A sample computation

Altan Erdnigor

May 27, 2024

Contents

1 Notation

- p a prime number.
- $\mathbf{SL}_3(\mathbb{Z})$ the special linear group over $\mathbb{Z}$.
- Γ_p the pth congruence subgroup of $\mathbf{SL}_3(\mathbb{Z})$.
- $Z_G(x)$ the centralizer of $x \in G$.
- $$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & p+2 \\ 0 & 1 & 2p \end{pmatrix} \in \mathbf{SL}_3(\mathbb{Z}) \tag{1}$$
- $$\tilde{A} = \mathbf{Id} + pA = \begin{pmatrix} 1 & 0 & p \\ p & 1 & 2p+p^2 \\ 0 & p & 1+2p^2 \end{pmatrix} \in \Gamma_p \tag{2}$$
- If C is a matrix, $\chi_C(\lambda) \coloneqq \det(\lambda \mathbf{Id} - C)$ is the characteristics polynomial.
- $f(t) \coloneqq \chi_A(t) = t^3 - 2pt^2 - (p+2)t - 1$.

2 Intro

Recall the Lucas primes (see `https://en.wikipedia.org/wiki/Lucas_number#Lucas_primes`, `https://t5k.org/top20/page.php?id=48`)

$$2, 3, 7, 11, 29, 47, 199, 521, 2207, 3571, 9349, 3010349, 54018521, 370248451, 6643838879, \dots \tag{3}$$

In this notes we establish the following results:

1. The regularor of $\tilde{A}$ grows as $\approx \ln^2(p)$.
   That is, $\mathrm{Reg}(\mathbb{Q}(\alpha)/\mathbb{Q}) \approx \ln^2(p)$ for α a root of $\chi_{\tilde{A}}$.
2. The index of the centralizers $[Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) : Z_{\Gamma_p}(\tilde{A})]$ grows as $O(\ln p)$ for p a Lucas prime.

This might be interesting.

3 Regulator

We refer to Keith Conrad's write-up on Dirichlet's unit theorem and regulators [1] for the definitions. The current proof mimics the proof of Theorem 5.12 of Conrad.

Notice that

$$\begin{aligned}\chi_{\tilde{A}}(\lambda) &= \det(\lambda \mathbf{Id} - \tilde{A}) \\ &= \det(\lambda \mathbf{Id} - (\mathbf{Id} + pA)) = \det((\lambda - 1)\mathbf{Id} - pA) \\ &= p^3 \det(\frac{\lambda - 1}{p}\mathbf{Id} - A) = p^3 \chi_A(\frac{\lambda - 1}{p}).\end{aligned} \tag{4}$$

Hence adding the root of χ_A or $\chi_{\tilde{A}}$ result in the same field; therefore we reduce to showing that $\mathrm{Reg}(\mathbb{Q}(\alpha)/\mathbb{Q}) \approx \ln^2(p)$ for α a root of $\chi_A(t) = f(t) = t^3 - (2pt^2 + (p+2)t + 1)$.

Lemma 3.1. *$\mathbb{Q}(\alpha)/\mathbb{Q}$ is totally real of degree 3 for primes $p \neq 2$.*

Proof. $f(t)$ is irreducible over $\mathbb{Q}$; indeed, by the rational roots theorem it's sufficient to check ± 1:

$$f(1) = -3p - 2, f(-1) = -p.$$

A simple computation shows that the discriminant of $f(t)$ equals

$$\mathrm{disc}_f(p) = 4p^4 - 12p^3 + 4p^2 - 24p + 5.$$

If $p > 4$ the discriminant $\mathrm{disc}_f(p) > 0$ is positive. Therefore the cubic extension is totally real. □

Proposition 3.2. $\mathbb{Z}[\alpha]^* = \{\pm \alpha^a (2\alpha + 1)^b \mid a, b \in \mathbb{Z}\}$.

Note that $\alpha, 2\alpha + 1$ are not necessarily fundamental units in $\mathbb{Q}(\alpha)/\mathbb{Q}$ as we don't claim that the ring of integers of $\mathbb{Q}(\alpha)/\mathbb{Q}$ coincides with $\mathbb{Z}[\alpha]$.

Proof. Note that $f(\alpha) = 0$ implies

$$\alpha(\alpha^2 - 2p\alpha - (p+2)) = 1 \quad (5)$$
$$(1+2\alpha)(1+p\alpha) = \alpha^3 \quad (6)$$

It shows that $\alpha, 1+2\alpha$ are indeed units.

