

Pascal's Treatise on the Arithmetical Triangle: Mathematical Induction, Combinations, the Binomial Theorem and Fermat's Theorem*

David Pengelley[†]

Introduction

Blaise Pascal (1623–1662) was born in Clermont-Ferrand in central France. Even as a teenager his father introduced him to meetings for mathematical discussion in Paris run by Marin Mersenne, who served as a primary conduit for transmitting mathematical ideas widely at that time, before the existence of any research journals. He quickly became involved in the development of projective geometry, the first in a sequence of highly creative mathematical and scientific episodes in his life, punctuated by periods of religious fervor. Around age twenty-one he spent several years developing a mechanical addition and subtraction machine, in part to help his father in tax computations as a local administrator. It was the first of its kind ever to be marketed. Then for several years he was at the center of efforts to understand vacuum, which led to an understanding of barometric pressure. In fact the scientific unit of pressure is named the *pascal*. He is also known for Pascal's Law on the behavior of fluid pressure.

Around 1654 Pascal conducted his studies on the Arithmetical Triangle (“Pascal's Triangle”) and its relationship to probabilities. His correspondence with Pierre de Fermat (1601–1665) in that year marks the beginning of probability theory. Several years later, Pascal refined his ideas on area problems via the method of indivisibles already being developed by others, and solved various problems of areas, volumes, centers of gravity, and lengths of curves. Later in the seventeenth century, Gottfried Leibniz, one of the two inventors of the infinitesimal calculus which supplanted the method of indivisibles, explicitly credited Pascal's approach as stimulating his own ideas on the so-called characteristic triangle of infinitesimals in his fundamental theorem of calculus. After only two years of work on the calculus of indivisibles, Pascal fell gravely ill, abandoned almost all intellectual work to devote himself to prayer and charitable work, and died three years later at age thirty-nine. In addition to his work in mathematics and physics, Pascal is prominent for his *Provincial Letters* defending Christianity, which gave rise to his posthumously published *Pensées* (Thoughts) on religious philosophy [1, 2]. Pascal was an extremely complex person, and one of the outstanding scientists of the mid-seventeenth century, but we will never know how much more he might have accomplished with more sustained efforts and a longer life.

Pascal's *Traité du Triangle Arithmétique* (in English translation in [5, vol. 30]) makes a systematic study of the numbers in his triangle. They have simultaneous roles in mathematics as figurate numbers¹, combination numbers, and binomial coefficients, and he elaborates on all these. Given

*With thanks to Joel Lucero-Bryan and Jerry Lodder.

[†]Mathematical Sciences; Dept. 3MB, Box 30001; New Mexico State University; Las Cruces, NM 88003; davidp@nmsu.edu.

¹Figurate numbers count the number of equally spaced dots in geometric figures. Especially important to Pascal were the numbers of dots in equilateral triangles, triangular pyramids, and so forth in higher dimensions.

their multifaceted nature, it is no wonder that these ubiquitous numbers had already been in use for over 500 years, in places ranging from China to the Islamic world [3]. Pascal, however, was the first to connect binomial coefficients with combinatorial coefficients in probability. In fact, a major motivation for Pascal was a question from the beginnings of probability theory, about the equitable division of stakes in an interrupted game of chance. The question had been posed to Pascal around 1652 by Antoine Gombaud, the Chevalier de Méré, who wanted to improve his chances at gambling: Suppose two players are playing a fair game, to continue until one player wins a certain number of rounds, but the game is interrupted before either player reaches the winning number. How should the stakes be divided equitably, based on the number of rounds each player has won [3, p. 431, 451ff]? The solution requires the combinatorial properties inherent in the numbers in the Arithmetical Triangle, as Pascal demonstrated in his treatise, since they count the number of ways various occurrences can combine to produce a given result. The Arithmetical Triangle overflows with fascinating patterns and applications, and we will see several of these in reading his treatise. We will study parts of Pascal's explanation of the connections between the numbers in his triangle and combination numbers. The reader is encouraged to read his entire treatise to see its many other aspects and connections.

From Pascal's treatise we will also learn the principle of mathematical induction. Pascal explains this in the specific context of proofs about the numbers in the triangle. The basic idea of mathematical induction had occurred in the mathematics of the Islamic world during the Middle Ages, and in southern Europe in the fourteenth century [3], but Pascal's was perhaps the first text to make a complete explicit statement and justification of this extremely powerful method of proof in modern mathematics. Mathematical induction is an astonishingly clever technique that allows us to prove claims about infinitely many interlinked phenomena all at once, even when proving just a single one of them in isolation would be very difficult! It will be a challenging technique to master, but will provide tremendous power for future mathematical work.

