Letter to S.D. Miller and N. Tabeli Zadeh on optimal strong approximation by integral points on quadrics; the case : $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/q\mathbb{Z})$.

Dear Steve and Naser,

I am following up on my letter "The Solovay-Kitaev Theorem and universal quantum Golden Gates" [Sa 1], and our discussions. The main problems that remain as far as the optimality of the universal arithmetic quantum gates are problems (1) and (3) on page 24. It turns out that the analogue of (1) for the split quadratic form $x_1x_4 - x_2x_3$ can be solved elementarily and even with a polynomial time algorithm. I give the details below.

Before discussing that, here are some analogous well studied 1-dimensional integral lifting problems. Given integers b and q the least nonnegative integer with $m \equiv b \,(q)$ lies in $[0, q-1]$ and it can be found in polynomial time (that is poly in $\max\{\log b, \log q\}$) with the division algorithm.

It is remarkable that introducing a quadratic equation into the picture makes for a very different story. In [A-M] it is shown that the problem of finding the smallest non-negative integer satisfying $x^2 \equiv b \pmod{q}$ is NP complete! This should be borne in mind below for the problem of the minimal integral lift on quadrics.

A much studied lifting problem in 1-dimension is to prime numbers. For a and q integers with $(a,q)=1$ let $m(a,q)$ be the least prime p congruent to a mod q. Let

$$m(q) = \max_{(a,q)=1} m(a,q) \qquad \text{——(1)}$$

The $\pi(x)$ prime numbers, less than x distribute themselves into the $\phi(q)$ such residue classes a mod q and $m(q)$ is the least x for which all the classes are occupied. Define the exponents

$$K(a,q) = \frac{\log m(a,q)}{\log \phi(q)}, \qquad \text{——(2)}$$

$$K(q) = \frac{\log m(q)}{\log \phi(q)} \qquad \text{——(3)}$$

and the mean exponent

$$K_\mu(q) = \frac{1}{\phi(q)} \sideset{}{^*}\sum_{a(q)} K(a,q) \qquad \text{——— (3).}$$

Note that $\log \phi(q) \sim \log q$ and that

$$1 \le \varliminf_{q\to\infty} K_\mu(q) \le \varliminf_{q\to\infty} K(q). \qquad \text{——— (4).}$$

The Linnik exponent K (in the literature it is called the Linnik constant but it is an exponent) is

$$K = \overline{\lim_{q\to\infty}} K(q) \ . \qquad \text{——— (5).}$$

Linnik's Theorem asserts that $K<\infty$ and it appears that the best known upper bound for K is still 5.5 [HB]. The generalized Riemann Hypothesis yields $K\le 2$, while what are today standard Conjectures concerning the distribution of low lying zeros for families together with GRH imply that $K=1$ [L-Y]. The q-analogue of a weak form of Cramer's conjecture, asserts that for some $B<\infty$

$$m(q) \ll q(\log q)^B. \qquad \text{——— (6.)}$$

While there is no reason to doubt such a strong statement about the least prime in a progression, it should be noted that the equidistribution of primes in progression fails for x as small as the right hand side of (6). This is shown in [F-G] following the archimedean analogue of irregular distribution of primes in short intervals [Ma].

The Golden Gates problem brings out the importance (in that setting) of the mean exponent

$$K_\mu = \overline{\lim_{q\to\infty}} K_\mu(q) . \qquad (7)$$

Under GRH, Turan [Tu] shows that

$$\sum_{a(q)}^{*} \left(\sum_{\substack{p\le x \\ p\equiv a(q)}} \log p - \frac{x}{\phi(q)} \right)^2 \ll x(\log x)^4 \qquad (8)$$

and hence that $K_\mu = 1$. That is for most $a \bmod q$, $(a,q)=1$, $K(a,q)$ is essentially 1.

As far as the algorithmic problem of finding the least prime in a progression, the simple linear search & testing whether $a+tq$ is prime for $t=0,1,2,\ldots$ [A-K-S] will terminate in polynomial time if (5) holds and in any case from (8) it will terminate in polynomial time for most a's under GRH.

