A Binomial Theorem Trick

Tyler Zhu

March 23, 2017

In this short article, I discuss a nice trick for evaluating powers of numbers modulo powers of primes that I have yet to see any exposition of. Along the way I throw together some random classical problems that have very little connection.

The trick too nice for me to lock up and forget about, so I decided to share it. This article came out of a short aside by Zeb Brady.

1 Binomial Theorem

In order to use the binomial theorem, we must recall what it is. Before we can recall the theorem, we have to recall what a binomial coefficient is.

Definition 1. Let $\binom{n}{k}$ be defined as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-(k-1))}{k(k-1)(k-2)\cdots 1}$$

where $n! = n \cdot (n-1)\cdots 2 \cdot 1$ is n factorial. We call this a **binomial coefficient**, and we pronounce it as *n choose k*.

Note that there are k terms in the numerator and k terms in the denomiator. For example,

$$\binom{5}{2} = \frac{5\cdot 4}{2\cdot 1}, \quad \binom{4}{3} = \frac{4\cdot 3\cdot 2}{3\cdot 2\cdot 1}, \quad \binom{10}{5} = \frac{10\cdot 9\cdot 8\cdot 7\cdot 6}{5\cdot 4\cdot 3\cdot 2\cdot 1}.$$

Of course, such an interesting definition would not exist if it did not have far-reaching applications, of which we present now a few of the more important ones.

Fact 2. The number of ways to choose k items out of n items with no regard for the order is $\binom{n}{k}$.

Proof. I have n choices for my 1st item, $n-1$ choices for my 2nd item, and so on, until I have $n-(k-1)$ choices for my kth item. However, I am overcounting every choice $k!$ times since there are $k!$ different ways with order that I could have picked these k items. This number is precisely our second definition of the binomial coefficient. □

Fact 3. $\binom{n}{k} = \binom{n}{n-k}$.

Proof. There are two different ways I can choose to pick k balls that I like to buy out of n total balls. I can either pick the k balls that I like, which is $\binom{n}{k}$, or I can set aside the ones I don't like, which has $\binom{n}{n-k}$ ways of occuring. □

Fact 4. The rows of Pascal's Triangle are binomial coefficients! Indeed, this is a good way to systematically work out the binomial coefficients if necessary.

Proof. Start at the 1 at the top of Pascal's Triangle. If I wish to get to the kth number in the nth row, then I have to descend k times to the right and $n-k$ times to the left. The number of ways to do this is the number of ways to rearrange k R's and $n-k$ L's, which is $\binom{n}{k}$. □

Now that you are adequately well versed in the arts of binomial coefficients, its time to introduct the sensei of binomials.

Theorem 5 (Binomial Theorem)**.** *For any numbers x, y and a positive integer n,*

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-2}x^2y^{n-2} + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

An easy way to memorize this is that the powers of x and y always sum to n, and since $\binom{n}{k} = \binom{n}{n-k}$, the coefficient is always n choose the exponent of x or the exponent of y. Here is an easy application of the binomial theorem.

Fact 6.

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n}.$$

Proof. Hint: Plug in something for x and y! □

Here is a classic problem that uses the previous fact:

Problem 1.1: Determine a value for

$$S = \binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + (n-1)\binom{n}{n-1} + n\binom{n}{n}.$$

Hmm this seems familiar... it's *definitely* not related to the fact we just proved right?

Proof. The key insight to this problem is to use Fact 3 to rewrite the givens as

$$S = 0\binom{n}{0} + 1\binom{n}{1} + 2\binom{n}{2} + \cdots + (n-1)\binom{n}{n-1} + n\binom{n}{n} \tag{1}$$

$$S = 0\binom{n}{n} + 1\binom{n}{n-1} + 2\binom{n}{n-2} + \cdots + (n-1)\binom{n}{1} + n\binom{n}{0} \tag{2}$$

Then if we reverse the order of (2), we get that

$$S = n\binom{n}{0} + (n-1)\binom{n}{1} + \cdots + 1\binom{n}{n-1} + 0\binom{n}{n} \tag{3}$$

Adding (1) and (3) then gives us

$$2S = n\binom{n}{0} + n\binom{n}{1} + \cdots + n\binom{n}{n-1} + n\binom{n}{n} = n(\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n}) = n2^n$$

and so we get that $\boxed{S = n2^{n-1}}$. □

If you want more problems like this, read any standard combinatorics textbook; good candidates are the AoPS Volumes 1/2 and their intermediate series.

