A CIRCULANT MATRIX PROBLEM AND CERTAIN GENERIC CYCLIC GALOIS EXTENSIONS

1. Trailer

In this note, we solve the following circulant matrix problem completely. Recall that an integer circulant matrix M of size $n \times n$ is of the following from:

$$\begin{pmatrix} c_1 & c_n & c_{n-1} & \dots & c_2 \\ c_2 & c_1 & c_n & \dots & c_3 \\ c_3 & c_2 & c_1 & \dots & c_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_n & c_{n-1} & c_{n-2} & \dots & c_1 \end{pmatrix}$$

Problem. *Let p be a prime, let g be a primitive generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Find an integer circulant matrix M of size $(p-1)\times(p-1)$ such that the following two conditions are satisfied:*

$$M \begin{pmatrix} 1 \\ g \\ g^2 \\ \vdots \\ g^{p-2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod p \tag{1}$$

$$\det M = \pm p \tag{2}$$

Theorem 1.1. *The above problem is solvable if and only if p is among the following primes:*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 37, 41, 43.$$

Note that these primes are among the list S of primes where $\mathbb{Q}(\zeta_{p-1})$ has class number one. Magenta colored primes are the ones where we can solve the circulant matrix problem.

$$S = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71\}.$$

This list S is also a complete list of primes p such that prime ideals above p in $\mathbb{Q}(\zeta_{p-1})$ are principal (see [Sch20]).

A true mathematician will certainly question the naturality of this problem. We will explain the connection between this problem with universal cyclic Galois extensions over $\mathbb{Q}$ in the appendix of this note.

2. The solution

An integer circulant matrix of size $n\times n$ can be viewed as a member in the group ring $\mathbb{Z}[C_n]$ where C_n is the cyclic group of order n. If σ is a generator of C_n, we may assign a cyclic permutation matrix to it

$$\sigma \mapsto \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

In this way, every circulant matrix M can be written as a polynomial $P(\sigma)$ in σ. This observation implies that the computation of the determinant of M is easy

$$\begin{aligned} \det M &= \prod_{k=1}^{p-1} P(\zeta_{p-1}^k) \\ &= P(1) \cdot P(-1) \cdots \underbrace{\prod_{k=1}^{(p-1)/d} P(\zeta_{p-1}^{kd})}_{\text{Galois orbit}} \cdots \prod_{(k,p-1)=1} P(\zeta_{p-1}^k). \end{aligned}$$

Suppose want $\det M = \pm p$, then exactly one of these factors will be $\pm p$, and the rest must be ± 1. Further more, the mod p vanishing condition on the cyclic vector $(1, g, g^2, \dots, g^{p-2})$ implies the factor of p has to come from the $\prod_{(k,p-1)=1} P(\zeta_{p-1}^k)$ part. Thus, to solve the circulant matrix problem for p, we necessarily want p to be the norm of an algebraic integer in $\mathbb{Q}(\zeta_{p-1})$.

Proposition 2.1. *The circulant problem is solvable only for primes p which are norms in $\mathbb{Q}(\zeta_{p-1})$, or equivalently, only for p such that prime ideals above it in $\mathbb{Q}(\zeta_{p-1})$ are principal. In other words, the circulant problem is only solvable for primes in the set S in the introduction*

$$S = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71\}.$$

Now to hunt for solutions, even for these small primes, the search space is still too large. For circulant matrices with only $0, 1$ values, there are already 2^{p-1} candidates to test. The idea is to do this search in a smart way which uses more available arithmetic information.

Suppose $P(x)$ is a degree $< p-1$ polynomial which solves the group ring problem (subbing $x = \sigma$), then the algebraic integer $P(\zeta_{p-1})$ must have norm p in the field $\mathbb{Q}(\zeta_{p-1})$. Thus we should start by solving the norm problem in the field $\mathbb{Q}(\zeta_{p-1})$ first, and lift back to the group ring. If $R(x)$ is a degree $< \phi(p-1)$ polynomial such that $R(\zeta_{p-1})$ has norm p, then any polynomial $P(x)$ lifts $R(x)$ in the group ring must be of the shape

$$P(x) = R(x) + \Phi_{p-1}(x)\, T(x)$$

($\Phi_{p-1}(x)$ is the cyclotomic polynomial for $(p-1)$-th root of unity).

