Carl Witty 2007

$\overline{\mathbb{Q}}$ QQbar

$\mathbb{R} \cap \overline{\mathbb{Q}}$ AA

SR = symbolic ring. ginac

reset('QQbar')

$\mathbb{Q}(\zeta_n)$ .roots(ring=____)

$((x^2-2)^2)$.roots(ring=QQbar)

α = (f(x), interval)

$f(x) \in \mathbb{Z}[x]$ see 1.414...?

P

x(P) = P[0]

y(P) = P[1]

b = QQbar(sqrt(2)) + QQbar(sqrt(3))

QQ[b]

(a, b)

real root isolation

$\begin{bmatrix} * & * & * \\ * & * & * \end{bmatrix}$

$(S_2 + S_3 + S_5 + S_7)^{-1}$

$(\mathbb{Z}/3\mathbb{Z})^{\oplus 2} \approx E(\bar{\mathbb{Q}})[3] = \{P \in E(\bar{\mathbb{Q}}) : 3P = P+P+P = O\}$

$\approx$  $\approx$ 

% time

$E = E_{\mathbb{Q}}$

$P \in E(\mathbb{Q})$

$P+P$

$E: y^2 = x^3 + x + 5$

$E(\mathbb{Q}) \approx \mathbb{Z}^r \oplus T$

$r = \text{rank}(E)$

E.division_polynomial(3)

E.lift_x( )

arithmetic

NTL C++

Victor Shoup

ZZX...

PARI

K.embeddings(QQbar)

C++ C._add_ ?? —

.pyx = Cython code

.pxd

.pyx

cdef int a —