On Some Generalizations of Fermat's, Lucas's and Wilson's Theorems

Tyler J. Evans
Department of Mathematics
Humboldt State University
Arcata, CA 95521 USA
evans@humboldt.edu

Version: December 6, 2005

We use actions by finite cyclic groups together with Burnside's theorem to derive generalizations of three classical divisibility theorems.

1. INTRODUCTION

In [1] and [4], the authors derive Fermat's (little), Lucas's and Wilson's theorems, among other results, all from a single combinatorial lemma. This lemma can be derived by applying Burnside's theorem to an action by a cyclic group of prime order. In this note, we generalize this lemma by applying Burnside's theorem to the corresponding action by an arbitrary finite cyclic group. Although this idea is not new, by revisiting the constructions in [1] and [4] we derive three divisibility theorems for which the aforementioned classical theorems are, respectively, the cases of a prime divisor, and two of these generalizations are new. Throughout, n and p denote positive integers with p prime and $\mathbb{Z}_n$ denotes the cyclic group of integers under addition modulo n.

2. GROUP ACTIONS AND BURNSIDE'S THEOREM

By an action of a group G on a set X, we mean a homomorphism $G \to \text{Aut}(X)$ where $\text{Aut}(X)$ denotes the group of permutations of X. We write gx for the image of $x \in X$ under the permutation $X \to X$ induced by $g \in G$. For each $x \in X$, let $Gx = \{gx \mid g \in G\}$ denote the orbit of x in X and for each $g \in G$, let $X^g = \{x \in X \mid gx = x\}$ denote the set of points fixed by g. If both G and X are finite, Burnside's theorem states that the number of distinct orbits is given by

$$\frac{1}{|G|}\sum_{g\in G}|X^g|.$$

In particular, $\sum_{g\in G}|X^g|$ is divisible by $|G|$. In the case that $G = \mathbb{Z}_n$, for all $g \in \mathbb{Z}_n$, $X^g = X^d$ where $d = (g, n)$ is the greatest common divisor of g and n. Each such g has order n/d and there are $\varphi(n/d)$ such elements, where φ denotes Euler's totient function. This observation, together with Burnside's theorem, gives us the following lemma from which we will derive all of our results in the sequel.

LEMMA 1. *If X is a finite set and $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is a group action, then the number of orbits is $(1/n)\sum_{d|n}\varphi\left(\frac{n}{d}\right)|X^d|$ so that in particular,*

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

■

When $n = p$ is prime, Lemma 1 reduces to $|X| \equiv |X^1| \pmod{p}$, and this is the combinatorial lemma in [1] and [4].

3. A GENERALIZATION OF FERMAT'S (LITTLE) THEOREM

If a is a positive integer and $A = \{1, \ldots, a\}$, then $\mathbb{Z}_n$ acts on the product $X = A^n$ by cyclically permuting the coordinates of elements $x \in X$. If $g \in \mathbb{Z}_n$ has order n/d then each of the coordinates of $x \in X$ has n/d distinct images under all powers of g so that g fixes a^d elements of X. Applying Lemma 1 gives our first theorem.

THEOREM 1. *For any two positive integers n and a,*

$$\sum_{d|n}\varphi\left(\frac{n}{d}\right)a^d \equiv 0 \pmod{n}.$$

■

COROLLARY 1 (Fermat's theorem). *For a prime p and any positive integer a, $a^p \equiv a \pmod{p}$.* ■

Theorem 1 has appeared numerous times in the literature [3, 5, 6], and a detailed history of it can be found in [2]. If $a = 1$, then obviously the number of orbits is also equal to 1 and hence, as a bonus, we recover the well known identity $\sum_{d|n}\varphi(d) = n$.

4. WILSON'S THEOREM

In this section, we revisit an action used in [1] (in the prime case) and derive a generalization of Wilson's theorem. Let X be the set of all cycles of length n in the symmetric group $\mathrm{Aut}(\{1,\ldots,n\})$. Then $|X| = (n-1)!$ and the action of $\mathbb{Z}_n$ on X is defined by

$$g(a_1,\ldots,a_n) = (a_1+g,\ldots,a_n+g),$$

where the addition in each position is done modulo n. Let d be a divisor of n, $g \in \mathbb{Z}_n$ be an element of order n/d, and let $0, a_2, \ldots, a_d \in \mathbb{Z}_n$ be a complete set of representatives for the set of cosets $\mathbb{Z}_n/\langle d\rangle$. Define a cycle $\pi = \pi(g, a_2, \ldots, a_d) \in X$ by

$$\pi = (0, a_2, \ldots, a_d, g, a_2+g, \ldots, a_d+g, \ldots, ((n/d)-1)g, \ldots, a_d+((n/d)-1)g) \tag{1}$$

