Cyclotomy and Cyclotomic Polynomials

The Story of how Gauss Narrowly Missed Becoming a Philologist

B Sury

B Sury is with the Indian Statistical Institute in Bangalore .

Cyclotomy – literally *circle-cutting* – was a puzzle begun more than 2000 years ago by the Greek geometers. In this pastime, they used two implements – a ruler to draw straight lines and a compass to draw circles. The problem of cyclotomy was to divide the circumference of a circle into n equal parts using only these two implements.

As these n points on the circle are also the corners of a regular n-gon, the problem of cyclotomy is equivalent to the problem of constructing the regular n-gon using only a ruler and a compass. Euclid's school constructed the equilateral triangle, the square, the regular pentagon and the regular hexagon. For more than 2000 years mathematicians had been unanimous in their view that for no prime p bigger than 5 can the p-gon be constructed by ruler and compasses. The teenager Carl Friedrich Gauss proved a month before he was 19 that the regular 17-gon is constructible. He did not stop there but went ahead to completely characterise all those n for which the regular n-gon is constructible! This achievement of Gauss is one of the most surprising discoveries in mathematics. This feat was responsible for Gauss dedicating his life to the study of mathematics instead of philology [1] in which too he was equally proficient.

In his mathematical diary [2] maintained from 1796 to 1814, he made his first entry on the 30th of March and announced the construction of the regular 17-gon. It is said that he was so proud of this discovery that he requested that the regular 17-gon be engraved on his tombstone! This wish was, however, not carried out.

An amusing story alludes to Kästner, one of his teachers at the university of Gottingen, and an amateur poet. When Gauss told him of his discovery, Kästner was skeptical and

By 18, Gauss was already an expert in Greek, Latin, French and German. At the age of 62, he took up the study of Russian and read Pushkin in the original.

[2] The diary was found only in 1898!

did not take him seriously. Gauss insisted that he could prove his result by reducing to smaller degree equations and, being fond of calculations, also showed the co-ordinates of the 17 points computed to several decimal places. Kästner is said to have claimed that he already knew such approximations long before. In retaliation, some time later, Gauss described Kästner as the best poet among mathematicians and the best mathematician among poets!

Gauss's proof was not only instrumental in making up his mind to take up mathematics as a career but it is also the first instance when a mathematical problem from one domain was rephrased in another domain and solved successfully. In this instance, the geometrical problem of cyclotomy was reset in algebraic terms and solved. So, let us see more in detail what cyclotomy is all about.

The unit circle is given to us[3] and we would like to divide it into n equal parts using only the ruler and compass. It should be noted that the ruler can be used only to draw a line joining two given points and not for measuring lengths. For this reason, one sometimes uses the word *straightedge* instead of a ruler.

[3] It is understood that the centre is also given.

If we view the plane as the complex plane, the unit circle has the equation $z = e^{i\theta}$. Since arc length is proportional to the angle subtended, the n complex numbers $e^{\frac{2\pi ik}{n}}$ $1 \leq k \leq n$ cut the circumference into n equal parts.

As we might fix a diameter to be the x-axis, the problem may also be variously posed as the problem of using only the ruler and the compass to:

(i) find the roots of $z^n = 1$, or

(ii) construct the angle $\frac{2\pi}{n}$.

Since, by coordinate geometry, a line and a circle have equations, respectively, of the form $ax+by = c$ and $(x-s)^2+(y-t)^2 = r^2$, their points of intersection (if any) are the common roots. Eliminating one of x, y leads to a quadratic equation for the other. Therefore, the use of ruler and compasses amounts in algebraic terms to solving a chain of quadratic

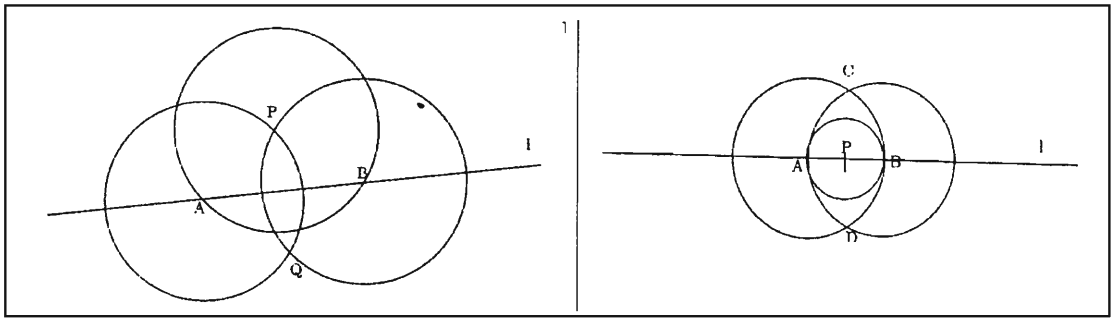


Figure 1 (left).
Figure 2 (right).

equations.

