Die ganzen zahlen hat Gott gemacht

Polynomials with Integer Values

B Sury

After a long stint (1981-1999) at the Tata Institute of Fundamental Research in Mumbai, the author moved to the Indian Statistical Institute, Bangalore due to his interest in undergraduate teaching.

A quote attributed to the famous mathematician L Kronecker is '*Die Ganzen Zahlen hat Gott gemacht, alles andere ist Menschenwerk.*' A translation might be '*God gave us integers and all else is man's work.*' All of us are familiar already from middle school with the similarities between the set of integers and the set of all polynomials in one variable. A paradigm of this is the Euclidean (division) algorithm. However, it requires an astute observer to notice that one has to deal with polynomials with real or rational coefficients rather than just integer coefficients for a strict analogy. There are also some apparent dissimilarities – for instance, there is no notion among integers corresponding to the derivative of a polynomial. In this discussion, we shall consider polynomials with integer coefficients. Of course a complete study of this encompasses the whole subject of algebraic number theory, one might say. For the most of this article (in fact, with the exception of 1.9, 2.3, 2.4 and 4.3), we adhere to fairly elementary methods and address a number of rather natural questions. To give a prelude, one such question might be "if an integral polynomial takes only values which are perfect squares, then must it be the square of a polynomial ?" Note that for a natural number n, the polynomial $\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n(n-1)\cdots 1}$ takes integer values at all integers although it does not have integer coefficients. By Z, we shall denote the set of integers.

A paradigm of the similarity between integers and polynomials in one variable is the Euclidean division algorithm.

1. Prime Values and Irreducibility

The first observation about polynomials taking integral values is

Lemma 1.1. *A polynomial P takes Z to Z if, and only if, $P(X) = a_0 + a_1\binom{X}{1} + \quad + a_n\binom{X}{n}$ with $a_i \in Z$.*

Proof: The sufficiency is evident. For the converse, we first note that any polynomial whatsoever can be written in this form for some n and some (possibly nonintegral) a_i's. Writing P in this form and assuming that $P(Z) \subset Z$, we have

$$\begin{aligned} P(0) &= a_0 \in Z \\ P(1) &= a_0 + a_1 \in Z \\ P(2) &= a_0 + a_1\binom{2}{1} + a_2 \in Z \end{aligned}$$

and so on. Inductively, since $P(m) \in Z\ \forall m$, we get $a_i \in Z\ \forall i$.

Corollary 1.2. *If a polynomial P takes Z to Z and has degree n, then $n!P(X) \in Z[X]$.*

Lemma 1.3. *A nonconstant integral polynomial $P(X)$ cannot take only prime values.*

Proof: If all values are composite, then there is nothing to prove. So, assume that $P(a) = p$ for some integer a and prime p. Now, as P is nonconstant,

$$\lim_{n\to\infty} |P(a + np)| = \infty.$$

So, for big enough n, $|P(a+np)| > p$. But $P(a+np) \equiv P(a) \equiv 0 \bmod p$, which shows $P(a + np)$ is composite.

Remark 1.4. Infinitely many primes can occur as integral values of a polynomial. For example, if $(a, b) = 1$, then the well-known (but deep) Dirichlet's theorem on primes in progression shows that the polynomial $aX + b$ takes infinitely many prime values. In general, it may be very difficult to decide whether a given polynomial takes infinitely many prime values. For instance, it is not known if $X^2 + 1$ represents infinitely many primes.

Dirichlet proved that an arithmetic progression {ax + b} with (a, b) =1, contains infinitely many primes. It is unknown whether $x^2 + 1$ represents infinitely many primes.

For a nonconstant, integral polynomial $P(X)$, not all values $P(0)$, $P(\pm 1)$, $P(\pm 2)$, etc. can be built from finitely many primes. However, it may be possible to build infinitely many such values from a finite set of primes.

In fact, there is no polynomial of degree ≥ 2 which is known to take infinitely many prime values.

