Combinatorial Proofs and Algebraic Proofs – II

Shailesh A Shirali

In Part I of this article we considered some binomial identities and also some identities involving the Fibonacci numbers, and proved them using methods which we described as ‘largely’ combinatorial. Now we shift our focus to number theory and to prime numbers in particular, and showcase some proofs having a strong combinatorial element. Throughout this article, $p$ denotes an odd prime.

1. Inverse of an Element Modulo a Prime Number

We start with a well-known and elementary result: *If $p$ is a prime number, and $a \in S_p := \{1, 2, \ldots, p-1\}$, then an element $b \in S_p$ exists such that $ab \equiv 1 \mod p$. This element is, of course, the ‘inverse’ of $a$ modulo $p$.*

Consider the $(p-1)$ numbers $a, 2a, 3a, \ldots, (p-1)a$ reduced modulo $p$. Each of these is necessarily an element of $S_p$, since it cannot be that $ka \equiv 0 \mod p$ for $k, a \in S_p$. On the other hand, no two of the reduced numbers can be equal; for, if $xa \equiv ya \mod p$ where $x, y \in S_p$ and $x \neq y$, then we again get a relation of the kind $ka \equiv 0 \mod p$ for $k, a \in S_p$. This implies that the numbers $a, 2a, 3a, \ldots, (p-1)a$ reduced modulo $p$ are just the numbers $1, 2, 3, \ldots, p-1$ in some permuted order.

Hence it must be that $ka \equiv 1 \mod p$ for some element $k$ in $S_p$, and so the looked-for inverse must exist.

Note that this is an ‘existence proof’; it does not give us the desired inverse though we are assured of its existence. But a ‘constructive proof’ (one which actually

Keywords
Primes, inverse, existence proof, Fermat’s little theorem, Wilson’s theorem, rotation operator, infinitude of the primes, totient function, Paul Erdős.
yields the inverse) can be worked out using Euclid’s gcd algorithm.

With a bit of extra work we get a result called ‘Wilson’s Theorem’:

For any prime $p$, we have: $(p - 1)! \equiv -1 \mod p$.

For example, for $p = 5$ we have: $4! = 24 \equiv -1 \mod 5$, and for $p = 7$ we have: $6! = 720 \equiv -1 \mod 7$.

For the proof we first establish a lemma: For any prime $p$, the only elements of $S_p$ that are their own inverses are $1$ and $p - 1$. This is true because if $x \in S_p$ is self-inverse, then $x^2 \equiv 1 \mod p$, hence $(x - 1)(x + 1) \equiv 0 \mod p$, implying that $x$ is either $1$ or $p - 1$. This in turn follows from a basic property of prime numbers: if a prime number is a divisor of a product of two integers, then it must divide at least one of those integers.

By pairing each number from $2$ till $p - 2$ with its inverse, we readily deduce that the product of these integers is $1 \mod p$. Since $1 \times (p - 1) \equiv -1 \mod p$, Wilson’s theorem follows.

2. Fermat’s ‘Little’ Theorem

With the above result, and a pinch of algebra, the beautiful ‘little’ theorem of Fermat (often called the LFT) is easily proved: For any odd prime $p$ and any element $a \in S_p$ we have the congruence $a^{p-1} \equiv 1 \mod p$.

From the argument presented, it follows that if $a \not\equiv 0 \mod p$, the numbers $a$, $2a$, $3a$, $\ldots$, $(p - 1)a$ reduced modulo $p$ are just the numbers $1$, $2$, $3$, $\ldots$, $p - 1$ in some permuted order. Hence, by multiplication:

$$a^{p-1} \cdot (p - 1)! \equiv (p - 1)! \mod p.$$  

From this the congruence $a^{p-1} \equiv 1 \mod p$ follows, since $(p - 1)!$ is coprime to $p$.

This is, of course, a ‘semi-combinatorial’ proof; the combinatorial component lies in the proof of the existence
A purely bijective proof is possible. But a purely bijective proof is possible. We first recast the theorem in a different but equivalent form: *For any integer a and any prime p we have: \( a^p = a \mod p \). This will follow if we can exhibit a set \( S \) with \( a^p - a \) elements which can be partitioned in some natural way into classes each of which has cardinality \( p \).

Here is how we produce such a set. We consider the collection of all \( p \)-tuples

\[
(x_0, x_1, \ldots, x_{p-2}, x_{p-1}),
\]

where \( x_i \in \{1, 2, \ldots, a\} \) for each \( i \). There are clearly \( a^p \) such tuples. Of these, there are exactly \( a \) tuples in which every entry is the same, namely, the tuples of the form \((k, k, \ldots, k)\) for some \( k \in \{1, 2, \ldots, a\} \). Let \( S \) be the set of tuples left after discarding all such tuples; then each tuple in \( S \) has two or more distinct elements, and there are \( a^p - a \) such tuples.