Before we go further, we need to clarify one point. On the one hand, we seem to be talking of constructing lengths and, on the other hand, we seem to want to mark off certain specific points on the plane corresponding to the vertices of the n-gon. To remove any confusion due to this, let us explain how these are equivalent. The reader is encouraged to consult Chapter 13 of the undergraduate text [1] for additional material.

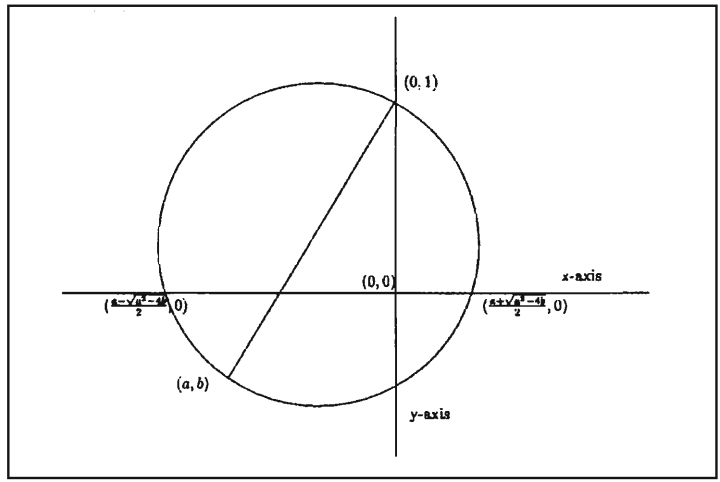
Some Easy Constructions Possible with a Ruler and a Compass

1. Drop a perpendicular on a given line l from a point P outside it (*Figure* 1). Draw a circle centred at P cutting l at A and B. Draw circles centred at A and B having radii AP and BP, respectively. The latter circles intersect at P and Q and PQ is perpendicular to l.

2. Draw a perpendicular to a given line l through a point P on it (*Figure* 2). Draw any circle centred at P intersecting l at A and B. Then, the circles centred at A and B with the common radius AB intersect at two points C and D. Then, CD passes through P and is perpendicular to l.

3. Draw a line parallel to a given line through a point outside.This follows by doing the above two constructions in succession.

Figure 3.



4. Bisect a given segment AB.This is obvious from *Figure* 2. The circles centred at A and B having the common radius AB intersect at two points. The line joining these two points is the perpendicular bisector.

Marking the point (a, b) *on the plane is, by these observations, equivalent to the construction of the lengths* $\mid a \mid$ *and* $\mid b \mid$. *Further, one can view the same as the construction of the complex number* $a + ib$.

5. If a and b are constructed real numbers, then the roots of the polynomial $x^2 - ax + b = 0$ are constructible as well.

Actually, in the discussion of cyclotomy, we will need to deal only with the case when the roots of such a quadratic equation are real. In this case, (*Figure* 3) draw the circle with the segment joining the points $(0, 1)$ and (a, b) as its diameter. The points of intersection of this circle with the x-axis are the roots $\frac{a \pm \sqrt{a^2 - 4b}}{2}$ of the given quadratic equation $x^2 - ax + b = 0$.

Even when the roots of $x^2 - ax + b = 0$ are not real, they can be constructed easily. In this case, we need to construct the points $(\frac{a}{2}, \frac{\sqrt{4b - a^2}}{2})$ and $(\frac{a}{2}, -\frac{\sqrt{4b - a^2}}{2})$. But, as we observed earlier, we can drop perpendiculars and it suffices to construct the absolute value of these roots which is $\sqrt{b}$. This

is accomplished by drawing the circle with the segment joining $(0,1)$ and $(0,-b)$ as diameter and noting that it meets the x-axis at the points $(\sqrt{b},0)$ and $(-\sqrt{b},0)$.