Lemma 1.5. *If P is a nonconstant, integral-valued polynomial, then the number of prime divisors of its values $\{P(m)\}_{m\in Z}$, is infinite i.e. not all terms of the sequence $P(0), P(1),$ can be built from finitely many primes.*

Proof: It is clear from 1.2 above that it is enough to prove this for $P(X) \in Z[X]$, which we will henceforth assume. Now, $P(X) = \sum_{i=0}^{n} a_i X^i$, where $n \geq 1$. If $a_0 = 0$, then clearly $P(p) \equiv 0 \bmod p$ for any prime p. If $a_0 \neq 0$, let us consider for any integer t, the polynomial

$$P(a_0 tX) = \sum_{i=0}^{n} a_i (a_0 tX)^i = a_0 \left\{ 1 + \sum_{i=1}^{n} a_i a_0^{i-1} t^i X^i \right\} =$$

$$a_0 Q(X).$$

There exists some prime number p such that $Q(m) \equiv 0 \bmod p$ for some m and some prime p, because Q can take the values 0,1,-1 only at finitely many points. Since $Q(m) \equiv 1 \bmod t$, we have $(p,t) = 1$. Then $P(a_0 tm) \equiv 0 \bmod p$. Since t was arbitrary, the set of p arising in this manner is infinite.

Remark 1.6. (a) Note that it may be possible to construct infinitely many terms of the sequence $\{P(m)\}_{m\in Z}$ using only a finite number of primes. For example take $(a,d) = 1, a \geq d \geq 1$. Since, by Euler's theorem, $a^{\varphi(d)} \equiv 1 \bmod d$, the numbers $\frac{a(a^{\varphi(d)n}-1)}{d} \in Z \ \forall\ n$. For the polynomial $P(X) = dX + a$, the infinitely many values $P(\frac{a}{d}(a^{\varphi(d)n} - 1)) = a^{\varphi(d)n+1}$ have only prime factors coming from primes dividing a.

(b) In order that the values of an integral polynomial $P(X)$ be prime for infinitely many integers, $P(X)$ must be irreducible over Z and of content 1. By content, we mean the greatest common divisor of the coefficients.

Box 1. Eisenstein's Criterion and More

Perhaps the only general criterion known to check whether an integral polynomial of a special kind is irreducible is due to G Eisenstein, a student of Gauss and an outstanding mathematician, whom Gauss is said to have rated above himself. Eisenstein died when he was 27.

Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ *be an integral polynomial satisfying the following property with respect to some prime* p. *The prime* p *divides* $a_0, a_1, \cdots, a_{n-1}$ *but does not divide* a_n. *Also, assume that* p^2 *does not divide* a_0. *Then,* f *is irreducible.*

The proof is indeed very simple high school algebra. Suppose, if possible, that $f(X) = g(X)h(X) = (b_0 + b_1X + \cdots + b_rX^r)(c_0 + c_1X + \cdots + c_sX^s)$ with $r, s \geq 1$. Comparing coefficients, one has

$$a_0 = b_0c_0, a_1 = a_0b_1 + b_0a_1, \cdots, a_n = b_rc_s, \quad r + s = n.$$

Since $a_0 = b_0c_0 \equiv 0 \mod p$, either $b_0 \equiv 0 \mod p$ or $c_0 \equiv 0 \mod p$.

To fix notations, we may assume that $b_0 \equiv 0 \mod p$. Since $a_0 \not\equiv 0 \mod p^2$, we must have $c_0 \not\equiv 0 \mod p$. Now $a_1 = b_0c_1 + b_1c_0 \equiv b_1c_0 \mod p$; so $b_1 \equiv 0 \mod p$. Proceeding inductively in this manner, it is clear that all the b_i's are multiples of p. This is a manifest contradiction of the fact that $a_n = b_rc_s$ is not a multiple of p. This finishes the proof.

It may be noted that one may reverse the roles of a_0 and a_n and obtain another version of the criterion:

Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ *be an integral polynomial satisfying the following property with respect to some prime* p. *The prime* p *divides* $a_1, a_2, \cdots, a_n$ *but does not divide* a_0. *Also, assume that* p^2 *does not divide* a_n. *Then,* f *is irreducible.*

The following generalisation is similar to prove and is left as an exercise.

Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ *be an integral polynomial satisfying the following property with respect to some prime* p. *Let* t *be such that the prime* p *divides* $a_0, a_1, \cdots, a_{n-t}$ *but does not divide* a_n. *Also, assume that* p^2 *does not divide* a_0. *Then,* f *is either irreducible or it has a nonconstant factor of degree less than* t.

Suppose p is a prime number with the decimal digits $a_n \ldots a_1, a_0$. Then, the polynomial $a_0 + a_1 X + \ldots + a_n X^n$ turns out to be irreducible.

In general, it is difficult to decide whether a given integral polynomial is irreducible or not. We note that the irreducibility of $P(X)$ and the condition that it have content 1, are not sufficient to ensure that $P(X)$ takes infinitely many prime values. For instance, the polynomial $X^n + 105X + 12$ is irreducible, by Eisenstein's criterion (see *Box* 1). But, it cannot take any prime value because it takes only even values and it does not take either of the values ± 2 since both $X^n + 105X + 10$ and $X^n + 105X + 14$ are irreducible, again by Eisenstein's criterion.

Lemma 1.7. *Let* $a_1, \quad , a_n$ *be distinct integers.*

Then $P(X) = (X - a_1) \quad (X - a_n) - 1$ *is irreducible.*

Proof: Suppose, if possible, $P(X) = f(X)g(X)$ with $\deg . f, \deg . g < n$. Evidently, as $f(a_i)g(a_i) = -1$, $f(a_i) = -g(a_i) = \pm 1 \; \forall 1 \leq i \leq n$. Now, $f(X) + g(X)$ being a polynomial of degree $< n$ which vanishes at the n distinct integers $a_1, \quad , a_n$ must be identically zero. This gives $P(X) = -f(X)^2$ but this is impossible as can be seen by comparing the coefficients of X^n.

Exercise 1.8. *Let* n *be odd and* $a_1, \quad , a_n$ *be distinct integers. Prove that* $(X - a_1) \quad (X - a_n) + 1$ *is irreducible.*

Let us consider the following situation. Suppose $p = a_n \cdot \quad a_0$ is a prime number expressed in the usual decimal system i.e. $p = a_0 + 10a_1 + 100a_2 + \quad + 10^n a_n, 0 \leq a_i \leq 9$. Then, is the polynomial $a_0 + a_1 X + \quad + a_n X^n$ irreducible? This is, in fact, true and, more generally

Lemma 1.9. *Let* $P(X) \in Z[X]$ *and assume that there exists an integer* n *such that*

(i) the zeros of P *lie in the half plane* $\mathrm{Re}\,(z) < n - \frac{1}{2}$.

(ii) $P(n-1) \neq 0$.

(iii) $P(n)$ is a prime number.

Then $P(X)$ is irreducible.

Proof: Suppose, if possible $P(X) = f(X)g(X)$ over Z. All the zeros of $f(X)$ also lie in $\mathrm{Re}(z) < n - \frac{1}{2}$. Therefore, $|f(n - \frac{1}{2} - t)| < |f(n - \frac{1}{2} + t)| \forall t > 0$. Since $f(n-1) \neq 0$ and $f(n-1)$ is integral, we have $|f(n-1)| \geq 1$. Thus $|f(n)| > |f(n-1)| \geq 1$. A similar thing holding for $g(X)$, we get that $P(n)$ has proper divisors $f(n), g(n)$ which contradicts our hypothesis.

It was first observed by Hilbert that the reducibility of a polynomial modulo every integer is not sufficient to guarantee its reducibility over Z.

2. Irreducibility and Congruence Modulo p

For an integral polynomial to take the value zero at an integer or even to be reducible, it is clearly necessary that these properties hold modulo any integer m. Conversely, if $P(X)$ has a root modulo any integer, it must itself have a root in Z. In fact, if $P(X) \in Z[X]$ has a linear factor modulo all but finitely many prime numbers, the $P(X)$ itself has a linear factor. This fact can be proved only by deep methods viz. using the so-called Ćebotarev density theorem. On the other hand, (see lemma 2.3) it was first observed by Hilbert that the reducibility of a polynomial modulo every integer is not sufficient to guarantee its reducibility over Z. Regarding roots of a polynomial modulo a prime, there is following general result due to Lagrange:

Lemma 2.1. *Let p be a prime number and let $P(X) \in Z[X]$ be of degree n. Assume that not all coefficients of P are multiples of p. Then the number of solutions* mod *p to $P(X) \equiv 0 \bmod p$ is, at the most, n.*

The proof is obvious using the division algorithm over Z/p. In fact, the general result of this kind (provable by the division algorithm again) is that a nonzero polynomial over any field has at the most its degree number of roots.

