2 Short paths in $X^{p,q}$ and $\mathrm{SU}(2)$

2.1 The discrete case: LPS Ramanjuan graphs

2.1.1 Introduction, background and assumptions

The goal of this section will be to discuss techniques due to [CP18] and [Sar19] for efficiently factoring typical elements of the LPS Ramanujan graphs $X^{p,q}$, under mild assumptions on the relationship between p and q, as well as, independently, standard number theoretic assumptions. It is worth noting that [Sar19, Theorem 1.9] argues, via reduction to the subset sum problem and assuming Cramér's conjecture and the generalized Riemann hypothesis, that the factorization problem for general elements is NP-complete. Nonetheless, it is heartening that only a vanishing proportion (as $q \to \infty$) fail to admit the sought-after factorization.

We begin with the following hypothesis, which can be imprecisely stated as "q is much larger than p."

Assumption 1. *p and q are fixed primes $p, q \equiv 1 \pmod 4$ where $\left(\frac{p}{q}\right) = 1$ and the following conditions are satisfied for some fixed constants γ and C_γ as in Conjecture 6:*

$$p \in o(q), \qquad q \geqslant 22p, \qquad q^2 \geqslant 22pC_\gamma(5\log q)^\gamma.$$

We assume this henceforth even when not explicitly stated, though it will not always be necessary; especially for results of [CP18], though, it simplifies matters greatly, and is often the case in practice.

We now briefly introduce the object of study: the LPS Ramanujan graphs $X^{p,q}$. Because they arise as Cayley graphs of $PSL_2(\mathbb{Z}/q\mathbb{Z})$, we will interchangeably refer to their elements by their group-theoretic properties as matrices and their graph-theoretic relations as vertices, and the "size" of a (possibly improper) subset or subgroup[1] will refer to the number of vertices. (Such a description can be found in any of [CP18, DSV03, Sar19], and many more. In particular, [DSV03, Chapter 4] covers the construction in great detail.)

We begin with the integer quaternions $\mathbb{H}(\mathbb{Z})$ with $\mathbb{Z}$-basis $\{1, i, j, k\}$ satisfying $i^2 = j^2 = k^2 = ijk = -1$. The quaternion $x = a + bi + cj + dk$ has *conjugate* equal to $\overline{x} = a - bi - cj - dk$ and *norm* equal to $N(x) = a^2 + b^2 + c^2 + d^2$. Identify

$$\Sigma = \{x = a + bi + cj + dk \in \mathbb{H}(\mathbb{Z}) : N(x) = p; 2 \nmid a > 0; 2 \mid b, c, d\}$$
$$\Omega = \{x = a + bi + cj + dk \in \mathbb{H}(\mathbb{Z}) : \exists e \in \mathbb{N}, N(x) = p^e; 2 \nmid a; 2 \mid b, c, d\}$$

and it is clear that we may pick $\frac{1}{2}(p+1)$ elements α_i of Σ that are inequivalent under conjugation. (Note also that we can view these quaternions as the matrices $x' = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ where $\det x' = N(x)$ and this equivalence of

[1] Typically not viewed as a subgraph.

elements is preserved under multiplication.) Say that $x \asymp y$ for $x, y \in \Omega$ if there is $n \in \mathbb{Z}$ with $\pm p^n x = y$. Let Ω' be the (multiplicative) group of Ω's $\asymp$-equivalence classes, denoted by $[x]$ for $x \in \Omega$. [LPS88, Corollary 3.2] argues that Ω' is a free group generated by $\Sigma' = \left\{[\alpha_1], \ldots, [\alpha_{\frac{1}{2}(p+1)}]\right\}$, so Ω''s Cayley graph with respect to Σ' is a $(p+1)$-regular tree, and so we have almost completed the construction. Introduce

$$\widehat{\Omega}' = \{[a + bi + cj + dk] \in \Omega' : 2q \mid b, c, d\} \lhd \Omega'$$

and by Assumption 1, we have the map ϕ as, for $x = a + bi + cj + dk$,

$$\Omega'/\widehat{\Omega}' \xrightarrow{\quad\sim\quad} PSL_2(\mathbb{Z}/q\mathbb{Z})$$

$$x \longmapsto \begin{pmatrix} a + b\iota & c + d\iota \\ -c + d\iota & a - b\iota \end{pmatrix} / \sqrt{N(x)}$$

taking $\iota^2 \equiv -1 \pmod{q}$ and $\sqrt{\cdot}$ to denote the modulo-q square root.[2] Finally, $X^{p,q}$ is the Cayley graph of $PSL_2(\mathbb{Z}/q\mathbb{Z})$ with respect to $\phi(\Sigma')$.

Theorem 2 ([LPS88, Lemma 3.1 and Theorems 3.4 and 4.1])**.** *The graphs $X^{p,q}$ are $(p+1)$-regular, connected, and Ramanujan, with*

$$\#X^{p,q} = \frac{1}{2}(q-1)q(q+1).$$

The proof of this theorem is omitted from this treatment, and we skip right to results about paths in these graphs.

Theorem 3 ([LPS88, Lemma 3.1])**.** *Take vertex $v \in X^{p,q}$ and $a_0 + a_1 i + a_2 j + a_3 k \in [v]$ where $\gcd(a_0, a_1, a_2, a_3, p) = 1$. Let $h \in \mathbb{N}$. There is a bijection between simple paths of the form $I_2 = v_0, v_1, \ldots, v_h = v$—that is, paths of length h—and solutions $(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$ to*

$$\begin{aligned} x_0^2 + x_1^2 + x_2^2 + x_3^2 &= p^h \\ x_i &\equiv \lambda a_i \pmod{2q} \end{aligned}$$

for some (possibly many) $\lambda \in \mathbb{Z}/2q\mathbb{Z}$.

(Observe that the representative exists by dividing out by p enough times, by the equivalence relation.) One of the key ideas is that since we can translate directly between paths in $X^{p,q}$ and solutions to a particular Diophantine system by noting that solving the system is equivalent to a lift up to Ω, which admits efficient factorizations (Theorem 10), and so computing the least h for which that system has solutions gives the shortest factorization of v in $PSL_2(\mathbb{Z}/q\mathbb{Z})$. This factorization is possible by another key result from [LPS88] about the structure of Ω.

[2] $\sqrt{\cdot}$ is of course only defined when it exists, but it certainly does for powers of p. Also, the sign of the square root is immaterial as this is quotiented away since the group is projective.