We turn to the 4-variable quadric lifting problem; That is from $SL_2(\mathbb{Z}/q\mathbb{Z}) := V_q$ to $SL_2(\mathbb{Z})$. Given $f=\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix} \in V_q$, to find $F \in SL_2(\mathbb{Z})$ with $F = \begin{bmatrix}a & b\\ c & d\end{bmatrix} \equiv \begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix} = f \pmod q$ and with $|F|$ as small as possible, Here $|F|^2 = a^2+b^2+c^2+d^2$. Let $m(f,q)$ be the size of the least such lift and set

$$m(q) = \max_{f \in V_q} m(f,q). \qquad \text{——(9)}$$

If $N(T) = \#\{F \in SL_2(\mathbb{Z}) : |F| \le T\}$. ——(10)

Then it is known [Del] That

$$N(T) \sim C_1 T^2 \quad \text{as } T \to \infty. \qquad (11)$$

Hence if the F's with $|F| \leq T$ are to cover all of V_q we must have

$$T \gg |V_q|^{1/2}. \qquad (12)$$

Note also that

$$\log |V_q| \sim 3 \log q \quad \text{as } q \to \infty. \qquad (13)$$

Given (12) we define the covering exponents (This agrees with the normalizations above with $m(a,q)$ and also with [Sa1], in fact as far as the latter goes it is clear that this lifting problem is simply the 'q-adic' analogue of the approximation problem at the real place and with $x_1 x_4 - x_3 x_1 = 1$ replacing $x_1^2 + x_2^2 + x_3^2 + x_4^2 = N$):

$$K(f,q) = \frac{\log m(f,q)}{\log |V_q|^{1/2}} \qquad (14)$$

$$K(q) = \max_{f \in V_q} K(f,q). \qquad (15)$$

and the mean exponent

$$K_\mu(q) = \frac{1}{|V_q|} \sum_{f \in V_q} K(f,q) \qquad \text{——— (16.)}$$

Let $$K = \overline{\lim_{q\to\infty}} K(q) \qquad \text{——— (17)}$$

$$K_\mu = \overline{\lim_{q\to\infty}} K_\mu(q) . \qquad \text{——— (18)}$$

Clearly $1 \le K_\mu \le K$.

In what follows I show that the 'big hole' feature from [Sa] persists here, namely that $K \ge \frac{4}{3}$. In this split case there is an elementary proof that $K \le \frac{4}{3}$ and hence we conclude that $K = \frac{4}{3}$. Moreover using the same spectral methods as in [Sa1] we show that $K_\mu = 1$ (as in the definite case).

We begin with $K \le \frac{4}{3}$. We break the argument into steps which will allow us to analyze the complexity of finding a lift. Let $f = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in V_q$ be given and take $\alpha, \beta, \gamma, \delta$ all to be integers in $[0, q-1)$.

(Now $(\gamma, \delta, q) = 1$ and assume that $\delta \neq 0$. Let $m = (\delta, q)$ and write $\delta = \delta_1 m$, $q = q_1 m$. Then $(\gamma + \lambda q_1 m, \delta_1 m)$ $= (\gamma + \lambda q_1 m, \delta_1)$ since $(\gamma, m) = 1$.

We seek the first $\lambda = 0, 1, 2, \ldots$ for which $(\gamma + \lambda q, \delta) = (\gamma + \lambda q, \delta_1) = 1$.

Lemma: Let $(\delta_1, q) = 1$ and γ be integers; the least $\lambda = 0, 1, 2, \ldots$, call it L s.t. $(\lambda q + \gamma, \delta_1) = 1$ satisfies $L \ll (\log \delta_1)^3$.

PROOF: The Jacobsthal function $g(n)$ is the maximal length of an interval of integers none of which are relatively prime to n. It is known [Iw], [Vaa] that

$$g(n) \ll (\log n)^2 (\log \log n)^4 \qquad \text{---------- (9)}$$

Let the the least $\chi = 0, 1, 2, \ldots$ for which $q^{-1}\gamma + \chi$ is invertible mod δ_1 be $\bar{\chi}$.

Then $\hat{x} \leq g(\delta_1) \ll (\log \delta_1)^3$.

Now $q(q^{-1}\gamma + \hat{x})$ is invertible mod δ_1

and hence $\gamma + \hat{x}q$ is prime to δ_1.

