Group Actions in Number Theory

Tyler J. Evans
Department of Mathematics
Humboldt State University

August 14, 2004

Algebra and Number Theory

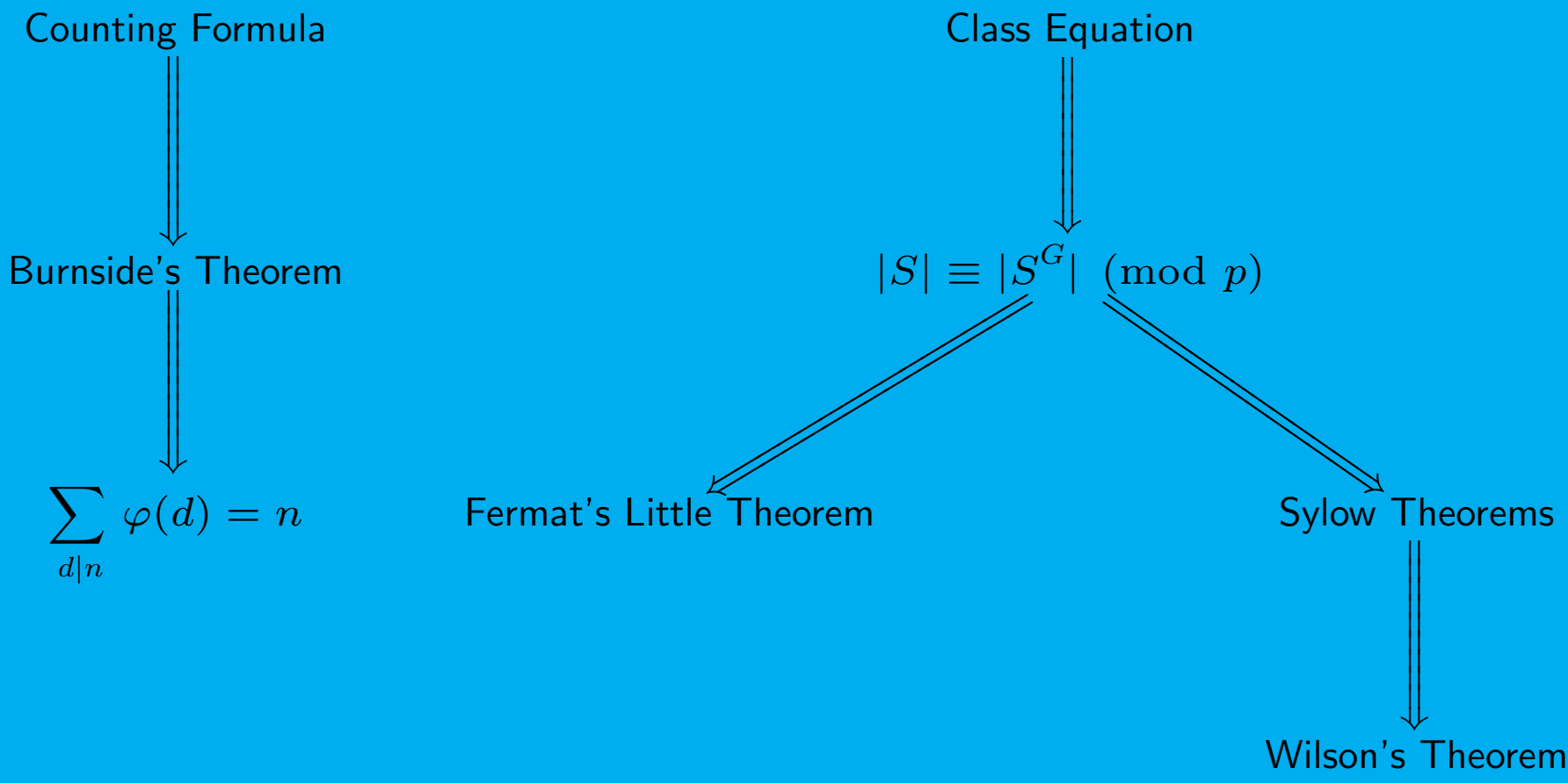
Students having had a semester course in abstract algebra are exposed to the elegant way in which one can use the theory of finite cyclic groups to derive familiar results from Number Theory.

We present 3 examples suitable for a **second semester course** in algebra.

Each uses the notion of the **action of a group on a set**.

This work was done with Ben Holt, who, at the time, was an HSU undergraduate student taking second semester algebra!

Logical Inference Summary



"Never under estimate a theorem that counts something".

-J. Fraleigh

Example 1: Fermat's Little Theorem

Theorem 1. *Let $p \in \mathbb{Z}$ be a prime integer and let $n \in \mathbb{N}$. If G is a group with p^n elements and G acts on a finite set S, then*

$$|S| \equiv |S^G| \pmod{p}.$$

That is, the total number of elements in the set S is congruent to the total number of fixed points modulo p.

Theorem 2. [Fermat] *If $a \geq 1$ is any integer and p is a prime, then $a^p \equiv a \pmod{p}$.*

Fermat's Little Theorem: The Whole Story

Fermat's Little Theorem is valid for any integer a.

It's trivial for $a = 0$.

The identity $(-a)^p \equiv -a^p \pmod{p}$ together with Theorem 1 proves the theorem for $a \leq -1$. In fact,...

Theorem 3. *If a is any integer and p is a prime, then*

$$a^{p^j} \equiv a \pmod{p}$$

for all $j \geq 1$.

Example 2: A Famous Identity

Theorem 4. [Burnside] *If a finite group G acts on a finite set S and r denotes the number of orbits under the G-action, then*

$$r \cdot |G| = \sum_{g \in G} |S^g|$$

where $|S^g|$ denotes the number of elements of S left fixed by $g \in G$.

Theorem 5. *If $n \geq 1$ is an integer, then* $\sum_{d|n} \varphi(d) = n$.

Example 2: The Dictionary

The dihedral group D_n acts on the set S of q^n colorings.

Two colorings are indistinguishable if and only if they are in the same orbit under this action.

Therefore the number of distinguishable colorings is the number of orbits under this D_n action.

According to Burnside, we need only determine $|S^g|$ for each element $g \in D_n$.

Example 3: Wilson's Theorem

Theorem 6. [Wilson] *If* $p \in \mathbb{Z}$ *is a prime, then* $(p-1)! \equiv -1 \pmod{p}$.

Here we let the symmetric group $G = S_p$ act on the set of all of its subgroups by conjugation and use the Sylow Theorems as well as the Counting Formula to derive:

$$\frac{p!}{p(p-1)} = \frac{|G|}{|N|} = |G\langle s\rangle| \equiv 1 \pmod{p}$$

where $s \in G$ is the p-cycle $s = (1, 2, \ldots, p)$, N is the normalizer of $\langle s\rangle$ in G and $G\langle s\rangle$ is the orbit of $\langle s\rangle$ under the conjugation action.

Thank You!

Tyler J. Evans
Department of Mathematics
Humboldt State University
Arcata, CA 95521 USA
evans@humboldt.edu
http://www.humboldt.edu/∼te8/