Theorem 4 ([LPS88, Corollary 3.2])**.** *Any matrix $v \in \Omega$ has a unique factorization in Σ into $v = \pm p^r \prod_{i=1}^{n} v_i$ for $v_i \in \Sigma$ and not all entries of v divisible by p^{r+1} (i.e. r is the largest it could be).*

In particular, $\det v = p^e$ for some $e \in \mathbb{N}$ and so $\log_p \det v = e = n + 2r$, i.e. $n \leqslant \log_p \det v$. (This will be useful shortly.)

Conjecture 5. *For all positive integers n, there exists an algorithm in* $\operatorname{poly}\log n$ *to factor n.*

Integer factorization is not known to lie in P, but that it might be is not an uncommonly belief (e.g. [Sar11, Coh]). Therefore, assuming the existence of some efficient blackbox algorithm is not an unreasonable step.

Conjecture 6 ([Sar19, Conjecture 1.1])**.** *Take any $N, a_0, a_1 \in \mathbb{N}$ satisfying $N \equiv a_0^2 + a_1^2 \pmod{4q}$ and $\gcd(N, 4q) = 1$. Let $r \in \mathbb{R}^+$ and define the following:*

$$Q(t_0, t_1) = \frac{N}{4q^2} - \left(t_0 + \frac{a_0}{2q}\right)^2 - \left(t_1 + \frac{a_1}{2q}\right)^2$$
$$A_{Q,r} = \left\{(t_0, t_1) \in \mathbb{Z}^2 : Q(t_0, t_1) \in \mathbb{Z}_{\geqslant 0}, t_0^2 + t_1^2 < r^2\right\}.$$

There exist absolute constants $\gamma, C_\gamma > 0$ such that for any Q, r where $\#A_{Q,r} > C_\gamma (\log N)^\gamma$, then there exists $(t_0, t_1) \in A_{Q,r}$ for which $Q(t_0, t_1)$ is the sum of two squares.

Roughly speaking, this Cramér-type conjecture posits that given enough nearby lattice points in the plane, the quadratic form Q will take on enough different integral values such that one is the sum of two squares.

Because Conjecture 5 and Conjecture 6 will so often be used in conjunction, we consider the following:

Assumption 7 ([Sar19, $(*)$])**.** *Conjecture 5 and Conjecture 6 both hold.*

Finally, it will be essential for the course of the algorithms to be able to write numbers as the sum of two squares. Towards this, we introduce a method whose proof we omit for sake of space that enables us to solve this problem efficiently for the case of a prime.

Theorem 8 ([Sch85, §4])**.** *Consider a prime $p \equiv 1 \pmod 4$. There is a $O(\log^6 p)$ algorithm to compute a square root of -1 modulo p.*

Now, we have an efficient way to tackle the problem we set out to solve:

Corollary 9. *Consider a prime $p \equiv 1 \pmod 4$. The Diophantine equation*

$$x^2 + y^2 = p$$

can be solved over $\mathbb{Z}$ in $O(\log^6 p)$ time.

Proof outline. Let $m \in \left[2, \frac{1}{2}(p-1)\right]$ be a quadratic residue of -1, computable using Theorem 8. The idea is to use the well-known fact that $\mathbb{Z}[i]$ has a Euclidean algorithm, and then the standard technique of finding $\gcd(p, m+i)$ (doable in $O(\log p)$ time since $|m+i| = m^2 + 1 < p^2$) whose real and imaginary parts are x and y (order does not matter). ■

2.1.2 Factoring in Ω

Theorem 10 ([CP18, Lemma 2])**.** *Taking Assumption 1, any vertex $v \in \Omega$ can be factored in Σ in time $O(p \log_p \det v)$.*

Note that this algorithm involves precomputing all of Σ, which can trivially be done in time $\Theta(p^4)$ by simply trying all 4-tuples.

Proof. As in Theorem 4, express v as its (unknown) factorization $\pm p^r \prod_{i=1}^{n} v_i$. We proceed by induction on n. When $n = 1$, we readily compute r and the sign and so $v = \pm p^r v_1$; v_1 is trivially recognizable (e.g. in time $\Theta(p)$, by a linear search) as one of the $p + 1$ elements of Σ. Now, suppose when v has n Σ-factors that the factorization is obtainable in time $\Theta(pn) \subset O(n \log_p \det v)$. Suppose v' has $n + 1 \leqslant \log_p \det v'$ Σ-factors. Write $v' = \pm p^{r'} \prod_{i=1}^{n+1} v'_i$. There is a unique matrix $v'' \in \Sigma$ for which $v'_{n+1} v'' = pI_2$, namely, $v'' = \overline{v'_{n+1}}$. Since r' is easily computable, we simply consider $\left(\frac{v'}{\pm p^r}\right) w = \left(\prod_{i=1}^{n+1} v'_i\right) w$ with w ranging over all of Σ, halting when p divides all of $\left(\prod_{i=1}^{n+1} v'_i\right) w$'s entries. Then we know that $w = \overline{v'_{n+1}}$ and so we write $v'_{n+1} = \overline{w}$ and do the same consideration on $\frac{1}{p}\left(\prod_{i=1}^{n+1} v'_i\right) w = \prod_{i=1}^{n} v'_i$ which by the induction hypothesis is factorable in the stated time. Since this search took only $\Theta(p)$ time, we are done. ∎

2.1.3 Factorization of diagonal elements

The main result of this section is that a path of *the shortest possible length* can be found between almost all pairs of diagonal vertices, and all diagonal vertices have short factorizations. Stated precisely, we have two theorems of [Sar19].

Introduce the notation

$$h_0 = \left\lceil 3 \log_p q + \gamma \log_p(5 \log q) + \log_p C_\gamma + \log_p 22 \right\rceil.$$

Theorem 11 ([Sar19, Theorem 1.3])**.** *Take Assumption 7. There exists a set $S \subset X^{p,q}$ of diagonal vertices such that $\#S \leqslant \frac{22\pi q^4}{p^{h_0 - 1}}$ and there exists an algorithm that, given any diagonal vertex $v \in X^{p,q} \smallsetminus S$, returns a shortest path between v and the identity, in particular, one of length at most h_0.*

Observe that this theorem extends immediately to finding shortest paths between diagonal vertices $v_1, v_2 \in X^{p,q}$ by finding a shortest path from the identity to $v = v_1^{-1} v_2$ and then translating each vertex in the path by v_1.

