Hamiltonian paths and Ramanujan graphs

Gergely Harcos

Alfréd Rényi Institute of Mathematics
http://www.renyi.hu/∼gharcos/

6 October 2020
Number Theory Seminar

Jacobi's four-square theorem (1 of 2)

- p is an odd prime number
- m is a positive integer

Theorem (Jacobi 1834)

The number of integral solutions of $p^m = x_1^2 + x_2^2 + x_3^2 + x_4^2$ *equals* $8(p^m + p^{m-1} + \cdots + p + 1)$.

Theorem (Jacobi 1834)

The number of integral solutions of $p^m = x_1^2 + x_2^2 + x_3^2 + x_4^2$, *with* $\gcd(x_1, x_2, x_3, x_4) = 1$, *equals* $8(p^m + p^{m-1})$.

Jacobi's four-square theorem (2 of 2)

- p is a prime number congruent to 1 mod 4
- m is a positive integer

Theorem (Jacobi 1834)

The number of integral solutions of $p^m = x_1^2 + x_2^2 + x_3^2 + x_4^2$*, with* $x_1 > 0$ *and* $2 \mid x_2, x_3, x_4$*, equals* $p^m + p^{m-1} + \cdots + p + 1$.

Theorem (Jacobi 1834)

The number of integral solutions of $p^m = x_1^2 + x_2^2 + x_3^2 + x_4^2$*, with* $x_1 > 0$ *and* $2 \mid x_2, x_3, x_4$ *and* $\gcd(x_1, x_2, x_3, x_4) = 1$*, equals* $p^m + p^{m-1}$.

Example ($p = 37$ and $m = 1$)

The 38 solutions are: $(1, \pm 6, 0, 0)$, $(1, 0, \pm 6, 0)$, $(1, 0, 0, \pm 6)$, $(1, \pm 4, \pm 4, \pm 2)$, $(1, \pm 4, \pm 2, \pm 4)$, $(1, \pm 2, \pm 4, \pm 4)$, $(5, \pm 2, \pm 2, \pm 2)$.

Structure of the solution set (1 of 2)

Definition

Let p be a prime number congruent to 1 mod 4.
Let G be the set of integral vectors $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ such that:

- the norm $x_1^2 + x_2^2 + x_3^2 + x_4^2$ is a power of p;
- $x_1 > 0$ and $2 \mid x_2, x_3, x_4$;
- $\gcd(x_1, x_2, x_3, x_4) = 1$.

Definition

We define the product of two vectors (a_1, a_2, a_3, a_4) and (b_1, b_2, b_3, b_4) lying in G as follows. We multiply the integral quaternions $a_1 + a_2\boldsymbol{i} + a_3\boldsymbol{j} + a_4\boldsymbol{k}$ and $b_1 + b_2\boldsymbol{i} + b_3\boldsymbol{j} + b_4\boldsymbol{k}$, and we factor out $\pm\gcd$ of the coordinates to arrive at a unique quaternion $c_1 + c_2\boldsymbol{i} + c_3\boldsymbol{j} + c_4\boldsymbol{k}$ with (c_1, c_2, c_3, c_4) lying in G.

Example ($p = 37$)

$$(27, -172, 54, -132)(61, 4, -146, 160) = (847, -568, 712, 572)$$

Structure of the solution set (2 of 2)

Observation

We defined a group law on G with identity element $(1,0,0,0) \in G$, because $(x_1, x_2, x_3, x_4) \in G$ has inverse $(x_1, -x_2, -x_3, -x_4) \in G$.

Theorem (after Dickson 1922)

Every element of G of norm p^m can be written uniquely as a product of m elements of G of norm p, none of which is inverse to its neighbors. In particular, G is a free group of rank $(p+1)/2$.

Example ($p = 37$)

$$\begin{aligned}
(27, -172, 54, -132) &= (1,2,4,4)(1,0,0,6)(5,-2,2,-2)\\
(61, 4, -146, 160) &= (5,2,-2,2)(1,4,4,2)(1,-6,0,0)\\
(847, -568, 712, 572) &= (1,2,4,4)(1,0,0,6)(1,4,4,2)(1,-6,0,0)
\end{aligned}$$

Cayley graphs (1 of 2)

Definition

Let p be a prime number congruent to 1 mod 4. Let S be the set of elements of G of norm p. The Cayley graph of G has vertex set G and edge set $\{(sg, g) : g \in G, s \in S\}$.

