Primality Testing and Factoring Using Pascal's Triangle

Bassam Abdul-Baki

December 21, 2021

Abstract

An interesting if not impractical way of primality testing and factoring a number using Pascal's Triangle.

Definition

Pascal's Triangle is a triangular array where the initial row starts with a one and every number under it is stacked diagonally and is equal to the sum of the two numbers above it. A picture[1] is worth a thousand words.

$$
\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 3 & & 1 & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}
$$

The general formula for each number using combinations is as follows:

$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ and n! = 1×2×…×n and 0! = 1.

Notation

In modular arithmetic, a mod b is the remainder of a divided by b, which ranges between 0 and b – 1.

For our purposes, we choose to use the range between $\left\lceil \frac{-b+1}{2} \right\rceil$ and $\left\lfloor \frac{b+1}{2} \right\rfloor$, where for even numbers, only the positive half is included.

Patterns

Many patterns emerge from Pascal's Triangle including the fact that for any prime number, all the numbers of that row, minus the first and last number which are always 1, are divisible by that prime number. See the prime number rows in the second diagonal column above.

A simple proof is to see that $\binom{p}{k}$ is an integer with p being multiplied in the numerator and for any 1 ≤ k ≤ p – 1, both k! and (p – k)! are relatively prime to p and cannot divide p.

For simplicity's sake, we will be using a tabular form to display Pascal's Triangle.

k n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1																
1	1	1															
2	1	2	1														
3	1	3	3	1													
4	1	4	6	4	1												
5	1	5	10	10	5	1											
6	1	6	15	20	15	6	1										
7	1	7	21	35	35	21	7	1									
8	1	8	28	56	70	56	28	8	1								
9	1	9	36	84	126	126	84	36	9	1							
10	1	10	45	120	210	252	210	120	45	10	1						
11	1	11	55	165	330	462	462	330	165	55	11	1					
12	1	12	66	220	495	792	924	792	495	220	66	12	1				
13	1	13	78	286	715	1,287	1,716	1,716	1,287	715	286	78	13	1			
14	1	14	91	364	1,001	2,002	3,003	3,432	3,003	2,002	1,001	364	91	14	1		
15	1	15	105	455	1,365	3,003	5,005	6,435	6,435	5,005	3,003	1,365	455	105	15	1	
16	1	16	120	560	1,820	4,368	8,008	11,440	12,870	11,440	8,008	4,368	1,820	560	120	16	1

Taking the modulus of each row using one more than the base gives us the following (with the mod column added at the end for consistency):

k n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	mod
0	0																	**1**
1	1	1																**2**
2	1	2	1															**3**
3	1	3	3	1														**4**
4	1	4	1	4	1													**5**
5	1	5	4	4	5	1												**6**
6	1	6	1	6	1	6	1											**7**
7	1	7	5	3	3	5	7	1										**8**
8	1	8	1	2	7	2	1	8	1									**9**
9	1	9	6	4	6	6	4	6	9	1								**10**
10	1	10	1	10	1	10	1	10	1	10	1							**11**
11	1	11	7	9	6	6	6	6	9	7	11	1						**12**
12	1	12	1	12	1	12	1	12	1	12	1	12	1					**13**
13	1	13	8	6	1	13	8	8	13	1	6	8	13	1				**14**
14	1	14	1	4	11	7	3	12	3	7	11	4	1	14	1			**15**
15	1	15	9	7	5	11	13	3	3	13	11	5	7	9	15	1		**16**
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1	**17**

Using our custom range for modular arithmetic gives us the following:

n \ k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	mod
0	1																	**1**
1	1	1																**2**
2	1	-1	1															**3**
3	1	-1	-1	1														**4**
4	1	-1	1	-1	1													**5**
5	1	-1	-2	-2	-1	1												**6**
6	1	-1	1	-1	1	-1	1											**7**
7	1	-1	-3	3	3	-3	-1	1										**8**
8	1	-1	1	2	-2	2	1	-1	1									**9**
9	1	-1	-4	4	-4	-4	4	-4	-1	1								**10**
10	1	-1	1	-1	1	-1	1	-1	1	-1	1							**11**
11	1	-1	-5	-3	6	6	6	6	-3	-5	-1	1						**12**
12	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1					**13**
13	1	-1	-6	6	1	-1	-6	-6	-1	1	6	-6	-1	1				**14**
14	1	-1	1	4	-4	7	3	-3	3	7	-4	4	1	-1	1			**15**
15	1	-1	-7	7	5	-5	-3	3	3	-3	-5	5	7	-7	-1	1		**16**
16	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	**17**

Primality Testing

For any row n, where n + 1 is prime, the row alternates between ± 1 mod (n + 1).