Theorem 12 ([Sar19, Theorem 1.3])**.** *Take Assumption 7. Pick any diagonal vertex $v \in X^{p,q}$. There is a lower bound q' such that if $q > q'$, the shortest path between v and the identity is of length at most*

$$\left\lceil \frac{4}{3} \log_p \#X^{p,q} + \log_p 56 \right\rceil.$$

Taken together, these theorems assert that all diagonal vertices have short factorizations, and almost all (in particular, asymptotically in q) have very short factorizations that can be found with an efficient (polynomial-time) algorithm.

The structure of this section will be to build up auxiliary results towards proving these two theorems. The outline is as follows.

We start by introducing a binary integral quadratic form F that takes on the same values on $\mathbb{Z}$ as Q from Conjecture 6 does on an index-q sublattice. Using two results about the structure of the sign of F's image (Lemmas 16 and 18), we show that Algorithm 1 can efficiently find the special pair $(t_0, t_1) \in A_{Q,r}$ guaranteed to exist by Conjecture 6, hence solving Problem 19 efficiently. Then, having found a long path (one of length h_0), shorter ones are found by changing h in the Diophantine system, and a solution to that system corresponds to a lift to Ω which is then factorable, by Theorem 10.

This approach is rather similar in spirit to Lenstra's algorithm [Len83] for finding lattice points in convex subsets of a fixed-dimensional real space. The analogy primarily extends until the step of accepting a candidate lattice point, where [Len83] has an unconditional means of accepting such a point in an efficient time while [Sar19] rests on Assumption 7.

It is worth noting that a similar result for diagonal matrices is proved in [CP18, Lemma 6]. They take similar steps, by also passing to a lattice in order to lift up to Ω, and searching for a value of a quadratic form to take on a sum of two squares. It is heuristically justified why this approach terminates in $\operatorname{poly}\log q$ time, but it is still highly conditional.

We first introduce some notation in the context of fixed $a_0, a_1, N \in \mathbb{Z}$ satisfying $a_0^2 + a_1^2 \equiv N \pmod{4q}$ with N coprime to 2 and q. Since clearly we cannot have $q \mid a_0, a_1$, without loss of generality let $q \nmid a_0$. By an appropriate transformation from (x_0, x_1, x_2, x_3) to

$$\begin{aligned} x_0 &= 2qt_0 + a_0 & \qquad x_2 &= 2qt_2 \\ x_1 &= 2qt_1 + a_1 & \qquad x_3 &= 2qt_3, \end{aligned}$$

we will seek (t_0, t_1, t_2, t_3) satisfying

$$\frac{N}{4q^2} - \left(t_0 + \frac{a_0}{2q}\right)^2 - \left(t_1 + \frac{a_0}{2q}\right)^2 = t_2^2 + t_3^2;$$

recall Conjecture 6. Let $k = \frac{N - a_0^2 - a_1^2}{4q}$. Because both sides are integers, we must have $a_0 t_0 + a_1 t_1 \equiv k \pmod{q}$, so let $L \subseteq \mathbb{Z}^2$ be the set of such integral pairs (t_0, t_1), and let u_0 be L's shortest vector. Let integer $c \in \left(-\frac{1}{2}(q-1), \frac{1}{2}(q-1)\right]$ be the unique value satisfying $c \equiv k a_0^{-1} \pmod{q}$, so $L = (c, 0) + L'$ where $L' = \{(t_0, t_1) \in \mathbb{Z} : a_0 t_0 + a_1 t_1 \equiv 0 \pmod{q}\}$ is a lattice with basis vectors $v_1 = (q, 0)$ and $v_2 = (-a_0^{-1} a_1, 1)$. Apply Gauss reduction on L' to obtain ordered basis u_1, u_2.

Lemma 13. $|u_0| < |u_2|$.

Proof. Write $(c,0)$ in $\operatorname{span}_{\frac{1}{q}\mathbb{Z}}\{u_1,u_2\}$ as

$$(c,0)=\left(h_1+\frac{r_1}{q}\right)u_1+\left(h_2+\frac{r_2}{q}\right)u_2$$

(with $h_1,r_1,h_2,r_2\in\mathbb{Z}$ and $0\leqslant r_1,r_2<q$) and since $u_0=(c,0)+\ell'$ for some $\ell'\in L'$ is a shortest vector of L, $u_0\in\left\{\left(\frac{r_1}{q}+i\right)u_1+\left(\frac{r_2}{q}+j\right)u_2 : i,j\in\{-1,0\}\right\}$ hence $u_0=h_1'u_1+h_2'u_2$ for $h_1',h_2'\in\frac{1}{q}\mathbb{Z}$ with $|h_1'|,|h_2'|<\frac{1}{2}$ in order to ensure that the vector is shortest (and strict inequality following from q's oddness). The claim follows. ■

Now, write the three vectors in terms of their components: $u_0=(u_{0,0},u_{0,1}),u_1=(u_{1,0},u_{1,1}),u_2=(u_{2,0},u_{2,1})$. Because $u_0\in L$ and $u_1,u_2\in L'$, we have the following integers:

$$u_0'=\frac{k-a_0u_{0,0}-a_1u_{0,1}}{q}\qquad u_1'=\frac{a_0u_{1,0}+a_1u_{1,1}}{q}\qquad u_2'=\frac{a_0u_{2,0}+a_1u_{2,1}}{q}.$$

These allow us to rewrite $Q(t_0,t_1)$ by parameterizing $L=(c,0)+L'=\left\{u_0+u_1x+u_2y:(x,y)\in\mathbb{Z}^2\right\}$ in that way:

$$F(x,y)=(u_0'-xu_1'-yu_2')-(u_{0,1}+xu_{1,1}+yu_{2,1})^2-(u_{0,2}+xu_{1,2}+yu_{2,2})^2.$$

By the preceding definitions of (integral) variable, (t_0,t_1) has the form $u_0+u_1x+u_2y$ if and only if $Q(t_0,t_1)\in\mathbb{Z}$. Now, we are prepared to characterize F's positive domain.

Lemma 14 ([Sar19, Lemma 3.1])**.** *When* $|(t_0,t_1)|<\frac{\sqrt{N}}{2q}-1$, $Q(t_0,t_1)>0$.