To construct the desired partition we define the following map \( f \) from \( S \) into itself:

\[
(x_0, x_1, \ldots, x_{p-2}, x_{p-1}) \xrightarrow{f} (x_{p-1}, x_0, x_1, \ldots, x_{p-2}).
\]

Observe that \( f \) performs a cyclic rotation by 1 unit (with ‘wrap-around’); hence \( f^{(p)} \) is the identity map. By starting with any one tuple in \( S \) and iterating the map, we get \( p \) tuples.

Are these tuples all distinct? Yes. If not, then we would have \( x_i = x_{i+k} \) for some \( k \in \{1, 2, \ldots, p - 1\} \) and all \( i \), addition of subscripts being done modulo \( p \). Hence we would have \( x_0 = x_k = x_{2k} = \cdots \). Since \( k \) and \( p \) are coprime, this would eventually lead to all the \( a \)'s having the same value; but we had expressly excluded this possibility at the start.

Thus the action of \( f \) allows us to divide \( S \) into equivalence classes, each with \( p \) elements. It follows that \( p \) is a divisor of \( a^p - a \).
A theorem about binomial coefficients. The cyclic rotation operator $f$ used above may be used to prove another such result, about binomial coefficients.

If $p$ is prime and $1 \leq i \leq p - 1$, then $\binom{p}{i}$ is a multiple of $p$.

For example, $\binom{7}{3} = 35 \equiv 0 \mod 7$. This result is generally proved using number theoretic reasoning, by examining the formula for $\binom{p}{i}$, but we show it directly, using combinatorial reasoning, without needing to invoke the formula.

For, $\binom{p}{i}$ is the number of subsets of cardinality $i$ drawn from a set $S$ of size $p$. Given a subset $T \subset S$ which is neither the empty set nor $S$ itself (that’s why we need the condition $1 \leq i \leq p - 1$), we apply $f$ to it (repeatedly) and this produces an equivalence class of $p$ such subsets (one of which is $T$); each one may be mapped to any of the others by using $f$ (repeatedly).

Distinctness of these $p$ subsets follows the same way as earlier. This implies that $\binom{p}{i}$ is a multiple of $p$.

History of Wilson’s theorem and Fermat’s little theorem. It is of interest to trace the history of these two well-known congruences of number theory. Alhazen (11th century, Iraq) knew of ‘Wilson’s theorem’, and we know of its association with the 18th century mathematician John Wilson as it was mentioned in a textbook written by Edward Waring\(^1\) in 1770. But no record of a proof by Wilson exists, and the theorem appears to have been first proved by Lagrange only in 1771.

In the case of the LFT, Fermat stated it in 1640 and surely knew how to prove it too, but he never offered a proof; trust him to act thus! The first published proof is due to Euler (1736), but Leibnitz appears to have given much the same proof earlier (though in an unpublished manuscript).

\(^1\) Wilson was Waring’s student; Waring is best known for the problem which later became known as ‘Waring’s problem’.

Wilson’s theorem was known to Alhazen in 11th century Iraq. It was first proved by Lagrange in 1771.
3. Central Binomial Coefficient

We now prove the following congruence combinatorially: *For any prime* \( p \),

\[
\binom{2p}{p} \equiv 2 \mod p^2.
\]  

(1)

Two examples: (i) for \( p = 2 \) we have \( \binom{4}{2} = 6 \equiv 2 \mod 2^2 \); (ii) for \( p = 3 \) we have \( \binom{6}{3} = 20 \equiv 2 \mod 3^2 \).

We prove it by once again drawing upon the cyclic rotation operator \( f \). We will not need to use the formula for \( \binom{2p}{p} \), nor any identity it satisfies.

Let \( S \) be a set with \( 2p \) elements, and let it be partitioned in any way as \( A \cup B \), where \( |A| = |B| = p \). We shall use this partition to define an equivalence relation on the class of all \( p \)-element subsets of \( S \) other than \( A \) and \( B \). There are \( \binom{2p}{p} - 2 \) such subsets, and each of them has non-empty intersection with both \( A \) and \( B \). For any such subset \( T \), write \( T_A = T \cap A \) and \( T_B = T \cap B \). Using the operator \( f \) we find \( p \) subsets of \( A \) in the equivalence class of \( T_A \), and \( p \) subsets of \( B \) in the equivalence class of \( T_B \). Each subset in one class can be paired with each subset in the other class, giving \( p^2 \) subsets in the equivalence class of \( T \).

