INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 5(1) (2005), #A26

DERIVING DIVISIBILITY THEOREMS WITH BURNSIDE'S THEOREM

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

Benjamin V. Holt
Department of Mathematics, Humboldt State University, Arcata, CA 95521, USA
bvh6@humboldt.edu

Received: 8/12/05, Accepted: 11/18/05, Published: 11/29/05

Abstract

We use the class equation of a finite group action together with Burnside's orbit counting theorem to derive classical divisibility theorems.

1. Introduction

Numerous authors (see [1, 3, 4, 6, 8] for example) have shown how one may deduce classical theorems in elementary number theory and group theory using various counting arguments. In [1] and [4] the authors show how one may derive Fermat's (little), Lucas's and Wilson's theorems as well as Cauchy's theorem for groups all from the following theorem.

Theorem 1 *If X is a finite set, p a prime integer and $f : X \to X$ a mapping satisfying $f^p(x) = x$ for all $x \in X$, then $|X| \equiv |X^0| \pmod{p}$, where X^0 denotes the set of fixed points of f.*

This theorem, or rather its proof, is essentially the main idea in [3] and [8] as well. In [6], the author uses iterates of a certain complex valued function to derive a more general divisibility theorem (Theorem 2 below) for which Fermat's little theorem is the special case of a prime divisor.

The purpose of this note is to show that Theorems 1 and 2 are both simple consequences of the class equation of a cyclic group action. Consequently, all of the arguments in [1, 3, 4, 6, 8] are unified by the theory of finite group actions. In addition to putting this robust theory at our disposal, this point of view also has the advantage of generalizing to non-cyclic actions.

We will illustrate these points by applying Burnside's theorem to the action in [6] to derive two more divisibility theorems (Theorems 3 and 4 below) undetected by the method in [6]. Just as with Theorem 2, Fermat's little theorem is a special case of Theorem 3, as is a well known identity involving the Euler φ-function. We then give some famous examples of this technique in group theory and conclude with a proof of Wilson's theorem in which the group action is by a non-cyclic group.

2. The Class Equation

Let X be a non-empty finite set with $|X|$ elements and let $\mathrm{Aut}(X)$ denote the group of permutations of X. If G is a group, then an action of G on X is a homomorphism $G \to \mathrm{Aut}(X)$. For each $x \in X$, let $Gx = \{gx | g \in G\}$ and $G_x = \{g \in G | gx = x\}$ denote the orbit of x and the stabilizer of x in G respectively so that if G is finite $|Gx| = (G : G_x)$ is a divisor of $|G|$. The class equation of the action is

$$|X| = |X^G| + \sum_{i=1}^{r} |Gx_i|, \tag{1}$$

where X^G is the set of fixed points under the action and $Gx_1, \ldots, Gx_r$ are the distinct non-trivial orbits. If p is a prime integer and G is a p-group (that is, G is a finite group of order p^n for some integer $n \geq 1$), then the class equation (1) implies the number of elements in X is congruent to the number of fixed points of the action modulo p. That is

$$|X| \equiv |X^G| \pmod{p}. \tag{2}$$

Theorem 1 follows immediately from (2). That is, for X, p and f as in the theorem, the map $\mathbb{Z}_p \to \mathrm{Aut}(X)$ defined by $1 \mapsto f$ gives an action of $\mathbb{Z}_p$ on X, where $\mathbb{Z}_p$ denotes the cyclic group of integers under addition modulo p. Clearly $X^{\mathbb{Z}_p} = X^0$ so that applying (2) proves Theorem 1.

3. Generalizations of Fermat's Little Theorem

In [6], the author uses iterates of complex function $f(z) = z^k$, where k is a fixed positive integer along with Möbius inversion to derive the following generalization of Fermat's little theorem.

Theorem 2 *For any two positive integers n and k, n divides*

$$P(k, n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) k^d$$

where μ is the Möbius function.

If $k > 1$, the argument in [6] shows for each integer $n \geq 1$, $\mathbb{Z}_n$ acts on the set P_n of all complex numbers z for which n is the smallest positive integer satisfying $f^n(z) = z$ via the mapping $\mathbb{Z}_n \to \mathrm{Aut}(P_n)$ given by $1 \mapsto f$. Moreover, the stabilizer of any point $z \in P_n$ is easily seen to be trivial so that by the class equation (1), $n||P_n|$. (If $k = 1$, then P_1 is the set of all complex numbers and $P_n = \emptyset$ if $n > 1$. We redefine $P_1 = \{0\}$ in this case so that we have $n||P_n|$ for all positive k and n.) This is the divisibility statement in Theorem 2. To express $|P_n|$ in terms of k, note that $1 \mapsto f$ also gives an action of $\mathbb{Z}_n$ on the set X_n of those complex numbers z for which $f^n(z) = z$. (If $k = 1$, we take $X_n = \{0\}$ for all $n > 0$ so that $|X_n| = k^n$ for all $k, n > 0$.) Moreover, X_n is a disjoint union of the (sub-$\mathbb{Z}_n$) sets P_d, where d is a positive divisor of n so that $k^n = \sum_{d|n} |P_d|$. The Möbius inversion formula is then employed to find $|P_n|$ in terms of k completing the proof of Theorem 2. If $n = p$ is a prime integer, then Theorem 2 reduces to Fermat's little theorem. A detailed history of Theorem 2 can be found in [2].

