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 Problem

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

We will solve $Ax = b$ modulo $m(z)$ where $m(z) = \Phi_k(z)$ is the minimal polynomial for β.

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	$z^2 - z + 1$	$\frac{1 \pm \sqrt{3}i}{2}$

cyclotomic polynomials of order 3–6

Example

$m(z) = z^2 + z + 1$

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

Solution vector:

$$x = \begin{bmatrix} -\frac{193028420497557977963092944211837 3}{837637134068527924278537117122 85} + \frac{293530015437001131689173724428409}{167527426813705584855707423424570}z \\ \frac{125712863214341440313988741186775 91}{234538397539187818797990392794398 0} + \frac{170534906127849498440359300473108931}{234538397539187818797990392794398 0}z \\ \vdots \end{bmatrix}$$

$ncd = 1276$ digits

Picking the Primes

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

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

Picking the Primes

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 );
```

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

How do we split $m(z)$ modulo $p = qk + 1$?

How do we split $m(z)$ modulo $p = qk + 1$?

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 do we split $m(z)$ modulo $p = qk + 1$?

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 $\gcd(i, k) = 1$.

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

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

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

How do we split $m(z)$ modulo $p = qk + 1$?

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 $\gcd(i, k) = 1$.

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

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

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

Theorem: $O($ powmod $\boxed{\log p\ M(d)}$ $+$ gcd $\boxed{\log d\ M(d)}$ $)$ arith. ops. in $\mathbb{Z}_p$.
$= O(\log pd^2 + d^2)$ using classical poly. arith.

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** $j = 1, 2, 3, ...$ **do**
3: Find a new machine prime $p_j = kq + 1$.
4: Compute the d 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 $Ax \equiv b \bmod m(z)$

..... $n = \dim A,\ d = \deg m,\ c = \log \parallel [A|b] \parallel,\ L =$ # primes.

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 $x = \text{FAIL}$.
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** $j = 1, 2, 3, ...$ **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: $A \in R^{n \times n}$, $b \in R^n$, $m \in R$, $R = \mathbb{Z}[z]$, assuming A is non-singular
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** $j = 1, 2, 3, ...$ **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** $j = 1, 2, 3, ...$ **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 $Ax \equiv b \bmod m(z)$

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

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 ..... $O(n^2dcL)$
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** ..... $O(n^3dL + n^2dcL + n^2d^2L + ndL^2)$.

Trial divisions.

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

Trial divisions.

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

We know $m|Ax - b \bmod P = p_1 \times ... \times p_j$.
Thus if $\underbrace{||A(Dx) - (Db) \bmod m(z)||}_{= \mathbf{B} - \text{bound this}} < 2P$ then $m|Ax - b$.

Trial divisions.

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

We know $m|Ax - b \bmod P = p_1 \times ... \times p_j$.
Thus if $\underbrace{||A(Dx) - (Db) \bmod m(z)||}_{= \mathbf{B} - \text{bound this}} < 2P$ then $m|Ax - b$.

Lemma: Let $N = \max_{i=1}^{n} ||Dx_i||_\infty$. Then

$$\mathbf{B} < 2(1 + ||m||_\infty)^{d-1}(D||b|| + ndN||A||).$$

How big can the integers in x be?

For random input, integers in x are nd times longer than those in A, b.

How big can the integers in x be?

For random input, integers in x are nd times longer than those in A, b.

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

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

How big can the integers in x be?

For random input, integers in x are nd times longer than those in A, b.

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 $L \in O(ndc)$ where $c = \log \| \, [A|b] \, \|$
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 $\mathbf{u}$ satisfying $A\mathbf{u} = b$ modulo $P = p_1 \times ... \times p_j$.
Solve $A\mathbf{v} = b$ modulo $Q = p_{j+1} \times ... \times p_{2j}$ for $\mathbf{v}$.

Asymptotically fast reconstruction

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

CRA($[\mathbf{u} \mod P, \mathbf{v} \mod Q]$)

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

Asymptotically fast reconstruction

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

CRA($[\mathbf{u} \mod P, \mathbf{v} \mod Q]$)

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

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 $m(z)$.

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 $m(z)$.

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

Compute

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

using Chinese remaindering and interpolation.

Bounds and costs

Lemma (bounds the number of primes needed)

$$\| N_j \|_\infty \leq d^n (1 + \| m \|_\infty)^{(n-1)(d-1)} \| b \| \quad \| A \|^{n-1}$$

$$\| D \|_\infty \leq d^n (1 + \| m \|_\infty)^{(n-1)(d-1)} \| A \|^{n-1}.$$

Number of primes L goes from $O(ndc + ...)$ to $O(nc + ...)$.

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

Timing on Random Systems

$$m(z) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1$$

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
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

Timings in CPU seconds on a AMD 150 @ 2.4 GHz

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
$\log_2 \parallel A \parallel$	10	5	2	4	11	2	3	3	2	5
$\log_2 \parallel x \parallel$	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
#primes	4	1	1	1	9	36	1	1	1	1
$p-$adic	.109	.443	.030	.029	1.183	2.374	.174	.612	2.761	.462
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

Timings in CPU seconds

Open Problems

- What do we do if A could be singular?
- For what other number fields is this approach feasible?
- Can $p-$adic lifting be used to construct $\det A^{(j)} \bmod m(z)$ and $\det A \bmod m(z)$?