The division algorithm shows that over any field, a non-zero polynomial has at the most its degree number of roots.

Remark 2.2. Since $1, 2, \quad , p-1$ are solutions to $X^{p-1} \equiv 1 \bmod p$, we have $X^{p-1} - 1 \equiv (X-1)(X-2) \quad (X-(p-1)) \bmod p$. For odd p, putting $X = 0$ gives Wilson's theorem that $(p-1)! \equiv -1 \bmod p$.

Note that we have observed earlier that any non-constant integral polynomial has a root modulo infinitely many primes. However, as first observed by Hilbert, the reducibility of a polynomial modulo every integer does not imply its reducibility over Z. For example, we have the following result:

Lemma 2.3. *Let p, q be odd prime numbers such that $(\frac{p}{q}) = (\frac{q}{p}) = 1$ and $p \equiv 1 \bmod 8$. Here $(\frac{p}{q})$ denotes the Legendre symbol defined to be 1 or -1 according as p is a square or not modulo q. Then, the polynomial $P(X) = (X^2 - p - q)^2 - 4pq$ is irreducible whereas it is reducible modulo any integer.*

Proof:

$$P(X) = X^4 - 2(p+q)X^2 + (p-q)^2 =$$
$$(X - \sqrt{p} - \sqrt{q})(X + \sqrt{p} + \sqrt{q})(X - \sqrt{p} + \sqrt{q})$$
$$(X + \sqrt{p} - \sqrt{q}).$$

Since $\sqrt{p}, \sqrt{q}, \sqrt{p} \pm \sqrt{q}, \sqrt{pq}$ are all irrational, none of the linear or quadratic factors of $P(X)$ are in $Z[X]$ i.e. $P(X)$ is irreducible. Note that it is enough to show that a factorisation of P exists modulo any prime power as we can use Chinese reminder theorem to get a factorisation modulo a general integer.

Now, $P(X)$ can be written in the following ways:

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X^2 + p - q)^2 - 4pX^2 \\ &= (X^2 - p + q)^2 - 4qX^2 \\ &= (X^2 - p - q)^2 - 4pq. \end{aligned}$$

The second and third equalities above show that $P(X)$ is reducible modulo any p^n and any q^n. Also since $p \equiv 1 \bmod 8, p$ is a square modulo any 2^n and the second equality above again shows that $P(X)$ is the difference of two squares modulo 2^n, and hence reducible mod 2^n.

If ℓ is a prime $\neq 2, p, q$, let us show now that $P(X)$ is reducible modulo l^n for any n.

At least one of $(\frac{p}{\ell}), (\frac{q}{\ell})$ and $(\frac{pq}{\ell})$ is 1 because, by the product formula for Legendre symbols, $(\frac{p}{\ell}) \cdot (\frac{q}{\ell}) \cdot (\frac{pq}{\ell}) = 1$. According as $(\frac{p}{\ell}), (\frac{q}{\ell})$ or $(\frac{pq}{\ell}) = 1$, the second, third or fourth equality shows that $P(X)$ is reducible mod ℓ^n for any n.

We end this section with a result of Schur whose proof is surprising and elegant as well. This is:

Schur's Theorem 2.4

For any n, the truncated exponential polynomial $E_n(X) = n!(1 + X + \frac{X^2}{2!} + \quad + \frac{X^n}{n!})$ is irreducible over $\mathbf{Z}$.