Learning about the connections of the Arithmetical Triangle to the binomial theorem in algebra will also allow an application to proving a famous and extremely important theorem on prime numbers discovered by Pascal's correspondent Pierre de Fermat (1601–1665) of Toulouse, on congruence remainders and prime numbers. This prepares one to understand the RSA cryptosystem, which today is at the heart of securing electronic transactions. We'll see how all these things are interconnected, and along the way we'll also acquire important mathematical tools, like notations for general indexing, summations, and products, and learn how to work with recurrence relations.

Part One: The Arithmetical Triangle and Mathematical Induction

Let us begin reading Blaise Pascal's

TREATISE ON THE ARITHMETICAL TRIANGLE

DEFINITIONS

I call *arithmetical triangle* a figure constructed as follows:

From any point, G, I draw two lines perpendicular to each other, GV, Gζ in each of which I take as many equal and contiguous parts as I please, beginning with G, which I number 1, 2, 3, 4, etc., and these numbers are the *exponents* of the sections of the lines.

Next I connect the points of the first section in each of the two lines by another line, which is the base of the resulting triangle.

In the same way I connect the two points of the second section by another line, making a second triangle of which it is the base.

Z	1	2	3	4	5	6	7	L	8	9	10
1	G 1	σ 1	π 1	λ 1	μ 1	δ 1	ζ 1	1	1	1	
2	φ 1	ψ 2	θ 3	R 4	S 5	N 6	7	8	9		
3	A 1	B 3	C 6	ω 10	ξ 15	21	28	36			
4	D 1	E 4	F 10	ρ 20	Y 35	56	84				
5	H 1	M 5	K 15	35	70	126					
6	P 1	Q 6	21	56	126						
7	V 1	7	28	84							
T	1	8	36								
8	1	9									
9	1										
10	1										

And in this way connecting all the points of section with the same exponent, I construct as many triangles and bases as there are exponents.

Through each of the points of section and parallel to the sides I draw lines whose intersections make little squares which I call *cells*.

Cells between two parallels drawn from left to right are called *cells of the same parallel row*, as, for example, cells *G, σ, π* , etc., or *φ, ψ, θ* , etc.

Those between two lines are drawn from top to bottom are called *cells of the same perpendicular row*, as, for example, cells *G, φ, A, D* , etc., or *σ, ψ, B* , etc.

Those cut diagonally by the same base are called *cells of the same base*, as, for example, *D, B, θ, λ* , or *A, ψ, π* .

Cells of the same base equidistant from its extremities are called *reciprocals*, as, for example, *E, R* and *B, θ* , because the parallel exponent of one is the same as the perpendicular exponent of the other, as is apparent in the above example, where *E* is in the second perpendicular row and in the fourth parallel row and its reciprocal, *R*, is in the second parallel row and in the fourth perpendicular row, reciprocally. It is very easy to demonstrate that cells with exponents reciprocally the same are in the same base and are equidistant from its extremities.

It is also very easy to demonstrate that the perpendicular exponent of any cell when added to its parallel exponent exceeds by unity the exponent of its base.

For example, cell F is in the third perpendicular row and in the fourth parallel row and in the sixth base, and the exponents of rows 3 and 4, added together, exceed by unity the exponent of base 6, a property which follows from the fact that the two sides of the triangle have the same number of parts; but this is understood rather than demonstrated.

Of the same kind is the observation that each base has one more cell than the preceding base, and that each has as many cells as its exponent has units; thus the second base, $\varphi\sigma$, has two cells, the third, $A\psi\pi$, has three, etc.

Now the numbers assigned to each cell are found by the following method:

The number of the first cell, which is at the right angle, is arbitrary; but that number having been assigned, all the rest are determined, and for this reason it is called the *generator* of the triangle. Each of the others is specified by a single rule as follows:

The number of each cell is equal to the sum of the numbers of the perpendicular and parallel cells immediately preceding. Thus cell F , that is, the number of cell F , equals the sum of cell C and cell E , and similarly with the rest.

Whence several consequences are drawn. The most important follow, wherein I consider triangles generated by unity, but what is said of them will hold for all others.