With this renewed knowledge, let us return to cyclotomy.

For $n=2$, one needs to draw a diameter and this is evidently achieved by the ruler.

For $n=3$, the equation $z^3-1=0$ reduces to the equations $z-1=0$ or $z^2+z+1=0$. The roots of the latter are $\frac{-1\pm i\sqrt{3}}{2}$. So, we have to bisect the segment $[-1,0]$ and the points of intersection of this bisector with the unit circle (*Figure* 4) are the points we want to mark off on the circle.

For $n=4$, again only bisection (of the x-axis) is involved. This already demonstrates clearly that *if the regular n-gon can be constructed, then so can the $2^r n$-gon for any r. In particular, the 2^r-gons are constructible.*

To construct the regular pentagon, one has to construct the roots of $z^5-1=0$. These are the 5-th roots of unity $\zeta^k; i \leq k \leq 5$ where $\zeta = e^{\frac{2\pi i}{5}}$ Now the sum of the roots of z^5-1 is $0=\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5$. On using this and the fact that $\zeta^5=1$, we get $(\zeta^2+\zeta^3)(\zeta+\zeta^4)=\zeta+\zeta^2+\zeta^3+\zeta^4=-1$. On the other hand, we also have their sum $(\zeta^2+\zeta^3)+(\zeta+\zeta^4)=-1$.

This means that $\zeta^2+\zeta^3$ and $\zeta+\zeta^4$ are the two roots of the quadratic polynomial $T^2+T-1=0$. Thus, $\zeta+\zeta^4$ (being

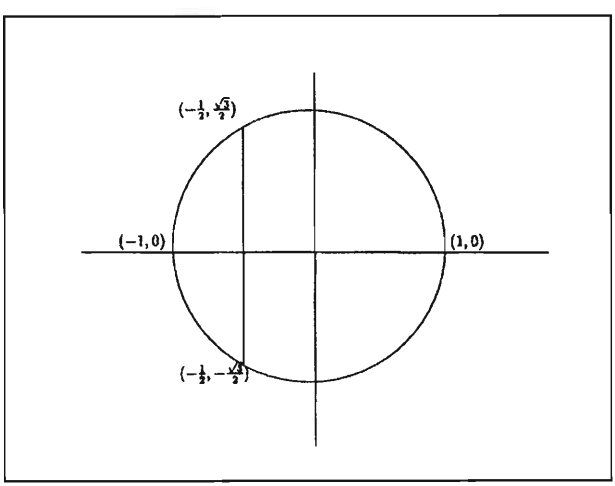


Figure 4.

positive) equals $\frac{-1+\sqrt{5}}{2}$. Multiplying this equality by ζ and using $\zeta^5 = 1$, one gets a quadratic equation for ζ ! This is the algebraic reasoning behind the construction. Following it, we can geometrically make the construction also with the aid of the dictionary between algebra and geometry that we have established above.

Let us now turn to the construction of the 17-gon. There are many ways of doing it – [2], [3] contain explicit geometric algorithms; Gauss's own appears in [4, *Art.*365] – and all of them succeed essentially because $17 - 1$ is a power of 2! This is the reason why the degree 16 equation $\frac{x^{17}-1}{x-1} = x^{16} + x^{15} + \quad + x + 1 = 0$ reduces to a chain of quadratic equations.

It would be ideal to use the language of Galois theory (see *Resonance*, Vol. 4, No. 10,1999) to discuss the constructibility or nonconstructibility of a regular polygon. However, we will keep the discussion elementary and will only make a few remarks for the reader familiar with basic Galois theory so that she/he can grasp the conceptual reason behind various explicit expressions, the appearance of which will seem magical without the added understanding[4] provided by Galois theory.

[4] Perhaps, an outstanding feature of mathematics is that knowing the conceptual reason behind a phenomenon is often much more important than a proof of the phenomenon itself.

