LUCAS' THEOREM

18.781 Handout (Spring 2013)

Lucas' theorem (named after the French mathematician François Édouard Anatole Lucas, 1842–1891) determines the congruence class of a binomial coefficient $\binom{n}{k}$ modulo a prime number p. Let

$$\begin{aligned} f(x) &= a_0 + a_1 x + \cdots \\ g(x) &= b_0 + b_1 x + \cdots \end{aligned}$$

be polynomials with integer coefficients a_i, b_i. Let $m \geq 1$. Define

$$f(x) \equiv g(x) \pmod{m}$$

if $a_i \equiv b_i \pmod{m}$ for all i.

Suppose that $f(x) \equiv g(x) \pmod{m}$ and $p(x) \equiv q(x) \pmod{m}$. It is elementary to show that

$$\begin{aligned} f(x) + p(x) &\equiv g(x) + q(x) \pmod{m} \\ f(x)p(x) &\equiv g(x)q(x) \pmod{m}. \end{aligned} \tag{3}$$

For instance, suppose that $f(x), g(x)$ are as above and

$$\begin{aligned} p(x) &= c_0 + c_1 x + \cdots \\ q(x) &= d_0 + d_1 x + \cdots . \end{aligned}$$

Then the coefficient of x^k in $f(x)p(x)$ is $\sum_{i=0}^{k} a_i c_{k-i}$, while the coefficient of x^k in $g(x)q(x)$ is $\sum_{i=0}^{k} b_i d_{k-i}$. Since $a_i \equiv b_i \pmod{m}$ and $c_i \equiv d_i \pmod{m}$, these two coefficients are congruent modulo m. Hence equation (3) holds.

Lemma. *Let p be prime and $1 \leq k \leq p-1$. Then*

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Proof. We have $\binom{p}{k} = p!/k!\,(p-k)!$. Since $p | p!$ but $p \nmid k!$ and $p \nmid (p-k)!$, the proof follows. $\square$

Theorem. $(x+1)^p \equiv x^p + 1 \pmod p$

Proof. We have
$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k.$$
By the lemma $\binom{p}{k} \equiv 0 \pmod p$ for $1 \le k \le p-1$, so
$$(x+1)^p \equiv \binom{p}{0} + \binom{p}{p} x^p \equiv 1 + x^p \pmod p. \ \square$$

From the above theorem we see that
$$(x+1)^{p^2} = ((x+1)^p)^p \equiv (x^p+1)^p \equiv x^{p^2} + 1 \pmod p,$$
and similarly
$$(x+1)^{p^r} \equiv x^{p^r} + 1 \pmod p \tag{4}$$
for every integer $r \ge 0$.

Now consider the base p expansions of the integers k and n, where we assume $0 \le k \le n$:
$$\begin{aligned} n &= a_0 + a_1 p + \cdots, \ 0 \le a_i < p \\ k &= b_0 + b_1 p + \cdots, \ 0 \le b_i < p. \end{aligned}$$
Of course both these sums are really finite, i.e., $a_i = b_i = 0$ for i sufficiently large.

Lucas' Theorem. $\binom{n}{k} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1} \cdots \pmod p$

Note that the product on the right is essentially finite, since for i sufficiently large we have $a_i = b_i = 0$ so $\binom{a_i}{b_i} = 1$.

Before turning to the proof of Lucas' theorem, let us consider some examples and consequences.

Example. What is $\binom{158}{64}$ modulo 3? Well, $158 = 2+1\cdot 3+2\cdot 3^2+2\cdot 3^3+1\cdot 3^4$

and $64 = 1 + 1\cdot 3^2 + 2\cdot 3^3$, so

$$\begin{aligned}\binom{158}{64} &\equiv \binom{2}{1}\binom{1}{0}\binom{2}{1}\binom{2}{2}\binom{1}{0} \pmod 3\\ &\equiv 2\cdot 1\cdot 2\cdot 1\cdot 1 \equiv 1 \pmod 3).\end{aligned}$$

Corollary. $\binom{n}{k} \not\equiv 0 \pmod p$ *if and only if* $b_i \le a_i$ *for all* i.

