Never Underestimate a Theorem That Counts Something!

Tyler J. Evans
Department of Mathematics
Humboldt State University

Occidental College
March 31, 2006

Our Motivation

In their (wonderful) note *Combinatorial proofs of Fermat's, Lucas's and Wilson's theorems* (MONTHLY, March 2005), Anderson, Benjamin and Rouse derive a host of classical divisibility theorems all from the following result:

lemma. 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 $|X| \equiv |X'| \pmod{p}$, where $X' = \{x \in X \mid f(x) = x\}$ denotes the set of fixed points of f.

Our Motivation

In their (wonderful) note *Combinatorial proofs of Fermat's, Lucas's and Wilson's theorems* (MONTHLY, March 2005), Anderson, Benjamin and Rouse derive a host of classical divisibility theorems all from the following result:

lemma. 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 $|X| \equiv |X'| \pmod{p}$, where $X' = \{x \in X \mid f(x) = x\}$ denotes the set of fixed points of f.

Remark. $|X| \equiv |X'| \pmod{p} \iff |X| + (p-1)|X'| \equiv 0 \pmod{p}$.

Our Motivation

In their (wonderful) note *Combinatorial proofs of Fermat's, Lucas's and Wilson's theorems* (MONTHLY, March 2005), Anderson, Benjamin and Rouse derive a host of classical divisibility theorems all from the following result:

lemma. 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 $|X| \equiv |X'| \pmod{p}$, where $X' = \{x \in X \mid f(x) = x\}$ denotes the set of fixed points of f.

Remark. $|X| \equiv |X'| \pmod{p} \iff |X| + (p-1)|X'| \equiv 0 \pmod{p}$.

ABR: Choose X and f "just right" and the **lemma** gives a classical theorem!

Famous Consequences of the lemma

Fermat's (little) Theorem. For a prime p and any $a \in \mathbb{Z}$,

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

Famous Consequences of the lemma

Fermat's (little) Theorem. For a prime p and any $a \in \mathbb{Z}$,

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

Wilson's Theorem. For a prime p,

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Famous Consequences of the lemma

Fermat's (little) Theorem. For a prime p and any $a \in \mathbb{Z}$,

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

Wilson's Theorem. For a prime p,

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Lucas's Theorem. For a prime p and integers $m, r \geq 0$, 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 $0 \leq m_j, r_j < p$. Then

$$\binom{m}{r} + (p-1)\binom{m_k}{r_k} \cdots \binom{m_1}{r_1}\binom{m_0}{r_0} \equiv 0 \pmod{p}.$$

An Example for Lucas's Theorem

Let $p = 3$, $m = 14$ and $r = 4$.

$$\begin{aligned} 14 &= 1 \cdot 3^2 + 1 \cdot 3 + 2; \\ 4 &= 0 \cdot 3^2 + 1 \cdot 3 + 1 \end{aligned}$$

and

$$\binom{14}{4} \equiv \binom{1}{0}\binom{1}{1}\binom{2}{1} \equiv 2 \pmod 3.$$

An Example for Lucas's Theorem

Let $p = 3$, $m = 14$ and $r = 4$.

$$\begin{aligned} 14 &= 1 \cdot 3^2 + 1 \cdot 3 + 2; \\ 4 &= 0 \cdot 3^2 + 1 \cdot 3 + 1 \end{aligned}$$

and

$$\binom{14}{4} \equiv \binom{1}{0}\binom{1}{1}\binom{2}{1} \equiv 2 \pmod 3.$$

What if $r = 7$? That is $7 = 0 \cdot 3^2 + 2 \cdot 3 + 1$ so

$$\binom{14}{7} \equiv \binom{1}{0}\binom{1}{2}\binom{2}{1}$$

An Example for Lucas's Theorem

Let $p = 3$, $m = 14$ and $r = 4$.

$$\begin{aligned} 14 &= 1 \cdot 3^2 + 1 \cdot 3 + 2; \\ 4 &= 0 \cdot 3^2 + 1 \cdot 3 + 1 \end{aligned}$$

and

$$\binom{14}{4} \equiv \binom{1}{0}\binom{1}{1}\binom{2}{1} \equiv 2 \pmod 3.$$

What if $r = 7$? That is $7 = 0 \cdot 3^2 + 2 \cdot 3 + 1$ so

$$\binom{14}{7} \equiv \binom{1}{0}\binom{1}{2}\binom{2}{1} \equiv 0 \pmod 3.$$

Something for the History Buffs...