It follows that the integer

$$c = \gamma + \hat{x}q$$

is prime to δ.

This completes the first step

That is we have the bottom row of our F, namely $[\times \; \times \; c \; d]$ with $d = \delta$

and $0 \leq c \leq q(\log q)^3$, $1 \leq d \leq q$.

If say $c \geq d$ (if $c < d$ Then use d as denominator) consider the Farey fractions with denominator at most c. If h/k is adjacent to d/c Then $1 \leq h \leq k \leq c$, $(h,k) = 1$ and $hd - kc = 1$. Thus we have $\tilde{F} = \begin{bmatrix} h & k \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$

with $|\tilde{F}| \ll q(\log q)^3$ and the bottom row of $\tilde{F}$ is congruent to the bottom row of f mod q. This completes step 2.

Since $\tilde{F}$ and f have the same bottom rows mod q it is easy to see that there is $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \in V_q$ such that $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \tilde{F} \equiv f \pmod q$.

Now choose t in $[0, q-1)$ as above then

$$F = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \tilde{F} \in SL_2(\mathbb{Z}) \text{ and}$$

$|F| \ll q^2 (\log q)^3$ and f lifts to F.

This completes step 3.

It follows that

$$m(q) \ll q^2 (\log q)^3 \qquad \text{——(20)}$$

and hence that

$$\overline{\lim_{q \to \infty}} \frac{\log m(q)}{\log \nu(q)^{1/2}} \leq \frac{4}{3}. \qquad \text{——(21)}$$

To prove that $K \geq \frac{4}{3}$ it suffices to produce a sequence of q's for which the limit of the $K(q)$'s is at least $4/3$. There are many ways of producing such q's and it seems likely that no matter how q is chosen this will happen. That is to say that

$$\underline{\lim_{q \to \infty}} \; K(q) \geq \frac{4}{3}. \qquad \text{——— (22)}$$

This if true would together with (21) imply that $K(q) \to 4/3$ as $q \to \infty$. I have not succeeded in showing (22).

A simple choice of q's giving that $K = 4/3$ in (17) is to take $q = 2^n$ and

$$f = \begin{bmatrix} 1-2^{n-1} & 0 \\ 0 & 1+2^{n-1} \end{bmatrix} \in V_q.$$ One checks that the minimal lift F of f is

$$F = \begin{bmatrix} 1-2^{n-1}+2^{2n-3} & 2^{2n-3} \\ 2^{2n-3} & 1+2^{n-1}+2^{2n-3} \end{bmatrix},$$

so that $|F| \gg 2^{2n} = q^2$. This shows that $K \geq \frac{4}{3}$.

The proof of (20) gives a (deterministic) polynomial time algorithm to find a lift F of a given f with $|F| \ll q^2 (\log q)^3$. Indeed each step is polynomial. Step 1 involves a direct search among the $(\log \delta_1)^3 \ll (\log q)^3$ λ's and for each the gcd is computed quickly using Euclid's algorithm. Similarly step 2 can be achieved quickly with continued fractions (Euclidian algorithm) and the t in step 3 is determined from the formula

$$\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \equiv \tilde{F} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}^{-1} \equiv \tilde{F} \begin{bmatrix} \delta & -\gamma \\ -\beta & \alpha \end{bmatrix} \bmod q.$$

While there are f's for which the algorithm giving the lift in (20) is essentially optimal, for most f's one can do better. This is to be expected since the procedure renders the bottom row to be of size q at the cost of the completion to F having its top row of size q^2. For most f's one can make all entries of size $f^{3/2}$, ie $K_\mu = 1$, as we show next.

We use the spectral theory of $\Gamma(q)\backslash\mathbb{H}$, where $\mathbb{H}$ is the upper half and $\Gamma(q)$ the congruence subgroup $\{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv I \pmod q\}$. The notation and theory is that of Selberg [Sel]. Let X be a large parameter and $k_X(z,\zeta)$ the point pair invariant

$$k_X(z,\zeta) = \begin{cases} 1 & \text{if } \frac{|z-\zeta|^2}{y\eta} \le X \\ 0 & \text{otherwise} \end{cases} \qquad (23)$$

Note that if $F = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ then with $i = \sqrt{-1}$,

$$k_X(Fi, i) = \begin{cases} 1 & \text{if } a^2+b^2+c^2+d^2 \le X \\ 0 & \text{otherwise} \end{cases} \qquad (24)$$

If $X = e^{\rho} + e^{-\rho} - 2$ then $\rho \sim \log X$ and $k_X(z,\zeta) = 1$ if $d(z,\zeta) \le \log X$ and is 0 otherwise.