Proof. In this case, $|t_0|,|t_1|<\frac{\sqrt{N}}{2q}-1$ too, and so, recalling that $|a_0|,|a_1|<q$,

$$\begin{aligned}Q(t_0,t_1)&=\frac{N}{4q^2}-\frac{a_0^2+a_1^2}{4q^2}-\left(t_0^2+t_1^2\right)-\frac{a_0t_0+a_1t_1}{q}\\&>\frac{N}{4q^2}-\frac{1}{2}-\left(\frac{N}{4q^2}-\frac{\sqrt{N}}{q}+1\right)-\left(\frac{\sqrt{N}}{q}-2\right)\\&=\frac{1}{2},\end{aligned}$$

so the result is proved. ■

Lemma 15 ([Sar19, Lemma 3.1])**.** *When* $|(t_0,t_1)|>\frac{\sqrt{N}}{2q}+\sqrt{2}$, $Q(t_0,t_1)<0$.

Proof. In this case, $|t_0|+|t_1|\leqslant\sqrt{2}\left(\frac{\sqrt{N}}{2q}+\sqrt{2}\right)$, and so, recalling that $|a_0|,|a_1|<$

q,

$$\begin{aligned} Q(t_0,t_1) &= \frac{N}{4q^2} - \frac{a_0^2+a_1^2}{4q^2} - \left(t_0^2+t_1^2\right) - \frac{a_0t_0+a_1t_1}{q} \\ &< \frac{N}{4q^2} - \left(\frac{N}{4q^2} + \sqrt{2}\frac{\sqrt{N}}{q} + 2\right) - \sqrt{2}\left(\frac{\sqrt{N}}{2q} + \sqrt{2}\right) \\ &= -\frac{3\sqrt{2N}}{2q}, \end{aligned}$$

so the result is proved. ■

Lemma 16 ([Sar19, Lemma 3.1])**.** *If* $\frac{\sqrt{N}}{q|u_2|} \geqslant \frac{2}{3}\sqrt{2}+4$*, then* $F(x,y) > 0$ *whenever*[3]

$$|x| \leqslant \frac{\sqrt{N}}{2q\,|u_1|} - 1 \qquad \textit{and} \qquad |y| \leqslant \frac{\sqrt{N}}{2q\,|u_2|} - 1$$

and $F(x,y) < 0$ *whenever*[4]

$$|x| > \frac{10\sqrt{N}}{2q\,|u_1|} - 10 \qquad \textit{or} \qquad |y| > \frac{10\sqrt{N}}{2q\,|u_2|} - 10.$$

Proof. Fix an identification of $(t_0,t_1) = u_0 + u_1x + u_2y$.

We have $|(t_0,t_1)| \leqslant |u_0| + |u_1|\,|x| + |u_2|\,|y| < |u_1|\,|x| + |u_2|\,(1+|y|)$ and by computation, when $|x| \leqslant \frac{\sqrt{N}}{2q|u_1|} - 1$ and $|y| \leqslant \frac{\sqrt{N}}{2q|u_2|} - 1$, we achieve the bound necessary to apply Lemma 14, thereby finishing the first part of the Lemma.

We also have

$$|(t_0,t_1)| = |u_0 + u_1x + u_2y| \geqslant |u_1x + u_2y| - |u_0| \geqslant \frac{1}{2}\left(|u_1|\,|x| + |u_2|\,|y|\right) - |u_2| \tag{17}$$

using almost-orthogonality and $|u_0| < |u_2|$. There are now two cases to complete for the second part of the Lemma:

- **Case I:** $|x| > \frac{5\sqrt{N}}{q|u_1|} - 10$**.** Since $y \in \mathbb{Z}$, $\frac{1}{2}\,|y| - 1 \geqslant -1$. Using these bounds, we have $|(t_0,t_1)| \geqslant \frac{5\sqrt{N}}{2q} - 5\,|u_1| - 1 = \frac{\sqrt{N}}{q} + \left(\frac{3\sqrt{N}}{2q|u_1|} - 5\right)|u_1|$. Now, $|u_2| \geqslant |u_1| \geqslant 1$ so we see that we can apply Lemma 15 to conclude this case of the Lemma's second part.
- **Case II:** $|y| > \frac{5\sqrt{N}}{q|u_2|} - 10$**.** Since $x \in \mathbb{Z}$, $\frac{1}{2}\,|y| \geqslant 0$. Using these bounds, we have $|(t_0,t_1)| \geqslant \frac{5\sqrt{N}}{2q} - 6\,|u_2| = \frac{\sqrt{N}}{q} + \left(\frac{3\sqrt{N}}{2q|u_2|} - 6\right)|u_2|$. Now, $|u_2| \geqslant 1$ so we see that we can apply Lemma 15 to conclude the Lemma's second part.

[3]For convenience, we refer to these bounds as A and B, respectively, and the set of such (x,y) as C.

[4]It follows that such (x,y) lie in $(10C)^c$.

Therefore we are done. ■

Lemma 18 ([Sar19, Lemma 3.2])**.** *If* $\frac{\sqrt{N}}{q|u_2|} < \frac{2}{3}\sqrt{2} + 4$ *and* $F(x, y) > 0$*, then* $|y| \leqslant 9$*.*

Proof. From (17) and (the contrapositive of) Lemma 15,

$$\left(\frac{1}{2}|y| - 1\right)|u_2| \leqslant |(t_0, t_1)| \leqslant \frac{\sqrt{N}}{2q} + \sqrt{2}$$

and so we conclude, since $|u_2| \geqslant 1$ hence $\frac{1}{|u_2|} \leqslant 1$,

$$|y| \leqslant \frac{\sqrt{N}}{q\,|u_2|} + 2\left(\sqrt{2} + 1\right) \approx 9.77$$

thereby showing the desired bound. ■

Problem 19. *Take* $N \in \operatorname{poly} q$ *coprime to 2 and* q*, and let* $a_0, a_1 \in \mathbb{Z}$ *be given values with* $a_0^2 + a_1^2 \equiv N \pmod{4q}$*. Find* $(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$ *with*

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = N \tag{20}$$

and, modulo $2q$*,*

$$\begin{aligned} x_0 &\equiv a_0 & x_2 &\equiv 0 \\ x_1 &\equiv a_1 & x_3 &\equiv 0. \end{aligned}$$

Theorem 21 ([Sar19, Theorem 1.11])**.** *Take Assumption 7. The (deterministic) algorithm specified in Algorithm 1 solves Problem 19, if a solution exists, in* $\operatorname{poly}\log q$ *time.*

It warrants clarifying here some of the notation in some lines of Algorithm 1.

3–4, 15–16: The factorization of $F(x, y)$ is given in terms of some primes $p_i \not\equiv 3 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for which $F(x, y) = \prod_{i=1}^{n} p_i^{e_i} \prod_{j=1}^{m} q_j^{f_j}$.