In the light of our dictionary, we describe a construction as follows:

Denote by ζ, the 17-th root of unity $e^{\frac{2\pi i}{17}}$ Then, $\zeta^{17} = 1$ gives $\zeta^{16}+\zeta^{15}+\cdot\ \cdot+\zeta+1 = 0$. Let us write $\alpha_1, \alpha_2, \alpha_3$ for the three real numbers $\zeta^3+\zeta^{-3}+\zeta^5+\zeta^{-5}+\zeta^6+\zeta^{-6}+\zeta^7+\zeta^{-7}$, $\zeta^3+\zeta^{-3}+\zeta^5+\zeta^{-5}$ and, $\zeta+\zeta^{-1}$, respectively. Look at the sequence of four quadratic equations:

$$T^2 - \alpha_3 T + 1 = 0,$$

$$T^2 - \frac{\alpha_2^3 - 6\alpha_2 - 2\alpha_1 + 1}{2} T + \alpha_2 = 0,$$

$$T^2 - \alpha_1 T - 1 = 0,$$

$$T^2 - T - 4 = 0.$$

A routine calculation shows that $\zeta, \alpha_3, \alpha_2, \alpha_1$ are roots of the four equations in that order. The roots of the last equation

are evidently constructible as it has integer coefficients. This means that one can construct ζ by recursively constructing the roots of these equations using a ruler and a compass. The reader may geometrically make the construction based on the dictionary above or consult one of the references quoted.

The reader familiar with basic Galois theory would recall that the four successive quadratic extension fields generated by the polynomials give a tower of corresponding Galois groups. The Galois group of the cyclotomic field [5] $Q(\zeta)$ over Q is a cyclic group of order 16 generated by the automorphism $\sigma : \zeta \mapsto \zeta^3$ (in other words, 3 is a primitive root modulo 17). The automorphisms σ^2, σ^4 and σ^8 fix α_1, α_2 and α_3, respectively.

[5] This is the field consisting of all rational polynomial expressions in ζ.

Now, the question remains as to what made this work and which other n-gons are constructible. Look at the regular n-gon for some n. To construct it, one needs to mark off the complex number $\zeta = e^{\frac{2\pi i}{n}}$ The question is whether ζ can be expressed in terms of a nested chain of square roots. For example, for the 17-gon, one gets

$$\text{Cos}\,(\frac{2\pi}{17}) = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{(34 - 2\sqrt{17})}$$
$$+ \frac{1}{8}\sqrt{(17 + 3\sqrt{17} - \sqrt{(34 - 2\sqrt{17})} - 2\sqrt{(34 + 2\sqrt{17})})}.$$

Of course, ζ is a root of the polynomial $z^n - 1 = 0$. But, it is a root of an equation of smaller degree. What is the smallest degree equation of which ζ is a root? Not only is there such a monic [6] polynomial but by the division algorithm, this polynomial is unique and divides any other polynomial of which ζ is a root. This polynomial is called a cyclotomic polynomial. The degree of this polynomial is of paramount importance because if it is a power of two, we know from our earlier discussion that ζ can be constructed. The cyclotomic polynomials are useful in many ways and have several interesting properties some of which will be discussed in the last three sections.

[6] Monic means that the top coefficient is 1.

For a prime number p such that $p-1$ is a power of 2, our dis-

cussion shows that the regular p-gon is constructible. Such a prime p is necessarily of the form $2^{2^n}+1$ since $2^{\text{odd}}+1$ is always a multiple of 3. Fermat thought that the numbers $2^{2^n}+1$ are primes for all n. However, the only primes of this form found until now are $3, 5, 17, 257$ and 65537(!) The number $2^{2^5}+1$ was shown by Euler to have 641 as a proper factor. For coprime numbers m and n, if the m-gon and the n-gon are constructible, then so is the mn-gon. The reason is, if we write $ma + nb = 1$ for integers a, b, then $\text{Cos}(\frac{2\pi}{mn}) = \text{Cos}(\frac{2\pi b}{m} + \frac{2\pi a}{n})$ which is constructible when $\text{Cos}(\frac{2\pi b}{m})$ and $\text{Cos}(\frac{2\pi a}{n})$ are. Thus, Gauss's analysis shows that *if n is a product of Fermat primes and a power of 2, the regular n-gon can be constructed by a ruler and a compass.* The converse is also true i.e. if the regular n-gon is constructible, then n is of this special form. Gauss did not give a proof of this although he asserted it to be true; see [5]. The construction of the regular 257-gon was published in four parts in *Crelle's Journal.* Details of the 65537-gon fill a whole trunk kept at the University of Göttingen !