For $f \in V_q$ let S_f be any integral lift of f. Then $F_\gamma = S_f\gamma$ for $\gamma \in \Gamma(q)$ varies over all the lifts of f.

Set

$$K_x(\xi,f) := \sum_{\gamma\in\Gamma(q)} k_x(\xi_f\gamma i,\xi) = \sum_{\substack{F\in SL_2(\mathbb{Z})\\ F=f(\mathrm{mod}\,q)}} k_x(Fi,\xi)$$

——(25)

Expanding $K_x(\xi,f)$ spectrally gives

$$K_x(\xi) = \sum_{\gamma\in\Gamma(q)} k_x(\gamma i,\xi_f^{-1}\xi) = \sum_{j=0}^{\infty} h_x(t_j)\phi_j(i)\overline{\phi_j(\xi_f^{-1}\xi)} + \text{cts}$$

——(26)

where $\phi_0,\phi_1,\ldots$ is the discrete spectrum of the Laplacian Δ on $L^2(\Gamma(q)\backslash\mathbb{H})$ and the eigenvalues are $\lambda_j = \frac{1}{4}+t_j^2$ and cts is a similar expression with continuous spectrum, which we ignore since it is handled similarly. h_x is the Selberg transform of k_x.

Of special interest is

$$\phi_0(z) = \frac{1}{\sqrt{V_q}}, \quad t_0 = \frac{i}{2}. \qquad ——(27)$$

Let $0<\lambda_j<\frac{1}{4}$ the exceptional spectrum (Selberg's $\frac{1}{4}$ conjecture. which is the archimedian Ramanujan Conjecture asserts that this set is empty) and write

$$t_1 = ir_1,\ t_2 = ir_2,\ \dots,\ t_\ell = ir_\ell,\quad 0<r_\ell\le r_{\ell+1}\le\cdots\le r_1<\tfrac{1}{2}.$$

(28)

Let $\mathcal{Y}_1$ be a fundamental domain for $SL_2(\mathbb{Z})$ and consider the variance W_i:

$$W_i = \sum_{f\in V_q}\int_{\mathcal{Y}_1}\left|\sum_{\gamma\in\Gamma(q)} k_X(s_f\gamma i,\zeta) - \frac{h_X(t_0)}{|V_q|}\right|^2 dA(\zeta)$$

$$= \sum_{f\in V_q}\int_{\mathcal{Y}_1}\left|\sum_{j\neq 0} h_X(t_j)\phi_j(i)\overline{\phi_j(s_f^{-1}\zeta)} + \text{cts}\right|^2 dA(\zeta)$$

$$= \sum_{f\in V_q}\int_{\mathcal{Y}_1}\sum_{\substack{j_1\neq 0\\ j_2\neq 0}} h_X(t_{j_1})\overline{h_X(t_{j_2})}\,\phi_{j_1}(i)\,\overline{\phi_{j_2}(i)}\,\phi_{j_1}(s_f^{-1}\zeta)\,\overline{\phi_{j_2}(s_f^{-1}\zeta)}\,dA(\zeta)$$

$$= \sum_{\substack{j_1 \neq 0 \\ j_2 \neq 0}} h_x(t_{j_1}) \overline{h(t_{j_2})} \, \phi_{j_1}(i) \overline{\phi_{j_2}(i)} \int_{\mathcal{Y}_{\Gamma(q)}} \phi_{j_1}(s) \overline{\phi_{j_2}(s)} \, dA(s)$$

$$= \sum_{j \neq 0} |h_x(t_j)|^2 |\phi_j(i)|^2 + \text{ets} \qquad (29)$$

One can estimate h_x;

$$h_x(it_j) = X^{1/2 + r_j} \quad \text{for} \quad \lambda_j < \frac{1}{4}$$

and

$$h_x(it_j) \ll \frac{X^{1/2}}{(1+|t_j|)^{3/2}} \quad \text{for } \lambda_j > \frac{1}{4}. \qquad (30)$$

