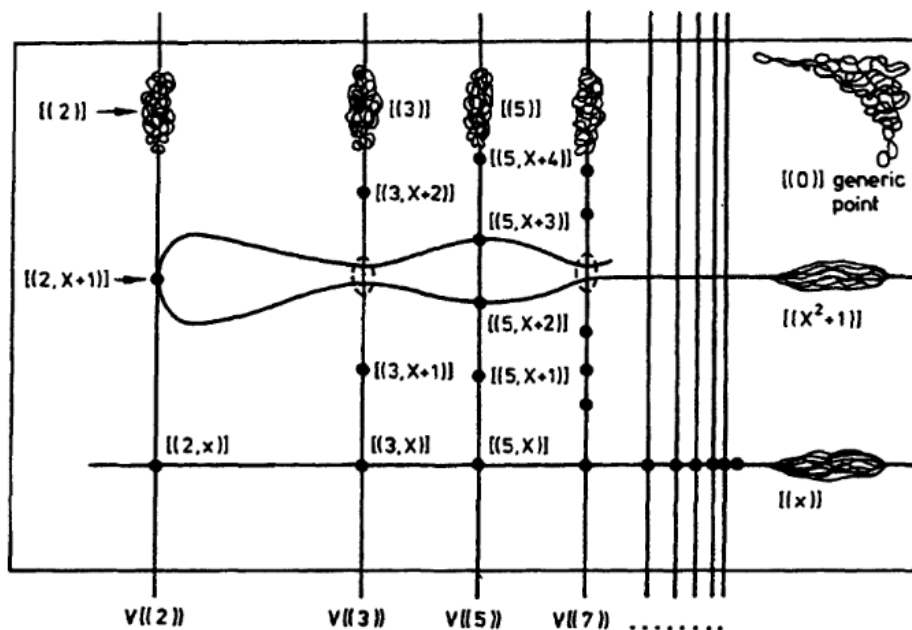


# Computing the prime ideals in the ring of polynomials with integer coefficients

rapha · 10 May 2025

We'll use ideas from [an older post](#) to compute all of the prime ideals in the ring  $\mathbb{Z}[x]$ . This is done in order to better understand the “arithmetic surface”  $\text{Spec } \mathbb{Z}[x]$ .



A picture of  $\text{Spec } \mathbb{Z}[x]$ , from *The Red Book of Varieties and Schemes* (Mumford, 1999)

Let's get the easy stuff out of the way: since  $\mathbb{Z}[x]$  is an integral domain, the zero ideal  $(0)$  is prime. Now suppose  $\mathfrak{p}$  is a prime ideal which isn't zero. Suppose  $\mathfrak{p}$  is a principal ideal, with  $\mathfrak{p} = (f)$  for some polynomial  $f \in \mathbb{Z}[x]$ . Because  $\mathbb{Z}[x]$  is a unique factorization domain, this is equivalent to  $f$  being  $\mathbb{Z}$ -irreducible. By Gauss' Lemma on polynomials, this is the same as  $f$  being  $\mathbb{Q}$ -irreducible and primitive in  $\mathbb{Z}[x]$ . Hence all principal prime ideals are exactly those that are principally generated by a  $\mathbb{Q}$ -irreducible polynomial with coefficients in  $\mathbb{Z}$ , written so that its coefficients are relatively prime.

Now suppose  $\mathfrak{p}$  is a prime ideal which is *not* principal. We know from [an older post](#) that in this case there exists two relatively prime polynomials  $f$  and  $g$  that lie in  $\mathfrak{p}$ . We know that these polynomials stay relatively prime when considered in the larger ring  $\mathbb{Q}[x]$ . This larger ring being an Euclidean domain, Bézout's Identity is verified: there must exist a pair of polynomials  $a, b \in \mathbb{Q}[x]$  such that

$$af + bg = 1.$$

We may put all coefficients that appear in  $a$  and  $b$  over the same denominator  $h \in \mathbb{Z}$ , and write  $a = a'/h$  and  $b = b'/h$  for some  $a', b' \in \mathbb{Z}[x]$ . This gives the following equation in  $\mathbb{Z}[x]$ :

$$a'f + b'g = h.$$

Therefore  $h$  is contained in the ideal generated by  $f$  and  $g$ , hence is contained in  $\mathfrak{p}$ . Because  $h$  is neither zero nor a unit in  $\mathbb{Z}$ , it admits a decomposition into its prime factors, one of which must lie in  $\mathfrak{p}$  because  $\mathfrak{p}$  is a prime ideal. Thus  $\mathfrak{p}$  contains at least one prime number  $q$ .

Consider the map of rings  $\mathbb{Z}[x] \rightarrow \mathbb{F}_q[x]$  which sends  $x$  to  $x$ . This is a surjective map, whose kernel is the prime ideal  $(q)$ . Hence the map induces an isomorphism of rings

$$\mathbb{Z}[x]/(q) \cong \mathbb{F}_q[x].$$

Because  $(q)$  is contained in  $\mathfrak{p}$ , the prime ideal  $\mathfrak{p}$  corresponds to a prime ideal in  $\mathbb{F}_q[x]$ . Note that because  $\mathbb{F}_q[x]$  is a principal ideal domain, we can write

$$\mathfrak{p} = (F) \pmod{(q)},$$

where  $F$  is some polynomial in  $\mathbb{F}_q[x]$ . In fact, as we've mentioned, the image of  $\mathfrak{p}$  in the quotient is a prime ideal, so the element  $F$  is an irreducible polynomial; without loss of generality we may suppose further that  $F$  is monic, since the coefficient ring is a field. The polynomial  $F$  in  $\mathbb{F}_q[x] \cong \mathbb{Z}[x]/(q)$  is its own representative when seen as an element of  $\mathbb{Z}[x]$ .

Let  $\pi : \mathbb{Z}[x] \rightarrow \mathbb{F}_q[x]$  be the map used in the previous paragraphs. From the previous equation mod  $(q)$ , we must have  $\pi^{-1}((F)) = \mathfrak{p}$ . In particular, this shows  $\mathfrak{p}$  is a maximal ideal, since  $(F)$  is a maximal ideal (every nonzero prime ideal in a PID is maximal). Also, it is not too hard to show by double inclusion that  $\pi^{-1}((F)) = (q, F)$ . Hence  $\mathfrak{p} = (q, F)$ . We could also simply show that  $(q, F) \subseteq \mathfrak{p}$ , and show that  $(q, F)$  is a maximal ideal because the quotient  $\mathbb{Z}[x]/(q, F)$  is isomorphic to the field  $\mathbb{F}_q$ .

In conclusion, the prime ideals of  $\mathbb{Z}[x]$  are precisely:

1. the zero ideal  $(0)$ ;
2. the ideals  $(p)$  where  $p \in \mathbb{Z}$  is a prime number;
3. the ideals  $(f)$  where  $f \in \mathbb{Z}[x]$  is a  $\mathbb{Q}$ -irreducible polynomial that is primitive, i.e. such that the greatest common divisor of its coefficients is 1;  
or
4. the ideals  $(p, f)$  where  $p \in \mathbb{Z}$  is a prime number and  $f \in \mathbb{Z}[x]$  is a monic polynomial which is irreducible modulo  $p$ .

As in the  $\mathbb{C}[x, y]$  case, the zero ideal is the two-dimensional generic point of the surface, the principal ideals are the one-dimensional points corresponding to curves, and the maximal ideals (those with two generators) are the “usual” zero-dimensional closed points.