We must see Gauss's feat in the light of the fact that complex analysis was in its infancy at that time. In fact, Gauss was the first one to give a rigorous proof (in his doctoral thesis) of the so-called fundamental theorem of algebra which asserts that every nonconstant complex polynomial has a root.

Abel's Theorem for the Lemniscate

Abel earned fame by proving that the general equation of degree at least five is not solvable by a 'formula' involving only square roots, cube roots and higher roots. One of his lesser-known achievements involves a problem analogous to cyclotomy viz., the division of the lemniscate. The name lemniscate literally means a ribbon and comes from its shape (*Figure* 5); this curve – also called the elastic curve – was discovered by Bernoulli.

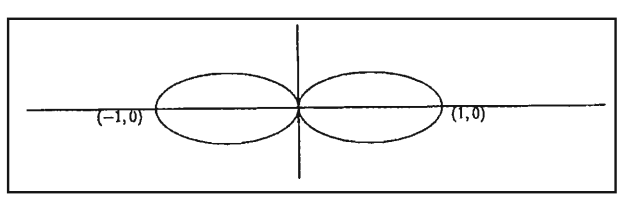


Figure 5.

It has an equation of the form $(x^2+y^2)^2 = x^2 - y^2$. The total arc length of the lemniscate is given by the integral $4\int_0^1 \frac{dt}{\sqrt{(1-t^4)}}$. Thus, the number ω which is half of this integral is the analogue of π for the unit circle. It is approximately 2.6205... Gauss had already asserted as entry 62 in his diary (see [6]) that the lemniscate is divisible into five equal parts by a ruler and a compass. The previous two entries show clearly that Gauss knew that the lemniscatic *trigonometric* functions are doubly-periodic functions; they are called elliptic functions nowadays. He hinted at a vast theory of his behind these functions but this work never appeared. It was Abel who published a comprehensive treatise on elliptic functions and in it he also looked at the problem of dividing the lemniscate into n equal parts for any n (see [7] for a more modern discussion). He discovered the remarkable fact that the answer is the same as for the circle! In other words, the lemniscate can be divided into n equal parts with the aid of a ruler and a compass if, and only if, n is a product of a power of 2 and distinct Fermat primes. The reason can again be understood using Galois theory. In the case of the circle, the Galois group of the cyclotomic extension is the multiplicative group of integers modulo n which are coprime to n. This latter group is a group of order a power of 2 exactly when n is as above. For the lemniscate, it turns out that one needs to know when the unit group of $Z[i]/nZ[i]$ is a group of order a power of 2 where the set $Z[i]$ of Gaussian integers consists of the complex numbers $a+bi$ with integral a, b.

Cyclotomic Polynomials

We introduced for any positive integer n, the cyclotomic polynomial $\Phi_n(X)$ as the unique monic integer polynomial of least degree having $\zeta = e^{\frac{2\pi i}{n}}$ as a root. What does $\Phi_n(X)$ look like ? Obviously $\Phi_1(X) = X - 1$ and $\Phi_2(X) = X + 1$. Moreover, for a prime number p, $\Phi_p(X) = X^{p-1} + X^{p-2} +$ $+ X + 1$. For any n, the n-th roots of unity are the complex numbers $e^{\frac{2\pi ir}{n}}; 1 \leq r \leq n$. In other words, $X^n - 1 = \prod_{r=1}^{n}(X - \zeta^r)$ where $\zeta = e^{\frac{2\pi i}{n}}$ The crucial fact is that along with ζ, all the powers ζ^r with r coprime [7] to n are the roots

[7] These are the *primitive* n-th roots of unity i.e., they are not m-th roots for any m smaller than n.

of $\Phi_n(X)$! So, $X^n-1 = \prod_{d|n} \prod_{(r,n)=d}(X-\zeta^r) = \prod_{d|n} \Phi_d(X)$. Here, we have denoted by (r,n) the greatest common divisor of r and n. From the above expression for $\Phi_n(X)$, it is not at all clear that $\Phi_n(X)$ has integer coefficients. However, one uses elementary number theory to invert the identity $X^n-1 = \prod_{d|n} \Phi_d(X)$. This is known as the Möbius inversion formula and yields the identity $\Phi_n(X) = \prod_{d|n}(X^d-1)^{\mu(n/d)}$ where the Möbius function $\mu(m)$ is defined to take the value $0, 1$ or -1 according as whether m is divisible by a square, is a square-free product of an even number of primes, or is a square-free product of an odd number of primes. The inversion formula is a very easy and pleasant exercise in elementary number theory. Now, from the above expression, it is not clear that the fractional expression on the right side is indeed a polynomial! But, this follows from induction on n once we recall the expression $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