Just for this proof, we need some nontrivial number theoretic facts. A reader unfamiliar with these notions but one who is prepared to accept at face value a couple of results can still appreciate the beauty of Schur's proof. Here is where we have to take recourse to some very basic facts about prime decomposition in algebraic number fields. Suppose, if possible, that $E_n(X) = f(X)g(X)$ for some nonconsant, irreducible integral polynomial f. Let us write $f(X) = a_0 + a_1 X + \cdot \cdot + X^r$ (evidently, we may take the top coefficients of f to be 1). Start with any (complex) root α of f and look at the field $K = \mathbf{Q}(\alpha)$ of all those complex numbers which can be written as polynomials in α with coefficients from $\mathbf{Q}$. The basic fact that we will be using (without proof) is that any nonzero ideal in 'the ring of integers of K' (i.e., the subring O_K of K made up of those elements, which satisfy a monic integral polynomial) is uniquely a product of

Look at the field $K=\mathbf{Q}(\alpha)$ of all those complex numbers which can be written as polynomials in α with coefficients from $\mathbf{Q}$. Any nonzero ideal in 'the ring of integers of K' (i.e., the subring O_K of K made up of those elements, which satisfy a monic integral polynomial) is uniquely a product of nonzero prime ideals and a prime ideal can occur at the most deg f times. This is a good replacement for K of the usual unique factorisation of natural numbers into prime numbers.

Bertrand's postulate says that there is always a prime between n and $2n$. Sylvester generalized this to the assertion that if $m \geq r$, then $(m+1)(m+2) \ldots (m+r)$ has a prime factor $p>r$.

nonzero prime ideals and a prime ideal can occur at the most deg f times. This is a good replacement for K of the usual unique factorisation of natural numbers into prime numbers. The proof also uses a fact about prime numbers observed by Sylvester but is not trivial to prove.

Sylvester's Theorem

If $m \geq r$, then $(m+1)(m+2) \quad (m+r)$ has a prime factor $p > r$.

The special case $m = r$ is known as Bertrand's postulate.

Proof of Schur's Theorem

Now, the proof uses the following fact which is interesting in its own right:

Observation: *Any prime dividing the constant term a_0 of f is less than the degree r of f.*

To see this, note first that $N(\alpha)$, the 'norm of α' (a name for the product of all the roots of the minimal polynomial f of α) is a_0 upto sign. So, there is a prime ideal P of O_K so that $(\alpha) = P^k I$, $(p) = P^l J$ where I, J are indivisible by P and $k, l \geq 1$. Here, (α) and (p) denote, respectively, the ideal of O_K generated by α and p. Since $E_n(\alpha) = 0$, we have

$$0 = n! + n!\alpha + n!\alpha^2/2! + \quad + \alpha^n.$$

We know that the exact power of p dividing $n!$ is

$$h_n = [n/p] + [n/p^2] +$$

Thus, in O_K, the ideal $(n!)$ is divisible by P^{lh_n} and no higher power of P. Similarly, for $1 \leq i \leq n$, the ideal generated by $n!\alpha^i/i!$ is divisible by $P^{lh_n - lh_i + ki}$. Because of the equality

$$-n! = n!\alpha + n!\alpha^2/2! + \quad + \alpha^n$$

it follows that we cannot have each $lh_n - lh_i + ki$ strictly bigger than lh_n which is the exact power of P dividing the left hand side. Therefore, there is some i so that $-lh_i + ki \leq 0$. Thus,

$$i \leq ki \leq lh_i = l([i/p] + [i/p^2] + \quad \cdot) < \frac{li}{p-1}.$$

Thus, $p - 1 < l \leq r$ i.e., $p \leq r$. This confirms the observation.

If an integral polynomial P takes only values which are squares, it turns out that P is itself the squre of an integral polynomial.

To continue with the proof, we may clearly assume that the degree r of f at most $n/2$. Now, we use Sylvester's theorem to choose a prime $q > r$ dividing the product $n(n-1) \quad (n-r+1)$. Note that we can use this theorem because the smallest term $n - r + 1$ of this r-fold consecutive product is bigger than r as $r \leq n/2$. Note also that the observation tells us that q cannot divide a_0. Now, we shall write $E_n(X)$ modulo the prime q. By choice, q divides the coefficients of X^i for $0 \leq i \leq n - r$.