Hence

$$W_i \ll X \sum_{\text{except.}} X^{2r_j} |\phi_j(i)|^2 + X \sum_{\lambda_j \geq \frac{1}{4}} \frac{|\phi_j(i)|^2}{(1+|t_j|)^3} \qquad (31)$$

A simple estimate with the same formula but with X small and $f=1$ yields for $d_j \geq \frac{1}{4}$

$$\sum_{t_j \leq R} |\phi_j(i)|^2 \ll R^2+1, \quad R \geq 0. \qquad (32)$$

Hence

$$W_i \ll X \sum_{\text{except } j} X^{2r_j} |\phi_j(i)|^2 + X \qquad (33)$$

(the cts spectrum is harmless since it obey $\lambda_1 \geq 1/4$).

Now if we replace i by $S_g i$ in the definition of W_i then $W_{S_g i} = W_i$ (since $\Gamma(q)$ is normal in $SL_2(\mathbb{Z})$) and hence

$$W_i = \frac{1}{|V_q|} \sum_{g \in V_q} W_{S_g i} \ll \frac{X}{|V_q|} \sum_{\text{except } j} X^{2r_j} \sum_{g \in V_q} |\phi_j(S_g i)|^2 + X \qquad (34)$$

Now $\phi_j(z)$ is an eigenfunction on $\mathbb{H}$ with $0 \le \lambda_j < \frac{1}{4}$, hence by Selberg's mean value property, for any z

$$|\phi_j(z)|^2 \ll \int_{B(z,1)} |\phi_j(\xi)|^2 \, dA(\xi) \qquad (35)$$

where $B(z,1)$ is a ball centered z of radius 1 in $\mathbb{H}$.

Hence

$$\sum_{g \in V_q} |\phi_j(S_g i)|^2 \ll \sum_{g \in V_q} \int_{B(S_g i, 1)} |\phi_j(\xi)|^2 \, dA(\xi)$$

$$\le \|\phi_j\|_2^2 = 1. \qquad (36)$$

It follows from this and (34) that

$$W_i \ll \frac{X}{|V_q|} \sum_{\text{except } j} X^{2r_j} + X \qquad (37)$$

Now apply a standard density theorem for the exceptional eigenvalues of $\Gamma(q)$ [HU] together with $\vartheta_j \le 7/64$ [K-S] in (37) (Selberg's "3/16 theorem" would suffice here too, giving a worse exponent) With $X \ge |V_q|$ this leads to:

$$W_i \ll X\left(\frac{X}{|V_q|}\right)^{7/32} \log X. \qquad (38)$$

Finally if $f \in V_q$ and $m(f,q) \ge 100 X^{1/2}$ then for $\zeta \in B(i,1)$ the contribution to the sum over $\gamma \in \Gamma(q)$ in the integrand in the definition of W_i is 0. Hence

$$\sum_{\substack{f \in V_q \\ m(f,q) \ge 100\sqrt{X}}} \left|\frac{X}{|V_q|}\right|^2 \ll X\left(\frac{X}{|V_q|}\right)^{7/32} \log X$$

or

$$\frac{1}{|V_q|} \sum_{\substack{f \in V_q \\ m(f,q) \ge 100\sqrt{X}}} 1 \ll \left(\frac{|V_q|}{X}\right)^{\frac{25}{32}} \log X \qquad (39).$$

With $X = V_q (\log q)^2$ (39) implies quite bit more than that $K_\mu \leq 1$.

One problem that remains as far as lifting from V_q to $SL_2(\mathbb{Z})$ is to find a (random) polynomial algorithm that produces a lift of size $q^{3/2}(\log q)$ for most f's. If f is <u>diagonal</u> then the Ross-Selinger algorithm for the definite setting [R-S] can be adapted here (see also [P-L-Q]) and it produces an essentially optimally small such lift. However for general f's it gives a lift of size $q^{3/2}$ (i.e. "K=3") which is much larger than the q^2 ($K=4/3$) deterministic algorithm above.

