Solving Linear Systems over Cyclotomic Fields

Michael Monagan

Centre for Experimental and Constructive Mathematics

This is joint work with Liang Chen

The Problem

Let $\beta \in \mathbb{C}$ be a primitive k'th root of unity.
Solve $Ax = b$ where $A_{i,j}, b_i \in \mathbb{Q}(\beta)$.

The minimial polynomial $m(z) \in \mathbb{Q}[z]$ for β is $\Phi_k(z)$.

k	$\Phi_k(z)$	β
3	$z^2 + z + 1$	$\frac{-1 \pm \sqrt{3}i}{2}$
4	$z^2 + 1$	i
5	$z^4 + z^3 + z^2 + z + 1$	$0.308 + 0.951i$
6	$z^2 - z + 1$	$\frac{1 \pm \sqrt{3}i}{2}$

Table 1: cyclotomic polynomials of order 3–6

Example

$$M = z^2 + z + 1$$

$$A^{196\times 196} = \begin{bmatrix} \frac{109}{91}z - \frac{121}{182}z^2 & \frac{545}{182}z - \frac{549}{182}z^2 & \cdots \\ \frac{423}{182}z + \frac{239}{182}z^2 & \frac{109}{182}z + \frac{41}{182}z^2 & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix} \qquad b^{196} = \begin{bmatrix} 0 \\ -1 \\ \vdots \end{bmatrix}$$

Solution vector:

$$x = \begin{bmatrix} -\frac{1930284204975579779630929442118373}{837637134068527924278537117122285} + \frac{2935300154370011316891737244428409}{1675274268137055848557074234245570}z \\ \frac{12571286321434144031398874118677591}{23453839753918781879799039279439800} + \frac{17053490612784949844035930047310893 1}{23453839753918781879799039279439800}z \\ \vdots \end{bmatrix}$$

A Modular Algorithm

Theorem
Let $m(z) = \Phi_k(z)$ and $d = \deg m = \phi(k)$.
Let p be a randomly chosen prime. Then

> Prob($m(z)$ splits modulo p) $\sim 1/d$.
> Moreover, $m(z)$ splits iff $p = kq + 1$.

Example

```
> m := numtheory[cyclotomic](5,z);
```

$$m := z^4 + z^3 + z^2 + 1$$

```
> mods( Factor(m), 11 );
```

$$(z-5)(z-4)(z-3)(z+2)$$

Chinese Remaindering

Input: $A \in R^{n\times n}$, $b \in R^n$, $m \in R$, $R = \mathbb{Z}[z]$
Output: $x \in \mathbb{Q}^n[z]$ satisfying $Ax \equiv b \bmod m(z)$

1: Set $X = 0, P = 1$ and $x = \mathrm{FAIL}$.
2: **for** $j = 1, 2, 3, ...$ **do**
3: Find a new machine prime $p_j = kq + 1$.
4: Compute the roots $\alpha_1, .., \alpha_d$ of $m(z)$ mod p_j.
5: Reduce the integers in A and b mod p_j
6: **for** $i = 1, 2, 3, ..., d$ **do**
7: Evaluate A and b at $z = \alpha_i$
8: Solve $A(\alpha_i)x_{i,j} = b(\alpha_i)$ for $x_{i,j} \in \mathbb{Z}_{p_j}^n$
9: If $A(\alpha_i)$ is singular **GOTO** Step 3.
10: **end for**
11: Interpolate $x_j(z) \in \mathbb{Z}p_j[z]$ from $(\alpha_1, x_{1,j}), ..., (\alpha_d, x_{d,j})$
12: Set X = CRT($[X, x_j], [P, p_j]$) and $P = P \times p_j$
13: If $j \in \{1, 2, 4, 8, \cdots\}$ set *x* = RR($X \mod P$)
14: If $x \neq FAIL$ and $m|Ax - b$ output x.
15: **end for**

Chinese Remaindering

Input: $A \in R^{n\times n}$, $b \in R^n$, $m \in R$, $R = \mathbb{Z}[z]$
Output: $x \in \mathbb{Q}^n[z]$ satisfying $Ax \equiv b \bmod m(z)$