Proof

For any prime row p, that row consists strictly of zeroes mod p with the exception of the first and last numbers which are always one. Since every number in a row is the sum of the two rows above it (above + above left), then every other number in a row alternates signs (± 1) since they have to add up to 0 when the row after is a prime number row. Thus, the reason we're using this custom modular range is to make it easier to observe.

A corollary of this is if we find all modulars for a row using the next integer and get the alternating signs for 1, then that number is one less than a prime.

The exception to this is when n = 3, since 4 is not a prime.

■

Factoring

Let $n + 1 = p_1{}^{e_1} \times \cdots \times p_m{}^{e_m}$, where m ≥ 1 and $p_i < p_j$ for i < j.

$\binom{n}{k} \equiv (-1)^k$ (mod (n + 1)) for all k < p_1.

Proof

$\forall\, k < p_1, (k, n+1) = 1.$

$\therefore\ \binom{n+1}{k} = \frac{(n+1)\times\cdots\times(n-k+2)}{k!}$ and (k!, n + 1) = 1.

Thus, $\binom{n+1}{k} \equiv 0$ (mod n) for all k < p_1.

Using the same reasoning as the alternate ± 1s above and $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$, we get $\binom{n}{k} \equiv (-1)^k$ (mod (n + 1)) for all k < p_1.

■

Observations

Prime Numbers

To determine if a number is prime (i.e., the modulus), one does not need to check if the previous row alternates between ± 1 (mod (n + 1)) for all k. One need only check up to the $\sqrt{n}$ since the smallest prime p_1 is always less or equal to than that.

Factoring

For factoring, one needs to count the number of alternating ± 1s at the start of the sequence there are and that will be the smallest prime divisor. Dividing n by that number and repeating the process on the smaller number will give us all the original number's factors. One can even only check the prime numbers for k to see if they're equal to ± 1.

E.g.: For n = 8, we start with {1, -1, 1} so we know 3 divides 9.

Twice the Prime

When the modulus is twice a prime and n is one less than twice a prime, another interesting pattern emerges. For n ≥ 21, the end columns are not shown, but the row is symmetric around the middle term(s).

k / n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	mod
3	1	-1	-1	1														4
5	1	-1	-2	-2	-1	1												6
7	1	-1	-3	3	3	-3	-1	1										8
9	1	-1	-4	4	-4	-4	4	-4	-1	1								10
13	1	-1	-6	6	1	-1	-6	-6	-1	1	6	-6	-1	1				14
21	1	-1	-10	10	1	-1	-10	10	-10	10	-10	-10	10	-10	10	-10	-1	22
25	1	-1	-12	12	-12	12	-12	12	1	-1	-12	12	-12	-12	12	-12	-1	25
33	1	-1	-16	16	-16	16	-16	16	-16	16	-16	16	-16	16	-16	16	-16	34

The entire row consists only of ± 1 and $\pm\frac{n-1}{2}$.

Powers of Two

For n one less than a power of two, the entire row consists of all the odd numbers.

Expansions of Expansions

E.g.: For n = 48, the expansion (mod 49) repeats p_1 (7) times for each of the alternating signs' expansion for the power of 6.

Expansion = {1, -1, 1, -1, 1, -1, 1, 6, -6, 6, -6, 6, -6, 6, 15, -15, 15, -15, 15, -15, 15, 20, -20, 20, -20, 20, -20, 20, 15, -15, 15, -15, 15, -15, 15, 6, -6, 6, -6, 6, -6, 6, 1, -1, 1, -1, 1, -1, 1}

Similar expansions exist for n = 5, 7, and 24 for all n ≤ 100.

Conclusion

Pascal's Triangle is really an interesting triangle that continues to generate new patterns.

References

[1] Pascal's Triangle, Wikipedia, The Free Encyclopedia.