An interesting feature of the cyclotomic polynomials is the following. The coefficients seem to be among $0, 1$ and -1 – for instance, for a prime p, $\Phi_p(X) = 1 + X +$ $+ X^{p-1}$ – and one might wonder whether this is true for any $\Phi_n(X)$. It turns out that Φ_{105} has one coefficient equal to 2! Using, some nontrivial results on how prime numbers are distributed, one can show that every integer occurs among the coefficients of the cyclotomic polynomials!

Infinitude of Primes ending in 1

$11, 31, 41, 61, 71, 101,$ where does it stop? *Are there infinitely many primes ending in* 1*?* Equivalently, does the arithmetic progression $\{1 + 10n; n \geq 1\}$ contain infinitely many primes? Any prime number other than 2 must obviously end in $1, 3, 7$ or 9. The natural question is whether there are infinitely many of each type? The answer is 'yes' by a deep theorem due to Dirichlet – *infinitely many primes occur in any arithmetic progression* $\{a + nd; n > 0\}$ *with* a, d *coprime.* For an arithmetic progression of the form $\{1 + nd; n > 0\}$ for some natural number d, one can use cyclotomic polynomials to prove this! This is not surprising because we have already noted in the last section that cyclotomic polynomials are related to the way prime numbers

are distributed.

Suppose $p_1, p_2, \ldots, p_r$ are prime numbers in this progression. We will use cyclotomic polynomials to produce another prime p in this progression different from the p_i's. This would imply that there are infinitely many primes in such a progression. Consider the number $N = dp_1p_2 \cdots p_r$. Then, for any integer n, the two values $\Phi_d(nN)$ and $\Phi_d(0)$ are equal modulo N But, $\Phi_d(0)$ is an integer which is also a root of unity and must, therefore, be ± 1. Moreover, as $n \to \infty$, the values $\Phi_d(nN) \to \infty$ as well. In other words, for large n, $\Phi_d(nN)$, is different from ± 1 and therefore, has a prime factor p. We note that as $\Phi_d(nN)$ is ± 1 modulo any of the p_i's or modulo d, any prime factor p of it is different from d as well as from any of the p_i's. One might wonder which primes divide some value $\Phi_d(a)$ of a cyclotomic polynomial. The answer is that these are precisely the primes occurring in the arithmetic progression $\{1 + nd; n > 0\}$. To show this, we use the idea that the nonzero integers modulo p form a group of order $p - 1$ under the multiplication modulo p. So, it is enough to prove that if p divides $\Phi_d(a)$ for some integer a, then a has order d modulo p i.e., p divides $a^d - 1$ and d is minimal. Let us prove this now. Since $X^d - 1 = \prod_{l|d} \Phi_l(X)$, it follows that p which divides $\Phi_d(a)$ has to divide $a^d - 1$. If d were not minimal, let k divide d with $k < d$ and p divides $a^k - 1$. Once again, the relation $a^k - 1 = \prod_{l|k} \Phi_l(a)$ shows that p divides $\Phi_l(a)$ for some l dividing k. Therefore, p divides both $\Phi_d(a + p)$ and $\Phi_l(a + p)$.[8] Now,

$$(a+p)^d - 1 = \prod_{m|d} \Phi_m(a+p) = \Phi_d(a+p)\Phi_l(a+p) \cdot (\text{other factors})$$

the expression on the right hand side is divisible by p^2. On the other hand, the left side is, modulo p^2, equal to $a^d + dpa^{d-1} - 1$. Since p^2 divides $a^d - 1$, it must divide dpa^{d-1} as well. This is clearly impossible since neither a nor d is divisible by p. This proves that any prime factor p of $\Phi_d(nN)$ occurs in the arithmetic progression $\{1 + nd; n > 0\}$ and thereby proves the infinitude of the primes in this progression.

Euclid's classical proof of the infinitude of prime numbers is

[8] For any polynomial $P(X)$, the values $P(a+p)$ and $P(a)$ are equal modulo p.

the special case of the above proof where we can use $d = 2$.

