Something Something

Fmoc

November 12, 2024

There are something I should have learnt back in my first two years as an undergraduate.

1 Polynomials

1.1 Resultant and Discriminant

Let K be a field. We want to know when are two polynomials $f, g \in K[X]$ coprime.

Lemma 1.1. $(f, g) \neq 1 \iff \exists u, v \in K[X] \setminus \{0\}$ s.t. $\begin{cases} fu = gv, \\ \deg u < \deg g, \ \deg v < \deg f. \end{cases}$

Proof. If $(f, g) \neq 1$, then put $u = g/(f, g)$, $v = f/(f, g)$.

If $(f, g) = 1$ and $fu = gv$, then $u \mid g$, $v \mid f$, so $g/u = f/v$ divides $(f, g) = 1$, meaning $u = g, v = f$. □

Now assume $fu = gv$ for some $u, v \in K[X]$ with $\deg u < \deg g, \deg v < \deg f$. Lemma 1.1 shows that, $(f, g) \neq 1$ iff $fu = gv$ has nonzero solution. This is a linear equation in the K-vector space $K \oplus KX \oplus \cdots \oplus KX^{m+n-1}$, and it has a nonzero solution iff and only if the discriminant is zero.

Definition 1. Let A be a commutative ring, $f, g \in A[X]$. We define the **resultant** of $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{j=0}^{m} b_j X^j$ to be[1]

$$\operatorname{res}_X(f, g) := \begin{vmatrix} \begin{matrix} \\ m \\ \\ \\ \end{matrix} \left\{ \begin{matrix} a_n & \cdots & a_0 & & & \\ & a_n & \cdots & a_0 & & \\ & & & \ddots & & \\ & & & a_n & \cdots & a_0 \end{matrix} \right. \\ \begin{matrix} \\ n \\ \\ \\ \end{matrix} \left\{ \begin{matrix} b_m & \cdots & b_0 & & & \\ & b_m & \cdots & b_0 & & \\ & & & \ddots & & \\ & & & b_m & \cdots & b_0 \end{matrix} \right. \end{vmatrix},$$

a determinant of an $(n + m) \times (n + m)$-matrix over A.

So we can rephrase Lemma 1.1 into: $f, g \in K[X]$ are coprime if and only if their resultant $\operatorname{res}_X(f, g) \neq 0$.

Now assume that both f and g split in K. Then $(f, g) \neq 1 \iff f$ and g share at least one same root. This suggests that $\operatorname{res}_X(f, g)$ should be divided by *all* $x - y$, where x is a root of f and y is a root of g; multiplicity are considered here.

[1] Of course, we require $\deg f = n$ and $\deg g = m$.

Theorem 1. If $f = \sum_{i=0}^n a_i X^i = \prod_{i=1}^n (X - x_i)$ and $g = \sum_{j=0}^m b_j X^j = \prod_{j=1}^m (X - y_j)$, are polynomials that splits in K, then

$$\text{res}_X(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j).$$

In particular, we can study if a polynomial has multiple roots (in its splitting field) using resultant.

Definition 2. Let A be a commutative ring and $f(X) = a_n X^n + \cdots + a_0 \in A[X]$. The **discriminant** of f is

$$\text{disc}(f) := \frac{(-1)^{\frac{1}{2}n(n-1)}}{a_n} \text{res}_X(f, f') \in A,$$

where $f'(X) = na_n X^{n-1} + \cdots + a_1$ is the derivative of f.

Note that $\text{res}_X(f, f')$ is a multiple of a_n, because its first column is ${}^t(a_n \ 0 \ \cdots \ 0 \ na_n \ 0 \ \cdots \ 0)$, and we require $a_n \neq 0$. Thus $\text{disc}(f)$ is well-defined.

So f has multiple roots iff $\text{disc}(f) = 0$.

Example 1. (1) If $f(X) = aX^2 + bX + c$, then $\text{disc}(f) = -\frac{\text{res}_X(f, f')}{a} = b^2 - 4ac$.

(2) If $f(X) = X^3 + pX + q$, then $\text{disc}(f) = -\text{res}_X(f, f') = -(4p^3 + 27q^2)$.

Proposition 1.1. Let $f(X) = a_n X^n + \cdots + a_0 \in K[X]$, then

$$\text{disc}(f) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2,$$

where $x_1, \ldots, x_n$ are all the roots of f in a fixed splitting field with multiplicity counted.

Proof. By Theorem 1,

$$\text{res}_X(f, g) = a_n^m \prod_{i=1}^n g(x_i).$$

Use this to compute. □

2 Elementary Number Theory

2.1 Valuation of Binomial Coefficients

Proposition 2.1. Let $n \in \mathbb{Z}_{\geq 1}$, then

$$v_p(n!) = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Proof. Think and you'll find it trivial. □

Corollary 2.1. Let $a, b \in \mathbb{Z}_{\geq 1}$, then
.

$$v_p\left(\binom{a+b}{b}\right) = \sum_{i \geq 1} \left(\left\lfloor \frac{a+b}{p^i} \right\rfloor - \left\lfloor \frac{a}{p^i} \right\rfloor - \left\lfloor \frac{b}{p^i} \right\rfloor \right).$$ □

Corollary 2.2 (Kummer). Expand $a, b \in \mathbb{Z}_{\geq 1}$ in base p, then

$$v_p\left(\binom{a+b}{b}\right) = \text{\# of carries when compute } a+b \text{ in base } p.$$

Proof. Note that if $n = \sum_{i \geq 0} n_i p^i$ for $0 \leq n_i \leq p-1$, then

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - (n_0 + n_1 p + \cdots + n_{i-1} p^{i-1})}{p^i}.$$

By definition, there is a carry at p^i in $a + b$ means that

$$(a_0 + a_1 p + \cdots + a_{i-1} p^{i-1}) + (b_0 + b_1 p + \cdots + b_{i-1} p^{i-1}) \geq p^i.$$

So Proposition 2.1 gives the result. $\square$