Classroom

In this section of *Resonance*, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

B Sury
Stat-Math Unit
Indian Statistical Institute
8th Mile Mysore Road
Bangalore 560 059, India.
Email:sury@isibang.ac.in

Revisiting Kummer's and Legendre's Formulae

In a beginning course in number theory, an elementary exercise is to compute the largest power of a prime p dividing $n!$. This number, called the p-adic valuation of $n!$, is easily proved to be

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \qquad (1)$$

Note that this is a finite series. The number $v_p(n!)$ comes up naturally in a few situations like the following. In the group of permutations of n objects, this would give the power of p which is the order of a p-Sylow subgroup. While discussing p-adic numbers as analogues of the usual real numbers, one looks at the analogue of the exponential series. The expression for $v_p(n!)$ leads one to determine that the exponential series has the radius of convergence $p^{-1/(p-1)}$.

Now, $v_p(n!)$ can also be computed in another manner by a beautiful observation due to the legendary mathematician Legendre. Legendre observed that the p-adic

Keywords
p-adic valuation, base-p expansion, Legendre's formula, Kummer's formula.

valuation of $n!$ can be read off from the base-p expansion of n. It is simply $\frac{n-s(n)}{p-1}$ where $s(n)$ is the sum of the digits of n in this expansion. A related result that Kummer proved is that, if $r \leq n$, then the p-adic valuation of the binomial coefficient $\binom{n}{r}$ is simply the number of 'carry-overs' when one adds r and $n-r$ in base-p. In [1], Honsberger deduces Kummer's theorem from Legendre's result and refers to Ribenboim's lovely book [2] for a proof of the latter. Ribenboim's proof is by verifying that Legendre's base-p formula agrees with the standard formula given in (1).

The p-adic valuation of $n!$ can be read off from the base-p expansion of n. It is simply $\frac{n-s(n)}{p-1}$ where $s(n)$ is the sum of the digits of n in this expansion.

Is it possible to prove Legendre's formula without recourse to the above formula (1)? We shall see that this is indeed possible and that the standard formula follows from such a proof. What is more, Kummer's formula also follows without having to use Legendre's result. The author's long-standing belief that these proofs are more natural than the ones quoted above was vindicated during a selection interview to an undergraduate programme, when an outstanding candidate Swarnendu Datta came up essentially with the same proof! Let us start by recalling Legendre's formula.

Legendre's Formula

Let p be a prime number and let $a_k \cdots a_1 a_0$ be the base-p expansion of a natural number n. We shall show that if Legendre's formula

$$v_p(n!) = \frac{n - s(n)}{p-1} = \frac{n - \sum_{i=0}^{k} a_i}{p-1} \qquad (2)$$

holds good for n, then it also holds good for $pn + r$ for any $0 \leq r < p$. Note that the base-p expansion of $pn+r$ is

$$a_k \cdots a_1 a_0\, r.$$

Let us denote, for convenience, the number $\frac{m-s(m)}{p-1}$ by

$f(m)$ for any natural number m. Evidently,

$$f(pn+r) = \frac{pn - \sum_{i=0}^{k} a_i}{p-1} = n + f(n).$$

On the other hand, it follows by induction on n that

$$v_p((pn+r)!) = n + v_p(n!). \tag{3}$$

For, if it holds good for all $n < m$, then

$$\begin{aligned} v_p((pm+r)!) &= v_p(pm) + v_p((pm-p)!) \\ &= 1 + v_p(m) + m - 1 + v_p((m-1)!) \;=\; m + v_p(m!). \end{aligned}$$

Since it is evident that $f(m) = 0 = v_p(m!)$ for all $m < p$, it follows that $f(n) = v_p(n!)$ for all n. This proves Legendre's formula.

Note also that the formula

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] +$$

follows inductively on using (3).

