Lec17B Factorization in Z[x] Michael Monagan

March 16, 2021 12:35 PM

# 8.7 Factorization in $\mathbb{Z}[x]$.

Given $a \in \mathbb{Z}[x] \setminus \mathbb{Z}$ find the irreducible factorization over $\mathbb{Z}$.

Eg.

Over $\mathbb{Z}$ $\quad x^4-4 = (x^2-2)(x^2+2)$

Over $\mathbb{R}$ $\quad x^4-4 = (x-\sqrt{2})(x+\sqrt{2})(x^2+2)$.

Consider $a = 36x^6 - 4x^2 = 4\cdot(9x^6 - x^2) = 4\cdot(9x^4-1)\cdot x^2$

content; do not factor; ?? $\quad (3x^2-1)(3x^2+1)$

Before 1970 polynomial factorization used integer factorization.

$a = 9x^4-1 \stackrel{?}{=} (3x^2-1)(3x^2+1)$

$x=10$ $\quad x-3 \quad x+3 \quad 2x+3 \quad 4x+3 \quad \times$

$a(10) = 8\,9999 = 7 \cdot 13 \cdot 23 \cdot 43$

$7\cdot 13 = 91 = 100-10+1 \longrightarrow x^2-x+1$

$7\cdot 23 = 161 = 200-40+1 \longrightarrow 2x^2-4x+1$

$7\cdot 43 = 301 = 300+1 \longrightarrow 3x^2+1$ ✓

$a(11) = 131768 = 2^3\cdot 7\cdot 13\cdot 181$ 6 factors → more combos.

✓ $a(12) = 186623 = 431\cdot 433$

Method is intractible — factorization over $\mathbb{Z}$.

Let $a \in \mathbb{Z}[x]$, $\text{cont}(a)=1$, $\gcd(a,a')=1$, $a = f_1\cdot f_2 \cdots f_e$ where $f_i$ is irreducible over $\mathbb{Z}$.

Factor $a$ mod $p$;

Let $p$ be a prime and suppose we factor $\phi_p(a)$ over $\mathbb{Z}_p$. Then

$\phi_p(a = f_1 f_2 \cdots f_e) = \phi_p(f_1)\cdot\phi_p(f_2)\cdot\cdots\cdot\phi_p(f_e)$

Factoring $\quad g_1\cdot g_2 \quad g_3\cdot g_4\cdot g_5 \quad g_{11}$

Eg. $a = 9x^4 - 1 = (3x^2-1)(3x^2+1)$ $\ell = 2$

$p=5 \quad = (3x^2-1)(3x^2+1)$

$p=7 \quad = (3x^2-1)\cdot 3(x-3)(x+3)$

× $p=3 \quad = 2$

**Lemma.** If $p \nmid lc(a)$, then # factors over $\mathbb{Z}_p \geq \ell$.

Let $D_p(a)$ be the set of possible degrees of factors of $a \in \mathbb{Z}[x]$ inferred from the factorization of $a$ over $\mathbb{Z}_p$.

Eg. $a = 85x^5 + 55x^4 + 37x^3 + 35x^2 - 97x - 50$ ?

$D_p(a)$ possible degrees of $a$.

$p=2 \quad a = (x+1)(x^4+x^3+x^2+x+1)$ $\{1,4,5\}$

$p=3 \quad a = (x+1)(x^4+x^2+x+1)$ $\{1,4,5\}$

× $p=5 \quad a = 0 \cdot x^4$

$p=7 \quad a = (x^2+5x+5)(x^3+6x+4)$ $\{2,3,5\}$

Now $\cap D_p(a) = \{5\} \Rightarrow a$ is irreducible over $\mathbb{Z}$.

Mignotte factor bound:

$f \mid a \Rightarrow \|f\|_\infty \leq 2^d \sqrt{d+1}\, \|a\|_\infty$

$p^n \geq 2 \cdot \|f\|_\infty \leq \lfloor 2 \cdot 2^4 \sqrt{5} \cdot 5 \rfloor = 357.$

$p^4 = 5^4 = 625 > 357.$

Eg. $a = 1x^4 + 5x^2 + 4 = ??$

$p=5 \quad a = (x-2)(x+2)(x-1)(x+1)$

Set $u_0 = x-2 \quad w_0 = (x+2)(x-1)(x+1)$

Lift $a - u_0 w_0 \equiv 0 \pmod p$ to $a - u^{(n)} w^{(n)} \equiv 0 \pmod{p^n}$ using H.L.

Similarly lift $u_0 = x+2$, $u_0 = x-1$, $u_0 = x+1$ and lift them.

Obtain $a = 1 \cdot (x-182)(x+82)(x-361)(x+361)$ mod $p^4$.

Test if $x-182$, $x+182$, $x-261$, $x+261$ divide $a$? None do.

$\Rightarrow a$ has no linear factor.

Test if products of pairs of these four factors mod 625 divide $a$?

$f_1 = (x-182)(x+182) = x^2 + 1 \pmod{625}$.

We find $x^2+1 \mid a$. $a \leftarrow a/f_1 = x^2+4$.

Since $x^2+4$ has no linear factor it's irreducible.

Output $(x^2+1)(x^2+4)$.