Further more, not every $R(x)$ would have a lift which satisfies the norm condition in the group ring, we want $P(x)$ to have norm ± 1 when subbing x with ζ_{p-1}^d for $d|(p-1)$ properly. Note that if ℓ is a prime which divides $p-1$, the cyclotomic polynomial will have some divisibility property (assuming ℓ^e is the largest ℓ-power dividing $p-1$)

$$\Phi_{p-1}(\zeta_{p-1}^{(p-1)/\ell^e}) = 0 \mod \ell$$

Thus we need the norms of $R(\zeta_{p-1}^{(p-1)/\ell^e})$ to be ± 1 modulo these primes. These "subfield filters" helps us to reduce the search size for R effectively.

Once $R(x)$ is found, we search for $T(x)$ such that $P(x) = R(x) + \Phi_{p-1}(x)T(x)$ satisfies $P(1) = \pm 1$ and $P(-1) = \pm 1$. These conditions also reduce the search size for T by a lot.

Algorithm 1: Finding a Circulant Matrix for Odd Integer p

Input : An odd integer p
Output: A polynomial $P(x)$ generating the matrix

`// Step 1: Find base polynomial R`

Find a polynomial $R(x)$ of degree $< \phi(p-1)$ such that $R(\zeta_{p-1})$ has norm p in the field $\mathbb{Q}(\zeta_{p-1})$;

`// Step 2: Subfield Norm Test`

Test the norms of $R(\zeta_{p-1}^{(p-1)/\ell^e})$ for prime factors ℓ;
if *the subfield norm test fails* **then**
  go to Step 1;

`// Step 3: Sum and Alternating Sum`

Find a polynomial $T(x)$ of degree $< p - 1 - \phi(p-1)$ such that $P(x)$ satisfies the sum and alternating sum conditions:

$$P(1) = \pm 1 \quad \text{and} \quad P(-1) = \pm 1$$

`// Step 4: Determinant Check`

Check the determinant $P(\sigma)$ using the product $\prod_{k=1}^{p-1} P(\zeta_{p-1}^k)$;
if *this fails* **then**
  go to Step 3

When the problem is solvable, this algorithm usual finds the solution within a few seconds (on 2024 commercial hardware) when we restrict our coefficients bounds to be {-1, 0, 1} (or $\{-2, -1, 0, 1, 2\}$ if necessary).

But if the above algorithm hangs up without finding any solution, then likely there isn't any. In that case we can show the non-existence of solutions. The idea is, the only freedom we have in $R(x)$ comes from the unit group of $\mathbb{Q}(\zeta_{p-1})$. If these units are unable to adjust the local norms for us, then there is no hope in finding a correct lift $P(x)$.

In actual experimentation, for all primes p in S, if we can't find solutions, then following algorithm always finds obstructions.

Algorithm 2: Computing local obstructions

```
// Step 1: Find fundamental units
```
In the field $\mathbb{Q}(\zeta_{p-1})$ find all fundamental units $U_1(x), U_2(x), \ldots, U_r(x)$ (these are polynomials of degree $< \phi(p-1)$);

```
// Step 2: Evaluate mod ℓ norms
```
Evaluate the mod ℓ norms of these fundamental units on $x = \zeta_{p-1}^{(p-1)/\ell^e}$. This should give us r vectors $(\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_r})$ in the group $\prod_\ell \mathbb{F}_\ell^\times$;

```
// Step 3: Find polynomial R with norm p
```
Find one polynomial $R(x)$ of degree $< \phi(p-1)$ such that the norm of $R(\zeta_{p-1})$ is p;

```
// Step 4: Evaluate subfield norms of R
```
Evaluate the subfield norms of $R(\zeta_{p-1}^{(p-1)/\ell^e})$. This should give us one vector $\mathbf{norm}_R$ in the group $\prod_\ell \mathbb{F}_\ell^\times$;

```
// Step 5: Check generation condition
```
Compute if $\mathbf{norm}_R$ lies in the subgroup generated by $(\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_r})$;

Appendix A. Writing down $\mathbb{Z}/p\mathbb{Z}$-extensions

(Side note: we actually know how to write down every $\mathbb{Z}/p\mathbb{Z}$ extensions in general, see [Sal84]. Here we just explore what we can do using endomorphisms on algebraic torus.)

