Practice Power Round

Lucas's Theorem

Misha Lavrov

ARML Practice 5/18/2014

0 Notation

If n and m are integers and $m > 0$, there is exactly one way to write $n = q \cdot m + r$, where q and r are integers and $0 \le r \le m - 1$. We say that q (which satisfies $q = \left\lfloor \frac{n}{m} \right\rfloor$) is the *quotient* and r the *remainder* when n is divided by m.

We write $r = n \bmod m$ (pronounced "n modulo m") for the remainder.

When $x \bmod m = y \bmod m$, we say that x and y are *congruent modulo* m and write $x \equiv y \pmod{m}$.

Suppose that $F(x)$ and $G(x)$ are polynomials in x. We write $F(x) \equiv G(x) \pmod{m}$ to mean that for all k, the coefficients of x^k in $F(x)$ and $G(x)$ are congruent modulo m. For example,

$$x^2 + 2x + 1 \equiv 10x^3 + x^2 + 22x - 9 \pmod{10}.$$

This is, in general, a stronger statement than simply saying $F(n) \equiv G(n) \pmod{m}$ for all integers n. For example, $n^2 + n \equiv 0 \pmod{2}$ for all n; however, $x^2 + x \not\equiv 0 \pmod{2}$ as a polynomial, since the coefficient of x is odd in $x^2 + x$ and even in 0.

1 Lucas's Theorem

What is the remainder when $\binom{n}{k}$ is divided by a prime p?

Lucas's theorem gives a surprising formula for the answer. To compute $\binom{n}{k} \bmod p$, first write both n and k in base p. Let the digits of n in base p be $n_t n_{t-1} n_{t-2} \dots n_1 n_0$; that is, suppose that

$$n = n_t \cdot p^t + n_{t-1} \cdot p^{t-1} + n_{t-2} \cdot p^{t-2} + \cdots + n_1 \cdot p + n_0$$

where $n_i \in \{0, 1, 2, \dots, p-1\}$ for all i.

Let the digits of k in base p be $k_t k_{t-1} k_{t-2} \dots k_1 k_0$ (if necessary, we pad k with zeroes on the left so that it has the same number of base-p digits as n).

Then

$$\binom{n}{k} \equiv \binom{n_t}{k_t} \cdot \binom{n_{t-1}}{k_{t-1}} \cdot \binom{n_{t-2}}{k_{t-2}} \cdot \dots \cdot \binom{n_1}{k_1} \cdot \binom{n_0}{k_0} \pmod{p}.$$

2 Practice problems

1. Use Lucas's theorem to compute $\binom{100}{50}$ mod 5 and $\binom{75}{25}$ mod 3.
2. Compute the last digit of $\binom{250}{125}$ in base 10. *(Note that $\binom{2}{1}\binom{5}{2}\binom{0}{5}$ will not work.)*
3. Give an expression of the form "$\binom{n}{k}$ mod m" which you *cannot* derive from Lucas's theorem.

3 Proof

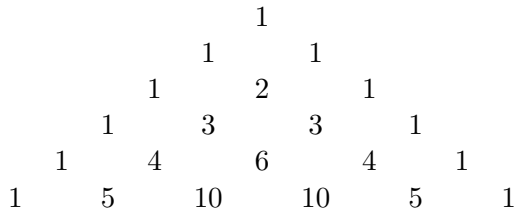
In this section, we will use generating functions to prove Lucas's theorem. (So don't use Lucas's theorem in this section!)

4. Prove that $(1+x)^p \equiv 1 + x^p \pmod{p}$.
5. For $n \geq p$, let $q = \left\lfloor \frac{n}{p} \right\rfloor$ and $r = n \bmod p$, so that $n = qp + r$. Prove that
$$(1+x)^n \equiv (1+x^p)^q (1+x)^r \pmod{p}.$$
6. For $0 \leq k \leq n$, let $q' = \left\lfloor \frac{k}{p} \right\rfloor$ and $r' = k \bmod p$, so that $k = q'p + r'$. Prove that the coefficient of x^k in $(1+x^p)^q(1+x)^r$ is
$$\binom{q}{q'}\binom{r}{r'}.$$
7. It follows from problems 5 and 6 that
$$\binom{qp+r}{q'p+r'} \equiv \binom{q}{q'}\binom{r}{r'} \pmod{p}.$$
Use this to prove Lucas's theorem.