Let $\alpha_1 > \alpha_2 > \alpha_3 \in \mathbb{R}$ be the three different roots of f. We shall compute them approximately.

$$\alpha_1 = 2p + \frac{1}{2} + O\left(\frac{1}{p}\right),$$
$$\alpha_2 = -\frac{1}{p} + O\left(\frac{1}{p^4}\right),$$
$$\alpha_3 = -\frac{1}{2} + O\left(\frac{1}{p}\right).$$

Remark 3.3. *A computation shows that for $p = 10000$ we have*

$\alpha_1 = 20000.5000874981, \alpha_2 = -0.000100000000000100, \alpha_3 = -0.499987498124648.$

It is not important that p is not a prime in this case as the estimate works for any sufficiently large p.

By the definition of the regulator we have

$$\operatorname{Reg}(\alpha, 2\alpha+1) = \begin{vmatrix} \ln|\alpha_1| & \ln|\alpha_2| \\ \ln|2\alpha_1+1| & \ln|2\alpha_2+1| \end{vmatrix}$$
$$\approx \begin{vmatrix} \ln|2p+\frac{1}{2}| & \ln|\frac{-1}{p}| \\ \ln|4p+2| & \ln|\frac{-2}{p}+1| \end{vmatrix} = \ln(2p+\frac{1}{2})(\ln(p-2)-\ln(p)) + \ln(4p+2)\ln(p)$$
$$= \ln(2p+\frac{1}{2})\ln(p-2) - \ln(2p+\frac{1}{2})\ln(p) + \ln(4p+2)\ln(p). \quad (7)$$

Therefore $\operatorname{Reg}(\alpha, 2\alpha+1) > 0$ for all prime p.

Hence $\alpha, 2\alpha+1$ are independent units.

It is left to prove that they are fundamental units in $\mathbb{Z}[\alpha]$. By Corollary 5.9 from Conrad it is sufficient to check

$$\frac{16\operatorname{Reg}(\alpha, 2\alpha+1)}{(\ln(\operatorname{disc}_f/4))^2} < 2.$$

Substituting, we obtain

$$\frac{16\operatorname{Reg}(\alpha, 2\alpha+1)}{(\ln(\operatorname{disc}_f/4))^2} \approx \frac{16(\ln(2p+\frac{1}{2})\ln(p-2) - \ln(2p+\frac{1}{2})\ln(p) + \ln(4p+2)\ln(p))}{(\ln((p^4+2p^3-5p^2-6p-23)/4))^2}.$$

Asymptotically, the latter equals

$$\xrightarrow{p\to\infty} \frac{16\ln(p)^2}{(\ln(p^4))^2} = 1.$$

Therefore it is < 2 for big enough p, QED. □

Remark 3.4. *One can do the estimate more carefully, but for now postpone it.*

Remark 3.5. *We just proved that the regulator is approximately*

$$\ln(2p+\frac{1}{2})\ln(p-2)-\ln(2p+\frac{1}{2})\ln(p)+\ln(4p+2)\ln(p),$$

which is close to $\ln^2 p$ *we wanted from the beginning.*

4 Centralizers

Proposition 4.1. *The centralizer of* $\tilde{A}$ *in* $\mathbf{SL}_3(\mathbb{Z})$ *is generated by* $A, A+\mathbf{Id}$.

$$Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A})=\{\pm A^a(2A+\mathbf{Id})^b \mid a,b\in\mathbb{Z}\}.$$

Proof. Since $\tilde{A}$ is regular, its centralizer in $\mathbf{Mat}_3(\mathbb{C})$ is $\mathbb{C}\left\langle \mathbf{Id}, A, A^2\right\rangle$. Now,

$$\mathbb{C}\left\langle \mathbf{Id}, A, A^2\right\rangle \cap \mathbf{SL}_3(\mathbb{Z}) \subset \mathbb{Z}\left\langle \mathbf{Id}, A, A^2\right\rangle.$$

Indeed,

$$\mathbf{Id}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, A=\begin{pmatrix}0&0&1\\1&0&p+2\\0&1&2p\end{pmatrix}, A^2=\begin{pmatrix}0&1&2p\\0&p+1&2p^2+4p+1\\1&p&4p^2+p+2\end{pmatrix}, \tag{8}$$

Considering the first matrix column we see that if a complex combination has integer coefficients, it is in fact integer combination.