Kummer's Algorithm

As before p is any prime number. For any natural numbers r and s, let us denote by $g(r,s)$ the number of 'carry-overs' when the base-p expansions of r and s are added. Kummer's result is that for $k \leq n$,

$$v_p\left(\binom{n}{k}\right) = g(k, n-k). \tag{4}$$

Once again, this is clear if $n < p$, as both sides are then zero. We shall show that if the formula holds good for n (and *every* $k \leq n$), it does so for $pn + r$ for $0 \leq r < p$ (and any $k \leq pn + r$). This would prove the result for all natural numbers.

Consider any binomial coefficient $\binom{pn+r}{pm+a}$ for $0 \leq a < p$.

First, suppose $a \leq r$.

Write $m = b_k \quad b_0$ and $n-m = c_k \quad c_0$ in base-p. Then the base-p expansions of $pm + a$ and $p(n-m) + (r-a)$ are, respectively,

$$\begin{aligned} pm + a &= b_k \quad b_0\ a, \\ p(n-m) + (r-a) &= c_k \cdot \ \cdot c_0\ r - a. \end{aligned}$$

Evidently, the corresponding number of carry-overs is

$$f(pm + a, p(n-m) + (r-a)) = f(m, n-m).$$

By the induction hypothesis, $f(m, n-m) = v_p(\binom{n}{m})$.

Now $v_p\left(\binom{pn+r}{pm+a}\right)$ is equal to

$$v_p((pn+r)!) - v_p((pm+a)!) - v_p((p(n-m)+r-a)!)$$

$$= n + v_p(n!) - m - v_p(m!) - (n-m) - v_p((n-m)!)$$

$$= v_p\left(\binom{n}{m}\right)$$

Thus, we are through in the case when $a \leq r$.

Now suppose that $r < a$. Then $v_p\left(\binom{pn+r}{pm+a}\right)$ is equal to

$$v_p((pn+r)!) - v_p((pm+a)!) - v_p((p(n-m-1)+(p+r-a))!)$$

$$= n + v_p(n!) - m - v_p(m!) - (n-m-1) - v_p((n-m-1)!)$$

$$= 1 + v_p(n) + v_p((n-1)!) - v_p(m!) - v_p((n-m-1)!)$$

$$= 1 + v_p(n) + v_p\left(\binom{n-1}{m}\right)$$

We need to show that

$$\begin{aligned} &f(pm + a, p(n-m-1) + (p+r-a)) \\ &\quad = 1 + v_p(n) + f(m, n-m-1). \end{aligned} \tag{5}$$

Note that $m < n$. Write $n = a_k \quad \cdot a_0$, $m = b_k \quad \cdot b_0$ and $n - m - 1 = c_k \cdot \quad \cdot c_0$ in base-p. If $v_p(n) = d$, then $a_i = 0$ for $i < d$ and $a_d \neq 0$. In base-p, we have

$$n = a_k \cdot \quad \cdot a_d \; 0 \cdot \quad \cdot 0$$

and, therefore,

$$n - 1 = a_k \quad \cdot a_{d+1} a_d - 1 \; p - 1 \qquad p - 1.$$

Now, the addition $m + (n - m - 1) = n - 1$ gives $b_i + c_i = p - 1$ for $i < d$ (since they must be $< 2p - 1$). Moreover, $b_d + c_d = a_d - 1$ or $p + a_d - 1$.

Note the base-p expansions

$$\begin{aligned} pm + a &= b_k \quad b_0 \; a, \\ p(n - m - 1) + (p + r - a) &= c_k \quad \cdot c_0 \; p + r - a. \end{aligned}$$

We add these using the fact that there is a carry-over in the beginning and that $1 + b_i + c_i = p$ for $i < d$. Since there is a carry-over at the first step as well as at the next d steps, we have

$$pn + r = * \; * \qquad a_d \; 0 \qquad 0 \; r$$

where there are d zeroes before r, and

$$f(pm+a, p(n-m-1)+(p+r-a)) = 1+d+f(m, n-m-1).$$

This proves Kummer's assertion also.

