

On 2-systoles of congruence quotients of SL_3 .

Mikhail Belolipetsky, Altan Erdnigor, Shmuel Weinberger

April 1, 2024

1 Notation

- p a prime number.
- $\mathbf{SL}_3(\mathbb{Z})$ the special linear group over \mathbb{Z} .
- Γ_p the p th congruence subgroup of $\mathbf{SL}_3(\mathbb{Z})$.
- $Z_G(x)$ the centralizer of $x \in G$.

•

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & p+2 \\ 0 & 1 & 2p \end{pmatrix} \in \mathbf{SL}_3(\mathbb{Z}) \quad (1)$$

•

$$\tilde{A} = \mathbf{Id} + pA = \begin{pmatrix} 1 & 0 & p \\ p & 1 & 2p+p^2 \\ 0 & p & 1+2p^2 \end{pmatrix} \in \Gamma_p \quad (2)$$

- If C is a matrix, $\chi_C(\lambda) := \det(\lambda \mathbf{Id} - C)$ is the characteristics polynomial.
- $f(t) := \chi_A(t) = t^3 - 2pt^2 - (p+2)t - 1$.

2 Intro

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

$$2, 3, 7, 11, 29, 47, 199, 521, 2207, 3571, 9349, 3010349, 54018521, 370248451, 6643838879, \dots \quad (3)$$

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

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

Hence adding the root of χ_A or $\chi_{\tilde{A}}$ result in the same field; therefore we reduce to showing that $\text{Reg}(\mathbb{Q}(\alpha)/\mathbb{Q}) \approx \ln^2(p)$ 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

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

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

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.

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

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

$$\begin{aligned} \text{Reg}(\alpha, 2\alpha + 1) &= \left| \begin{array}{cc} \ln |\alpha_1| & \ln |\alpha_2| \\ \ln |2\alpha_1 + 1| & \ln |2\alpha_2 + 1| \end{array} \right| \\ &\approx \left| \begin{array}{cc} \ln |2p + \frac{1}{2}| & \ln |\frac{-1}{p}| \\ \ln |4p + 2| & \ln |\frac{-2}{p} + 1| \end{array} \right| = \ln(2p + \frac{1}{2})(\ln(p - 2) - \ln(p)) + \ln(4p + 2) \ln(p) \\ &= \ln(2p + \frac{1}{2}) \ln(p - 2) - \ln(2p + \frac{1}{2}) \ln(p) + \ln(4p + 2) \ln(p). \quad (7) \end{aligned}$$

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

Hence α and $2\alpha + 1$ 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

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

Substituting, we obtain

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

Asymptotically, the latter equals

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

Therefore it is < 2 for big enough p . □

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 $A, 2A + \mathbf{Id}$.

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

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

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

Indeed,

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

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 $\mathbb{Z}[A]$

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

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 considering *Lucas primes*.

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

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

where ϕ is a root of $x^2 - x - 1$.

The RHS of (9) being invariant under the change $\phi \rightarrow (-\phi)^{-1}$ 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 equation (9) can be taken modulo p to have the form

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

which implies

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

□

Theorem 4.3. *If p is a Lucas prime, then the index of the centralizer is bounded by $4\log_\phi p$:*

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

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 $\begin{pmatrix} 3 \\ -1 \end{pmatrix}, \begin{pmatrix} 4k \\ 0 \end{pmatrix}$; 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. □

The observation that comes next is that the sequence of Lucas primes is very sparse. It is conjectured that there are infinitely many of them but even this is not known. In any respect, it is not hard to see that the number of Lucas primes less or equal than N grows at most as fast as $O(\frac{\log \log N}{N})$. From a more general point of view we are interested in the order of the generators of $Z_{\mathbf{SL}_3(\mathbb{Z})}(\tilde{A}) \bmod p$. One of the generators can be chosen as \tilde{A} and is equal to one mod p . We are left with the other generator. This can sometimes have very small order compared to p , like in the case with the Lucas primes considered in Proposition 4.2. However, in most of the cases the order will be $\sim p$ which implies that the index of the centralizer will be also of order p .

References

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