Pierre de Fermat [1601-1665]

Well, there's too much history here!

It seems that number theory was the subject closest to Fermat's heart.

Something for the History Buffs...

Pierre de Fermat [1601-1665]

- Well, there's too much history here!
- It seems that number theory was the subject closest to Fermat's heart.

John Wilson [1741-1793]

- Best known for the result we're discussing today.
- Never published or proved the result himself.
- First proof is attributed to Lagrange (1773).

Something for the History Buffs...

Pierre de Fermat [1601-1665]

- Well, there's too much history here!
- It seems that number theory was the subject closest to Fermat's heart.

John Wilson [1741-1793]

- Best known for the result we're discussing today.
- Never published or proved the result himself.
- First proof is attributed to Lagrange (1773).

François Edouard Anatole Lucas [1842-1891]

- French number theorist.
- Lucas-Lehmer primality test.
- Gave the well known Formula for the Fibonacci sequence

$$\sqrt{5}f_n = ((1+\sqrt{5})/2)^n - ((1-\sqrt{5})/2)^n.$$

- Published games under the name M. Claus (Tower of Hanoi).

Finite Cyclic Group Actions

For $n \geq 1$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ denotes the cyclic group of order n under addition modulo n.

Finite Cyclic Group Actions

For $n \geq 1$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ denotes the cyclic group of order n under addition modulo n.

An *action by* $\mathbb{Z}_n$ *on a set* X is a homomorphism $\mathbb{Z}_n \to \mathrm{Aut}(X)$, where $\mathrm{Aut}(X)$ denotes the group of permutations on the set X.

$gx \in X$ denotes the image of $x \in X$ under the permutation induced by $g \in \mathbb{Z}_n$.

Finite Cyclic Group Actions

For $n \geq 1$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ denotes the cyclic group of order n under addition modulo n.

An *action by* $\mathbb{Z}_n$ *on a set* X is a homomorphism $\mathbb{Z}_n \to \mathrm{Aut}(X)$, where $\mathrm{Aut}(X)$ denotes the group of permutations on the set X.

$gx \in X$ denotes the image of $x \in X$ under the permutation induced by $g \in \mathbb{Z}_n$.

Orbit: For all $x \in X$, let $\{gx \mid g \in \mathbb{Z}_n\}$.

Fixed Points: For all $g \in \mathbb{Z}_n$, let $X^g = \{x \in X \mid gx = x\}$.

Burnside's Theorem

Burnside's Theorem [for $\mathbb{Z}_n$]. If X is finite and $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is a group action, then the number of orbits is given by $(1/n)\sum_{g\in\mathbb{Z}_n} |X^g|$. In particular,

$$\sum_{g\in\mathbb{Z}_n} |X^g| \equiv 0 \pmod{n}.$$

Burnside's Theorem

Burnside's Theorem [for $\mathbb{Z}_n$]. If X is finite and $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is a group action, then the number of orbits is given by $(1/n)\sum_{g\in\mathbb{Z}_n} |X^g|$. In particular,

$$\sum_{g\in\mathbb{Z}_n} |X^g| \equiv 0 \pmod{n}.$$

Claim. If $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is an action, then for all $g \in \mathbb{Z}_n$,

$$X^g = X^{(g,n)},$$

where (g, n) denotes the greatest common divisor of g and n.

Burnside's Theorem

Burnside's Theorem [for $\mathbb{Z}_n$]. If X is finite and $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is a group action, then the number of orbits is given by $(1/n)\sum_{g\in\mathbb{Z}_n} |X^g|$. In particular,

$$\sum_{g\in\mathbb{Z}_n} |X^g| \equiv 0 \pmod{n}.$$

Claim. If $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is an action, then for all $g \in \mathbb{Z}_n$,

$$X^g = X^{(g,n)},$$

where (g, n) denotes the greatest common divisor of g and n.

Proof. The inclusion $X^{(g,n)} \subseteq X^g$ follows since $g = k(g, n)$ for some $k \in \mathbb{Z}$.