Moreover, the centralizer of $\tilde{A}$ is a group, therefore it lies inside the multiplicative group of $\mathbb{Z}[A]$

$$Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) \subset \mathbb{C}\left\langle \mathbf{Id}, A, A^2\right\rangle \cap \mathbf{SL}_3(\mathbb{Z}) \subset \mathbb{Z}[A]^*.$$

There is an isomorphism of $\mathbb{Z}$-algebras $\mathbb{Z}[A]\simeq\mathbb{Z}[x]/(f(x))=\mathbb{Z}[\alpha]$. Applying Proposition 3.2 end the proof

$$Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) \subset \mathbb{Z}[A]^*=\{\pm A^a(2A+\mathbf{Id})^b \mid a,b\in\mathbb{Z}\}.$$

□

We are to study the centralizer of $\tilde{A}$ in Γ_p.

$$Z_{\Gamma_p}(\tilde{A}) \subset Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) \cong \mathbb{Z}^2.$$

In general this subgroup can be difficult to describe; that leads to cosidering *Lucas primes.*

4.1 Lucas primes give small degree $\log(p)$

Proposition 4.2. *Let* p *be a Lucas prime. Let* k *be the integer part of* $\log_\phi p$ *where* ϕ *is the golden ratio.*

The centralizer $Z_{\Gamma_p}(\tilde{A})$ *contains* $\tilde{A}$ *and* A^{4k}.

Proof. The only thing to prove is that $A^{4k} \in \Gamma_p$.

It suffices to show that the eigenvalues of $A \pmod p$ are $4k$-th roots of unity. Computing

$$\chi_A(t) = f(t) \equiv t^3 - 2t - 1 = (t+1)(t^2 - t - 1) \pmod p,$$

shows that it is left to work with the golden ratio in $\mathbb{F}_p$ which we denote by ϕ_p. That is, $\phi_p \in \mathbb{F}_{p^2}$ satisfies $\phi_p^2 - \phi_p - 1 = 0$.

By the definition of a Lucas number we have

$$p = \phi^k + (-\phi)^{-k} \tag{9}$$

where ϕ is a root of $x^2 - x - 1$.

The RHS of (9) being invariant under the change $\phi \to (-\phi)^{-1}$ manifests it as a symmetric polynomial in the roots of $x^2 - x - 1$, thus having a presentation

$$\phi^k + (-\phi)^{-k} = P(\phi, (-\phi)^{-1}),$$

where P is a *universal* polynomial. This observation justifies that the Equation (9) can be taken modulo p to have the form

$$0 = \phi_p^k + (-\phi_p)^{-k},$$

which implies

$$1 = \phi_p^{4k}.$$

$\square$

Theorem 4.3. *The index of the centralizers is bounded by* $4 \log_\phi p$

$$[Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) : Z_{\Gamma_p}(\tilde{A})] \le 4 \log_\phi p.$$

In particular, it grows as $O(\ln p)$.

Proof. Identify $Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^2$ as in Proposition 4.1.

Observe that by (6) we have

$$1 + p\alpha = \alpha^3 (2\alpha + 1)^{-1}.$$

By the previous Proposition $Z_{\Gamma_p}(\tilde{A})$ contains $\binom{3}{-1}, \binom{4k}{0}$; Clearly, the index

$$\mathbb{Z}\left\langle \begin{pmatrix} 3 \\ -1 \end{pmatrix}, \begin{pmatrix} 4k \\ 0 \end{pmatrix} \right\rangle \subset \mathbb{Z}^2,$$

equals $4k \approx 4 \log_\phi p$ and the index $[Z_{\Gamma_p}(\tilde{A}) : Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A})]$ has to divide it. $\square$

4.2 Bounds on the degree $log(p) \prec \deg \prec p$

Motivated by geometric considerations, we call the degree deg the index $[Z_{\Gamma_p}(\tilde{A}) : Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A})]$.

Proposition 4.4. *We have* $O(log(p)) \le \deg \le O(p)$.

Proof. The proof of the previous Theorem shows that $Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A})$ is generated by $\alpha^3(2\alpha+1)^{-1}, \alpha^{\deg}$.

So, the goal is to show that the multiplicative order of ϕ_p is bounded by $\log(p)$ from below and by p from above.

First let us show $\log(p) < \deg$. Indeed, lifting ϕ_p to ϕ we notice that

$$\phi_p^k = 1 \Rightarrow (-\phi_p^{-1})^k = (-1)^k \Rightarrow \phi^k + (-\phi^{-1})^k - (1+(-1)^k) \in p\mathbb{Z}.$$

Thus the degree $\deg > \log(p) - \epsilon$ for p big enough and some small ϵ.

Finally, we shall show $\deg \leq O(p)$. What we show in reality is that if $\sqrt{5} \in \mathbb{F}_p$, the degree deg divides $p-1$, $\deg | p-1$ and if $\sqrt{5} \notin \mathbb{F}_p$, $\deg | 2p+2$.