Thus the class of all \( p \)-element subsets of \( S \), other than \( A \) and \( B \), can be partitioned into equivalence classes each of which has cardinality \( p^2 \).

It follows that \( \binom{2p}{p} - 2 \) is a multiple of \( p^2 \).

**Remark.** A stronger result exists: *For any prime* \( p \geq 5 \),

\[
\binom{2p}{p} \equiv 2 \mod p^3.
\]  

(2)

Example: For \( p = 5 \) we have: \( \binom{10}{5} = 252 \equiv 2 \mod 5^3 \).

But it is far from clear whether a purely combinatorial proof exists for this relation. The restriction \( p \geq 5 \) will
likely cause difficulties. Indeed, the stated congruence is actually false for \( p = 2 \) and \( p = 3 \).

For the sake of completeness, we give the (algebraic) proof of this statement. We start with the following identity which itself has a nice combinatorial proof (it is well known so we do not give it here):

\[
\binom{2p}{p} - 2 = \binom{p}{1}^2 + \binom{p}{2}^2 + \binom{p}{3}^2 + \cdots + \binom{p}{p-1}^2.
\]

Since \( \binom{p}{i} = \frac{p}{i} \times \frac{p-1}{2} \times \cdots \times \frac{p-i+1}{i} \), we have, modulo \( p \):

\[
\frac{1}{p} \binom{p}{i} \equiv \frac{(-1) \times (-2) \times \cdots \times (-i-1)}{2 \times 3 \times \cdots \times i}
\]

\[
\equiv (-1)^{i-1} \frac{(i-1)!}{i!} \equiv (-1)^{i-1}i^{-1} \text{ mod } p,
\]

where \( i^{-1} \) is the inverse of \( i \) modulo \( p \). Now as \( i \) takes all values from 1 till \( p - 1 \), its inverse \( i^{-1} \) takes exactly the same values (in some other order). Hence, modulo \( p \):

\[
\frac{1}{p^2} \binom{p}{1}^2 + \frac{1}{p^2} \binom{p}{2}^2 + \cdots + \frac{1}{p^2} \binom{p}{p-1}^2
\]

\[
\equiv 1^2 + 2^2 + \cdots + (p-1)^2 \text{ mod } p
\]

\[
\equiv \frac{(p-1)p(2p-1)}{6} \text{ mod } p.
\]

The right side is 0 mod \( p \) if \( p \geq 5 \), but not if \( p = 2 \) or \( 3 \), because of the ‘6’ in the denominator.

Thus the stated congruence follows, and we also see why the condition \( p \geq 5 \) cannot be dropped.

4. Three Proofs for the Infinitude of the Primes

We now give combinatorial proofs of the ancient theorem asserting that there exist infinitely many primes.
Though we continue to classify these proofs as ‘combinatorial’, the reader will see that the role played by algebra is very much more than earlier.

4.1 Proof using Euler’s Totient Function

The first proof uses the formula for the totient function $\varphi(n)$, defined to be the number of integers in the set $\{1, 2, \ldots, n\}$ which are coprime with $n$. The proof is by the German mathematician Ernst Kummer. It shows the following:

Let $k > 1$. Given any finite collection of $k$ prime numbers $p_1, p_2, \ldots, p_k$, there exists a prime number distinct from all the $p_i$.

For the proof we consider the number $N = p_1 p_2 \cdots p_k$. Then since $p_2 \geq 3$,

$$\varphi(N) = (p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1) > 1.$$

The fact that $\varphi(N) > 1$ means that there exists a number in the interval $[1 \ldots N]$ which is coprime to $N$. Let $m$ be the least such number. This number must be prime. (For, if not, the prime factors of this number would be smaller than it and also be coprime to $N$.) Thus we have demonstrated the existence of a prime number distinct from all the $p_i$.

The proof overlaps in its construction with Euclid’s classic proof from The Elements, but the thread of reasoning is completely different.

4.2 A Proof by Paul Erdős

We suppose, as earlier, that there are just $k$ prime numbers ($k < \infty$). Let the set of primes be $S$; then $|S| = k$, and every positive integer is uniquely representable as a product of powers of the elements of $S$.

Let $N$ be an integer strictly greater than $4^k$. (The $4^k$ seems to appear from nowhere, but if you study the
proof carefully you will see why this upper bound has been chosen.) Each of the \( N \) integers

\[ 1, 2, 3, 4, \ldots, N - 1, N \]

(3)
is uniquely expressible in the form \( a^2b \), where \( a \) is a positive integer \( \leq \sqrt{N} \), and \( b \) is a square-free positive integer \( \leq N \). (‘Square-free’ means that the number is not divisible by any square exceeding 1.)