Giving an argument such as the one in [6] from this point of view is not just a matter of semantics. The above argument (for $k > 1$) shows that $|P_n|/n$ is the number of orbits in the action of $\mathbb{Z}_n$ on P_n, and since Burnside's theorem[1] also calculates this number, it is natural to apply it to the action of $\mathbb{Z}_n$ on X_n as well. If $z \in X_n$, then for all $j = 1, \ldots, n$, $f^j(z) = z$ if and only if $f^{(j,n)}(z) = z$, where (j, n) denotes the greatest common divisor of j and n. Therefore, the set of fixed points for f^j and f^i in X_n are equal if and only if $(j, n) = (i, n)$ and in this case the number of such fixed points is $k^{(j,n)}$. Given a divisor d of n, there are $\varphi(n/d)$ elements j in $\{1, \ldots, n\}$ with $(j, n) = d$, where φ is Euler's totient function, so that applying Burnside's theorem gives the following.

Theorem 3 *For any two positive integers n and k, n divides*

$$X(k, n) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) k^d.$$

If we take $n = p$ to be prime, then Theorem 3 reduces to Fermat's little theorem. If we take $k = 1$, then clearly the number of orbits is also 1 and we recover the identity $\sum_{d|n} \varphi(d) = n$. Theorem 3 was first shown in [7].

We can say more. Since P_n is a sub-$\mathbb{Z}_n$ set of X_n, the orbits in P_n are among the orbits in X_n. That is, we should expect $X(k, n)$ to be a sum of $P(k, n)$ and another expression $Q(k, n)$, where $Q(k, n)/n$ is the number of orbits in the set $Q_n = X_n - P_n$. Using the identity

[1]For convenience, we recall that Burnside's theorem states if G is a finite group acting on a finite set X and r denotes the number of distinct orbits, then

$$r = \frac{1}{|G|} \left(\sum_{g \in G} |X^g| \right)$$

where for each $g \in G$, $X^g = \{x \in X | gx = x\}$.

$\varphi(n) = \sum_{d|n} \mu(n/d)d$, we can write

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) k^d = \sum_{d|n} \left(\sum_{e|(n/d)} \mu\left(\frac{n}{de}\right) e \right) k^d = \sum_{e|n} \left(\sum_{d|(n/e)} \mu\left(\frac{n}{de}\right) k^d \right) e, \tag{3}$$

and recover a third divisibility theorem.

Theorem 4 *For any two positive integers n and k, n divides*

$$Q(k,n) = \sum_{\substack{e \neq 1 \\ e|n}} \sum_{d|(n/e)} \mu\left(\frac{n}{de}\right) k^d e.$$

Since $X(k,n) = P(k,n) + Q(k,n)$, any two of Theorems 2, 3 or 4 imply the third. In fact, equation (3) shows that Theorem 2 implies Theorem 3 directly.

Remark. Fermat's little theorem can be derived from (the class equation of) an action by a cyclic group of prime order as in [4], and once again applying Burnside's theorem to this action gives the same divisibility result. By considering the corresponding action by an arbitrary finite cyclic group, we obtain another proof of Theorem 3. Namely, if k and n continue to denote positive integers and we let $A = \{1, \ldots, k\}$, then $\mathbb{Z}_n$ acts on the product $X = A^n$ by cyclically permuting the coordinates of elements $x \in X$. Every element $g \in \mathbb{Z}_n$ has order n/d for some divisor d of n and there are exactly $\varphi(n/d)$ such elements each of which fixes k^d elements of X. Therefore

$$\sum_{g \in \mathbb{Z}_n} |X^g| = \sum_{d|n} \varphi\left(\frac{n}{d}\right) k^d = X(k,n).$$

By Burnside's theorem, the number of orbits in the action is therefore $X(k,n)/n$ and hence $n|X(n,k)$.

4. More Examples

Examples of proofs using (2) in elementary group theory are abundant. The usual argument for showing the center of a p-group is non-trivial uses (2) with the group acting on itself by conjugation. The $\mathbb{Z}_2$ action of inversion on a group of even order shows the existence of an element of order 2. More generally, a famous application of (2) is McKay's elegant proof of Cauchy's theorem for groups [8]. The cyclic actions here are induced by a function as in Theorem 1. A beautiful line of argumentation credited to R. J. Nunke in [5] uses (2) repeatedly to establish the three Sylow theorems.

We conclude with a (non-cyclic) group action proof of Wilson's theorem: if p is a prime integer, then $(p-1)! \equiv -1 \pmod{p}$. Let $G = S_p$ denote the symmetric group on p letters,

and $s \in G$ be the p-cycle defined by $s = (1, 2, \ldots, p)$. Note that $x = \langle s \rangle$ is a Sylow p-subgroup of G. Let X denote the set of all subgroups of G and let G act on X by conjugation. Then the stabilizer of $x \in X$ is the normalizer $N = N(x)$ of x. It is easy to show, using the fact that any two p-cycles in G are conjugate, that $|N| = p(p-1)$. Now, using the Sylow theorems (and hence equation (2)), the size of orbit Gx in X satisfies

$$|Gx| \equiv 1 \pmod{p}.$$

We also have that

$$|Gx| = (G : N) = \frac{|G|}{|N|} = \frac{p!}{p(p-1)} = (p-2)!,$$

and Wilson's theorem follows.

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] S. W. Golomb. Combinatorial proof of Fermat's little theorem. *Amer. Math. Monthly*, 63(10):718, December 1956.

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

[5] Thomas Hungerford. *Algebra*. Springer-Verlag, New York, 1974.

[6] Lionel Levine. Fermat's little theorem: A proof by function iteration. *Mathematics Magazine*, 72(4):308–309, October 1999.

[7] 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.

[8] James H. McKay. Another proof of Cauchy's group theorem. *Amer. Math. Monthly*, 66(2):119, February 1959.