where the multiplication is done modulo n. There are $\varphi(n/d)$ choices for g, $(n/d)^{d-1}$ choices for the elements $a_2, \ldots, a_d$ and $(d-1)!$ ways to order them. Hence, the number of cycles of the form (1) is given by

$$\varphi\left(\frac{n}{d}\right)\left(\frac{n}{d}\right)^{d-1}(d-1)!.$$

EXAMPLE 1. Let $n = 12$, $d = 4$, $g = 8$, $a_2 = 9$, $a_3 = 6$ and $a_4 = 3$. Then the cycle π defined above is

$$\pi = (0,9,6,3,8,5,2,11,4,1,10,7).$$

The reader can verify that π is a fixed point only for the elements in the subgroup $\langle 4\rangle$ of $\mathbb{Z}_{12}$. The cycle π is 1 of $324 = 2 \cdot 3^3 \cdot 3!$ 12-cycles fixed by the elements in the subgroup $\langle 4\rangle$. ∎

Let $\pi = \pi(g, a_2, \ldots, a_d)$. Since g has order n/d, we have $d = kg$ for some $1 \le k \le (n/d) - 1$. It is then easy to see that $d\pi$ is obtained from π by cyclically permuting the entries in each position kd spaces to the left, hence $\pi \in X^d$. On the other hand, if $\pi = (a_1, \ldots, a_n) \in X^d$ where $a_1 = 0$ and $a_{k+1} = d$, then $d\pi$ is obtained from π by cyclically permuting the entries k spaces to the left. It follows that $k \in \mathbb{Z}_n$ has order n/d so that $d = uk$ for some $u \in \mathbb{Z}_n$. Therefore *subtracting* d from each entry in π a total of u times is equivalent to moving each entry *right* d spaces. Since $a_1 = 0$, this implies $a_{jd+1} = jud$ for all $j = 0, \ldots (n/d) - 1$. Therefore the order of ud is n/d so that $a_2 \notin \langle ud\rangle$ and, by similar reasoning, $a_{jd+2} = a_2 + jud$ for all $j = 0, \ldots (n/d) - 1$ exhausting the coset $a_2 + \langle ud\rangle$. Continuing, we see that $a_2, \ldots, a_d$ represent distinct cosets in $\mathbb{Z}_n/\langle d\rangle$ and $\pi = \pi(ud, a_2, \ldots, a_d)$ has the form (1). We have shown $|X^g| = \varphi(n/d)(n/d)^{d-1}(d-1)!$ so that an application of Lemma 1 gives our second divisibility theorem.

THEOREM 2. *For any positive integer n,*

$$\sum_{d|n}\left[\varphi\left(\frac{n}{d}\right)\right]^2\left(\frac{n}{d}\right)^{d-1}(d-1)!\equiv 0 \pmod{n}.$$

■

COROLLARY 2 (Wilson's theorem). *For a prime p,*

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

■

5. LUCAS'S THEOREM

In this final section, we reanalyze an action used in [4] (in the prime case) to derive a generalization of Lucas's theorem (see Corollary 3 below). Let $m, r \geq 0$ and use the division algorithm to write $m = Mn + m_0$ and $r = Rn + r_0$ with $0 \leq m_0, r_0 < n$. For $1 \leq k \leq n$, let

$$A_k = \{(k,1),(k,2),\ldots,(k,M)\} \text{ and let } B = \{(0,1),(0,2),\ldots,(0,m_0)\}.$$

Let $A = A_1 \cup A_2 \cup \cdots \cup A_n \cup B$ so that $|A| = Mn+m_0 = m$. Given $C \subseteq A$, let $C_j = C \cap A_j$ for $1 \leq j \leq n$ and $C_0 = C \cap B$ so that $C = C_1 \cup C_2 \cup \cdots \cup C_n \cup C_0$. If X is the collection of all $C \subseteq A$ with $|C| = r$, then $|X| = \binom{m}{r}$. (Note: $\binom{m}{r} = 0$ if $m < r$.) Define $f : A \to A$ by

$$\begin{aligned} f(k,x) &= (k+1,x) \text{ if } 1 \leq k \leq n-1; \\ f(n,x) &= (1,x); \\ f(0,x) &= (0,x), \end{aligned}$$

and note easily that $f \in \operatorname{Aut}(A)$. Clearly f^n is the identity map so that the map $1 \mapsto f$ gives an action $\mathbb{Z}_n \to \operatorname{Aut}(X)$. Moreover, an element $C \in X$ is fixed by $g \in \mathbb{Z}_n$ of order n/d if and only if for all $1 \leq k \leq d$, $\pi_2(C_k) = \pi_2(C_{lg+k})$ for $l = 0, \ldots, (n/d)-1$ where π_2 is projection onto the second coordinate. Therefore

$$Rn + r_0 = r = |C| = \frac{n}{d}\sum_{k=1}^{d}|C_k| + |C_0|.$$

But, $0 \leq r_0, |C_0| < n$ so that there exists $j \in \{-(d-1), \ldots, d-1\}$ such that

$$R = \frac{1}{d}\sum_{k=1}^{d}|C_k| + \frac{j}{d} \quad \text{and} \quad |C_0| - r_0 = (n/d)j. \tag{2}$$