7, 19: This line simply runs and returns Theorem 9 on the prime $p_i \not\equiv 3 \pmod 4$, writing it as $x_i^2 + y_i^2 = p_i$.

8, 20: It is an elementary fact that the product of sums of two squares is again a sum of two squares: $(x_0^2 + x_1^2)(y_0^2 + y_1^2) = (x_0y_0 + x_1y_1)^2 + (x_0y_1 - x_1y_0)^2$. Since all primes $p_i \not\equiv 3 \pmod 4$ can be so decomposed e.g. via Theorem 9, finite products of such primes also have such decompositions. In particular, given a finite list of tuples $(x_0, x_1), (y_0, y_1), (z_0, z_1), \ldots$, we define $\textsc{Combine}(\{(x_0, x_1), (y_0, y_1)\}) = (x_0y_0 + x_1y_1, x_0y_1 - x_1y_0)$ and for longer lists, $\textsc{Combine}(\{(x_0, x_1), (y_0, y_1), (z_0, z_1), \ldots\}) = \textsc{Combine}(\{(x_0y_0 + x_1y_1, x_0y_1 - x_1y_0), (z_0, z_1), \ldots\})$, i.e. a call of Combine on a shorter input.

Algorithm 1 Algorithm to solve Problem 19.

Require: $p, q, N, a_0, a_1, u_1, u_2, F$

if $\frac{\sqrt{N}}{q|u_2|} \geqslant \frac{2}{3}\sqrt{2} + 4$ **then**
  for $(x, y) \in 10C$ **do**
    $\ell \leftarrow \textsc{Factor}(F(x, y))$
    $\ell \leftarrow \{(p_i, e_i) : i \in [n]\} \cup \{(q_j, f_j) : j \in [m]\}$
    if $2 \mid f_j$ for all $j \in [m]$ **then**
      for $(p_i, e_i) \in \ell$ **do**
        $(x_i, y_i) \leftarrow \textsc{Schoof}(p_i)$
      $(X, Y) \leftarrow \textsc{Combine}(\{(x_{i,j}, y_{i,j}) : i \in [n], j \in [e_i], (x_{i,j}, y_{i,j}) = (x_i, y_i)\})$
      return $\prod_{i=1}^{m} q_j^{f_j/2}(X, Y)$
else
  for $y \in [-9, 9] \cap \mathbb{Z}$ **do**
    $G(x) \leftarrow F(x, y)$
    $G(x) \leftarrow A'x^2 + B'x + C'$
    for $x \in \left[\frac{-B' - \sqrt{B'^2 - 4A'C'}}{2A'}, \frac{-B' + \sqrt{B'^2 - 4A'C'}}{2A'}\right] \cap \mathbb{Z}$ **do**
      $\ell \leftarrow \textsc{Factor}(F(x, y))$
      $\ell \leftarrow \{(p_i, e_i) : i \in [n]\} \cup \{(q_j, f_j) : j \in [m]\}$
      if $2 \mid f_j$ for all $j \in [m]$ **then**
        for $(p_i, e_i) \in \ell$ **do**
          $(x_i, y_i) \leftarrow \textsc{Schoof}(p_i)$
        $(X, Y) \leftarrow \textsc{Combine}(\{(x_{i,j}, y_{i,j}) : i \in [n], j \in [e_i], (x_{i,j}, y_{i,j}) = (x_i, y_i)\})$
        return $\prod_{i=1}^{m} q_j^{f_j/2}(X, Y)$

Proof. **Case I:** $\frac{\sqrt{N}}{q|u_2|} \geqslant \frac{2}{3}\sqrt{2}+4$ **(lines 1–9).** If $4AB > C_\gamma(\log N)^\gamma$ then it suffices to simply search radially outward from the origin $(0,0)$, and Conjecture 6 ensures that in time $C_\gamma(\log N)^\gamma \in \operatorname{poly}\log q$ a satisfactory lattice point will be found. By Conjecture 5, lines 3–4 run in polynomial time. Theorem 9 is well-known to be in $\operatorname{poly}\log p_i$ as it has the same runtime as the Euclidean algorithm. The other steps are trivially efficient.

If $4AB \leqslant C_\gamma(\log N)^\gamma$ then as $N \in \operatorname{poly} q$, we have $400AB \in \operatorname{poly}\log q)$ (where $400AB \approx \#(10C)$). Therefore it is a simple task of running through $10C$ (which we want to do since $A_{Q,r} \subset 10C$ for all $r \geqslant \sqrt{A^2+B^2}$). By Conjecture 5, lines 3–4 run in polynomial time. Theorem 9 is well-known to be in $\operatorname{poly}\log p_i$ as it has the same runtime as the Euclidean algorithm. The other steps are trivially efficient.

Case II: $\frac{\sqrt{N}}{q|u_2|} < \frac{2}{3}\sqrt{2}+4$ **(lines 10–21).** By writing $F(x,y)$ as a polynomial G in just x for fixed $y \in [-9,9]$, we see that by construction, G's leading coefficient is negative, so there are only finitely many integer values that x can take for which $G(x) \geqslant 0$; these are given in line 14. Again using Conjecture 6 in the case that there are more than $C_\gamma(\log N)^\gamma$ pairs (x,y) thusly obtained, we run through these points, where lines 15–16 run in polynomial time and Theorem 9 is well-known to be in $\operatorname{poly}\log p_i$ as it has the same runtime as the Euclidean algorithm. The other steps are trivially efficient. ■

Take $v \in X^{p,q}$ of the form $v = \begin{pmatrix} a+b\iota & \\ & a-b\iota \end{pmatrix}$. v's *lattice* in $\mathbb{Z}^2$ is

$$L_v = \left\{(x,y) \in \mathbb{Z}^2 : ax+by \equiv 0 \pmod q\right\}.$$

Theorem 22 ([Sar19, Theorem 1.13])**.** *Take Assumption 7. Let* $v = \begin{pmatrix} a+b\iota & \\ & a-b\iota \end{pmatrix} \in X^{p,q}$ *be any diagonal matrix with lattice* L_v *having Gauss reduced basis* $\{u_1,u_2\}$*,* u_1 *being a shortest vector of* L_v*. Then, the shortest path from the identity to* v *is of length* h*, where*

$$h < \begin{cases} \lceil 4\log_p q - 2\log_p |u_1| + \log_p 22 \rceil & \frac{|u_2|}{|u_1|} \geqslant C_\gamma(5\log q)^\gamma \\ \lceil 3\log_p q + \gamma\log_p(5\log q) + \log_p C_\gamma + \log_p 22 \rceil & \textit{otherwise.} \end{cases}$$

For both cases, the approach to this proof will be the same. First, we will quickly argue why we want to solve the particular class of Diophantine equations. Then, we establish that a path exists of length up to some upper bound (specifically, the bound given in the Theorem statement). Finally, we will verify that all paths lengths, in increasing order, can be checked efficiently.

