L lattice in $\mathbb{R}^n$,

with a given basis having $\le t$-bit integers as entries.

Can find in time $\text{poly}(n,t)$ a $2^{O(n)}$-approximate shortest vector.

Suppose $\alpha \in \mathbb{C}$ is a root of some irreducible polynomial $P(X) \in \mathbb{Z}[X]$. Given $\tilde{\alpha}$ s.t. $|\tilde{\alpha} - \alpha| \le 2^{-t}$. Let us try to find $P(X)$. Suppose all coefficients of $P(X)$ are $\le r$-bit integers.

deg d

We will see how to find $P(X)$ when t is big enough in terms of d, r.

Suppose $\alpha_0 \in \mathbb{C}$ s.t. $P(\alpha_0) = 0$. $\deg \le d$
$P(X) \in \mathbb{Z}[X]$

each coeff $\le U$.

Suppose $\beta_0 \in \mathbb{C}$ s.t. $Q(\beta_0) = 0$ deg $\le d$

$Q(x) \in \mathbb{Z}[x]$

each coeff $\le U$.

If $\alpha_0 \neq \beta_0$

then $|\alpha_0 - \beta_0| \gg$ —.

$$\mathrm{Res}(P,Q) = \det \begin{bmatrix} & & \\ & \text{coeffs of } P, Q. & \\ & & \end{bmatrix}$$

$$= \prod_{\substack{\text{roots } \alpha \text{ of } P \\ \beta \text{ of } Q}} (\alpha - \beta) \neq 0 \text{ if } P, Q \text{ irreducible distinct.}$$

$$1 \le |\mathrm{Res}(P,Q)| \le U^{2d} \cdot (2d)!$$

All roots of P, Q are at most $d \cdot U$.

So $$\left| \left[\prod_{\substack{\alpha,\beta \\ (\alpha,\beta) \neq (\alpha_0,\beta_0)}} (\alpha - \beta) \right] \cdot (\alpha_0 - \beta_0) \right| \ge 1$$

$$|\alpha_0 - \beta_0| \ge \frac{1}{\cdot d^2}$$

$(dU)^n$

Plan Find $a_0, a_1, \ldots a_d$ s.t.

$$\left|\sum a_i (\tilde{\alpha})^i\right| \quad \boxed{\text{very small.}} \quad -(*)$$

$a_0, a_1, \ldots, a_d \in \mathbb{Z}$ are not too big.

Then claim that

$$\boxed{\sum a_i \alpha^i = 0.}$$

If we found $r(X) = \sum a_i X^i$

s.t. $a_i \in \mathbb{Z}$,

$|a_i| \leq U$

$r(\tilde{\alpha}) \leq \epsilon$

Want to say: $r(\alpha)$ is quite small.

$$|r(\alpha)| \leq |r(\tilde{\alpha})| + |\alpha - \tilde{\alpha}| \cdot U d^2 \left(\max(|\alpha|, |\tilde{\alpha}|)\right)^d$$

$$\leq \epsilon + 2^{-t} \cdot \left(1 + 2U d^2 (1 + |\alpha| + |\tilde{\alpha}|)\right)^d$$

$$\leq \epsilon + 2^{-t} \left(1 + \text{poly}(U, d)\right)^d$$

If $\gamma(\alpha)$ is quite small,

then $\gamma(\alpha) = 0$.

Let $P(x)$ be the minimal poly of α.

Let α_i be the other roots.

Then $\left(\prod_i \gamma(\alpha_i) \right) \cdot \gamma(\alpha) \in \mathbb{Z}$.