FIRST CONSEQUENCE

In every arithmetical triangle all the cells of the first parallel row and of the first perpendicular row are the same as the generating cell.

For by definition each cell of the triangle is equal to the sum of the immediately preceding perpendicular and parallel cells. But the cells of the first parallel row have no preceding perpendicular cells, and those of the first perpendicular row have no preceding parallel cells; therefore they are all equal to each other and consequently to the generating number.

Thus $\varphi = G + 0$, that is, $\varphi = G$,
 $A = \varphi + 0$, that is, φ ,
 $\sigma = G + 0$, $\pi = \sigma + 0$,

And similarly of the rest.

SECOND CONSEQUENCE

In every arithmetical triangle each cell is equal to the sum of all the cells of the preceding parallel row from its own perpendicular row to the first, inclusive.

Let any cell, ω , be taken. I say that it is equal to $R + \theta + \psi + \varphi$, which are the cells of the next higher parallel row from the perpendicular row of ω to the first perpendicular row.

This is evident if we simply consider a cell as the sum of its component cells.

For ω equals $R + C$

$$\begin{array}{c} \underbrace{\theta + B} \\ \underbrace{\psi + A} \\ \underbrace{\varphi,} \end{array}$$

for A and φ are equal to each other by the preceding consequence.

Therefore $\omega = R + \theta + \psi + \varphi$.

THIRD CONSEQUENCE

In every arithmetical triangle each cell is equal to the sum of all the cells of the preceding perpendicular row from its own parallel row to the first, inclusive.

Let any cell, C , be taken. I say that it is equal to $B + \psi + \sigma$, which are the cells of the preceding perpendicular row from the parallel row of cell C to the first parallel row.

This is also apparent, as above, simply by the interpretation of cells.

For $C = B + \theta$

$$\begin{array}{c} \underbrace{\psi + \pi} \\ \underbrace{\sigma,} \end{array}$$

for $\pi = \sigma$ by the first consequence.

Therefore $C = B + \psi + \sigma$.

FOURTH CONSEQUENCE

In every arithmetical triangle each cell exceeds by unity the sum of all the cells within its parallel and perpendicular rows, exclusive.

Let any cell, ξ , be taken. I say that $\xi - G = R + \theta + \psi + \varphi + \lambda + \pi + \sigma + G$, which are all the numbers between row $\xi\omega CBA$ and row $\xi S\mu$ exclusive.

This is also apparent by interpretation.

For $\xi = \lambda + R + \omega$

$$\begin{array}{c} \underbrace{\pi + \theta + C} \\ \underbrace{\sigma + \psi + B} \\ \underbrace{G + \varphi + A} \\ \underbrace{G.} \end{array}$$

Therefore $\xi = \lambda + R + \pi + \theta + \sigma + \psi + G + \varphi + G$.

N.B. I have written in the enunciation *each cell exceeds by unity* because the generator is unity. If it were some other number, the enunciation should read: *each cell exceeds by the generating number*.

1. Pascal's Triangle and its numbers

- (a) Let us use the notation $T_{i,j}$ to denote what Pascal calls the number assigned to the cell in *parallel row i* (which we today call just *row i*) and *perpendicular row j* (which we today call *column j*). We call the i and j by the name *indices* (plural of *index*) in our notation. Using this notation, explain exactly what Pascal's rule is for determining all the numbers in all the cells. Be sure to give full details. This should include explaining for exactly which values of the indices he defines the numbers.
 - (b) In terms of our notation $T_{i,j}$, explain his terms *exponent*, *base*, *reciprocal*, *parallel row*, *perpendicular row*, and *generator*.
 - (c) Rewrite Pascal's first two "Consequences" entirely in the $T_{i,j}$ notation.
 - (d) Rewrite his proofs of these word for word in our notation also.
 - (e) Do you find his proofs entirely satisfactory? Explain why or why not.
 - (f) Improve on his proofs using our notation. In other words, make them apply for arbitrary prescribed situations, not just the particular examples he lays out.
2. Modern mathematical notation

Read in a modern textbook about index, summation, and product notations, and recurrence relations. Do some exercises.

FIFTH CONSEQUENCE

In every arithmetical triangle each cell is equal to its reciprocal.

For in the second base, $\varphi\sigma$, it is evident that the two reciprocal cells, φ, σ , are equal to each other and to G .

In the third base, A, ψ, π , it is also obvious that the reciprocals, π, A , are equal to each other and to G .