Sum of Primitive Roots

For a prime number p, Gauss defined a primitive root modulo p to be an integer a whose order modulo p is $p - 1$. In other words, a is a generator of the multiplicative group of integers modulo p. He also showed that primitive roots modulo n exist if, and only if, n is $2, 4, p^\alpha$ or $2p^\alpha$ for some odd prime p. For instance, the primitive roots modulo 5 among the integers modulo 5 are 2 and 3. Their sum is 0 modulo 5. Now, look at the integers modulo 7. In this case, the primitive roots are 3 and 5. Modulo 7, these sum to 1. What about 11? The primitive roots here are $2, 6, 7$ and 8 and these give the sum 1 modulo 11. What is the pattern here? Without letting out the secret, let us go on to investigate the problem for a general prime p.

When is an integer modulo p a primitive root? As we already observed, an integer a is a primitive root modulo p exactly when p divides the integer $\Phi_{p-1}(a)$ i.e. when a is a root of the cyclotomic polynomial Φ_{p-1} modulo p. Hence the sum of all the primitive roots modulo p is simply the sum of the roots of Φ_{p-1} modulo p. Then, one has the beautiful result that *for any positive integer n, the sum of the roots of* $\Phi_n(X)$ *is* $\mu(n)$.

To see why this is so, we look at the cyclotomic polynomial

$$\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(\frac{n}{d})} = \frac{\prod_{d\in A}(X^d - 1)}{\prod_{d\in B}(X^d - 1),}$$

where $A = \{d|n : \mu(\frac{n}{d}) = 1\}$ and $B = \{d|n : \mu(\frac{n}{d}) = -1\}$.

Let us write $\Phi_n(X) = X^{\phi(n)} + d_{\phi(n)-1}X^{\phi(n)-1} + \quad \cdot$. The degree $\phi(n)$ is actually the number of integers $d \leq n$ which are coprime to n.

Let us further write $\prod_{d\in A}(X^d - 1) = X^{a_1} - X^{a_2} + \cdot$ where $a_1 > a_2 > \quad \cdot$, and $\prod_{d\in B}(X^d - 1) = X^{b_1} - X^{b_2} +$ where $b_1 > b_2 > \quad \cdot$.

Then, we get

$$X^{a_1}-X^{a_2}+\cdot\quad =(X^{\phi(n)}+d_{\phi(n)-1}X^{\phi(n)-1}+\cdot\ \cdot)(X^{b_1}-X^{b_2}+\cdot\ \cdot).$$

We have $a_1 = \sum_{d\in A} d$, $b_1 = \sum_{d\in B} d$, and $a_1 = b_1 + \phi(n)$.

Coefficient of X^{a_1-1} on the left hand side of the above equation is -1 or 0 according as $1 \in A$ or not. Comparing the coefficients of $X^{b_1+\phi(n)-1}$ on both sides of the equation, we get $t_A = d_{\phi(n)-1} + t_B$ where, we have written t_C for a set C to denote -1 or 0 according as 1 is in C or not. This clearly implies that $d_{\phi(n)-1} = -\mu(n)$ and proves that *the sum of the primitive roots modulo p is $\mu(p-1)$*.

The discussion above shows that cyclotomic polynomials have nice applications in number theory. Perhaps, the reader will feel enthused enough to look for more such results. For example, she/he could verify that the sum s_2 of the squares of the primitive roots modulo p is $\mu(p-1) + 2\mu(\frac{p-1}{2})$ or she/he could study the analogue of the problem with the set of integers replaced by the set of polynomials over a finite field!

Suggested Reading

[1] M Artin, *Algebra*. Prentice Hall, 1991.

[2] D Suryaramana, *Resonance*, Vol. 2, No. 6, 1997.

[3] Ian Stewart, Gauss, *Scientific American*, 1977.

[4] C F Gauss, *Disquisitiones Arithmeticae*, English Edition, Springer, 1985.

[5] J Pierpont, *Bull. Amer. Math. Soc.*, pp.77-83, 1895-96.

[6] J Gray, English translation and commentary on Gauss's mathematical diary, *Expo. Math.*, Vol.2, 1984.

[7] M Rosen, *Amer. Math. Monthly*, 1981.

Address for Correspondence
B Sury
Indian Statistical Institute
Bangalore 560 059, India.