(bounded)

$$= \left[\prod_i \left(\prod_{\substack{\text{Roots} \\ \beta \text{ of } \gamma(x)}} (\alpha_i - \beta) \right) \right] \cdot \left(\prod_{\beta} (\alpha - \beta) \right)$$

$$= \operatorname{Res}(P(x), \gamma(x)) \in \mathbb{Z}.$$

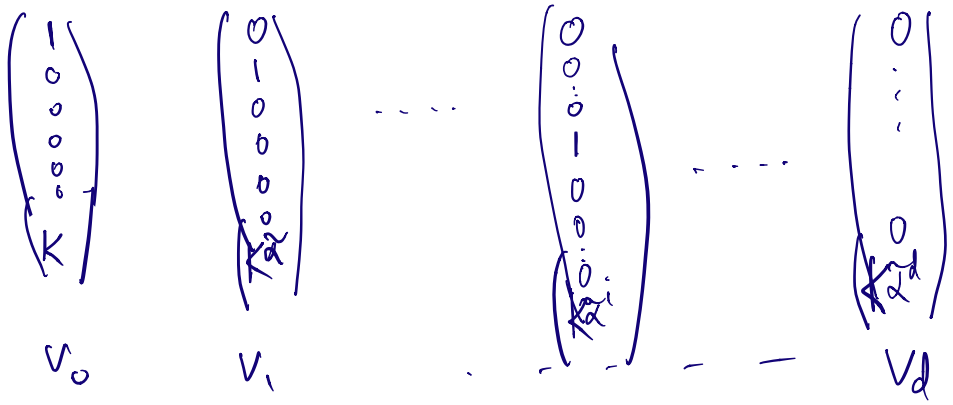
If $\gamma(\alpha) \neq 0$, then all $\gamma(\alpha_i) \neq 0$,

and so $\prod(\gamma(\alpha_i)) \cdot \gamma(\alpha) \geq 1$

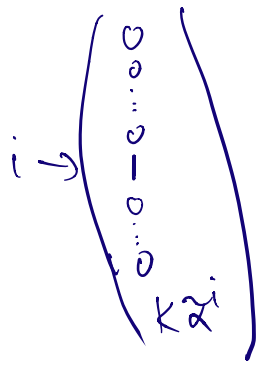
But $\gamma(\alpha) \geq \frac{1}{\prod \gamma(\alpha_i)}$

and $r(2) \leq$ quite small.

Finding a $r(X) \in \mathbb{Z}[X]$ with small coeffs.
s.t. $r(2)$ is very small.



$d+1$ vectors in $\mathbb{R}^{d+1}$.

$v_i =$ 

Consider lattice L generated by the v_i.

The vector $\sum a_i v_i$ looks like:

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \\ \underline{K} \cdot \sum a_i \tilde{\alpha}^i \end{pmatrix} \in \mathbb{R}^{d+2}.$$

We know that there is a nonzero vector of length $\leq \sqrt{(d+1)U^2 + \left(K \cdot d \cdot U \cdot 2^{-t}\right)^2} = \lambda$ in this lattice.

(+)

LLL gives us a quite short vector, namely, $a_0, \ldots a_d$ s.t.

each $a_i \leq 2^{O(d)} \cdot \lambda$

and $K \cdot \left|\sum a_i \tilde{\alpha}^i\right| \leq 2^{O(d)} \cdot \lambda.$

i.e. $\left|\left(\sum a_i \tilde{\alpha}^i\right)\right| \leq \frac{2^{O(d)} \cdot \lambda}{K}.$

Choose K so that $\frac{2^{O(d)} \cdot \sqrt{(d+1)v^2+1}}{K}$

is very small. (*).

Choose t so that. (+) ≤ 1.

Then we can find the suitable $V(x)$ that very small on $\tilde{\alpha}$, and so quite small on α, and so 0 on α.

Runtime: Poly (d, r), needs $t = \text{poly}(d,r)$

Factoring polynomials over $\mathbb{Q}$.

Given $P(x) \in \mathbb{Q}[x]$.

Want to factor into irreducibles in $\mathbb{Q}[X]$.

Step 0 Get rid of multiple roots. via GCD with $p'(x)$.

Step 1 Find all roots in $\mathbb{C}$, to t bits of precision.

Step 2 For each root, find the minimal polynomial (knowing that it has small coefficients).