Discovering a Binomial Identity

Binomial identities are formula involving binomial coefficients. These identities have applications in many areas of mathematics including number theory, combinatorics, and probability. By studying binomial coefficients modulo an integer, divisibility properties can be examined. In practice however, computing large binomial coefficients can be time consuming because of the factorials involved. Consequently, mathematical shortcuts are often needed to make statements about certain binomial quantities without having to resort to direct computation. Discovering one of these shortcuts is the goal of this lab, specifically we will investigate the following product.

$$\prod_{i=0}^{p-1} \binom{p-1}{i} \mod p$$

We would like to say what this quantity is for *any* prime p.

Exercises:

1. To accomplish this, first construct Pascal's Triangle mod p using either PascGaloisJE or one of the supporting Java applets. Do this for several different primes p. Examine the value of $\binom{p-1}{i} \mod p$ for each $i = 0, 1, \ldots, p-1$. Make sure you are looking at the correct row of your graphical output!

2. Based on the empirical evidence collected in Exercise 1, make a conjecture about the value of $\binom{p-1}{i} \mod p$ that holds for any prime p and $i = 0, 1, \ldots, p-1$.

3. Obtaining your previous conjecture should not have been too difficult using the software PascGaloisJE. However, the software cannot prove your conjecture - it can only provide numerical evidence to support it. (Or, if your conjecture is not correct, the software could provide a counter-example). Next, give a rigorous mathematical proof of your conjecture. You may want to use the fact that $n - j \equiv -j \mod n$ in your proof. It may also help to revisit some of the basic theorems from number theory regarding the arithmetic of congruences (e.g. addition, multiplication, and division). *Be particularly careful in your proof if you use division.* In fact, you may need the following result from number theory:

   Theorem Suppose that $a, b, c \in \mathbb{Z}$ such that $ac \equiv bc \mod n$. Then $a \equiv b \mod \frac{n}{d}$, where $d = \gcd(c, n)$.

4. Notice that your conjecture and proof in Exercises 2 and 3 use a prime modulus. We are now going to determine if your formula can be generalized to non-prime moduli. Replace p in your formula from Exercises 2 and 3 with n, where n can be any positive integer. In other words, consider the value of $\binom{n-1}{i} \mod n$ for $i = 0, 1, \ldots, n-1$. **IF** your proof from Exercise 3 generalizes, what should $\binom{n-1}{i} \mod n$ equal?

5. To see if this generalization in Exercise 4 is true or false, construct Pascal's Triangle mod n for various composite values n and examine the value of $\binom{n-1}{i} \mod n$ for each $i = 0, 1, \ldots, n-1$. Based on empirical evidence, does it appear that your result generalizes to composite moduli? If so, explain why your proof can be generalized. If not, give a counter-example and also explain where in your proof for the prime case the proof breaks down if n is not prime.

6. Using your formula for $\binom{p-1}{i} \mod p$ from Exercises 2 and 3, now investigate

   $$\prod_{i=0}^{p-1} \binom{p-1}{i} \mod p$$

   for various primes p. Make a conjecture as to what this quantity should be and then give a proof for your conjecture.

Challenge Exercise - Optional: Generalize the result in Exercise 6 for

$$\prod_{i=0}^{p^n-1} \binom{p^n - 1}{i} \quad \text{mod } p \text{ for } n \geq 1$$

Along the way you will need to investigate $\binom{p^n-1}{i}$ mod p for each $i = 0, 1, \ldots, p^n - 1$. Does your proof in Exercise 3 generalize from $p - 1$ to $p^n - 1$ for $n > 1$?