2 Number Theory

Finally! Two boring pages of combinatorics later is the fun number theory! This time the theorems are harder, so I'll just cite the theorems and cut right to the chase. We'll need two more classical theorems, the first of which is due to Fermat.

Theorem 7 (Fermat's Little Theorem)**.** *If a and p are relatively prime integers, with p being a prime, then*

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

What happens when a and p are not relatively prime? Can you modify the theorem so that it covers this case too?

This theorem does a lot for us already; it lets us to compute powers modulo primes very quickly.

Problem 2.1: Find the remainder when 2^{2017} is divided by 2011.

Proof. We open up Google and search, "Is 2011 prime?", and find out that it is. Hence, by FLT,

$$2^{2017} = 2^{2010} \cdot 2^7 \equiv 1 \cdot 2^7 \equiv \boxed{128} \pmod{2011}.$$

□

The next theorem is a generalization of this to arbitrary moduli, and is due to Euler.

Theorem 8 (Euler's Totient Theorem)**.** *If a and $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ are relatively prime integers and $p_1, p_2, \cdots, p_k$ are distinct primes, then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

where

$$\begin{aligned}\varphi(n) &= \#\text{ of positive integers } a \text{ less than } n \text{ that are relatively prime to } n \\ &= n\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\cdots\left(\frac{p_k-1}{p_k}\right)\end{aligned}$$

is Euler's Totient Function.

Note that an easy way to calculate $\varphi(n)$ for any integer n is to note that $\varphi(p^k) = p^k - p^{k-1}$ and that for relatively prime integers m and n, $\varphi(mn) = \varphi(m)\varphi(n)$. In particular, $\varphi(p) = p - 1$, FLT!

Problem 2.2: Determine the units digit of 317^{2008}.

Proof. Since we want the units digit, this is equivalent to finding 7^{2008} modulo 10. $\varphi(10) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4$, so by Euler's Totient Theorem,

$$a^4 \equiv 1 \pmod{10}$$

. Hence, since $\gcd(7, 10) = 1$, we have that

$$7^{2008} = (7^4)^{502} \equiv 1^{502} \equiv \boxed{1} \pmod{10}.$$

□

In particular, this implies that the units digit of powers of 7 cycles in groups of 4! What can you say about other numbers?

Exercise 2.3: Find the tens digit of 1337^{401}. Hint: $\varphi(100) = 40$.

3 Binomial Theorem Bashing

At last, we can demonstrate our nice trick. All we need now is a willing... *victim*.

Problem 3.1: Compute the remainder when 14^{70} is divided by 169.

Proof. Lets try attacking this with what we already know. We find that $\varphi(169) = 156$, so we know that by Euler's Totient Theorem, $14^{156} \equiv 1 \pmod{169}$... Very helpful.

Now that I've convinced you that the only way to do this is to bash[1], let me show you the much nicer solution. Note that since $14 = 1 + 13$, we have that

$$14^{70} = (1+13)^{70} = 1 + \binom{70}{1}13 + \binom{70}{2}13^2 + \binom{70}{3}13^3 + \cdots$$

where we used our handy Binomial Theorem to expand the binomial. However, note that all of the terms after the second one die out because they contain two or more powers of 13, and usually 13^2 is 0 modulo 169. Hence, we see that

$$14^{70} \equiv 1 + \binom{70}{1}13 \equiv 1 + 70 \cdot 13 \equiv 911 \equiv \boxed{66} \pmod{13^2}.$$

□

Easy right? Fun right? Let's do it again!

