feature

Set theory revisited

As easy as PIE

Principle of Inclusion and Exclusion – Part 2

In Part–I of this article we solved some problems using the PIE or the 'Principle of Inclusion and Exclusion'. We saw how the law $|A \cup B| = |A| + |B| - |A \cap B|$ *generalizes, and we used the PIE to find a formula for Euler's totient function* $\varphi(N)$ *which counts the number of integers in the set* $\{1, 2, \ldots, N\}$ *which are coprime to* N*. Now in Part–II we use the PIE to find a generalization of the formula connecting the* gcd *and* lcm *of two numbers. We also discuss a problem about a secretary who loves mixing up job offers sent to applicants, and another problem concerning placement of rooks on a chessboard.*

B Sury

I. The Möbius function

You would have noticed in the first part of this article (PIE-I) that the same kind of sum has been coming up repeatedly, in which terms are alternately positive and negative. A convenient way of writing such sums is through the use of a function called the *Möbius function*, written $\mu(n)$ and read aloud as 'mew of n'. It is defined as follows: $\mu(1) = 1$, and:

- If n is the product of unequal prime numbers, then $\mu(n) = 1$ if the number of primes is even, and $\mu(n) = -1$ if the number of primes is odd. So $\mu(p) = -1$ for any prime p; $\mu(pq) = 1$ for any two unequal primes p, q; and so on. Here is a more compact way of writing this: if n is the product of r distinct primes, then $\mu(n) = (-1)^r$. Examples: $\mu(5) = -1$, $\mu(10) = 1$, $\mu(30) = -1$.
- If n is divisible by the square of any prime number, then $\mu(n) = 0$. Examples: $\mu(4) = 0$, $\mu(12) = 0$.

Using this function, an expression such as

$$N - \left(\frac{N}{p} + \frac{N}{q} + \frac{N}{r} + \cdots\right) + \left(\frac{N}{pq} + \frac{N}{qr} + \frac{N}{pr} + \cdots\right) - \cdots$$

can be written compactly as

$$\sum_{d|N} \mu(d)\frac{N}{d}.$$

Hence, we have:

$$\varphi(N) = \sum_{d|N} \mu(d)\frac{N}{d}. \qquad (1)$$

Incidentally, the name Möbius is popularly known in another context — the so-called *Möbius strip*, which will be a topic for another day.

The Möbius function has numerous nice properties which make it a very useful function in number theory and combinatorics.

II. Relation between GCD and LCM of several numbers

To demonstrate how unexpectedly useful the PIE formula can be, we describe a nice application of the formula. Here is the context. We all know the pleasing formula that relates gcd ('greatest common divisor', also known as 'highest common factor') and lcm ('lowest common multiple') of any two positive integers a and b:

$$\gcd(a,b) \times \operatorname{lcm}(a,b) = ab. \qquad (2)$$

This formula relates the gcd and lcm of two integers a, b. Here is the corresponding formula for the case of three integers. If a, b, c be any three positive integers, then:

$$\operatorname{lcm}(a,b,c) = \frac{abc \times \gcd(a,b,c)}{\gcd(a,b) \times \gcd(b,c) \times \gcd(a,c)}. \qquad (3)$$

For the general case we need the following result which is actually the PIE in another incarnation (though it may not look like it):

Theorem (PIE′). *If $n_1, n_2, \cdots, n_r$ is a finite sequence of positive integers, then*

$$\max(n_1, \cdots, n_r) = \sum_i n_i - \sum_{i<j} \min\left(n_i, n_j\right) + \sum_{i<j<k} \min\left(n_i, n_j, n_k\right) - \cdots + (-1)^{r-1} \min\left(n_1, \cdots, n_r\right). \qquad (4)$$

Here, 'max' and 'min' stand for maximum and minimum respectively. The symbol $\sum_{i<j}$ means: 'the sum over all pairs of indices i, j where $i < j$. Similarly for the symbol $\sum_{i<j<k}$ and others like it. The formula may look mysterious, so it will help if we examine it more closely.

- Take the case of two positive integers a, b. Then the claim is that

  $$\max(a,b) = a + b - \min(a,b).$$

  This is clearly true.

- Take the case of three positive integers a, b, c. Then the claim is that

  $$\max(a,b,c) = a + b + c - \min(a,b) - \min(a,c) - \min(b,c) + \min(a,b,c).$$

  To see why this is true, suppose (there is no loss of generality in assuming this) that $a \le b \le c$. The above claim then reduces to the following:

  $$c = a + b + c - (a + a + b) + a,$$

  which is clearly true.

- Take the case of four positive integers a, b, c, d where (without any loss of generality, as earlier) $a \le b \le c \le d$. Then the claim reduces to the following claim:

  $$d = a + b + c + d - (a + a + a + b + b + c) + (a + a + a + b) - a,$$

  which is clearly true. The general case may be similarly reasoned out and is left as an exercise.