1: Set $X = 0, P = 1$ and $x = \text{FAIL}$.
2: **for** $j = 1, 2, 3, \ldots$ **do**
3:     Find a new machine prime $p_j = kq + 1$.
4:     Compute the roots $\alpha_1, .., \alpha_d$ of $m(z)$ mod p_j.
5:     Reduce the integers in A and b mod p_j
6:     **for** $i = 1, 2, 3, \ldots, d$ **do**
7:         Evaluate A and b at $z = \alpha_i$
8:         Solve $A(\alpha_i)x_{i,j} = b(\alpha_i)$ for $x_{i,j} \in \mathbb{Z}_{p_j}^n$
9:         If $A(\alpha_i)$ is singular **GOTO** Step 3.
10:     **end for**
11:     Interpolate $x_j(z) \in \mathbb{Z}p_j[z]$ from $(\alpha_1, x_{1,j}), \ldots, (\alpha_d, x_{d,j})$
12:     Set X = CRT($[X, x_j], [P, p_j]$) and $P = P \times p_j$
13:     If $j \in \{1, 2, 4, 8, \cdots\}$ set x = RR($X \mod P$)
14:     If $x \neq FAIL$ and $m|Ax - b$ output x.
15: **end for**

Chinese Remaindering

Input: $A \in R^{n\times n}$, $b \in R^n$, $m \in R$, $R = \mathbb{Z}[z]$
Output: $x \in \mathbb{Q}^n[z]$ satisfying $Ax \equiv b \bmod m(z)$

1: Set $X = 0, P = 1$ and $x = \mathrm{FAIL}$.
2: **for** $j = 1, 2, 3, \ldots$ **do**
3: Find a new machine prime $p_j = kq + 1$.
4: Compute the roots $\alpha_1, .., \alpha_d$ of $m(z)$ mod p_j.
5: Reduce the integers in A and b mod p_j
6: **for** $i = 1, 2, 3, ..., d$ **do**
7: Evaluate A and b at $z = \alpha_i$
8: Solve $A(\alpha_i)x_{i,j} = b(\alpha_i)$ for $x_{i,j} \in \mathbb{Z}_{p_j}^n$
9: If $A(\alpha_i)$ is singular **GOTO** Step 3.
10: **end for**
11: Interpolate $x_j(z) \in \mathbb{Z}p_j[z]$ from $(\alpha_1, x_{1,j}), ..., (\alpha_d, x_{d,j})$
12: Set X = CRT($[X, x_j], [P, p_j]$) and $P = P \times p_j$
13: If $j \in \{1, 2, 4, 8, \cdots\}$ set *x* = RR($X \mod P$)
14: If $x \neq FAIL$ and $m|Ax - b$ output x.
15: **end for**

Chinese Remaindering

Input: $A \in R^{n \times n}$, $b \in R^n$, $m \in R$, $R = \mathbb{Z}[z]$
Output: $x \in \mathbb{Q}^n[z]$ satisfying $Ax \equiv b \bmod m(z)$

1: Set $X = 0, P = 1$ and $x = \mathrm{FAIL}$.
2: **for** $j = 1, 2, 3, ...$ **do**
3: Find a new machine prime $p_j = kq + 1$.
4: Compute the roots $\alpha_1, .., \alpha_d$ of $m(z)$ mod p_j.
5: Reduce the integers in A and b mod p_j
6: **for** $i = 1, 2, 3, ..., d$ **do**
7: Evaluate A and b at $z = \alpha_i$
8: Solve $A(\alpha_i)x_{i,j} = b(\alpha_i)$ for $x_{i,j} \in \mathbb{Z}_{p_j}^n$
9: If $A(\alpha_i)$ is singular **GOTO** Step 3.
10: **end for**
11: Interpolate $x_j(z) \in \mathbb{Z}p_j[z]$ from $(\alpha_1, x_{1,j}), ..., (\alpha_d, x_{d,j})$
12: Set X = CRT($[X, x_j], [P, p_j]$) and $P = P \times p_j$
13: If $j \in \{1, 2, 4, 8, \cdots\}$ set x = RR($X \mod P$)
14: If $x \neq FAIL$ and $m | Ax - b$ output x.
15: **end for**