Proof. The numbers a_i and b_i satisfy $0 \le a_i, b_i < p$. Thus $\binom{a_i}{b_i}$ is divisible by p if and only if $b_i > a_i$ [why?] (in which case $\binom{a_i}{b_i} = 0$). The product $\binom{a_0}{b_0}\binom{a_1}{b_1}\cdots$ will be divisible by p if and only if one of its factors $\binom{a_i}{b_i}$ is divisible by p, i.e., if and only if $b_i > a_i$, so the proof follows. $\square$

Let $\#S$ denote the cardinality (number of elements) of the finite set S.

Corollary. Let $b(n)$ denote the number of 1's in the binary expansion of n. Define

$$f(n) = \#\{k\,:\, 0 \le k \le n,\ \binom{n}{k} \text{ is odd}\},$$

the number of elements in the nth row of Pascal's triangle that are odd (counting the top row as the 0th row). Then $f(n) = 2^{b(n)}$.

Proof. Let $n = a_0 + a_1\cdot 2 + a_2\cdot 2^2 + \cdots$ be the binary expansion of n, so $b(n)$ of the a_i's are odd. Let $k = b_0 + b_1\cdot 2 + b_2 \cdot 2^2 + \cdots$ be the binary expansion of k. By the previous corollary, $\binom{n}{k}$ is odd if and only if $b_i \le a_i$ for all i. If $a_i = 0$ then $b_i = 0$ (one choice), while if $a_i = 1$ then $b_i = 0$ or 1 (two choices). Hence there are $2^{b(n)}$ choices in all for k. $\square$

Proof of Lucas' theorem. All congruences below are modulo p. We have

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}x^k &= (x+1)^n\\ &= (x+1)^{a_0+a_1p+a_2p^2+\cdots}\\ &= (x+1)^{a_0}(x+1)^{a_1p}(x+1)^{a_2p^2}\cdots.\end{aligned}$$

By equation (4) we get

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}x^k &\equiv (1+x)^{a_0}(1+x^p)^{a_1}(1+x^{p^2})^{a_2}\cdots \\ &\equiv \prod_{i\geq 0}\left(\sum_{b_i=0}^{a_i}\binom{a_i}{b_i}x^{b_ip^i}\right).\end{aligned}$$

Since $\binom{a_i}{b_i}=0$ if $b_i>a_i$, we get

$$\sum_{k=0}^{n}\binom{n}{k}x^k = \prod_{i\geq 0}\left(\sum_{b_i=0}^{p-1}\binom{a_i}{b_i}x^{b_ip^i}\right). \tag{5}$$

The coefficient of x^k on the left-hand side of (5) is $\binom{n}{k}$. What is the coefficient of x^k on the right-hand side? When we expand the product, a typical term will look like

$$\binom{a_0}{b_0}x^{b_0}\binom{a_1}{b_1}x^{b_1p}\binom{a_2}{b_2}x^{b_2p^2}\cdots.$$

In order for the exponent of x to be k we need

$$k = b_0 + b_1p + b_2p^2 + \cdots. \tag{6}$$

Since $0\leq b_i\leq p-1$, there is exactly on way to do this, namely, (6) must be the base p expansion of k. Hence the coefficient of x^k on the right-hand side of (5) is $\binom{a_0}{b_0}\binom{a_1}{b_1}\cdots$. Since the coefficients of x^k on both sides of (5) are congruent modulo p, we get

$$\binom{n}{k}\equiv\binom{a_0}{b_0}\binom{a_1}{b_1}\cdots,$$

as was to be proved. □

For "cultural" purposes we mention an amusing related theorem due to Ernst Eduard Kummer (1810–1893).

Theorem. *Let $p^j\|\binom{n}{k}$. Then j is the number of carries in adding k and $n-k$ (using the usual addition algorithm) in base p.*

Note. For further information on the topic of binomial coefficient congruences, see `www.cecm.sfu.ca/organics/papers/granville`.