So, $f(X)g(X) \equiv X^n + n!\frac{X^{n-1}}{(n-1)!} + \quad + n!\frac{X^{n-r+1}}{(n-r+1)!} \bmod q.$

Write $f(X) = a_0 + a_1X + \quad + X^r$ and $g(X) = b_0 + b_1X + \quad + X^{n-r}$.

The above congruence gives $a_0b_0 \equiv 0$, $a_0b_1 + a_1b_0 \equiv 0$ etc. mod q until the coefficient of X^{n-r} of $f(X)g(X)$. As $a_0 \not\equiv 0 \bmod q$, we get recursively (this is just like the proof of Eisenstein's criterion – see *Box* 1) that

$$b_0 \equiv b_1 \equiv \quad \cdot b_{n-r} \equiv 0 \bmod q.$$

This is impossible as $b_{n-r} = 1$. Thus, Schur's assertion follows.

3. Polynomials Taking Square Values

If an integral polynomial takes only values which are squares, is it true that the polynomial itself is a square of a polynomial? In this section, we will show that this, and more, is indeed true.

More generally, if P takes only k-th powers as values, P is itself the k-th power of an integral polynomial.

Lemma 3.1. *Let $P(X)$ be a Z-valued polynomial which is irreducible. If P is not a constant, then there exist arbitarily large integers n such that $P(n) \equiv 0$ and $P(n) \not\equiv 0 \bmod p^2$ for some prime p.*

Proof: First, suppose that $P(X) \in Z[X]$. Since P is irreducible, P and P' have no common factors. Write $f(X)P(X) + g(X)P'(X) = 1$ for some $f, g \in Z[X]$. By lemma 1.5, there is a prime p such that $P(n) \equiv 0 \bmod p$, where n can be as large as we want. So, $P'(n) \not\equiv 0 \bmod p$ as $f(n)P(n) = g(n)P'(n) = 1$. Since $P(n+p) - P(n) \equiv P'(n) \bmod p^2$, either $P(n+p)$ or $P(n)$ is $\not\equiv 0 \bmod p^2$. To prove the result for general P, one can replace P by $m!\ P$ where $m = \deg P$.

Lemma 3.2. *Let $P(X)$ be a Z-valued polynomial such that the zeros of smallest multiplicity have multiplicity m. Then, there exist arbitrarily large integers n such that $P(n) \equiv 0 \bmod p^m, P(n) \not\equiv 0 \bmod p^{m+1}$ for some prime p.*

Proof: Let $P_1(X),\quad , P_r(X)$ be the distinct irreducible factors of $P(X)$. Write $P(X) = P_1(X)^{m_1}\quad \cdot P_r(X)^{m_r}$ with $m = m_1 \leq\quad \cdot m_r$. By the above lemma, one can find arbitrarily large n such that for some prime p, $P_1(n) \equiv 0 \bmod p$, $P_1(n) \not\equiv 0 \bmod p^2$ and, $P_i(n) \not\equiv 0 \bmod p$ for $i > 1$. Then, $P(n) \equiv 0 \bmod p^m$ and $\not\equiv 0 \bmod p^{m+1}$.

Corollary 3.3. *If $P(X)$ takes at every integer, a value which is the k-th power of an integer, then $P(X)$ itself is the k-th power of a polynomial.*

Proof: If $P(X)$ is not an exact k-th power, then one can write $P(X) = f(X)^k g(X)$ for polynomials f, g so that $g(X)$ has a zero whose multiplicity is $< k$. Once again, we can choose n and a prime p such that $g(n) \equiv 0 \bmod p, \not\equiv 0 \bmod p^k$. This contradicts the fact that $P(n)$ is a k-th power.

[2] is an excellent source of results of this nature.

4. Cyclotomic Polynomials

These were referred to already in an earlier article ([1]). It was also shown there that one could use these polynomials to prove the existence of infinitely many primes congruent to 1 modulo n for any n. For a natural number d, recall that the cyclotomic polynomial $\Phi_d(X)$ is the irreducible, monic polynomial whose roots are the primitive d-th roots of unity i.e. $\Phi_d(X) = \prod_{a \leq d:(a,d)=1}(X - e^{2\pi i a/d})$. Note that $\Phi_1(X) = X - 1$ and that for a prime p, $\Phi_p(X) = X^{p-1} + \quad + X + 1$. Observe that for any $n \geq 1$, $X^n - 1 = \prod_{d/n} \Phi_d(X)$.