Suggested Reading

[1] **R Honsberger, *In Polya's Footsteps*, published and distributed by the Mathematical Association of America, pp.229-233, 1997.**

[2] **P Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, pp.30-32, 1996.**

The Maximal and Prime Ideals of $R[x]$, R a PID

Dinesh Khurana and Chanchal Kumar*
Department of Mathematics
Panjab University
Chandigarh 160014, India
Email:dkhurana@pu.ac.in

* Department of Mathematics
University of Jammu
Jammu 180006, India
Email: chanchal_ jammu@yahoo.com

For the cognoscenti, the PID of the title stands for 'principal ideal domain'. Thanks to expositions dealing with Fermat's last theorem, several readers who are not mathematicians have become familiar with the importance of this concept vis-a-vis number theory. In a nutshell, it is this property (rather the absence of it) which stands between problems like Fermat's last theorem being a trivial exercise and being one of the deepest mathematical theorems proved in recent times. In this context, the various complex roots of unity is the world one works with and already it becomes clear that this world is intimately connected with the world of polynomials over rational numbers.

In most undergraduate mathematics courses in the country, the syllabus in algebra has hardly changed in 25 years. Even a small variation of the questions discussed elicits a response of "too advanced and outside the scope" from teachers. For example, a standard topic taught in an undergraduate algebra course is that of polynomials over real or complex numbers (or general fields). After introducing prime and maximal ideals in general, and drawing a brief analogy between the ring of polynomials over fields with the ring of usual integers, courses typically do not go further in this direction. Natural questions like the structure of prime and maximal ideals in the ring of polynomials over integers, are almost never discussed.

This note began with an undergraduate student approaching the first author some five years back with an ideal of $\mathbb{Z}[x]$ and asking to check whether it was a prime ideal. We soon started thinking if all prime and maximal ideals of $R[x]$, R a principal ideal domain (PID), were known. A little search in the literature showed this to be the case. One source for this was Kaplansky's book [1]. But

Keywords
Polynomial ring, prime ideals, marximal ideals, prime elements, irreducible elements.

A PID R contains infinitely many irreducible elements precisely when maximal ideals in $R[x]$ are nonprincipal.

as the results used in this book were 'beyond the scope' of undergraduate students, we started looking for elementary proofs. This made us look for an argument which uses only elementary properties of domains. We were able to write a very simple and elementary argument which we present in Theorem 1. In the bargain we also found a number of characterizations of PID's having infinitely many prime elements which we present in Theorem 2. Finally, in Theorem 4, we describe all prime ideals of $R[x]$, R a PID.

Although, we had proved these results five years back, a motivation for writing this now came from a recent article [2] in the American Mathematical Monthly where Zanello proves that a PID R has infinitely many irreducibles if and only if every maximal ideal in $R[x]$ has length 2. This follows as a simple corollary to our results (see Corollary 5). After proving our results, we found a paper by Lemmer and Naudé [3], which also describes prime and maximal ideals of $R[x]$ using, besides some other results, Hilbert Basis Theorem and results in simple field extensions. Our approach is more elementary which also results in three other characterizations of PID's with infinitely many primes besides the one obtained by Zanello in [2].

Throughout this article, R will denote a PID. A polynomial $f(x)$ in $R[x]$ will be called *irreducible* if $f(x)$ cannot be expressed as a product of two non-units in $R[x]$. Clearly, irreducible polynomials of non-zero degree are primitive. What makes the characterization of maximal and prime ideals in $R[x]$, R a PID, a non-trivial exercise is the fact that $R[x]$ is not a PID if R contains a non-unit.

Theorem 1. *Let I be a maximal ideal in $R[x]$. Then*

(i) $I \cap R = 0$ implies that $I = f(x)R[x]$ for some non-constant irreducible polynomial $f(x) \in R[x]$ (which, clearly, is invertible modulo $g(x)R[x]$ for every $g(x) \notin I$);

(ii) $I \cap R \neq 0$ implies that $I = pR[x] + f(x)R[x]$ for some prime element $p \in R$ and some $f(x) \in R[x]$ which is irreducible modulo $pR[x]$.

