamma_1,\ \ldots,\ \gamma_n) \in \Gamma_a^n$ for which $(\gamma_1,\ \ldots,\ \gamma_n) = (\gamma_{i1},\ \ldots,\ \gamma_{in})$ is equal to the number of $(\gamma_1,\ \ldots,\ \gamma_n) \in \Gamma_a^n$ such that

$$\gamma_{ij_t} = \ldots = \gamma_{i^{o(i)}j_t},$$

for all $1 \le t \le s$. But we have a choices for defining

$$\gamma_{ij_t} = \ldots = \gamma_{i^{o(i)}j_t},$$

for each $1 \le t \le s$, so the requested number is equal to $a^s = a^{n/o(i)}$. □

We now let $\mathcal{B} = \{e_1,\ \ldots,\ e_a\}$ be a basis of V, therefore,

$$\mathcal{B}^{\otimes} = \{e_{\gamma_1}\otimes\ldots\otimes e_{\gamma_n} |\ (\gamma_1,\ \ldots,\ \gamma_n) \in \Gamma_a^n\}$$

is a basis of $\overset{n}{\otimes} V$. For each $i \in G$,

$$T_i(e_{\gamma_1} \otimes \ldots \otimes e_{\gamma_n}) = e_{\gamma_{i1}} \otimes \ldots \otimes e_{\gamma_{in}},$$

which shows that the elements of the matrix of T_i with respect to $\mathcal{B}^{\otimes}$ are equal to 0 or 1. Therefore, tr T_i is equal to the number of $(\gamma_1, \ \ldots, \ \gamma_n) \in \Gamma_a^n$ for which $e_{\gamma_1} \otimes \ldots \otimes e_{\gamma_n} = e_{\gamma_{i1}} \otimes \ldots \otimes e_{\gamma_{in}}$. Lemma 3.3 now implies that tr $T_i = a^{n/o(i)}$. So,

$$\begin{aligned}
\operatorname{tr} T &= \operatorname{tr} \left(\tfrac{1}{n} \textstyle\sum_{i \in G} f(i) T_i \right) \\
&= \tfrac{1}{n} \textstyle\sum_{i \in G} f(i) \operatorname{tr} T_i \\
&= \tfrac{1}{n} \textstyle\sum_{i \in G} f(i) a^{n/o(i)}.
\end{aligned}$$

Hence, by Lemma 3.2,

$$\sum_{i \in G} f(i) a^{n/o(i)} \equiv 0 \pmod{n}.$$

Thus the Main Theorem follows, but only for positive a. The following lemma will complete the proof of the Main Theorem.

Lemma 3.4 *Let $F(X)$ be a polynomial in $\mathbb{C}[X]$ that takes on values in $\mathbb{Z}$ for non-negative integer values of X. Then $F(X)$ takes on values in $\mathbb{Z}$ for all values of X in $\mathbb{Z}$.*

Proof. For integers $k \geq 0$ define the polynomials $\binom{X}{k}$ of degree k, as follows. For $k = 0$, this is just the constant polynomial 1 and for $k > 0$,

$$\binom{X}{k} = \frac{X(X-1)\ldots(X-k+1)}{k!} \ .$$

Now these "binomial coefficients" form a basis for the full space $\mathbb{C}[X]$, and thus we can write

$$F(X) = \sum_{k=0}^{m} a_k \binom{X}{k},$$

where the coefficients a_k are complex numbers and m is the degree of F. Since the binomial-coefficient polynomials $\binom{X}{k}$ take on integer values for all integer values of X, it suffices to show that all of the coefficients a_j lie in $\mathbb{Z}$ for $0 \leq j \leq m$. We prove this by induction on j, starting with $j = 0$. We have $\binom{j}{j} = 1$ and $\binom{j}{k} = 0$ for $k > j$, and thus

$$a_j = F(j) - \sum_{k=0}^{j-1} a_k \binom{j}{k}.$$

We see, therefore, that each coefficient a_j is an integer combination of the integer $F(j)$ and the integers a_k for $0 \leq k < j$. The result then follows. $\square$

We now apply this lemma to the polynomial

$$F(X) = \frac{1}{n} \sum_{i \in G} f(i) X^{n/o(i)} \in \mathbb{C}[X].$$

By the remarks just before Lemma 3.4, $F(X)$ takes on values in $\mathbb{Z}$ for non-negative integer values of X. Therefore, by Lemma 3.4, $F(X)$ takes on values in $\mathbb{Z}$ for all values of X in $\mathbb{Z}$. In other words,

$$\sum_{i \in G} f(i) a^{n/o(i)} \equiv 0 \pmod{n}$$

holds true for any integer a, thus the Main Theorem follows. $\square$

Acknowledgment: This work was done while the author was a Postdoctoral Research Associate at the School of Mathematics, Institute for Studies in Theoretical Physics and Mathematics (IPM). He would like to thank the IPM for the financial support. Also he would like to express his thanks to Professor I. M. Isaacs for making useful suggestions and comments which led to improvement and simplification of the first draft.

References

[1] L. E. Dickson, "*History of the Theory of Numbers*", vol. 1, Chelsea, New York, 1971.

[2] I. M. Isaacs, M. R. Pournaki, *Generalizations of Fermat's Little Theorem via Group Theory*, Amer. Math. Monthly **112** (2005), no. 8, 734-740.

[3] J. Petersen, Tidsskrift for Mathematik (3) **2** (1872), 64-65.

[4] C. J. Smyth, *A Coloring Proof of a Generalization of Fermat's Little Theorem*, Amer. Math. Monthly **93** (1986), no. 6, 469-471.

[5] T. Szele, *Une Généralisation de la Congruence de Fermat*, Mat. Tidsskr. B. **1948** (1948), 57-59.

[6] A. Thue, "*Ein Kombinatorischer Beweis eines Satzes von Fermat*", In Selected

Mathematical Papers of Axel Thue, Universitelsforlaget, 1977 (Originally Kra. Vidensk. Selsk, Skrifter. I. Mat. Nat. Kl. 1910, No. 3).

The Author's Address

M. R. Pournaki, School of Mathematics, Institute for Studies in Theoretical Physics and Mathematics, P.O. Box 19395-5746, Tehran, Iran.
E-mail address: `pournaki@ipm.ir`