In the fourth base it is obvious that the extremes, D, λ , are again equal to each other and to G .

And those between, B, θ , are obviously equal since $B = A + \psi$ and $\theta = \pi + \psi$. But $\pi + \psi = A + \psi$ by what has just been shown. Therefore, etc.

Similarly it can be shown for all the other bases that reciprocals are equal, because the extremes are always equal to G and the rest can always be considered as the sum of cells in the preceding base which are themselves reciprocals.

3. Symmetry in the triangle: first contact with mathematical induction
- Write the Fifth Consequence using our index notation. Use index notation and the ideas in Pascal's proof to prove the Consequence in full generality, not just for the example he gives. Explain the conceptual ideas behind the general proof.
4. Mathematical induction: gaining more familiarity
- (a) Read in a modern textbook about mathematical induction.

- (b) Prove Pascal's First Consequence by mathematical induction. (Hint: for a proof by mathematical induction, always first state very clearly exactly what the n -th mathematical statement $P(n)$ says. Then state and prove the base step. Then state the inductive step very clearly before you prove it.)
- (c) Write the general form of Pascal's Second Consequence, and give a general proof using summation notation, but following his approach.
- (d) Now prove the Second Consequence by mathematical induction, i.e., a different proof.
- (e) **Optional:** More patterns.
 - i. Write the Fourth Consequence using summation notation. Hint: You can write it using a sum of sums. Try writing Pascal's proof in full generality, using summation notation to help. If you don't complete it his way, explain why it is difficult.
 - ii. Prove the Fourth Consequence by mathematical induction.

SEVENTH CONSEQUENCE

In every arithmetical triangle the sum of the cells of each base is double that of the preceding base.

Let any base, $DB\theta\lambda$, be taken. I say that the sum of its cells is double the sum of the cells of the preceding base, $A\psi\pi$.

For the extremes $\underbrace{D,}_{A,}$ $\underbrace{\lambda,}_{\pi,}$
 are equal to the extremes
 and each of the rest $\underbrace{B,}_{A + \psi,}$ $\underbrace{\theta,}_{\psi + \pi,}$
 is equal to two cells of the other base ...
 Therefore $D + \lambda + B + \theta = 2A + 2\psi + 2\pi$.

The same thing is demonstrated in the same way of all other bases.

EIGHTH CONSEQUENCE

In every arithmetical triangle the sum of the cells of each base is a number of the double progression beginning with unity whose exponent is the same as that of the base.

For the first base is unity.

The second is double the first; therefore it is 2.

The third is double the second; therefore it is 4.

And so on to infinity.

N.B. If the generator were not unity but some other number, such as 3, the same thing would be true. But we should have to take not the numbers of the double progression beginning with unity, that is, 1, 2, 4, 8, 16, etc., but those of the double progression beginning with the generator 3, that is, 3, 6, 12, 24, 48, etc.

5. Sums of bases in the triangle: a geometric progression

- (a) Use our index notation $T_{i,j}$ to explain exactly which are the numbers in the n -th base.
- (b) In full generality, write the Seventh Consequence and its proof, using our $T_{i,j}$ notation.
- (c) Write the statement of the Eighth Consequence in our notation, using modern exponential notation to describe his double progression. Use summation notation as needed, and introduce additional new notation if helpful. Then prove the Eighth Consequence by mathematical induction.

The next consequence is the most important and famous in the whole treatise. Pascal derives a formula for the ratio of consecutive numbers in a base. From this he will obtain an elegant and efficient formula for all the numbers in the triangle.

TWELFTH CONSEQUENCE

In every arithmetical triangle, of two contiguous cells in the same base the upper is to the lower as the number of cells from the upper to the top of the base is to the number of cells from the lower to the bottom of the base, inclusive.

Let any two contiguous cells of the same base, E, C , be taken. I say that

$E : C :: 2 : 3$
 the lower cell because there are two cells from E to the bottom, namely E, H ,
 the upper cell because there are three cells from C to the top, namely C, R, μ .

Although this proposition has an infinity of cases, I shall demonstrate it very briefly by supposing two lemmas:

The first, which is self-evident, that this proportion is found in the second base, for it is perfectly obvious that $\varphi : \sigma :: 1 : 1$;

The second, that if this proportion is found in any base, it will necessarily be found in the following base.