Conversely, for all $j \in \{-(d-1), \ldots, d-1\}$ and all choices of $\alpha_k = |C_k|$ $(1 \le k \le d)$ that satisfy (2), we can independently choose subsets $C_k \subset A_k$ and $C_0 \subset B$ with $|C_0| = r_0 + (n/d)j$, and a unique fixed point of X is determined. If we define the length $||\alpha||_d$ of an element $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{N}^d$ by

$$||\alpha||_d = \frac{1}{d}\sum_{j=1}^{d} \alpha_j,$$

then we have shown if $g \in \mathbb{Z}_n$ has order n/d, then

$$|X^g| = \sum_{j=-(d-1)}^{d-1} \sum_{\substack{||\alpha||_d= \\ R-(j/d)}} \binom{M}{\alpha_1} \cdots \binom{M}{\alpha_d} \binom{m_0}{r_0 + (n/d)j} \equiv 0 \pmod{n}$$

Applying Lemma 1, we have our third divisibility theorem.

THEOREM 3. *For $n \ge 1$, $m = Mn + m_0$, $r = Rn + r_0$, $0 \le m_0, r_0 < n$*

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) \sum_{j=-(d-1)}^{d-1} \sum_{\substack{||\alpha||_d= \\ R-(j/d)}} \binom{M}{\alpha_1} \cdots \binom{M}{\alpha_d} \binom{m_0}{r_0 + (n/d)j} \equiv 0 \pmod{n}.$$

■

COROLLARY 3 (Lucas's theorem). *Let p be prime and suppose*

$$\begin{aligned} m &= m_k p^k + \cdots + m_1 p + m_0; \\ r &= r_k p^k + \cdots + r_1 p + r_0 \end{aligned}$$

with $0 \le m_j, r_j < p$. Then

$$\binom{m}{r} \equiv \binom{m_k}{r_k} \cdots \binom{m_1}{r_1} \binom{m_0}{r_0} \pmod{p}.$$

Proof. We will show that if $m = Mp + m_0$, $r = Rp + r_0$, $0 \le m_0, r_0 < p$, then

$$\binom{m}{r} \equiv \binom{M}{R} \binom{m_0}{r_0} \pmod{p},$$

leaving the induction for the reader. Taking $n = p$, Theorem 3 gives

$$(p-1)\binom{M}{R}\binom{m_0}{r_0} + \sum_{j=-(p-1)}^{p-1} \sum_{\substack{||\alpha||_p= \\ R-(j/p)}} \binom{M}{\alpha_1} \cdots \binom{M}{\alpha_p} \binom{m_0}{r_0 + (n/p)j} \equiv 0 \pmod{p}.$$

Selecting subsets $C_k \subseteq A_k$ with $|C_k| = \alpha_k$ $(1 \leq k \leq p)$ and $C_0 \subset B$ with $|C_0| = r_0 + (n/p)j$ uniquely determines a subset $C \in X$ provided $||\alpha||_p = R - (j/p)$ for some $j \in \{-(p-1), \ldots, p-1\}$. Therefore

$$\sum_{j=-(p-1)}^{p-1} \sum_{\substack{||\alpha||_p= \\ R-(j/p)}} \binom{M}{\alpha_1} \cdots \binom{M}{\alpha_p} \binom{m_0}{r_0 + (n/p)j} = \binom{m}{r}$$

and the proof is complete. ∎

ACKNOWLEDGMENT

The author gratefully acknowledges Mr. Jon Miller at Salisbury University, Dr. Joe Carrol at Humboldt State University and the anonymous referee for their valuable suggestions.

REFERENCES

[1] Peter G. Anderson, Arthur T. Benjamin, and Jeremy A. Rouse. Combinatorial proofs of Fermat's, Lucas's and Wilson's theorems. *Amer. Math. Monthly*, 112(3):266–268, March 2005.

[2] L. E. Dickson. *History of the Theory of Numbers*, volume 1. Carnegie Institution of Washington, Washington, D.C., 1919.

[3] M.L. Fredman, L.E. Mattics, and L. Carlitz. Elementary Problems and Solutions: E2242. *Amer. Math. Monthly*, 78(5):545–546, May 1971.

[4] Melvin Hausner. Applications of a simple counting technique. *Amer. Math. Monthly*, 90(2):127–129, February 1983.

[5] Calvin T. Long. Problems and Solutions: 6468. *Amer. Math. Monthly*, 92(10):742, December 1985.

[6] P.A. MacMahon. Applications of the theory of permutations in circular procession to the theory of numbers. *Proc. London Math. Soc.*, 23:305–313, 1891-2.