Exercise 4.1. *Prove that for any d, $\Phi_d(X)$ has integral coefficients, and is irreducible over Z*

Factorising an integral polynomial into irreducible factors is far from easy. Even if we know the irreducible factors, it might be difficult to decide whether a given polynomial divides another given one.

Factorising an integral polynomial into irreducible factors is far from easy. Even if we know the irreducible factors, it might be difficult to decide whether a given polynomial divides another given one.

Exercises 4.2. *(a) Given positive integers $a_1 <$ $< a_n$, consider the polynomials $P(X) = \prod_{i>j}(X^{a_i - a_j} - 1)$ and $Q(X) = \prod_{i>j}(X^{i-j} - 1)$. By factorising into cyclotomic polynomials, prove that $Q(X)$ divides $P(X)$. Conclude that $\prod_{i>j} \frac{a_i - a_j}{i-j}$ is always an integer.*

(b) *Consider the $n \times n$ matrix A whose (i,j)-th entry is the Gaussian polynomial* $\begin{bmatrix} a_i \\ j-1 \end{bmatrix}$

Compute $\det A$ *to obtain part (a) again.*

Here, for $m \geq r$, the Gaussian polynomial is defined as

$$\begin{bmatrix} m \\ r \end{bmatrix} = \frac{(X^m-1)(X^{m-1}-1)\cdots(X^{m-r+1}-1)}{(X^r-1)(X^{r-1}-1)\cdots(X-1)}.$$

A consequence of the prime number theorem is that for any constant c, there is n such that there are atleast cn primes between 1 and 2^n.

Note that $\begin{bmatrix} m \\ r \end{bmatrix} = \begin{bmatrix} m-1 \\ r-1 \end{bmatrix} + X^r \begin{bmatrix} m-1 \\ r \end{bmatrix}$

It seems from looking at $\Phi_p(X)$ for prime p as though the coefficients of the cyclotomic polynomials $\Phi_d(X)$ for any d are all 0, 1 or -1. However, the following rather amazing fact was discovered by Schur. His proof uses a consequence of a deep result about prime numbers known as the prime number theorem. The prime-number theorem tells us that $\pi(x) \sim x/\log(x)$ as $x \to \infty$. Here $\pi(x)$ denotes the number of primes until x. The reader does not need to be familiar with the prime number theorem but is urged to take on faith the consequence of it that for any constant c, there is n such that $\pi(2^n) \geq cn$.

Proposition 4.3. *Every integer occurs as a coefficient of some cyclotomic polynomial.*

Proof: First, we claim that for any integer $t > 2$, there are primes $p_1 < p_2 <$ $< p_t$ such that $p_1 + p_2 > p_t$. Suppose this is not true. Then, for some $t > 2$, every set of t primes $p_1 <$ $< p_t$ satisfies $p_1 + p_2 \leq p_t$. So, $2p_1 < p_t$. Therefore, the number of primes between 2^k and 2^{k+1} for any k is less than t. So, $\pi(2^k) < kt$. This contradicts the prime-number theorem as noted above. Hence, it is indeed true that for any integer $t > 2$, there are primes $p_1 < p_2 <$ $< p_t$ such that $p_1 + p_2 > p_t$.

Now, let us fix any odd $t > 2$. We shall demonstrate that both $-t+1$ and $-t+2$ occur as coefficents. This will prove that all negative integers occur as coefficients. Then, using the fact that for an odd $m > 1$, $\Phi_{2m}(X) = \Phi_m(-X)$, we can conclude that all integers are coefficients.