Burnside's Theorem

Burnside's Theorem [for $\mathbb{Z}_n$]. If X is finite and $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is a group action, then the number of orbits is given by $(1/n)\sum_{g\in\mathbb{Z}_n} |X^g|$. In particular,

$$\sum_{g\in\mathbb{Z}_n} |X^g| \equiv 0 \pmod{n}.$$

Claim. If $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is an action, then for all $g \in \mathbb{Z}_n$,

$$X^g = X^{(g,n)},$$

where (g, n) denotes the greatest common divisor of g and n.

Proof. The inclusion $X^{(g,n)} \subseteq X^g$ follows since $g = k(g, n)$ for some $k \in \mathbb{Z}$.

The opposite inclusion follows since there are integers $a, b \in \mathbb{Z}$ such that

$$(g, n) = ag + bn.$$

Grouping Terms and Generalizing the lemma

Since there are $\phi(n/d)$ elements $g \in \mathbb{Z}_n$ with $(g, n) = d$, where ϕ denotes Euler's totient function, we have shown the following:

Lemma. If X is a finite set and $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is a group action, then

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

Grouping Terms and Generalizing the lemma

Since there are $\phi(n/d)$ elements $g \in \mathbb{Z}_n$ with $(g, n) = d$, where ϕ denotes Euler's totient function, we have shown the following:

Lemma. If X is a finite set and $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is a group action, then

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

Lemma $\implies$ lemma:

Grouping Terms and Generalizing the lemma

Since there are $\phi(n/d)$ elements $g \in \mathbb{Z}_n$ with $(g, n) = d$, where ϕ denotes Euler's totient function, we have shown the following:

Lemma. If X is a finite set and $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is a group action, then

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

Lemma $\implies$ lemma: $\mathbb{Z}_p \to \mathrm{Aut}(X)$ is defined by $1 \mapsto f$, $X = X^p$ and $X' = X^1$.

Grouping Terms and Generalizing the lemma

Since there are $\phi(n/d)$ elements $g \in \mathbb{Z}_n$ with $(g, n) = d$, where ϕ denotes Euler's totient function, we have shown the following:

Lemma. If X is a finite set and $\mathbb{Z}_n \to \mathrm{Aut}(X)$ is a group action, then

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

Lemma $\implies$ lemma: $\mathbb{Z}_p \to \mathrm{Aut}(X)$ is defined by $1 \mapsto f$, $X = X^p$ and $X' = X^1$.Finally,

$$\sum_{d|p} \phi(p/d)|X^d| = \phi(1)|X^p| + \phi(p)|X^1| = |X^p| + (p-1)|X^1|.$$

Generalizing Fermat's (little) Theorem

Let $a \geq 1$, $A = \{1, \ldots, a\}$ and $X = A^n$.

Define $\mathbb{Z}_n \to \mathrm{Aut}(X)$ by $1(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$.

Generalizing Fermat's (little) Theorem

Let $a \geq 1$, $A = \{1, \ldots, a\}$ and $X = A^n$.

Define $\mathbb{Z}_n \to \mathrm{Aut}(X)$ by $1(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$.

For every divisor d of n

$$x \in X^d \iff \begin{array}{ccc} x_1 & = & x_{d+1} \end{array}$$

Generalizing Fermat's (little) Theorem

Let $a \geq 1$, $A = \{1, \ldots, a\}$ and $X = A^n$.

Define $\mathbb{Z}_n \to \mathrm{Aut}(X)$ by $1(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$.

For every divisor d of n

$$x \in X^d \iff x_1 = x_{d+1} = x_{2d+1}$$

Generalizing Fermat's (little) Theorem

Let $a \geq 1$, $A = \{1, \ldots, a\}$ and $X = A^n$.

Define $\mathbb{Z}_n \to \mathrm{Aut}(X)$ by $1(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$.

For every divisor d of n

$$x \in X^d \iff x_1 = x_{d+1} = x_{2d+1} = \cdots = x_{(n/d-1)d+1}$$

Generalizing Fermat's (little) Theorem

Let $a \geq 1$, $A = \{1, \ldots, a\}$ and $X = A^n$.

Define $\mathbb{Z}_n \to \mathrm{Aut}(X)$ by $1(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$.

For every divisor d of n

$$x \in X^d \iff \begin{array}{ccccccccc} x_1 & = & x_{d+1} & = & x_{2d+1} & = & \cdots & = & x_{(n/d-1)d+1} \\ x_2 & = & x_{d+2} & = & x_{2d+2} & = & \cdots & = & x_{(n/d-1)d+2} \\ \vdots & & & & & & & & \\ x_d & = & x_{d+d} & = & x_{2d+d} & = & \cdots & = & x_{(n/d-1)d+d} \end{array}$$

Generalizing Fermat's (little) Theorem

Let $a \geq 1$, $A = \{1, \ldots, a\}$ and $X = A^n$.