Proof. We seek to find paths of length h by first translating the task to one of Diophantine equations (accomplished in Theorem 3), and then to efficiently solving said Diophantine equations (accomplished in Theorem 21).

Let $\widehat{p} \in \mathbb{Z}$ satisfy $\widehat{p}^2 \equiv p \pmod{q}$. ($\widehat{p}$ exists by Assumption 1.) Fix h_0 as on the right-hand side of the h-bound in the Theorem statement. Letting

$$\begin{aligned} x_0 &= 2qt_0 + a\widehat{p}^{h_0} & x_2 &= 2qt_2 \\ x_1 &= 2qt_1 + b\widehat{p}^{h_0} & x_3 &= 2qt_3, \end{aligned}$$

Theorem 3 tells us that there is a path of length h_0 from the identity to v if and only if there is $(t_0, t_1, t_2, t_3) \in \mathbb{Z}^4$ satisfying

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = p^{h_0}.$$

We solve this using Algorithm 1 (recall the notation from there) and as noted in the proof of Theorem 21, if $4AB \geqslant C_\gamma(\log q^5)^\gamma \geqslant C_\gamma(\log p^{h_0})^\gamma$ then a solution is guaranteed to exist, by Conjecture 6, and is found efficiently, by Theorem 10, and projected back down by ϕ.

Case I: $\frac{|u_2|}{|u_1|} \geqslant C_\gamma(5\log q)^\gamma$**.** We observe that

$$p^{h_0} \geqslant \frac{22q^4}{|u_1|^2}$$

and so

$$B = \frac{\sqrt{p^h}}{4q\,|u_2|} - 1 \geqslant \frac{\sqrt{22}q^2}{2q\,|u_1|\,|u_2|} - 1.$$

By almost-orthogonality we have $|u_1|\,|u_2| \leqslant \frac{2}{\sqrt{3}}q$ and so we verify that $B \geqslant \frac{\sqrt{3\cdot 22}}{4} - 1 > 1$. From the definitions of A and B and the fact that $|u_2| \geqslant |u_1|$, we have $A \geqslant \frac{|u_2|}{|u_1|}B \geqslant C_\gamma(5\log q)^\gamma B$, hence $4AB \geqslant 4C_\gamma(5\log q)^\gamma B^2 > C_\gamma(5\log q)^\gamma$. This shows existence of the path of length h_0, thereby bounding from above the length of the shortest path.

To show that *the* shortest path can be found in polynomial time, increment h from 1 to h_0, and halt once the following system has a solution: letting

$$\begin{aligned} x_0 &= 2qt_0 + a\widehat{p}^{h} & x_2 &= 2qt_2 \\ x_1 &= 2qt_1 + b\widehat{p}^{h} & x_3 &= 2qt_3, \end{aligned}$$

find $(t_0, t_1, t_2, t_3) \in \mathbb{Z}^4$ satisfying

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = p^{h}.$$

If this system has a solution but no smaller h suffices then by Theorem 3 there will be a path of length h and none shorter.

Case II: $\frac{|u_2|}{|u_1|} < C_\gamma(5\log q)^\gamma$**.** We repeat much of the logic from **Case I**. We observe that

$$p^{h_0} \geqslant 22C_\gamma(5\log q)^\gamma q^3.$$

The hypothesis also implies that $|u_2|^2 < C_\gamma(5\log q)^\gamma |u_1||u_2| \leqslant C_\gamma(5\log q)^\gamma \frac{2}{\sqrt{3}}q$ and combining these gives

$$\begin{aligned} B = \frac{\sqrt{p^{h_0}}}{2q|u_2|} - 1 &\geqslant \frac{\sqrt{22}\sqrt{C_\gamma(5\log q)^\gamma}q^{3/2}}{2q\sqrt{C_\gamma(5\log q)^\gamma}\sqrt{\frac{2}{\sqrt{3}}q}} - 1 \\ &= \frac{\sqrt{22}}{2\sqrt{\frac{2}{\sqrt{3}}}} - 1 \\ &> 1 \end{aligned}$$

and since $A \geqslant B \geqslant 1$, we have $A \geqslant \frac{1}{2}(A+1) = \frac{\sqrt{p^{h_0}}}{4q|u_1|}$ and $B \geqslant \frac{1}{2}(B+1) = \frac{\sqrt{p^{h_0}}}{4q|u_2|}$, therefore

$$4AB \geqslant (A+1)(B+1) \geqslant \frac{p^{h_0}}{16q^2|u_1||u_2|} \geqslant \frac{22\sqrt{3}}{32}C_\gamma(5\log q)^\gamma > C_\gamma(\log p^{h_0})^\gamma.$$

This shows existence of the path of length h_0, thereby bounding from above the length of the shortest path.

To show that *the* shortest path can be found in polynomial time, increment h from 1 to h_0, and halt once the following system has a solution: letting

$$\begin{aligned} x_0 &= 2qt_0 + a\widehat{p}^h & x_2 &= 2qt_2 \\ x_1 &= 2qt_1 + b\widehat{p}^h & x_3 &= 2qt_3, \end{aligned}$$

find $(t_0, t_1, t_2, t_3) \in \mathbb{Z}^4$ satisfying

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = p^h.$$

If this system has a solution but no smaller h suffices then by Theorem 3 there will be a path of length h and none shorter. ■

Proof of Theorem 11. Suppose that vertex $v = \begin{pmatrix} a+b\iota & \\ & a-b\iota \end{pmatrix} \in X^{p,q}$ is of distance h from the identity, and that $h > h_0$. By Theorem 22, $h \leqslant \lceil 4\log_p q - 2\log_p |u_1| + \log_p 22 \rceil$ and exponentiating and rearranging reveals

$$|u_1|^2 \leqslant \frac{22q^4}{p^{h-1}}. \tag{23}$$

The question then is how many such v there can be. The lattice L_v is determined by its shortest vector, since if (α, β) is a shortest vector then considering vectors $(\alpha\lambda, \beta\lambda) \bmod q$ for various $\lambda \in \mathbb{Z}$ gives rise to a vector outside of $\operatorname{span}_{\mathbb{Z}} \langle(\alpha, \beta)\rangle$. Further, v, as a member of a projective group, is uniquely determined by L_v by deducing all possible values of (a, b) and noting that they must all differ by some multiplicative constant $\lambda \in \mathbb{F}_q^\times$. Hence, u_1 determines v. Since there are at most $\frac{22\pi q^4}{p^{h-1}} \in O(q)$ integer vectors u_1 satisfying (23), these are at most that many v at distance $h > h_0$. ■