Problem 3.2: Compute the remainder when 3^{2018} is divided by 13^2.

Proof. Here's the problem; we can't exactly write 3 as a multiple of 13 plus or minus 1. However, what we can do is look for the closest *power* of 3 that is a multiple of 13 plus or minus 1. It doesn't take us long to find 3^3, which is

$$3^3 = 27 = 26 + 1 = 2 \cdot 13 + 1,$$

and we're back in business! Hence, we see that

$$\begin{aligned} 3^{2018} &= (3^3)^{672} \cdot 3^2 \\ &= (1 + 2 \cdot 13)^{672} \cdot 9 \\ &= \left(1 + \binom{672}{1}(2 \cdot 13) + \binom{672}{2}(2 \cdot 13)^2 + \cdots\right) \cdot 9 \\ &\equiv (1 + 672 \cdot 2 \cdot 13) \cdot 9 \pmod{13^2} \\ &= 9 + 9 \cdot 672 \cdot 2 \cdot 13 \end{aligned}$$

Here we use another cool trick; Note that since we're working modulo 13^2, if we have something like $13k$, then we only actually care about k modulo 13 (Why?). Hence, since

$$9 \cdot 672 \cdot 2 \equiv 9 \cdot 9 \cdot 2 \equiv 9 \cdot 5 \equiv 6 \pmod{13}$$

we have that

$$3^{2018} \equiv 9 + 6 \cdot 13 \equiv \boxed{87} \pmod{13^2}.$$

□

[1] Hi Alicia!

For those of you who were keen enough to notice, we could have drastically simplified our solution using Euler's Totient Theorem and a tricky application of the Binomial Theorem.

Negative BT Proof. Note that since $\varphi(13^2) = 13^2 - 13 = 156$, we have that

$$\begin{aligned} 3^{2018} \equiv 3^{-10} &\equiv (1 + 2 \cdot 13)^{-4} \cdot 3^2 \pmod{13^2} \\ (!!) &\equiv (1 - 4 \cdot 2 \cdot 13) \cdot 9 \pmod{13^2} \\ &= (1 - 8 \cdot 13) \cdot 9 \\ &\equiv 9 + 5 \cdot 9 \cdot 13 \equiv 9 + 6 \cdot 13 \equiv \boxed{87} \pmod{13^2}. \end{aligned}$$

Here, we used our Binomial Theorem when the power n was -4. In theory this holds is precisely the way you'd expect it to hold, except you need to be careful about how you define your binomial coefficients especially with negative numbers! Google "generalized Binomial Theorem" if you're interested. Another way to see the result is to instead raise the binomial to the $-4 \equiv 152$ power, which means we would have $(1 + 152 \cdot 2 \cdot 13) \cdot 9$, but this is the same since $152 \equiv -4 \pmod{13}$. $\square$

Neat! (PM if you have problems for me to add here)

4 Advanced Musings

Really what we we're doing is that we were using the fact that

$$n = \text{ord}_p(a) \cdot q + r$$

where $0 \leq r < \text{ord}_p(a)$ to write a^n as

$$a^n = \left(a^{\text{ord}_p(a)}\right)^q \cdot a^r$$

This was good, because $a^{\text{ord}_p(a)} \equiv 1 \pmod{p}$ implies that $a^{\text{ord}_p(a)} = 1 + p \cdot m$ for some integer m[2], and thus

$$\begin{aligned} a^n &= (a^{\text{ord}_p(a)})^q \cdot a^r \pmod{p^k} \\ &= (1 + p \cdot m)^q \cdot a^r \pmod{p^k} \\ &= \left(1 + \binom{q}{1}(pm) + \binom{q}{2}(pm)^2 + \cdots\right) a^r \pmod{p^k} \\ &= a^r \left(1 + \binom{q}{1}(pm) + \binom{q}{2}(pm)^2 + \cdots + \binom{q}{k-1}(pm)^{k-1}\right) \end{aligned}$$

That is all.

[2] 1 - pm works as well, you just need to account for sign changes.