Indeed, the first part is clear by Fermat's little theorem. To show the second, let's decompose

$$x^2 - x - 1 = (x-\alpha_1)(x-\alpha_2),$$

where $\alpha_1, \alpha_2 \in \mathbb{F}_{p^2}$. The Frobenius automorphism $\mathrm{Frob} : t \mapsto t^p$ acts on the roots α_1, α_2 by permuting them; thus we have $\alpha_1^p = \alpha_2 = -1/\alpha_1$ implying $\alpha_1^{2p+2} = (-1)^2 = 1$. ☐

5 Enter family

Let $f_{a,b}(t) = t^3 - apt^2 - (bp+a)t - b$. Here $a, b \in \mathbb{Z}$. Note that $f_{2,1}(t) = f(t)$ is the characteristic polynomial of A.

We can now define

$$A_{a,b} = \begin{pmatrix} 0 & 0 & b \\ 1 & 0 & bp+a \\ 0 & 1 & ap \end{pmatrix} \in \mathbf{Mat}_3(\mathbb{Z}), \tag{10}$$

$$\tilde{A}_{a,b} = \mathbf{Id} + pA_{a,b} = \begin{pmatrix} 1 & 0 & bp \\ p & 1 & bp^2+ap \\ 0 & p & 1+ap^2 \end{pmatrix} \in \Gamma_p. \tag{11}$$

Here $\tilde{A}_{a,b}$ is indeed invertible thanks to

$$\begin{aligned} \det(\tilde{A}_{a,b}) &= p^3 \det\left(\frac{1}{p}\mathbf{Id} + A_{a,b}\right) = -p^3 \det\left(\frac{-1}{p}\mathbf{Id} - A_{a,b}\right) \\ &= -p^3 f_{a,b}\left(\frac{-1}{p}\right) = 1 + ap^2 - (bp+a)p^2 + bp^3 = 1. \end{aligned} \tag{12}$$

Actually, a generic element in Γ_p is conjugate to $\tilde{A}_{a,b}$.

Proposition 5.1. *An element $\tilde{B} \in \Gamma_p$ is either*

1. $\mathbf{Id}$*;*
2. *conjugate to*

$$\begin{pmatrix} 1 & p & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

over $\mathbb{Q}$;

3. *conjugate to $\tilde{A}_{a,b}$ over $\mathbb{Q}$ for some $a, b \in \mathbb{Z}$.*

The proof goes by applying the Frobenius normal form over $\mathbb{Q}$.

Proof. Define $B = \frac{1}{p}(\tilde{B} - \mathbf{Id}) \in \mathbf{Mat}_3(\mathbb{Z})$.

There are three cases: the minimal polynomial $\mathrm{minpoly}_B$ of B is of degree $1, 2$ or 3.

1. $\deg \mathrm{minpoly}_B = 1$. Hence $\tilde{B}$ is scalar, hence $\mathbf{Id}$;

2. $\deg \mathrm{minpoly}_B = 2$. Hence $\frac{\chi_B}{\mathrm{minpoly}_B}$ is linear, thus dividing $\mathrm{minpoly}_B$; we obtain χ_B decomposes into a product of linear multiples over $\mathbb{Z}$

$$\chi_B(\lambda) = (\lambda - a)^2(\lambda - b), a, b \in \mathbb{Z}.$$

The condition $-p^3\chi_B(\frac{-1}{p}) = \chi_{\tilde{B}}(0) = 1$ now reads

$$(1 + ap)^2(1 + bp) = 1,$$

thus $a, b = 0$ if $p > 2$ and B is nilpotent. Therefore $\tilde{B}$ is conjugate to

$$\begin{pmatrix} 1 & p & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

3. The Frobenius normal form of B consists of the unique 3×3 block.

Pick $C \in \mathbf{GL}_3(\mathbb{Q})$ such that

$$C^{-1}BC = \begin{pmatrix} 0 & 0 & r_0 \\ 1 & 0 & r_1 \\ 0 & 1 & r_2 \end{pmatrix} \in \mathbf{SL}_3(\mathbb{Q}).$$

This matrix is actually integer $C^{-1}BC \in \mathbf{Mat}_3(\mathbb{Z})$. Indeed, the coefficients in the last column are the coefficients of the characteristic polynomial. Therefore, $C^{-1}\tilde{B}C \in \Gamma_p$.

We now show that $C^{-1}\tilde{B}C = \tilde{A}_{a,b}$. This follows from the equation $\det(C^{-1}\tilde{B}C) = 1$ which reads

$$1 + r_2p - r_1p^2 + r_0p^3 = 1,$$

implying

$$r_0 = b, r_1 = bp + a, r_2 = ap,$$

for some $a, b \in \mathbb{Z}$.

□

6 The Unknown

Problem 6.1. *What is the behavior of* Reg, deg *for an arbitrary member of the family $\tilde{A}_{a,b}$?*

References

[1] Keith Conrad. Dirichlet's unit theorem. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/unittheorem.pdf`.