p_j, ϕ nicht eindeutig

Wähle $p_j \in \mathbb{Z}[X]$, zu geg. $(p_1, \dots, p_r)$ normiere ϕ via $a_j(1) = 1$.

Satz: $\exists \mathcal{O}_j \subseteq K_j$: $a_j(\ell) \in \mathcal{O}$ $\forall \ell$.
(1 Ordng)

Folgerung: Es gilt $N_j \in \mathbb{Z}_{>0}$ mit $N_j a_j(\ell) \in \mathbb{Z}[X \bmod p_j]$ $(\ell = 1, 2, \dots)$

(denn $\exists N_j : N_j \mathcal{O}_j \subseteq \mathbb{Z}[X \bmod p_j]$)

Also gilt es insbesondere N_j mit $\{N_j a_j(\ell)\}_{\ell \le d_p}$ Erz. von $\mathbb{Z}[X]$.

Problem: K Zahlkörper. Gilt es ein "kanonisches" normiertes $p \in \mathbb{Z}[X]$ mit $K \simeq \mathbb{Q}[X]/(p)$?

vorl. Antwort (H. Cohen): Wähle das p mit $\sum_{\substack{\alpha \in \mathbb{C} \\ p(\alpha)=0}} |\alpha|^2 = \underline{\min}$!

nicht völlig 1-deutig, aber dadurch Koeffizienten von p im gewissen Sinne klein; vernünftig zu Rechnung in K, LLL-Algorithmus um von geg. $\hat{p}$ zu p zu kommen

polred ( ) in Pari

Problem: Wie eindeutig ist p? (nur Abänderung mod Einheitswurzeln?)

Algorithmen zur Berechnung der p_j, $a_j(\ell)$

1) Thetareihen

Basis für $M_k(m, \chi)$ mit Thetareihen:

Hijikata/Pizer/Shemanske: "The basis problem for mod. forms on $\Gamma_0(N)$"
((Con. Math ?, AMS)

Beispiel

Satz Sei p Primzahl, Sei Q die Quat-Algebra, die genau bei p, ∞ verzweigt ist, sei $\mathcal{O}$ eine Max Ordnung in Q, $L_1, \dots, L_h$ Vertretersystem für $\mathcal{O}$-Linksideal (mod rechts-Mult mit $Q^\times$). Dann ist

$$\Theta_{L_j} := \sum_{\alpha \in L_j} q^{n(\alpha)/(\mathcal{O}:L_j)} \qquad (1 \le j \le h)$$

Basis von $M_2(p)$. $\qquad (n() = \text{Norm})$