To convince ourselves that the above can indeed be useful in unexpected ways, let us look at a set

$a_1, a_2, \cdots, a_r$ of positive integers. Then we will show the following:

$$\text{lcm}\ (a_1, \cdots, a_r) = \frac{(\prod_i a_i)\left(\prod_{i<j<k} \gcd(a_i, a_j, a_k)\right)\cdots}{\left(\prod_{i<j} \gcd(a_i, a_j)\right)\left(\prod_{i<j<k<l} \gcd(a_i, a_j, a_k, a_l)\right)\cdots}. \quad (5)$$

This will be deduced from statement (4) about maxima and minima. To see the connection, consider the prime numbers dividing the a_i's. Then, clearly: *the exponent of a prime p dividing the* gcd *of a collection of numbers is equal to the minimum of the exponents of p dividing the numbers, and the exponent of a prime p dividing the* lcm *of a collection of numbers is equal to the maximum of the exponents of p dividing the numbers*.

Thus, if $p^{n_1}, \cdots, p^{n_r}$ are the powers of a fixed prime p dividing the numbers $a_1, \cdots, a_r$, then the gcd of the a_i's is exactly divisible by $p^{\min(n_1, \cdots, n_r)}$, and the lcm of the a_i's is exactly divisible by $p^{\max(n_1, \cdots, n_r)}$. Let us use the short form $\text{Ord}_p(N)$ for the largest integer e such that p^e divides N. Then if we raise p to each of the terms of the equality

$$\begin{aligned}\max(n_1, \cdots, n_r) &= \sum_i n_i - \sum_{i<j} \min(n_i, n_j) \\ &\quad + \sum_{i<j<k} \min(n_i, n_j, n_k) \\ &\quad - \cdots + (-1)^{r-1} \min(n_1, \cdots, n_r),\end{aligned}$$

(to see why, you need to use repeatedly the fact that $p^{a+b} = p^a \times p^b$ and $p^{a-b} = p^a \div p^b$), we obtain

$$\text{Ord}_p(\text{lcm}\ (a_1, \cdots, a_r)) = \text{Ord}_p\left(\frac{(\prod_i a_i)\left(\prod_{i<j<k} \gcd(a_i, a_j, a_k)\right)\cdots}{\left(\prod_{i<j} \gcd(a_i, a_j)\right)\left(\prod_{i<j<k<l} \gcd(a_i, a_j, a_k, a_l)\right)\cdots}\right).$$

We have obtained expression (5) for the lcm of the a_i's.

III. The secret(ary) adversary

Here is another well-known problem concerning a particularly careless (or perhaps mischievous) secretary. The scenario is that a rich person writes a letter each to Alka, Beena, Chanda and Deepa offering different financial scholarships to each, but the secretary puts each letter in a wrongly addressed envelope. The financier is naturally cross and asks the secretary to correct his mistake. However, the secretary *again* puts each letter in a wrong envelope! How many ways can he make such a mistake? A bit of counting (which we leave as an exercise for you) shows that the number is 9.

What is the best way to figure out this number if there are n people and n envelopes (and each letter must go to the wrong person)? Once again, the PIE comes to the rescue. The total number of ways of distributing n letters among n persons (one letter to each person) is of course $n!$. Let N_1 be the number of ways of distributing the letters so that at least one person (it could be any of the n persons) gets his or her correct letter; let N_2 be the number of ways of distributing the letters so that at least two persons get their correct letters; let N_3 be the number of ways of distributing the letters so that at least three persons get their correct letters; and similarly for N_4, N_5, ... (Note that by this notation we could say that $N_0 = n!$.) Then the PIE tells us that the number of ways of distributing the letters so that no one gets their letter is

$$N_0 - N_1 + N_2 - N_3 + N_4 - + \cdots + (-1)^n N_n.$$

Computing $N_1, N_2, \ldots$is easy. Suppose that at least r people receive their correct letters. Let us look at a *fixed* set of r people. For the remaining $n - r$ persons no restriction has been placed, so the number of ways of distributing the letters is $(n - r)!$. This is so for each fixed set of r persons, and there are $\binom{n}{r}$ such sets; hence $N_r = \binom{n}{r} \times (n - r)!$. It follows that the number of possibilities in which when *no one* receives their correct letter is

$$n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \cdots + (-1)^n \binom{n}{n} 0! = n! \sum_{r=0}^{n} \frac{(-1)^r}{r!}$$

This is called the *derangement number* and it is denoted by D_n; so $D_n = n! \sum_{r=0}^{n} (-1)^r / r!$.

Here are the values of the first few such numbers:

n	1	2	3	4	5	6	$\cdots$
D_n	0	1	2	9	44	265	$\cdots$

IV. Chess-'bored' Rooks?

The next example we mention is to do with a chess board. We know that there are 8! ways of placing 8 rooks on a chess board such that no two attack each other. This is because on the top row, one can place a rook on any one of the 8 places; the second rook can be placed on the second row on any one of the 7 columns other than the column containing the first one. Then, the third rook can be placed on the third row on any of the 6 columns not containing either of the two rooks, etc.