4 The Sierpiński triangle

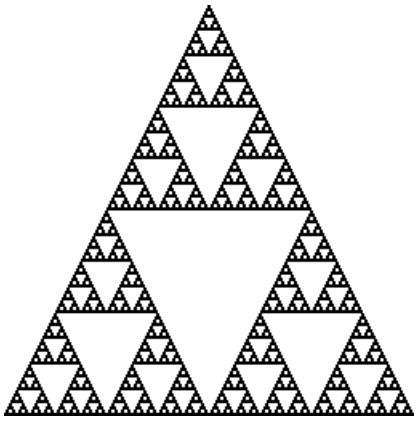
The binomial coefficients $\binom{n}{k}$ can be arranged in a triangular array called Pascal's triangle. The n^{th} row of *Pascal's triangle* is the sequence of binomial coefficients $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}, \binom{n}{n}$.

Starting with the 0^{th} row, which has 1 element, the n^{th} row has $n+1$ elements. Writing the rows one after the other, we get Pascal's triangle:



Pascal's identity states that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. Therefore each entry in Pascal's triangle is the sum of the two entries above it.

If you take Pascal's triangle modulo 2, drawing even entries as white and odd entries as black, a fractal pattern emerges:



The first 128 rows of Pascal's triangle, modulo 2

In this section, we will prove that this pattern continues.

8. In words, we can describe the pattern by saying that the first 2^t rows of Pascal's triangle modulo 2 are made up of 3 congruent sub-triangles and a white inverted triangle in the middle.

   (a) Write down a sequence of equivalences modulo 2 that says that the top triangle is colored in the same way as the left triangle.

   (b) Write down a sequence of equivalences modulo 2 that says that the top triangle is colored in the same way as the right triangle.

   (c) Describe the set S of pairs (n, k) such that $0 \leq k \leq n < 2^t$, and the binomial coefficient $\binom{n}{k}$ is contained in the inverted white triangle.

9. (a) Use Lucas's theorem to prove the equivalences in parts 8(a) and 8(b).

   (b) Prove the following lemma: if $x < y$ and x and y are written in base 2, there is at least one position in which x has a 0 but y has a 1.

   (c) Use Lucas's theorem to show that for all $(n, k) \in S$, where S is the set defined in part 8(c), $\binom{n}{k} \equiv 0 \pmod 2$.

10. If you dare, use Pascal's identity to prove the results in 9(a) and 9(c) without applying Lucas's theorem.

5 Another application

(The following problem is due to Po-Shen Loh.)

Let $C(n)$ be the number of entries in the n^{th} row of Pascal's triangle which are *not* divisible by 3. We say that if $C(n)$ is a prime power (expressible as $C(n) = p^k$ for some prime p and some $k \geq 1$), then the n^{th} row is *cool*.

For example, the 10^{th} row of Pascal's triangle is

$$1,\ 10,\ 45,\ 120,\ 210,\ 252,\ 210,\ 120,\ 45,\ 10,\ 1.$$

All of these entries except for the first two (1 and 10) and the last two (10 and 1) are divisible by 3. Therefore $C(10) = 4$. Since $4 = 2^2$ is a prime power, the 10^{th} row of Pascal's triangle is cool.

11. Compute the smallest $n > 0$ such that the n^{th} row is uncool. (We don't consider 1 to be a prime power, and $C(0) = 1$, so the 0^{th} row is also uncool, but that doesn't count.)
12. Let the digits of n in base 3 be $n_t n_{t-1} n_{t-2} \ldots n_1 n_0$. Find, with proof, a formula for $C(n)$ in terms of $n_0, n_1, \ldots, n_t$, and use it to compute $C(100)$.
13. How many of the first 3^n rows (rows 0 through $3^n - 1$) are cool? Find, with proof, a general formula in terms of n.

6 Meta-power round

This is what power round writers think about when writing the power rounds they write.

14. List all problems in this power round that do not require a proof.
15. We say that a "happy dependency" is a situation in which you can use an earlier problem to solve a later problem, without having solved the earlier problem. List all happy dependencies between the problems in this power round. *(Don't bother trying to find dependencies between problems in different sections.)*
16. We say that a "sad dependency" is a situation in which a later problem is impossible to even begin until an earlier problem has been solved. List all sad dependencies between the problems in this power round. *(Don't bother trying to find dependencies between problems in different sections.)*

Almost any dependency between problems can be made happy or sad. For example, $12 \to 13$ is currently a sad dependency, since you don't know the formula in problem 12 until you solve problem 12. This could be made into a happy dependency by writing problem 12 as "Prove that the formula $C(n) =$ _____ holds." Then problem 13 could be solved simply by using the formula.

For homework: Download the 2013 ARML contest from `http://www.arml.com`, and solve problems 14–16 for that power round. (Not the problems 14–16 in the 2013 power round, which only goes up to 10; the problems on this page, just applied to... you get the idea.)