

Greetings, Vegetarians and non. This email has all these \$ signs in it, they're not typos, they're markups for a mathematical typesetting language, indicating: here begins a formula. The other dollar sign signifies the end of the formula and the return to plain text. This can be used to give pretty output; I've posted the resulting pretty form to my web page under a link titled 12thman. Click on <http://www.math.tamu.edu/Doug.Hensley/> and follow your eyes to that link. It's an adobe pdf document, readable on most systems. You may have to magnify the file a couple of steps to make it legible.

Let's talk a little first about the roots of 1.

From one perspective, these are complex numbers. The fourth roots of one, for instance, are the four complex numbers $1, i, -1$ and $-i$. In general, there are n roots of the polynomial equation $z^n = 1$, and they are evenly spaced complex numbers around the unit circle.

For $n = 2$, these are ± 1 , and for $n = 4$ they've just been listed above. For $n = 6$, these numbers are ± 1 and $\pm(1/2) \pm i\sqrt{3}/2$. For the case $n = 5$ there is again a representation of these numbers in terms of i and square roots of integers, but in general this doesn't work. We don't really need it.

The n^{th} roots of 1 are the complex numbers $\cos(2k\pi/n) + i\sin(2k\pi/n) = e^{2\pi ik/n}$. Their sum is zero, and their product is 1 if n is odd, or -1 if n is even.

First problem: Prove that their sum is zero. If n is even, this is easy, because they come in pairs: if z is such a root, then so is $-z$. If n is odd, your best bet is to use the formula involving e , and think about geometric series.

Now, let's bring in congruence arithmetic. What happens when we look at the equation $z^3 = 1 \pmod{7}$? That is, suppose that we take for our number system the numbers $0, 1, 2, 3, 4, 5, 6$, with multiplication and addition done mod 7?

The polynomial $z^3 - 1$ has three zeros mod 7: 1, 2, and 4. This is not exactly a coincidence; the polynomial $z^6 - 1$ has six zeros mod 7; every congruence class except zero works. This is

Fermat's little theorem:

$$a^{p-1} \equiv 1 \pmod{p}$$

Thus, $2^6 = 64 = 63 + 1 = 9 * 7 + 1 \equiv 1 \pmod{7}$, and $3^6 = 729 = 728 + 1 = 7 * (104) + 1 \equiv 1 \pmod{7}$.

Let's take a closer look at $3^6 \pmod{7}$. The powers of 3, mod 7, go $3, 9 \equiv 2, 27 \equiv 6, 81 \equiv 18 \equiv 4, 243 \equiv 54 \equiv 12 \equiv 5$, and finally, multiplying 5 by 3 gives $15 \equiv 1$. So, the powers of 3, mod 7, go $3, 2, 6, 4, 5, 1$. Not only is the sixth power congruent to 1, the other powers simply walk through the list of nonzero congruence classes.

This makes 3 what is called a PRIMITIVE ROOT mod 7, and the theorem is that for every prime p , there are primitive roots mod p .

For instance, mod 11, the powers of 2 go $2, 4, 8, 16 \equiv 5$, and then $10, 20 \equiv 9, 18 \equiv 7, 14 \equiv 3$, and finally, 6 and 1. So, 2 is a primitive root mod 11.

Now back to the cube roots of 1 mod 7: they are the second, fourth and sixth powers of

the primitive root 3: $3^2 \equiv 2$, $3^4 \equiv 4$, and $3^6 \equiv 1$. Now these numbers form a geometric series, just like with complex numbers.

The sum of a finite geometric series $a + ar + ar^2 + \dots + a^n$ is $a(r^{n+1} - 1)/(r - 1)$. This works in arithmetic mod 7 as well as in complex numbers, but here, with $r = 2$, division by 1 presents no difficulty. Either using this idea, or just head-on, $1 + 2 + 4 \equiv 0 \pmod{7}$.

Now what does this have to do with the binomial theorem?

The binomial coefficient n choose k , written $C(n, k)$ or $\binom{n}{k}$, can be defined as $n!/(k!(n - k)!)$. Although the definition involves division, and so on its face gives a rational number which might not be an integer, this expression always works out to an integer. If $k = 0$ or if $k = n$, it gives 1. If $n > k > 0$ then it gives a positive integer greater than 1.

The binomial coefficients are often thought of as forming a triangle of numbers. The top row is called the zeroth row, and consists of simply the number 1. The next row is 1,1.

The table then goes:

1
 1,1
 1,2,1
 1,3,3,1
 1,4,6,4,1
 1,5,10,10,5,1
 1,6,15,20,15,6,1

and so on. The binomial coefficients obey the formula $C(n, k) = C(n-1, k-1) + C(n-1, k)$. Pictorially, this says that any time you have

oldrowentrya, oldrowentryb

nextrowentrya, nextrowentryb,

nextrowentryb is equal to oldrowentrya+oldrowentryb.

In each row, we count entries starting from zero, so the entries in the number four row of the Pascal triangle are entry number zero is 1, entry 1 is 4, entry number 2 is 6, entry number 3 is 4, and entry number 4 is again 1.

The 6 in the middle is the sum of the 3 directly above, and the 3 above and diagonally left, in the row above.

The binomial theorem says that $(a + b)^n = a^n + C(n, 1)a^{n-1}b + C(n, 2)a^{n-2}b^2 + \dots$

Problem: Find the value, in the complex plane, of the number $C(12, 0) + C(12, 3) + C(12, 6) + C(12, 9) + C(12, 12)$. Then do the same for 99 in place of 12.

Hint: Let $w = (-1/2) + \sqrt{3}/2$ be one of the cube roots of 1. Think about $(1 + w)^{12}$ and $(1 + w^2)^{12}$ and $(1 + 1)^{12}$. What happens when we expand this? You will get a 3 by 13

array of numbers to be summed. Evaluate $1 + w$, then evaluate the 12th power of this number. Going at it this way gives an easily evaluated answer.

Summing in the other direction, see what you get. Put it all together.

Problem: Find the value mod 7 of the sum of binomial coefficients $C(12, 0) + C(12, 3) + C(12, 6) + C(12, 9) + C(12, 12)$. Then do the same with 99 in place of 12.

(It's the same idea.)

Now to almost totally change the subject, let's talk about the combinatorial side of the binomial theorem.

The coefficients $C(n, k)$ give the number of subsets of $\{1, 2, \dots, n\}$ with k elements.

A Putnam problem from a few years back involved this kind of issue:(I paraphrase). 20 students must each choose a subset of 6 available humanities courses to enroll in next semester. Prove or disprove that these 20 students can arrange matters so that no two students take the same humanities schedule, nor even, any student takes a schedule which is a subset of another student's schedule.