Define $\mathbb{Z}_n \to \mathrm{Aut}(X)$ by $1(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$.

For every divisor d of n

$$x \in X^d \iff \begin{array}{ccccccccc} x_1 & = & x_{d+1} & = & x_{2d+1} & = & \cdots & = & x_{(n/d-1)d+1} \\ x_2 & = & x_{d+2} & = & x_{2d+2} & = & \cdots & = & x_{(n/d-1)d+2} \\ \vdots & & & & & & & & \\ x_d & = & x_{d+d} & = & x_{2d+d} & = & \cdots & = & x_{(n/d-1)d+d} \end{array}$$

It follows that $|X^d| = a^d$.

Generalizing Fermat's (little) Theorem cont.

Theorem. For $n, a \geq 1$

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

Generalizing Fermat's (little) Theorem cont.

Theorem. For $n, a \geq 1$

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

Corollary. [Fermat's (little) Theorem] For a prime p and any integer a,

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

Proof. The result is trivial for $a = 0$ and follows from the above theorem for all $a \neq 0$ since $(-a)^p \equiv -a^p \pmod{p}$.

Wilson's Theorem

X is the set of all cycles of length n in the symmetric group $\mathrm{Aut}(\{1, \ldots, n\})$.

The action of $\mathbb{Z}_n$ on X is defined by

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

Wilson's Theorem

X is the set of all cycles of length n in the symmetric group $\mathrm{Aut}(\{1, \ldots, n\})$.

The action of $\mathbb{Z}_n$ on X is defined by

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

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

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

where the multiplication is done modulo n.

Wilson's Theorem

X is the set of all cycles of length n in the symmetric group $\mathrm{Aut}(\{1,\ldots,n\})$.

The action of $\mathbb{Z}_n$ on X is defined by

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

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

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

where the multiplication is done modulo n.

Claim. $\pi \in X^d$ iff. $\pi = \pi(g, a_2, \ldots, a_d)$.

Example

Example. Let $n = 12$, $d = 4$, $g = 8$, $a_2 = 9$, $a_3 = 6$ and $a_4 = 3$.

Example

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

$$\pi = (0, 9, 6, 3,$$

Example

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

$$\pi = (0, 9, 6, 3, 8, 5, 2, 11,$$

Example

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

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

Example

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

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

Note that

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

and

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

You 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 $\langle 4 \rangle$.

Generalized Wilson's Theorem

Given d, there are $\phi(n/d)$ choices for the element g, $(n/d)^{(d-1)}$ choices for the elements $a_2, \ldots, a_d$ and $(d-1)!$ ways to order them. Therefore, for every divisor d of n,

$$|X^d| = \phi\left(\frac{n}{d}\right)\left(\frac{n}{d}\right)^{d-1}(d-1)!$$

Generalized Wilson's Theorem

Given d, there are $\phi(n/d)$ choices for the element g, $(n/d)^{(d-1)}$ choices for the elements $a_2, \ldots, a_d$ and $(d-1)!$ ways to order them. Therefore, for every divisor d of n,

$$|X^d| = \phi\left(\frac{n}{d}\right)\left(\frac{n}{d}\right)^{d-1}(d-1)!$$

Theorem. For $n \geq 1$,

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

Generalized Wilson's Theorem

Given d, there are $\phi(n/d)$ choices for the element g, $(n/d)^{(d-1)}$ choices for the elements $a_2, \ldots, a_d$ and $(d-1)!$ ways to order them. Therefore, for every divisor d of n,

$$|X^d| = \phi\left(\frac{n}{d}\right)\left(\frac{n}{d}\right)^{d-1}(d-1)!$$

Theorem. For $n \geq 1$,

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

Corollary. [Wilson's Theorem] For a prime p,

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

And Lucas?

Theorem. For $n \geq 1$,

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

where the *length* $||\alpha||_d$ of an element $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{N}^d$ is defined by

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

Thank You!

eprint : arXiv:math.NT/0510620

Tyler J. Evans
evans@humboldt.edu
http://www.humboldt.edu/∼te8/