Suppose p is a prime where we can solve the group ring problem, let $M = P(\sigma)$ be the solution. Then we have the following exact sequence of C_{p-1}-modules

$$0 \to \mathbb{Z}[C_{p-1}] \overset{P(\sigma)}{\to} \mathbb{Z}[C_{p-1}] \to \mu_p \to 1,$$

where μ_p is the group of p-th roots of unity equipped with the natural C_{p-1} action.

This sequence can be seen as a sequence of Galois module as well, given that $\mathrm{Gal}(\mathbb{Q}) \to C_{p-1}$ is the Galois representation arising from cyclotomic $(p-1)$-th root of unity. The data of a Galois module on the rank $(p-1)$ free abelian group $\mathbb{Z}[C_{p-1}]$ is equivalent to a representation $\psi\colon \mathrm{Gal}(\mathbb{Q}) \to \mathrm{GL}_{p-1}(\mathbb{Z})$ (with image being the cyclic group C_{p-1}). With this representation, we can twist the algebraic torus $\mathbb{G}_m^{p-1}$ to the Weil torus $T = \mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p)}(\mathbb{G}_m)$. The same thing can be done for μ_p, and we get the constant group $\mathbb{Z}/p\mathbb{Z}$ in return.

The key point of the above construction (turning Galois modules to groups of multiplicative type) is that it's an *anti-equivalence*. It's just the Pontrygian duality endowed with Galois actions. That being said, on the torus side we obtain the following exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to T \overset{P(\sigma)}{\to} T \to 1.$$

The sequence above allows us to compute the Galois cohomology group $H^1(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z})$ (since $H^1(\mathbb{Q}, T) = 0$)

$$H^1(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}) \approx \mathbb{Q}(\zeta_p)^\times/(\mathbb{Q}(\zeta_p)^\times)^{P(\sigma)}.$$

This effectively means that *all* Galois $\mathbb{Z}/p\mathbb{Z}$ extensions arise from looking at the pre-image of $P(\sigma)$ on $\mathbb{Q}(\zeta_p)^\times$, which is given by algebraic equations! In other words, we can produce a family of algebraic equations, such that they classify every Galois $\mathbb{Z}/p\mathbb{Z}$ extensions.

For example, in the case when $p = 3$, we have the following exact sequence ($T = \mathrm{Res}_{\mathbb{Q}}^{\mathbb{Q}(w)}(\mathbb{G}_m)$)

$$0 \to \mathbb{Z}/3\mathbb{Z} \to T^\times \overset{\sigma-2}{\to} T^\times \to 1$$

Thus every $\mathbb{Z}/3\mathbb{Z}$ extension arises from the solutions to the following equation ($\theta^2 = -3$)

$$\frac{(x-\theta y)}{(x+\theta y)^2} = u + \theta v, \quad u, v, \in \mathbb{Q}.$$

In fact for $p = 3$, one can do better using the norm one torus N in $\mathbb{Q}(w)$. In that case, we have

$$0 \to \mathbb{Z}/3\mathbb{Z} \to N \overset{3}{\to} N \to 1$$

Using the fact that $H^1(\mathbb{Q}, N)$ is a two-torsion, we obtain the classification $H^1(\mathbb{Q}, \mathbb{Z}/3\mathbb{Z}) = N/N^3$. Furthermore, since N is a rational conic (defined by $x^2+3y^2 = 1$), the family of equations we get from N can be written down using one parameter by rationally parametrizing N. The *universal cubic Galois equation* we obtain from N is the following

$$3x^3 - 9tx^2 - 3x + t = 0, \quad \Delta = 18^2(3t^2+1)^2, \quad t \in \mathbb{Q}.$$

Unfortunately this is a split nodal cubic, not some mysterious elliptic curve.

References

[Sal84] David J Saltman. "Retract rational fields and cyclic Galois extensions". In: *Israel Journal of Mathematics* 47.2 (1984), pp. 165–215.

[Sch20] René Schoof. "Heights and Principal Ideals of Certain Cyclotomic Fields". In: *Class Groups of Number Fields and Related Topics*. Springer, 2020, pp. 89–96.