Now, what if we fix a subset T of the n^2 squares in a $n \times n$ chess board where the rooks do not like to sit (let us say these seats are 'boring')? That is, we place n mutually non-attacking rooks on the chess board such that none of the rooks are on the T-squares. How many ways can this be done? (Of course, this will depend on T.)

Let us look at an example where the chessboard has size 4×4. Denote the 16 squares by ordered pairs (i, j) where $1 \leq i, j \leq 4$. Suppose $T = \{(1,1), (2,2), (3,3), (3,4), (4,4)\}$. Counting carefully gives us 6 possibilities of placing 4 non-attacking rooks with no rook on any of the 5 T-squares. Indeed, the possible arrangements are these:

$$(1,2), (2,4), (3,1), (4,3)$$

$$(1,3), (2,4), (3,1), (4,2)$$

$$(1,4), (2,3), (3,1), (4,2)$$

$$(1,4), (2,1), (3,2), (4,3)$$

$$(1,3), (2,4), (3,2), (4,1)$$

$$(1,4), (2,3), (3,2), (4,1)$$

In general, let us look at an $n \times n$ chessboard and a fixed subset T of squares. Let T_r denote the number of ways of placing r non-attacking rooks on T. Then, by the PIE, the number N of ways of placing n mutually non-attacking rooks such that none of them lies on a T-square is given as

$$N = n! - (n-1)!\, T_1 + (n-2)!\, T_2 - \cdots + (-1)^n T_n.$$

The proof of this is left to the reader as an exercise.

V. Deep waters

Finally, we draw attention to some connections of the Möbius function with prime numbers at a basic but deep level. One of the great discoveries of the great Carl Friedrich Gauss is a prediction known as the *prime number theorem*. At the ripe old age of 15 (in 1792), Gauss conjectured that the number $\pi(x)$ of prime numbers not exceeding a given number x is 'asymptotic' to $x/\log(x)$. By 'asymptotic', one means here that the ratio $\pi(x) \div x/\ln x$ gets arbitrarily close to 1 as x gets arbitrarily large.

More precisely, he predicted that $\pi(x)$ is asymptotic to the following integral:

$$\int_1^x \frac{dt}{\ln t}.$$

This most amazing statement became a theorem only a century later when it was proved simultaneously and independently by Hadamard and by de la Valle Poussin. The remarkable fact is that this theorem is equivalent to the simply-stated assertion that

$$\frac{1}{x} \sum_{n \leq x} \mu(n) \to 0 \quad \text{as } x \to \infty.$$

Of course, this is only neat as a statement. Proving it is just as difficult as proving the prime number theorem!

At this point of time, is there any single problem in mathematics which could be held as a show-piece in that it embodies the most difficult of open problems in mathematics? If such a thing is at all admissible, the winner would certainly be the so-called *Riemann hypothesis* stated by Gauss's student, the great Bernhard Riemann (1800–1840). We do not state it here as it is not easy to do so in simple terms. However, the equivalent statement in terms of the Möbius function is the following:

Conjecture. For any constant $t > 1/2$, there exists a constant $C > 0$ such that

$$\sum_{n \leq x} \mu(n) \leq C x^t \quad \text{for all } x > 0.$$

But I would not advise readers to try proving this!

Exercises

(1) Let n be any positive integer exceeding 1. Show that the sum $\mu(d)$ over all the divisors d of n equals 0.

Example: Take $n = 6$. Its divisors are $1, 2, 3, 6$, and their μ-values are $1, -1, -1, 1$, whose sum is 0.

(2) Let n be any positive integer exceeding 1. Show that the sum $|\mu(d)|$ over all the divisors d of n equals 2^k where k is the number of distinct prime divisors of n.

Example: Take $n = 6$. Its divisors are $1, 2, 3, 6$, and their $|\mu|$-values are $1, 1, 1, 1$, whose sum is 4. The number of distinct prime divisors of 6 is 2, and $2^2 = 4$.

(3) In proving that

$$\begin{aligned}\max(a, b, c) = a + b + c - \min(a, b) \\ - \min(a, c) - \min(b, c) \\ + \min(a, b, c),\end{aligned}$$

we said: "there is no loss of generality in assuming that $a \leq b \leq c$". Why is there 'no loss of generality' in assuming that $a \leq b \leq c$?

(4) Try proving the general relation (4). (It is not as difficult as it looks!)

Further reading

i. V Balakrishnan, *Combinatorics: Including Concepts Of Graph Theory* (Schaum Series)

ii. I Niven, H S Zuckerman & H L Montgomery, *An Introduction to the Theory of Numbers* (John Wiley, Fifth Edition)

B. SURY has been at the Tata Institute of Fundamental Research Bombay from 1981 until 1999. He moved to the Indian Statistical Institute in Bangalore in 1999. He has always been interested in expository writing and in interacting with mathematically talented students. He is the regional co-ordinator for the Math Olympiad in Karnataka and a member of the editorial committees of the newsletter of the Ramanujan Mathematical Society, and of the magazine *Resonance*. His research interests are in algebra and number theory. Mathematical limericks are an abiding interest. He may be contacted at sury@isibang.ac.in. His professional web page is www.isibang.ac.in/~sury.