There are infinitely many prime elements in a PID R if, and only if, maximal ideals of $R[x]$ restrict to non-zero ideals in R.

Proof. (i) Let $f(x)$ be a polynomial of least degree in I. Clearly, $f(x)$ is non-constant and we may assume $f(x)$ to be irreducible in view of 'minimality' of $f(x)$ and the fact that $I \cap R = 0$. If $g(x) \in I$, then for some $t \in R$ and $q(x)$, $r(x) \in R[x]$, we have $tg(x) = f(x)q(x) + r(x)$, with either $r(x) = 0$ or degree of $r(x)$ is smaller than that of $f(x)$. As $r(x) \in I$, the 'minimality' of $f(x)$ forces $r(x) = 0$. Thus $f(x)|tg(x)$ implying $f(x)|g(x)$.

(ii) As $I \cap R \neq 0$, we pick a prime $p \in R$ such that $p \in I$. As $pR[x] \subset pR[x] + xR[x] \neq R[x]$, $pR[x]$ is not a maximal ideal and, in particular, $pR[x] \neq I$. Thus $I/pR[x]$ is a maximal ideal of Euclidean domain $R[x]/pR[x]$. Thus for some $f(x) \in R[x]$ which is irreducible modulo $pR[x]$, $I/pR[x] = \overline{f(x)}(R[x]/pR[x]) \Rightarrow I = pR[x] + f(x)R[x]$ □

Theorem 2. *For a PID R, the following conditions are equivalent:*

(i) R has infinitely many prime elements;

(ii) Every maximal ideal of $R[x]$ has non-zero intersection with R;

(iii) Every maximal ideal of $R[x]$ is of the form $pR[x] + f(x)R[x]$ for some prime element $p \in R$ and some $f(x) \in R[x]$ which is irreducible modulo $pR[x]$;

(iv) No maximal ideal of $R[x]$ is principal.

Proof. The implication '$(ii) \Rightarrow (iii)$' follows from Theorem 1, and '$(iii) \Rightarrow (iv)$' is clear.

$(i) \Rightarrow (ii)$ Suppose $I \cap R = 0$ for some maximal ideal I of $R[x]$. By Theorem 1, $I = f(x)R[x]$ for some non-constant polynomial $f(x) = a_0 + a_1x + \ldots + a_nx^n$ with $a_n \neq 0$. Let p be a prime in R. As $R[x]/I$ is a field and $p \notin I$ $pg(x) - 1 = f(x)h(x)$ for some $g(x)$, $h(x) \in R[x]$.

Let $f(x)$ be some non-constant irreducible polynomial in $R[x]$, R a PID. Then $f(x)R[x]$ is always a prime ideal of $R[x]$, which is never maximal if R has infinitely many primes.

This implies that $\overline{f(x)} = \bar{a_0} + \bar{a_1}x + ... + \bar{a_n}x^n$ is a unit in $(R/pR)[x]$ implying that $\bar{a_1}x + ... + \bar{a_n}x^n = 0$. Thus every prime in R divides $a_1x + ... + a_nx^n$ forcing it to be zero, a contradiction.

$(iv) \Rightarrow (i)$ Suppose R has only finitely many primes $p_1, ..., p_n$ and let $I = f(x)R[x]$, where $f(x) = 1 - p_1...p_nx$. Then I is a maximal ideal because otherwise I is contained in some maximal ideal which, in view of Theorem 1, should be of the form $pR[x] + g(x)R[x]$ for some prime $p \in R$ and some $g(x) \in R[x]$ which is irreducible modulo $pR[x]$. Thus, modulo $pR[x]$, $g(x)|f(x) = 1$, a contradiction. □