Chinese Remaindering

Input: $A \in R^{n \times n}$, $b \in R^n$, $m \in R$, $R = \mathbb{Z}[z]$

Output: $x \in \mathbb{Q}^n[z]$ satisfying $Ax \equiv b \bmod m(z)$

```
1: Set X = 0, P = 1 and x = FAIL.
2: for j = 1, 2, 3, ... do
3:     Find a new machine prime p_j = kq + 1.
4:     Compute the roots α_1, .., α_d of m(z) mod p_j.
5:     Reduce the integers in A and b mod p_j
6:     for i = 1, 2, 3, ..., d do
7:         Evaluate A and b at z = α_i
8:         Solve A(α_i)x_{i,j} = b(α_i) for x_{i,j} ∈ Z_{p_j}^n
9:         If A(α_i) is singular GOTO Step 3.
10:    end for
11:    Interpolate x_j(z) ∈ Zp_j[z] from (α_1, x_{1,j}), ..., (α_d, x_{d,j})
12:    Set X = CRT([X, x_j], [P, p_j]) and P = P × p_j
13:    If j ∈ {1, 2, 4, 8, ···} set x = RR(X mod P)
14:    If x ≠ FAIL and m|Ax − b output x.
15: end for
```

Chinese Remaindering

Input: $A \in R^{n \times n}$, $b \in R^n$, $m \in R$, $R = \mathbb{Z}[z]$

Output: $x \in \mathbb{Q}^n[z]$ satisfying $Ax \equiv b \bmod m(z)$

```
1:  Set X = 0, P = 1 and x = FAIL.
2:  for j = 1, 2, 3, ... do
3:      Find a new machine prime p_j = kq + 1.
4:      Compute the roots α_1, .., α_d of m(z) mod p_j.
5:      Reduce the integers in A and b mod p_j
6:      for i = 1, 2, 3, ..., d do
7:          Evaluate A and b at z = α_i
8:          Solve A(α_i) x_{i,j} = b(α_i) for x_{i,j} ∈ Z_{p_j}^n
9:          If A(α_i) is singular GOTO Step 3.
10:     end for
11:     Interpolate x_j(z) ∈ Zp_j[z] from (α_1, x_{1,j}), ..., (α_d, x_{d,j})
12:     Set X = CRT([X, x_j], [P, p_j]) and P = P × p_j
13:     If j ∈ {1, 2, 4, 8, ···} set x = RR(X mod P)
14:     If x ≠ FAIL and m | Ax − b output x.
15: end for
```

Chinese Remaindering

Input: $A \in R^{n\times n}$, $b \in R^n$, $m \in R$, $R = \mathbb{Z}[z]$

Output: $x \in \mathbb{Q}^n[z]$ satisfying $Ax \equiv b \bmod m(z)$

.... $n = \dim A,\ d = \deg m,\ c = \log ||Ab||,\ L =$ # primes.

1: Set $X = 0, P = 1$ and $x = \mathrm{FAIL}$.
2: **for** $j = 1, 2, 3, ...$ **do**
3: Find a new machine prime $p_j = kq + 1$.
4: Compute the roots $\alpha_1, .., \alpha_d$ of $m(z)$ mod p_j.
5: Reduce the integers in A and b mod p_j .... $O(n^2dcL)$
6: **for** $i = 1, 2, 3, ..., d$ **do**
7: Evaluate A and b at $z = \alpha_i$ .... $O(n^2d^2L)$
8: Solve $A(\alpha_i)x_{i,j} = b(\alpha_i)$ for $x_{i,j} \in \mathbb{Z}_{p_j}^n$ .... $O(n^3dL)$
9: If $A(\alpha_i)$ is singular **GOTO** Step 3.
10: **end for**
11: Interpolate $x_j(z) \in \mathbb{Z}p_j[z]$ from $(\alpha_1, x_{1,j}), ..., (\alpha_d, x_{d,j})$ ..... $O(nd^2L)$
12: Set X = CRT($[X, x_j], [P, p_j]$) and $P = P \times p_j$ .... $O(ndL^2)$
13: If $j \in \{1, 2, 4, 8, \cdots\}$ set *x* = RR($X \mod P$) .... $O(ndL^2)$
14: If $x \neq FAIL$ and $m | Ax - b$ output x.
15: **end for** .... $O(ndL(nc + nd + n^2 + L))$.