Proof of Theorem 12. **Case I:** $\frac{|u_2|}{|u_1|} \geqslant C_\gamma(5\log q)^\gamma$**.** As a shortest vector of a sublattice of $\mathbb{Z}^2$, $|u_1| \geqslant 1$, so $-2\log_p|u_1| \leqslant 0$ and vanishes when we upper-bound the quantity. Then, note that $q^3 = \frac{2\#X^{p,q}}{1-\frac{1}{q^2}}$, so $4\log_p q = \frac{4}{3}\log_p \#X^{p,q} - \frac{4}{3}\log_p\left(1-\frac{1}{q^2}\right) + \frac{4}{3}\log_p 2$. There is a lower bound $q_1 = 20$ for which when $q > q_1$, $22\left(\frac{2}{1-\frac{1}{q^2}}\right)^{4/3} \leqslant 56$, as $22\cdot 2^{4/3} \approx 55.4$.[5] Therefore, we find that the first bound on h from Theorem 22 becomes $\left\lceil \frac{4}{3}\log_p \#X^{p,q} + \log_p 56\right\rceil$.

Case II: $\frac{|u_2|}{|u_1|} < C_\gamma(5\log q)^\gamma$**.** Observe that there is a lower bound q_2 for which when $q > q_2$, $C_\gamma(5\log q)^\gamma \leqslant q$, hence the second bound on h from Theorem 22 becomes $\left\lceil 4\log_p q + \log_p 22\right\rceil \leqslant \left\lceil \frac{4}{3}\log_p \#X^{p,q} + \log_p 56\right\rceil$ when also $q > q_1$.

Therefore, in both cases, we have the claimed bound when $q > \max\{q_1, q_2\}$. ■

This completes the proof of Theorems 11 and 12. We now move onto how we can leverage this factorization only twice (in contrast with [Sar19], which uses it four times) to factor general elements.

2.1.4 Factorization of general elements

We shall prove the following result:

Theorem 24 ([CP18, Lemma 7])**.** *Taking Conjecture 5, any vertex $v \in X^{p,q}$ can be written in the form $v = X_1\phi(v_2)X_3$ where $X_1, X_3 \in X^{p,q}$ are diagonal and $v_2 \in \Omega$ in $\operatorname{poly}\log q$ time.*

From this, it is immediate to efficiently obtain a factorization of nearly all elements of length up to $(7+o(1))\log_p q$ by applying the algorithms of Theorems 10 and 11. For completeness' sake, we write this out:

Theorem 25 ([CP18, Lemma 8])**.** *Taking Conjecture 5, asymptotically-all vertices $x \in X^{p,q}$ can be efficiently written as the product of up to $(7+o(1))\log_p q$ elements of S.*

Proof of Theorem 24. First, we note the decomposition of generic elements into diagonal matrices; in a sense, for any ring R, $R^{2\times 2}$ is a two-dimensional module over its subring of diagonal matrices spanned by $I_2 = \begin{pmatrix}1 & \\ & 1\end{pmatrix}$ and $J = \begin{pmatrix} & 1\\ -1 & \end{pmatrix}$, via the (trivially) unique representation

$$M = \begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a & \\ & d\end{pmatrix} I_2 + \begin{pmatrix}b & \\ & -c\end{pmatrix} J,$$

[5] 56 is not special beyond being the "smallest nice number" on the interval $\left(22\cdot 2^{4/3}, \infty\right)$.

so in a sense, we can take M's I_2- and J-"components."[6] Therefore, decompose $v = D + EJ$. We seek diagonal $X_1, X_3 \in X^{p,q}$ and nondiagonal $v_2 = X_2 + Y_2 J \in \Omega$ satisfying $v = X_1\phi(v_2)X_3$, or, for some $e \in \mathbb{N}$,

$$\begin{aligned} D + EJ &= X_1\phi(X_2 + Y_2 J)X_3 \\ \implies D &= X_1\phi(X_2)X_3 \qquad (26) \\ \implies E &= X_1\phi(Y_2)\overline{X_3} \qquad (27) \\ \det v_2 = p^e &= \det X_2 + \det Y_2 \qquad (28) \end{aligned}$$

with the last line coming from the definition of Ω. From (26) and (27), we conclude

$$\begin{aligned} \det X_2 &\equiv p^e \frac{\det D}{\det v} \pmod{q} \\ \det Y_2 &\equiv p^e \frac{\det E}{\det v} \pmod{q} \end{aligned}$$

and so having chosen some $e \in \mathbb{N}$, we attempt to find $1 \leqslant d \leqslant p^e$ such that both d and $p^e - d$ can be efficiently represented as the sum of two squares. This is desirable because both X_2 and Y_2 take the form $M = \begin{pmatrix} a+bi & \\ & a-bi \end{pmatrix}$ and so $\det M = a^2 + b^2$, which can be found using Theorem 9; if $d = \det X_2$ then by (28), $\det Y_2 = p^e - d$. We do this by searching that interval for such d in an arithmetic progression of difference q such that $d \equiv p^e \frac{\det D}{\det v} \pmod{q}$, and as in Algorithm 1 we factor d and $p^e - d$ in each iteration (using our blackbox factoring algorithm, Conjecture 5) to find the representation. If no such d exists, we increment e. Having found such an e and hence fixing X_2, Y_2, and hence v_2, we now move on to finding X_1 and X_3.

Write

$$\begin{aligned} K_1 &= \overline{D}\phi(Y_2)E^{-1}\overline{\phi(X_2)}^{-1} \\ K_3 &= E\phi(X_2)D^{-1}\phi(Y_2)^{-1}. \end{aligned}$$

Clearly $X_1K_1 = \overline{X_1}$ and $X_3K_3 = \overline{X_3}$ by manipulating (26) and (27). We solve this now for $XK = \overline{X}$, as identical reasoning suffices for both equations. If $K = I_2$ then just pick $X = I_2$. Otherwise, write $K = \begin{pmatrix} w_0 + x_0\iota & \\ & w_0 - x_0\iota \end{pmatrix}$ and we wish to find $X = \begin{pmatrix} w + x\iota & \\ & w - x\iota \end{pmatrix}$. Solving the system of two variables in two equations gives $w = x_0$ and $x_0 = w_0 - 1$. (Clearly this is degenerate if and only if $K = I_2$, which is why we treat that separate case.) This completes the decomposition.