For the definite quadric $x_1^2 + x_2^2 + x_3^2 + x_4^2 = N$ and for the problem of approximating "q adically" i.e.

i.e. the minimal N for which there is a global lift of solutions mod q, the story is very similar to the archimedian approximation problem [Sa]. One has $\frac{4}{3} \leq K \leq 2$ and $K_\mu = 1$ and most likely $K = 4/3$. This with say $N = p^\ell$ $(\ell \to \infty)$ becomes the question of the diameters of the Ramanujan Graphs $X_{p,q}$ ([L-P-S]).

It is shown there that

$$\operatorname{diam}(X_{p,q}) \leq 2 \log_p n + O(1) \qquad (40)$$

where $|X| = n$ and $p = k-1$ is the degree of regularity of $X_{p,q}$. The coefficient 2 in (40) is the same as $K \leq 2$ for the exponent above. In [Sa 2] I suggested that for $X_{p,q}$ the 2 can be replaced by $1 + o(1)$ which amounts to $K = 1$. This was naive and indeed the big hole feature applies

here and I now expect that

$$\operatorname{diam}(X_{p,q}) \sim \frac{4}{3}\log_p n. \qquad (41)$$

Naser [TZ] constructs related Ramanujan Graphs with diameter $\geq \frac{4}{3}\log_{k-1} n$ as $n \to \infty$. He also shows that $K_\mu = 1$ for all Ramanujan Graphs, namely that for any x most points y are at a distance of at most $\log_{k-1} n$ from x. In his thesis [TZ] he determines the exact lifting exponent K for approximation (archimedian and p-adic) for integral quadratic forms (split or not) in 5 or more variables. His method is based on Kloosterman's circle technique as developed in smooth form (known as the 'S-method') in [D-F-I] and [H-B].

For abstract Ramanujan Graphs the diameter can be studied through the number of steps it takes for a simple nonbacktracking random walk on the graph to become equidistributed. This has been investigated in a recent preprint [L-P] who shows that there is sharp transition at $\log_{k-1} n$ steps of the walk. This recovers $K_\mu = 1$ for Ramanujan Graphs together with much more probalistic information.

References (ones omitted are in [Sa1])

[A-M] L. Adleman and K. Manders Eighth annual symposium ACM: STOC (1976) 23-29.

[Del] J. Delsarte C.R. Acad. Sc Paris 214 (1942) 147-179.

[D-F-I] W. Duke, J. Friedlander & H. Iwaniec Invent. Math. 112 (1993), 1-8.

[F-G] J. Friedlander and A. Granville Ann Math 129, 363-382

[HB1] R. Heath Brown Proc. London Math Soc. 64 (1992) 265-338

[HB2] R. Heath Brown J. Reine 481 (1996) 149-206

[HU] M. Huxley, In "The Selberg trace formula and related topics" 341-349, CONT MATH 53, AMS 1986.

[Iw] H. Iwaniec Acta Arith 19 (1971), 1-30

[L-Y] J. Liu - Y. Ye Acta Arith 119 (2005) 13-38.

[K-S] H. Kim + P. Sarnak JAMS 16 (2003) 139-183.

[L-P-S] A. Lubotzky, R. Phillips + P. Sarnak COMBINATORICA 8 (1988) 261-277.

[L-P] E. Lubetzky and Y. Peres arXiv 1507.04725.

[Ma] H. Maier Michigan Math Jl 32 (1985) 221-225

[P-L-Q] C. Petit, K. Lauter, J. Quisquater, cryptoeprint, REPORT 2008/173

[Sa1] P. Sarnak "Letter to Aaronson and Kitaev on the Solovay-Kitaev theorem and Golden Gates" publication.ias.edu/sarnak/paper/2637

[Sa2] P. Sarnak "Some applications of modular forms" CUP Vol 99 1990

[Sel] A. Selberg J. INDIAN MATH SOC. 20 (1956) 47-87

[Tu] P. Turan. Acta Sci Math (Szeged) 1936/37 226-235

[TZ1] N. TALIBIZADEH SARDARI "Diameter of Ramanujan Graphs" preprint 2015

[TZ2] Thesis in preparation 2015

[Va] R. Vaughan Proc Edinburgh Math Soc. (1976) 20, 329-331