Splitting $m(z) = \Phi_k(z)$ mod $p = qk + 1$

Lemma: Let $\alpha \in \mathbb{Z}_p$ be a prim. elem. and let $\beta = \alpha^q$. Then

$m(\beta^i) = 0$ for $0 < i < k$ with $\gcd(i, k) = 1$.

How fast can we compute α?

Pick $\alpha \in \mathbb{Z}_p$ at random and compute

$$g := \gcd((x+\alpha)^{(p-1)/2} - 1,\ m(z)) \text{ in } \mathbb{Z}_p[z].$$

If $g \notin \{1, m\}$ split the smaller of $g, m/g$ until we get $x - \beta$.

Theorem: $O(\underbrace{\boxed{\log p\ M(d)}}_{\text{powmod}} + \underbrace{\boxed{\log d\ M(d)}}_{\text{gcd}})$ arith. ops. in $\mathbb{Z}_p$.

= $O(\log p d^2 + d^2)$ using classical poly. arith.

Those trial divisions $m|Ax-b$

Let $D = \mathrm{LCM}_{i=1}^{n}\mathrm{denom}(x_i)$.
Test if $m|A(Dx) - Db$ over $\mathbb{Z}$.

Lemma: Let $N = \max_{i=1}^{n} ||Dx_i||_\infty$ and $P = \Pi p_j$. Then
$P > 2(1 + ||m||_\infty)^{d-1}(D||b|| + ndN||A|| \implies m|Ax - b$.

Proof (idea). We know $m|Ax - b \bmod P$.
Thus if $\underbrace{||A(Dx) - (Db) \bmod m(z)||}_{\text{bound this}} < 2P$ then $m|Ax - b$.

How big can the integers in x be?

For random input, integers in x are nd times longer than those in A, b. Here $n = \dim A$, $d = \deg m(z)$.

Lemma: Let $D = \mathrm{LCM}_{i=1}^{n} \mathrm{denom}(x_i)$. Then

$$D \leq \| m \|_\infty^{d-1} (1 + \| m \|_\infty)^{(n-1)(d-1)d} d^{nd+d} n^{nd/2} \| \mathbf{A} \|^{\mathbf{nd}}$$

For $\| m \|_\infty = 1$, $\log D \in O(nd(\log \| A \| + d \log 2 + \log nd))$.

For $L \in O(ndc)$ where $c = \log \max(\| A \|, \| b \|)$
Cost of Algorithm 1 is $O(\underbrace{n^4 d^2 c}_{\text{solves}} + \underbrace{n^3 d^3 c^2}_{\text{CRT+RR}})$.

Asymptotically fast reconstruction

Given u satisfying $A\mathbf{u} = b$ modulo $P = p_1 p_2 \times ... \times p_j$
next solve $A\mathbf{v} = b$ modulo $Q = p_{j+1} p_{j+2} \times ... \times p_{2j}$.
for v.

To solve $\mathbf{x} \equiv \mathbf{u} \bmod P$ and $\mathbf{x} \equiv \mathbf{v} \bmod Q$ compute

1: $\mathbf{w} = (\mathbf{v} - \mathbf{u}) P^{-1} \bmod Q$.
2: $\mathbf{x} = \mathbf{u} + \mathbf{w} P$.