Consider now primes $p_1 < p_2 <$ $< p_t$ such that $p_1 + p_2 > p_t$. Write $p_t = p$ for simplicity. Let $n = p_1 \cdot p_t$ and let us write $\Phi_n(X)$ modulo X^{p+1}. Since $X^n - 1 =$ $_{d/n} \Phi_d(X)$, and since $p_1 + p_2 > p_t$, we have

$$\Phi_n(X) \equiv \prod_{i=1}^{t} \frac{1-X^{p_i}}{1-X} \equiv (1+\cdot\ \cdot+X^p)(1-X^{p_1}) \quad (1-X^{p_t})$$

$$\equiv (1+\quad +X^p)(1-X^{p_1}-\quad -X^{p_t}) \text{mod } X^{p+1}$$

Therefore, the coefficients of X^p and X^{p-2} are $1-t$ and $2-t$, respectively. This completes the proof. Note that in the proof, we have used the fact that if $P(X) = (1-X^r)Q(X)$ for a polynomial $Q(X)$, then $Q(X) = P(X)(1+X^r+X^{2r}+\quad +\ \cdot)$ modulo any X^k.

It is conjectured that a nonconstant irreducible integral polynomial whose coefficients have no nontrivial common factor always takes on a prime value.

Exercise 4.4. (a) Let $A = (a_{ij})$ be a matrix in $GL(n, Z)$ i.e., both A and A^{-1} have integer entries. Consider the polynomials $p_i(X) = \sum_{j=0}^{n} a_{ij}X^j$ for $0 \leq i \leq n$. Prove that any integral polynomial of degree at most n is an integral linear combination of the $p_i(X)$. In particular, if $a_0, \quad , a_n \in Q$ are distinct, show that any rational polynomial of degree at most n is of the form $\sum_{i=0}^{n} \lambda_i(X+a_i)^n$ for some $\lambda_i \in Q$.

(b) Prove that $1+X+\ .+X^n = \sum_{i=0}^{[\frac{n}{2}]}(-1)^i \binom{n-i}{i} X^i(1+X)^{n-2i}$. Conclude that $\sum_{i\geq 0}\binom{n-i}{i} = \frac{\alpha^{n+1}-\beta^{n+1}}{\sqrt{5}}$, where $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$. This is known as Binet's formula. Further, compute $\sum_{i\geq 0}(-1)^i \binom{n-i}{i}$.

Remark 4.5. It is easily seen by induction that $\sum_{i\geq 0}\binom{n-i}{i}$ is just the $(n+1)$-th Fibonacci number F_{n+1}.

As we remarked earlier, even for a polynomial of degree 2 (like X^2+1) it is unknown whether it takes infinitely many prime values. A general conjecture in this context is:

Conjecture 4.6. (Bouniakowsky, Schinzel and Sierpinski)

Many number-theoretic questions involve a statement which can be understood by the proverbial man on the street but an answer which proves elusive to professional mathematicians to this day.

A nonconstant irreducible integral polynomial whose coefficients have no nontrivial common factor always takes on a prime value.

We end with an open question, which is typical of many number-theoretic questions – a statement which can be understood by the proverbial layman but an answer which proves elusive to this day to professional mathematicians. For any irreducible, monic, integral polynomial $P(X)$, define its *Mahler measure* to be $M(P) = \prod_i Max(|\alpha_i|, 1)$, where the product is over the roots of P. The following is an easy exercise.

Exercise 4.7. *$M(P) = 1$ if, and only if, P is cyclotomic.*

D H Lehmer posed the following question:

Does there exist $C > 0$ such that $M(P) > 1 + C$ for all noncyclotomic (irreducible) polynomials P?

This is expected to have an affirmative answer and, indeed, Lehmer's calculations indicate that the smallest possible value of $M(P) \neq 1$ is 1.176280821...., which occurs for the polynomial

$$P(X) = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

Lehmer's question can be formulated in terms of discrete subgroups of Lie groups. One may not be able to predict when it can be answered but it is more or less certain that one will need tools involving deep mathematics.

Suggested Reading

[1] B Sury, Cyclotomy, *Resonance*, Vol.4, No.12, pp.41-53, 1999.
[2] Polya and Szego – *Problems in analysis*, I & II, Springer-Verlag, 1945.

Address for Correspondence
B Sury
Statistics & Mathematics Unit
Indian Statistical Institute
Bangalore 560 059, India.
Email: sury@isibang.ac.in