Whence it is apparent that it is necessarily in all the bases. For it is in the second base by the first lemma; therefore by the second lemma it is in the third base, therefore in the fourth, and to infinity.

It is only necessary therefore to demonstrate the second lemma as follows: If this proportion is found in any base, as, for example, in the fourth, $D\lambda$, that is, if $D : B :: 1 : 3$, and $B : \theta :: 2 : 2$, and $\theta : \lambda :: 3 : 1$, etc., I say the same proportion will be found in the following base, $H\mu$, and that, for example, $E : C :: 2 : 3$.

For $D : B :: 1 : 3$, by hypothesis.

Therefore $\underbrace{D + B} : B :: \underbrace{1 + 3} : 3$
 $E : B :: 4 : 3$

Similarly $B : \theta :: 2 : 2$, by hypothesis

Therefore $\underbrace{B + \theta} : B :: \underbrace{2 + 2} : 2$
 $C : B :: 4 : 2$

But $B : E :: 3 : 4$

Therefore, by compounding the ratios, $C : E :: 3 : 2$.

Q.E.D.

The proof is the same for all other bases, since it requires only that the proportion be found in the preceding base, and that each cell be equal to the cell before it together with the cell above it, which is everywhere the case.

6. Pascal's Twelfth Consequence: the key to our modern factorial formula

- (a) Rewrite Pascal's Twelfth Consequence as a generalized modern formula, entirely in our $T_{i,j}$ terminology. Also verify its correctness in a couple of examples taken from his table in the initial definitions section.
- (b) Adapt Pascal's proof by example of his Twelfth Consequence into modern generalized form to prove the formula you obtained above. Use the principle of mathematical induction to create your proof.

Now Pascal is ready to describe a formula for an arbitrary number in the triangle.

PROBLEM

Given the perpendicular and parallel exponents of a cell, to find its number without making use of the arithmetical triangle.

Let it be proposed, for example, to find the number of cell ξ of the fifth perpendicular and of the third parallel row.

All the numbers which precede the perpendicular exponent, 5, having been taken, namely 1, 2, 3, 4, let there be taken the same number of natural numbers, beginning with the parallel exponent, 3, namely 3, 4, 5, 6.

Let the first numbers be multiplied together and let the product be 24. Let the second numbers be multiplied together and let the product be 360, which, divided by the first product, 24, gives as quotient 15, which is the number sought.

For ξ is to the first cell of its base, V , in the ratio compounded of all the ratios of the cells between, that is to say, $\xi : V$

in the ratio compounded of $\xi : \rho, \rho : K, K : Q, Q : V$
 or by the twelfth consequence $3 : 4 \quad 4 : 3 \quad 5 : 2 \quad 6 : 1$

Therefore $\xi : V :: 3 \cdot 4 \cdot 5 \cdot 6 : 4 \cdot 3 \cdot 2 \cdot 1$.

But V is unity; therefore ξ is the quotient of the division of the product of $3 \cdot 4 \cdot 5 \cdot 6$ by the product of $4 \cdot 3 \cdot 2 \cdot 1$.

N.B. If the generator were not unity, we should have had to multiply the quotient by the generator.

7. Pascal's formula for the numbers in the Arithmetical Triangle

- (a) Write down the general formula Pascal claims in solving his "Problem." Your formula should read $T_{i,j} =$ "some formula in terms of i and j ." Also write your formula entirely in terms of factorials.

- (b) Look at the reason Pascal indicates for his formula for a cell, and use it to make a general proof for your formula above for an arbitrary $T_{i,j}$. You may try to make your proof just like Pascal is indicating, or you may prove it by mathematical induction.

VARIOUS USES OF THE ARITHMETICAL TRIANGLE WHOSE GENERATOR IS UNITY

Having given the proportions obtaining between the cells and the rows of arithmetical triangles, I turn in the following treatises to various uses of those triangles whose generator is unity. But I leave out many more than I include; it is extraordinary how fertile in properties this triangle is. Everyone can try his hand. I only call your attention here to the fact that in everything that follows I am speaking exclusively of arithmetical triangles whose generator is unity.

Part Two: Combinations and the Arithmetical Triangle

We continue reading Pascal's *Treatise on the Arithmetical Triangle*:

USE OF THE ARITHMETICAL TRIANGLE FOR COMBINATIONS

The word *combination* has been used in several different senses, so that to avoid ambiguity I am obliged to say how I understand it.