Since there are just \( k \) primes, the number of square-free numbers is \( 2^k \); so \( b \) can take just \( 2^k \) different values. Also, \( a \) can take at most \( \sqrt{N} \) different values. Therefore, the product \( a^2b \) can take at most \( 2^k\sqrt{N} \) different values.

Since \( 2^k < \sqrt{N} \) by choice, it follows that the number of distinct values of \( a^2b \) is strictly less than \( N \). But this means that there is an integer in the list (3) which cannot be written in the form \( a^2b \), contradicting our earlier statement. This contradiction shows that there must be infinitely many primes.

4.3 A Proof of Divergence

Our next proof is again by Paul Erdős. It proves a much stronger result which was first shown by Leonhard Euler – the divergence of the series

\[ \sum \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots. \]

(4)

This result obviously implies that there are infinitely many primes.

On studying the proof carefully we see that it is organized along exactly the same lines as the above proof, and we thus get a glimpse of the working of Erdős’s mind: how from a simple insight he is able to coax out so much more.

Let \( p_1, p_2, p_3, \ldots \) be the primes in increasing order. To set up the contradiction we shall assume that \( \sum \frac{1}{p} \) converges. Then, by the definition of convergence, there

Each positive integer is uniquely expressible as a product of a perfect square and a square-free number.

On studying this proof, we see that it is organized on the same lines as the earlier one.
exists a least positive integer \( k \) such that

\[
\frac{1}{p_{k+1}} + \frac{1}{p_{k+2}} + \frac{1}{p_{k+3}} + \cdots < \frac{1}{2}.
\] (5)

Let \( S \cup B \) be a disjoint partition of the primes, defined as follows:

\[
S = \{p_1, p_2, p_3, \ldots, p_k\} \quad \text{('S' for 'small primes'),}
\]
\[
B = \{p_{k+1}, p_{k+2}, p_{k+3}, \ldots\} \quad \text{('B' for 'big primes').}
\]

Let \( N \) be a large number whose size we shall fix presently; then we have:

\[
\sum_{p \in B} \frac{N}{p} < \frac{N}{2}.
\] (6)

Let \( N_S \) be the number of positive integers \( \leq N \) all of whose prime factors are in \( S \), and let \( N_B \) be the number of positive integers \( n \leq N \) which are divisible by at least one prime in \( B \). Then \( N_S + N_B = N \).

Now we make estimates for \( N_S \) and \( N_B \). Consider \( N_S \) first. Write each positive integer \( n \in N_S \) in the form \( a^2b \), where \( b \) is square-free. We must have \( a^2 \leq n \), hence \( a \leq \sqrt{n} \leq \sqrt{N} \). So \( a \) can take at most \( \sqrt{N} \) different values. Next, note that the prime factors of any such \( n \) lie in \( S \), so the prime factors of \( b \) too lie in \( S \). As there are \( k \) primes in \( S \), and \( b \) is square-free, \( b \) can take at most \( 2^k \) different values. It follows that

\[
N_S \leq 2^k \sqrt{N}.
\] (7)

Next consider \( N_B \). The number of positive integers \( n \leq N \) divisible by any given prime \( p \) is \( \left\lfloor \frac{N}{p} \right\rfloor \), so the number of positive integers \( n \leq N \) which are divisible by at least one prime in \( B \) is at most \( \sum_{p \in B} \left\lfloor \frac{N}{p} \right\rfloor \). It follows that

\[
N_B \leq \sum_{p \in B} \left\lfloor \frac{N}{p} \right\rfloor \leq \sum_{p \in B} \frac{N}{p} < \frac{N}{2},
\] (8)

from (6).
Now consider (7) and (8). It is clear that if \( 2^k \sqrt{N} < \frac{N}{2} \), then we get \( N_S + N_B < N \), which is absurd.

But the condition \( 2^k \sqrt{N} < \frac{N}{2} \) is easy to obtain; all we need is \( 2^{k+1} < \sqrt{N} \), i.e., \( N > 2^{2k+2} \).

This contradiction shows that the sum \( \sum \frac{1}{p} \) must diverge.

**Suggested Reading**


This book is highly recommended; it has a rich collection of proofs of all kinds – some of the most famous and beautiful proofs in mathematics.

We have taken Erdős’s proof of the divergence \( \sum \frac{1}{p} \) of from this book.

**Address for Correspondence**

Shailesh A Shirali
Sahyadri School
Tiwai Hill, Rajgurunagar
Pune 410 513, India.