If $p \in R$ is prime and $f(x)$ is irreducible modulo $pR[x]$, then $pR[x] + f(x)R[x]$ is a maximal ideal of $R[x]$. This is because $S = R[x]/pR[x] \cong (R/pR)[x]$ is a Euclidean domain and $S/\overline{f(x)}S \cong R[x]/(f(x)R[x] + pR[x])$ is a field. This, in view of Theorem 2, gives

Corollary 3. *Let R be a PID with infinitely many primes. An ideal I of $R[x]$ is maximal if and only if $I = pR[x] + f(x)R[x]$ for some prime element $p \in R$ and some $f(x) \in R[x]$ which is irreducible modulo $pR[x]$. In other words, maximal ideals in $R[x]$ have length 2.*

Theorem 4. *An ideal P of $R[x]$, R a PID, is prime if and only if P is either maximal or $P = f(x)R[x]$ for some irreducible $f(x)$ in $R[x]$ such that $f(x)$ is non-unit modulo $pR[x]$ for some prime p in R.*

Proof. The 'if' part is clear. Now let P be a prime ideal which is not maximal. If $P \cap R = 0$, $P = f(x)R[x]$ where $f(x)$ is a least degree polynomial in P (see the proof of Theorem 1). As $P = f(x)R[x]$ is not maximal, it must be contained in some maximal ideal which, in view of Theorem 1, should be of the form $pR[x] + g(x)R[x]$, where p is a prime and $g(x) \in R[x]$ is irreducible modulo $pR[x]$. Thus modulo $pR[x]$, $g(x)|f(x)$. As $g(x)$ modulo $pR[x]$ is irreducible, $f(x)$ modulo $pR[x]$ is non-unit.

Now suppose that $P \cap R \neq 0$. Then P contains a prime p of R. We show that $P = pR[x]$. If $pR[x] \neq P$, then $P/pR[x]$ is a non-zero prime ideal of $R[x]/pR[x]$. As non-zero prime ideals of a PID are maximal, $P/pR[x]$ is maximal. Which implies that P is maximal ideal of $R[x]$, a contradiction. □

Corollary 5 (Zanello [2]) *A PID R has infinitely many primes if and only if every maximal ideal in $R[x]$ has length 2.*

Proof. If R has infinitely many primes, then, by Corollary 3, every maximal ideal has length at least 2. But as $dim(R[x]) = dim(R) + 1 = 2$, every maximal ideal has length 2. Conversely, if R has only finitely many primes, then as in the proof of Theorem 2, there exists a maximal ideal of the form $f(x)R[x]$ for some irreducible polynomial $f(x) \in R[x]$, which, in view of Theorem 4, has length 1. □.

Let $f(x)$ be some non-constant irreducible polynomial in $R[x]$, R a PID. Then $f(x)R[x]$ is always a prime ideal of $R[x]$, which is never maximal if R has infinitely many primes. But if R has finitely many primes, $f(x)R[x]$ may be maximal. The following result tells us exactly when it is so.

Corollary 6. *Let R be a PID with finitely many primes and $f(x)$ be a non-constant irreducible polynomial in $R[x]$. Then $f(x)R[x]$ is maximal if and only if $f(x)$ is unit modulo $pR[x]$ for every prime $p \in R$.*

Proof. If $f(x)R[x]$ is maximal then clearly $f(x)$ is unit modulo every prime $p \in R$. Conversely, suppose that $f(x)$ is unit modulo every prime $p \in R$. In view of Theorem 4, $f(x)R[x]$ is maximal. □

Suggested Reading

[1] A Lemmer and G Naudé, The prime and maximal ideals in $R[x]$, R a principal ideal domain, *Int. J. Math. Edu. Sci. Tech.*, Vol.21, pp.87-91, 1990.

[2] I Kaplansky, *Commutative Rings*, University of Chicago Press, 1974.

[3] F Zanello, When are there infinitely many irreducible elements in a principal ideal domain, *Amer. Math. Monthly*, Vol.111, pp.150-152, 2004.