When of many things we may choose a certain number, all the ways of taking as many as we are allowed out of all those offered to our choice are here called the *different combinations*.

For example, if of four things expressed by the four letters, A, B, C, D , we are permitted to take, say any two, all the different ways of taking two out of the four put before us are called *combinations*.

Thus we shall find by experience that there are six different ways of choosing two out of four; for we can take A and B , or A and C , or A and D , or B and C , or B and D , or C and D .

I do not count A and A as one of the ways of taking two; for they are not different things, they are only one thing repeated.

Nor do I count A and B and B and A as two different ways; for in both ways we take only the same two things but in a different order, and I am not concerned with the order; so that I could make myself understood at once by those who are used to considering combinations, simply by saying that I speak only of combinations made without changing the order.

We shall also find by experience that there are four ways of taking three things out of four; for we can take ABC or ABD or ACD or BCD .

Finally we shall find that we can take four out of four in one way only, $ABCD$.

I shall speak therefore in the following terms:

- 1 in 4 can be combined 4 times.
- 2 in 4 can be combined 6 times.
- 3 in 4 can be combined 4 times.
- 4 in 4 can be combined 1 time.

Or:

the number of combinations of 1 in 4 is 4.
the number of combinations of 2 in 4 is 6.
the number of combinations of 3 in 4 is 4.
the number of combinations of 4 in 4 is 1.

But the sum of all the combinations in general that can be made in 4 is 15, because the number of combinations of 1 in 4, of 2 in 4, of 3 in 4, of 4 in 4, when joined together, is 15.

After this explanation I shall give the following consequences in the form of lemmas:

LEMMA 1.

There are no combinations of a number in a smaller number; for example, 4 cannot be combined in 2.

...

PROPOSITION 2

The number of any cell is equal to the number of combinations of a number less by unity than its parallel exponent in a number less by unity than the exponent of its base.

Let any cell be taken, say F in the fourth parallel row and in the sixth base. I say that is equal to the number of combinations of 3 in 5, less by unity than 4 and 6, for it is equal to the cells $A + B + C$. Therefore by the preceding proposition, etc.

1. Combinations according to Pascal

- (a) Explain in your own words what Pascal says about how many combinations there are for choosing two things out of four things.
- (b) Write Pascal's Proposition 2 using our $T_{i,j}$ notation for numbers in the triangle. In other words, fill in a sentence saying " $T_{i,j}$ is the number of combinations of choosing _____ things from _____ things." Pascal's justification for his Proposition 2 is based on his Lemma 4 and Proposition 1, which are not included in this project. However, the reader is encouraged to study and understand them, to wit:
- (c) **Optional:** From Pascal's treatise [5, vol. 30], rewrite his statements and explanations of his Lemma 4 and Proposition 1 in your own words. State and prove Lemma 4 in the general case; that is, show that the number of combinations of k in n is the sum of the combinations of $k - 1$ in $n - 1$ and the combinations of k in $n - 1$. Also explain why Proposition 2 follows from Proposition 1.

2. Combinations and Pascal's recursion formula

- (a) The modern symbol $\binom{n}{r}$ means the number of ways (“combinations”) of choosing r things from amongst n things. Explain how this is related to what we have been learning about the Arithmetical Triangle from reading Pascal. In particular, explain how the numbers $T_{i,j}$ are related to the numbers $\binom{n}{r}$. Do this by writing an equation expressing $T_{i,j}$ in $\binom{n}{r}$ notation, and also writing an equation expressing $\binom{n}{r}$ in $T_{i,j}$ notation. Now use the formula we learned earlier, from Pascal’s solution to his *Problem*,² to write a formula for the combination number $\binom{n}{r}$, and manipulate it to express it entirely in terms of factorials.
- (b) Now read in a modern textbook about the multiplication rule for counting possibilities, about permutations, and about combinations. Explain how a combination is different from a permutation.
- (c) Read in a modern textbook about the algebra of combinations, Pascal’s recursion formula, and how the text presents Pascal’s Triangle. How is it different from Pascal’s presentation?

Part Three: The Binomial Theorem and Fermat’s Theorem

Now we can put together all of what we have learned from Pascal to prove an extremely important result in number theory, called *Fermat’s Little Theorem*, which is at the heart of today’s encryption methods in digital communications. The ingredients will be the binomial theorem, proof by mathematical induction as learned from Pascal, Pascal’s formula for the numbers in his triangle (solved in his *Problem*), and uniqueness of prime factorization.