If we compute $\mathbf{v}$ recursively, using the same method then using only fast integer $\times$ and $\div$ for scalar arithmetic

$$O(ndj^2) \longrightarrow O(nd\,M(j) \;+\; j^2).$$

Cramer's Rule

$$x_i = \frac{\det A^{(j)}}{\det A} \bmod m(z)$$

The factor of d increase in size is due to inverting $\det A$ modulo $m(z)$. But

$$x_i = \boxed{\frac{\det A^{(j)} \bmod m(z)}{\det A \bmod m(z)}} \bmod m(z).$$

Compute

$$N = \det(A^{(j)} \bmod m(z) \in \mathbb{Z}[z] \text{ and}$$
$$D = \det A \bmod m(z) \in \mathbb{Z}[z]$$

using Chinese remaindering and interpolation.

Bounds and costs

Lemma (bounds the number of primes needed)

$$N_\infty \leq d^n(1+\parallel m \parallel_\infty)^{(n-1)(d-1)} \parallel b \parallel \quad \parallel A \parallel^{n-1}$$

$$D_\infty \leq d^n(1+\parallel m \parallel_\infty)^{(n-1)(d-1)} \parallel A \parallel^{n-1}.$$

Size of x goes from $O(n^2d^2c + ...)$ to $O(n^2dc + ...)$.
Number of primes L goes from $O(ndc + ...)$ to $O(nc + ...)$.
Cost : $O(\underbrace{n^3dL}_{\text{solves}} + \underbrace{n^2dcL}_{\text{mod } p} + \underbrace{n^2d^2L}_{\text{eval}} + \underbrace{ndL^2}_{\text{CRT+RR}})$.

OLD($L \in O(ndc)$) : $O(n^3dc(nd + d^2c))$
NEW($L \in O(nc)$) : $O(n^3dc(n + d + c))$.

Timing on Random Systems

$$M := e^6 + e^5 + e^4 + e^3 + e^2 + e + 1$$

n	Coefficient Length c							Remark
	2 digits	4 digits	8 digits	16 digits	32 digits	64 digits	128 digits	
10	1.947	2.185	2.375	2.744	3.623	6.210	15.317	GE
	.050	.097	.183	.418	1.019	2.359	5.685	CRT
	.058	.091	.152	.309	.803	2.084	6.384	$p-$adic
	.009	.011	.016	.021	.037	0.070	0.148	Cramer
20	16.041	17.927	20.759	26.141	37.817	71.288	186	GE
	.167	.347	.727	1.616	4.759	12.149	30.983	CRT
	.158	.276	.521	1.054	3.005	8.219	26.581	$p-$adic
	.028	.040	.053	0.093	0.182	0.371	0.711	Cramer
40	148	181	207	291	476	1033	2829	GE
	.797	1.795	3.899	8.756	31.120	85.780	234	CRT
	.500	.973	1.932	3.998	11.891	33.412	113	$p-$adic
	.149	.222	0.309	0.447	1.121	2.282	4.68	Cramer

Timing on Real Systems

n	49	100	100	144	196	225	256	576	900	900
k	5	24	8	4	3	5	12	7	24	4
d	4	8	4	2	2	4	4	6	8	2
$\|\|A\|\|$	10	5	2	4	11	2	3	3	2	5
$\|\|x\|\|$	45	14	1	1	229	875	2	1	2	1
CRT	.144	.788	.029	.036	3.344	3.056	.155	.842	2.358	1.458
L	4	1	1	1	9	36	1	1	1	1
Lift 1	.109	.443	.030	.029	1.183	2.374	.174	.612	2.761	.462
Lift 2	.111	.294	.100	.163	1.973	1.678	.640	3.022	7.627	5.711
Cramer	.293	4.159	.305	.147	6.206	4.644	3.748	53.69	338	25.74
GE	109	3080	30.15	10.49	4419	769	848	2055	2265	1195

Questions

Can $p-$adic lifting be used to construct

$$\det A^{(j)} \bmod m(z) \text{ and } \det A \bmod m(z)?$$

For what other number fields is this approach feasible?