AMSI SUMMER RESEARCH SCHOLARSHIPS 2024–25

Get a TASTE for Research this Summer

Modular Algorithms in Quadratic Algebraic Number Fields

Mitchell Holt

Supervised by Dr Paul Vrbik

The University of Queensland

AMSI AUSTRALIAN MATHEMATICAL SCIENCES INSTITUTE

AMSI CONNECT

Computer Algebra

Theorem (Chinese Remainder Theorem (CRT))

Essentially... there is a u satisfying

$$\begin{aligned} u &\equiv u_1 \pmod{m_1}, \\ &\vdots \\ u &\equiv u_n \pmod{m_n}, \end{aligned}$$

when m_i and m_j are coprime.

Proof sketch.

$$\begin{aligned}\phi : \mathbb{Z}_{m_1 \cdots m_n} &\to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n} \\ u &\mapsto (u \mod m_1, \ldots, u \mod m_n)\end{aligned}$$

is an isomorphism. $\square$

Find u with

$$
\begin{aligned}
u &\equiv 49 \pmod{32771},\\
u &\equiv -21 \pmod{65537},\\
u &\equiv -30 \pmod{131101}.
\end{aligned}
$$

$$u = v_0 + v_1(m_1) + v_2(m_1 m_2) + \cdots + v_{n-1}\Big(\prod_{i=1}^{n-1} m_i\Big)$$

$$-104905043721354 = 49 - 28(32771) - 48845(32771 \cdot 65537)$$

Modular Algorithms

$$
\begin{aligned}
22x + 44y + 74z &= 1,\\
15x + 14y - 10z &= -2,\\
-25x - 28y + 20z &= 34.
\end{aligned}
$$

Fraction-free Gaussian elimination:

$$
\begin{aligned}
1257315840x &= 7543895040, \\
-57150720y &= 314328960, \\
162360z &= 243540.
\end{aligned}
$$

$$
\left\{ x = 6, \qquad y = -\frac{11}{2}, \qquad z = \frac{3}{2} \right\}
$$

Solve $A\vec{x} = \vec{b}$ [TI61],[CL77].

$p_1, \ldots, p_k \leftarrow$ distinct primes

for $i = 1, \ldots, n$ **do**

  $d_i \leftarrow \det A \pmod{p_i}$

  $\vec{x}_i \leftarrow$ solve $A\vec{x} = \vec{b} \pmod{p_i}$

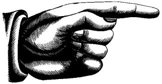
$D \leftarrow$ CRT on $\{d_1 \pmod{p_1}, \ \ldots, \ d_n \pmod{p_n}\}$

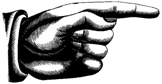
$\vec{y} \leftarrow$ pointwise CRT on $\{d_1 \cdot \vec{x}_1 \pmod{p_1}, \ \ldots, \ d_n \cdot \vec{x}_n \pmod{p_n}\}$

return $\frac{1}{D} \cdot \vec{y}$

Modular linear solver:

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{-7380}\begin{bmatrix} -44280 \\ 40590 \\ -11070 \end{bmatrix} = \begin{bmatrix} 6 \\ -11/2 \\ 3/2 \end{bmatrix}$$

$\mathbb{Q}$  $\mathbb{Z}$

$\mathbb{Q}(\sqrt{M})$  ?

Quadratic Integers

Let $M \in \mathbb{Z}$ be *squarefree*. The *quadratic integers* of $\mathbb{Q}(\sqrt{M})$ are

$$R = \begin{cases} \mathbb{Z}[\sqrt{M}] & M \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{M}}{2}] & M \equiv 1 \pmod 4 \end{cases}$$

[Mar77]. Write $R = \mathbb{Z}[\gamma]$.

- What are the primes?
- Are any primes $p \in \mathbb{Z}$ also prime in R (*inert*)?

Chebotarëv Density Theorem implies infinitely many inert primes.

Algorithm: ([IR13] Proposition 5.2.2)

- Input: Set of odd primes P.
- Output: An odd inert prime not contained in P.

Proposition

Let $p \in \mathbb{Z}$ be an inert prime in $R = \mathbb{Z}[\gamma]$. Then

$$R/pR \simeq \begin{cases} \mathbb{Z}_p[x]/\langle x^2 - M \rangle & M \equiv 2, 3 \pmod 4 \\ \mathbb{Z}_p[x]/\langle x^2 - x - \frac{M-1}{4} \rangle & M \equiv 1 \pmod 4 \end{cases}$$

Moreover, the isomorphism is given by

$$\phi([a + b\gamma]) = [a + bx].$$

Modular Algorithms in $\mathbb{Q}(\sqrt{M})$

- Use Garner's integer CRT algorithm in $\mathbb{Z}[\gamma]$ (for inert primes).
- Use the same modular linear solver!

- No unique factorisation in R.
- No GCD.

- Rational reconstruction $\mathbb{Z}_k[\gamma] \rightsquigarrow \mathbb{Q}[\gamma] = \mathbb{Q}(\sqrt{M})$.

Solve $Ax = b$, where:

$$A = \begin{pmatrix} 81 - 19\sqrt{122} & 78 - 89\sqrt{122} & -81 - 80\sqrt{122} \\ 22 - 53\sqrt{122} & -8 + 66\sqrt{122} & -43 - 19\sqrt{122} \\ 50 - 30\sqrt{122} & -90 + 154\sqrt{122} & -2 - 124\sqrt{122} \end{pmatrix}, \quad b = \begin{pmatrix} 26851 - 2700\sqrt{122} \\ -41098 + 883\sqrt{122} \\ -67029 + 1076\sqrt{122}. \end{pmatrix}$$

$$x = \begin{pmatrix} \frac{5\sqrt{122}}{2} \\ \frac{33}{2} - 3\sqrt{122} \\ 15 \end{pmatrix}$$

- Fraction-free Gaussian elimination: 105-bit integers
- Modular solver: 57-bit integers (seven 16-bit primes)

AMSI SUMMER RESEARCH SCHOLARSHIPS 2024–25

Get a TASTE for Research this Summer

AMSI AUSTRALIAN MATHEMATICAL SCIENCES INSTITUTE

Jane Street®

AMSI CONNECT

[CL77] S Cabay and TPL Lam. Congruence techniques for the exact solution of integer systems of linear equations. *ACM Transactions on Mathematical Software (TOMS)*, 3(4):386–397, 1977.

[IR13] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer Science & Business Media, 2013.

[Mar77] D.A. Marcus. *Number Fields*. Springer-Verlag, 1977.

[TI61] H Takahasi and Y Ishibashi. A new method for ‘exact computation’ by a digital computer. In *Inf. Processing in Japan*, pages 28–42, 1961.