1. The binomial theorem and combinations

Read in a modern textbook about the binomial theorem. Write an explanation of the proof of the binomial theorem using the idea of counting combinations.

2. Discovering Fermat’s “Little” Theorem: prime numbers and congruence remainders

- (a) Make a table of the remainders of a^n upon division by n for positive integer values of both a and n ranging up to 14. To do this you should learn about congruence arithmetic, and figure out how to do these calculations quickly and easily without a calculator.
- (b) Based on your table, make a conjecture of the form $a^p \equiv ? \pmod{p}$ for p a prime number and a any integer. This is called Fermat’s “Little” Theorem; it is one of the most important phenomena in number theory. Also make some other interesting conjectures from patterns in your table, and try to prove them, perhaps using the binomial theorem.
- (c) Write up the details of proving Fermat’s Theorem by mathematical induction on a , with p held fixed. Use the binomial theorem, our knowledge of Pascal’s “factorial” formula for binomial coefficients, and the Fundamental Theorem of Arithmetic (uniqueness of prime factorization) to analyze divisibility of the binomial coefficients by a prime p .
- (d) **Optional:** Read about what Fermat was trying to do when he discovered his Theorem [4, p. 159ff]. Describe what you find in your own words.

3. **Optional:** The RSA cryptosystem

²Given the perpendicular and parallel exponents of a cell, to find its number without making use of the arithmetical triangle.

Read and study the RSA cryptosystem and its applications to digital security, including how it works, which follows from Fermat's Theorem. Write up the details in your own words, with some example calculations.

Notes to the Instructor

The project's primary aim is for students of introductory discrete mathematics to learn the concept of mathematical induction and its application directly from reading the pioneering work *Treatise on the Arithmetical Triangle* of Blaise Pascal in the 1650s. There are three project parts, covering several standard topics: mathematical induction, combinations, and the binomial theorem and Fermat's Theorem. The project even ends with optional application to the RSA cryptosystem. With the entirety of its applications the project can constitute as much as 20% of a semester course. It works well to have students complete and submit small pieces of the project as one goes along.

In some places the instructor should give students guidance on reading and exercises from their textbook recommended by the project. There are also some places, especially in the third part, where the project expects either substantial independent learning from the student or more substantial instructor guidance.

In his treatise, Pascal, after arranging the figurate numbers in a defining triangular table, notices several patterns in the table, which he would like to claim continue indefinitely. Exhibiting unusual rigor for his day, Pascal offers a condition for the persistence of a pattern, stated verbally in his Twelfth Consequence, a condition known today as mathematical induction. This is perhaps the first complete enunciation and justification in the literature of the logical principle of mathematical induction, all provided in the context of a particular application. Moreover, this Twelfth Consequence immediately results in the modern formula for the combination numbers or binomial coefficients.

When Pascal's original writing becomes a student's initial contact for learning the idea of mathematical induction, a textbook is then merely a supplement. We have found that students come to grips with mathematical induction better by first seeing how Pascal eases into the idea through the proof of several patterns in the triangle, and then formalizes the principle and applies it further. Have students first read and work quite a bit with Pascal's verbal description, and then hold an instructor-moderated class discussion comparing this to the axiomatic formulation of induction students can read in the textbook. We intentionally wait on having students read the textbook approach until they have become comfortable with Pascal's. In fact, many students become and remain more comfortable with Pascal's more verbal way of handling mathematical induction than with their textbooks. Students can become so comfortable with Pascal's treatise that, on a final exam, many will voluntarily choose a question requiring new analysis of a part of Pascal's treatise using mathematical induction that they have never seen, over an analogous exercise from their modern textbook.

References

- [1] *Encyclopædia Britannica*, Chicago, 1986.
- [2] Gillispie, C. C., Holmes, F. L., (editors) *Dictionary of Scientific Biography*, Scribner, New York, 1970.

- [3] Katz, V., *A History of Mathematics: An Introduction*, Second Edition, Addison-Wesley, New York, 1998.
- [4] Laubenbacher, R., Pengelley, D., *Mathematical Expeditions: Chronicles by the Explorers*, Springer Verlag, New York, 1999.
- [5] Pascal, B., "Treatise on the Arithmetical Triangle," in *Great Books of the Western World*, Mortimer Adler (editor), Encyclopædia Britannica, Inc., Chicago, 1991.