[6] J also enjoys the following nice properties, which are trivial to check:

- If M decomposes into $M_1 + M_2 J$ then $\det M = \det M_1 + \det M_2$.
- $JM = \overline{M}J$.

The naïve approach specified above for searching the intervals $[p^e]$ is sufficiently fast when the number of terms considered (which comprise the set I_e), about $\frac{p^e}{q}$, is small, but in the case that $\frac{p^e}{q} \in \omega(\log q)$ this routine becomes superlinear and possibly even exponential. We seek some assurance then that the algorithm typically halts for $e \in O(\log q)$. We primarily rest on a belief, in the style of Cramér's conjecture and Conjecture 6, that sums of squares are dense in $\mathbb{N}$. Seeking to analogize Conjecture 6 in particular, we note that the operative aspect is that a dense cluster of lattice points will represent a sum of two squares, and that a point accomplishing this will be found quickly even through a linear search. We see that for small sets of values of e, e.g. $[n]$ for $n \in O(\log q)$, we get a similarly dense subset of $\mathbb{N}^2$ by looking at $D_e = \{(i, p^e - i) : i \in I_e\}$ and $\bigcup_{k=1}^{n} D_k \subset \mathbb{N}^2$. ■

2.1.5 Changes made to values in [Sar19]

Here lists how each result in this summary can be modified to agree exactly with the statements in [Sar19]. These are primarily cosmetic alterations, made to fit the specifics here, and do not alter the thrust of the arguments in any way.

- Assumption 1 has the added inequalities simply to make it additionally evident why the bounds later proved will hold.
- [Sar19]'s definition of h_0 has $\cdots + \gamma \log_p \log q + \cdots$.
- Theorem 11 is stated in terms of a parameter α whose use does not arise in our setting.
- In Theorems 11, 12, and 22, [Sar19] has 89 instead of 22π, 56, and 22, respectively.
- In Lemma 14, [Sar19] has $\frac{\sqrt{N}}{q} - 1$. In Lemma 15, [Sar19] has $\frac{\sqrt{N}}{q} + 1$.
- In Lemma 16, [Sar19] has $\frac{14}{3} = 4.\bar{6}$ rather than the value given, $\frac{2}{3}\sqrt{2} + 4 \approx 4.94$.
- In Lemma 18, [Sar19] has 13 rather than 9.
- In Theorem 22, [Sar19] has $C_\gamma (\log 2q)^\gamma$ as the cutoff for $\frac{|u_2|}{|u_1|}$.

References

[AKS04] M. Agrawal, N. Kayal, and N. Saxena. "PRIMES is in P." In: *Annals of Mathematics* (2004).

[Coh] H. Cohn. "Factoring may be easier than you think." (n.d.).

[CP18] E. Carvalho Pinto and C. Petit. "Better path-finding algorithms in LPS Ramanujan graphs." In: *Journal of Mathematical Cryptology* 12(4) (2018).

[Día18] D. Díaz. "matrix: A native implementation of matrix operations." In: *Hackage: The Haskell Package Repository* (2018).

[DSV03] G. Davidoff, P. Sarnak, and A. Valette. *Elementary number theory, group theory, and Ramanujan graphs.* Cambridge University Press (2003).

[FL20] D. Fischer and A. Lelechenko. "arithmoi: Efficient basic number-theoretic functions." In: *Hackage: The Haskell Package Repository* (2020).

[Gv66] R. L. Graham and J. H. van Lint. "On the Distribtion of $n\theta$ modulo 1." In: *Canadian Journal of Mathematics* 20 (1966), pp. 1020–1024.

[HW38] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 1938. ISBN: 9780199219865.

[Len83] H. W. Lenstra, Jr. "Integer Programming with a Fixed Number of Variables." In: *Mathematics of Operations Research* 8(4) (1983).

[Lit14] J. E. Littlewood. "Sur la distribution des nombres premiers." In: *Comptes Rendus* 158 (1914), pp. 1869–1872.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. "Ramanujan graphs." In: *Combinatorica* 8(4) (1988).

[Moz20] C. J. Mozzochi. "A Proof of Sarnak's Golden Mean Conjecture." In: *Journal of Number Theory* (2020), to appear.

[MSS16] F. Motta, P. Shipman, and B. Springer. "Optimally Topologically Transitive Orbits in Discrete Dynamical Systems." In: *American Mathemtatical Monthly* 123(2) (2016), pp. 115–135.

[PS18] O. Parzanchevski and P. Sarnak. "Super-Golden-Gates for $PU(2)$." In: *Advances in Mathematics* 327 (2018), pp. 869–901.

[Rid87] J. N. Ridley. "Descriptive Phyllotaxis on Surfaces with Circular Symmetry." In: *Mathematical Modeling* 8 (1987), pp. 751–755.

[RS94] M. Rubinstein and P. Sarnak. "Chebyshev's bias." In: *Experimental Mathematics* 3(3) (1994), pp. 173–197.

[RS16] N. Ross and P. Selinger. "Optimal ancilla-free Clifford+T approximation of z-rotations." In: *Quantum Information & Computation* (2016).

[RS18] N. Ross and P. Selinger. "newsynth: Exact and approximate synthesis of quantum circuits." In: *Hackage: The Haskell Package Repository* (2018).

[Sar11] P. Sarnak. "Mobius Randomness and Dynamics." Mahler lectures (2011).

[Sar15] P. Sarnak. "Letter to Scott Aaronson and Andy Pollington on the Solovay–Kitaev Theorem and Golden Gates." (2015).

[Sar19] N. Sardari. "Complexity of Strong Approximation on the Sphere." In: *International Mathematics Research Notices* (2019).

[Sch85] R. Schoof. "Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p." In: *Mathematics of Computation* 44(170) (1985).

[Sla50] N. Slater. "The distribution of the integer N for which $\{\theta N\} < \phi$." In: *Proceedings of the Cambridge Philosophical Society* 46 (1950), pp. 525–537.

[Sós57] V. Sós. "On the theory of diophantine approximations I." In: *Acta Mathematica* 8 (1957), pp. 461–472.

[Sti20] Z. Stier. "Optimal topological generators of U(1)." In: *Journal of Number Theory* (2020), to appear.