Observation

1. *The Cayley graph of G is a $(p+1)$-regular tree on which G acts freely (from the right).*
2. *The number of paths of length m starting at a given vertex is $p^m + p^{m-1}$.*
3. *The number of paths of length in $\{m, m-2, m-4, \dots\}$ starting at a given vertex is $p^m + p^{m-1} + \cdots + p + 1$.*

Cayley graphs (2 of 2)

Definition

Let $q > p$ be two prime numbers satisfying $p, q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$. Let H be the set of $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ such that:

- the norm $x_1^2 + x_2^2 + x_3^2 + x_4^2$ is a power of p;
- $x_1 > 0$ and $2q \mid x_2, x_3, x_4$;
- $\gcd(x_1, x_2, x_3, x_4) = 1$.

Theorem

H is a maximal normal subgroup of G with index equal to $N = q(q^2 - 1)/2$. In fact G/H is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$.

Observation

Consider the Cayley graph of G, and fix a vertex $g \in G$.
There is a bijection between the paths from g to gH with length in $\{m, m-2, m-4, \ldots\}$, and the integral solutions of $p^m = x_1^2 + x_2^2 + x_3^2 + x_4^2$ with $x_1 > 0$ and $2q \mid x_2, x_3, x_4$.

Ramanujan graphs (1 of 2)

Definition

Let $q > p$ be two prime numbers satisfying $p, q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$. The graph $X^{p,q}$ has vertex set G/H and edge set $\{(sgH, gH) : g \in G, s \in S\}$.

Observation

1. *$X^{p,q}$ is a $(p+1)$-regular connected graph on N vertices.*
2. *G acts transitively on $X^{p,q}$ (from the right).*
3. *Fix a vertex v of $X^{p,q}$. There is a bijection between the non-backtracking walks from v to v with length in $\{m, m-2, m-4, \dots\}$, and the integral solutions of $p^m = x_1^2 + x_2^2 + x_3^2 + x_4^2$ with $x_1 > 0$ and $2q \mid x_2, x_3, x_4$.*
4. *The girth of $X^{p,q}$ is at least $\log_p(4q^2)$.*

Ramanujan graphs (2 of 2)

Definition

We label the eigenvalues of the adjacency matrix of $X^{p,q}$ as

$$p + 1 = \lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_N.$$

We write $\lambda_j = \sqrt{p}(\kappa_j + \kappa_j^{-1})$, where $\kappa_j \in \mathbb{C}^\times$. E.g., $\kappa_1 = \sqrt{p}$.

Theorem (Lubotzky–Phillips–Sarnak 1988)

For $j \geqslant 2$ we have $|\lambda_j| \leqslant 2\sqrt{p}$. Equivalently, $|\kappa_j| = 1$.

Proof (sketch).

We count, in two ways, the number of closed non-backtracking walks in $X^{p,q}$ with length in $\{m, m-2, m-4, \ldots\}$. Using deep results of Siegel (1935), Eichler (1954), Igusa (1959), we get

$$p^{m/2} \sum_{j=1}^{N} \frac{\kappa_j^{m+1} - \kappa_j^{-m-1}}{\kappa_j - \kappa_j^{-1}} = \frac{p^{m+1} - 1}{p - 1} + O_{\varepsilon,q}(p^{m/2} p^{\varepsilon m}).$$

The contribution of $j = 1$ equals the main term on the RHS. $\square$

Choosing the primes p and q (1 of 3)

Theorem (Lubotzky–Phillips–Sarnak 1988)

Let $q > p$ be two prime numbers satisfying $p, q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$. Then $X^{p,q}$ is $(p+1)$-regular on $q(q^2-1)/2$ vertices, the girth of $X^{p,q}$ is at least $2\log_p q$, and each eigenvalue of $X^{p,q}$ besides $\lambda_1 = p+1$ is of absolute value at most $2\sqrt{p}$.

Question (Soltész 2018)

Let $k > 0$ and $\varepsilon > 0$ be fixed real numbers. Let $x > 0$ be large. Can we find two prime numbers, p and q, such that:

- $p, q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$;
- $x < p^k < q < (1+\varepsilon)x$?

Answer (Harcos 2018)

Yes!

Choosing the primes p and q (2 of 3)

First Idea

Choose $p \approx x^{1/k}$ first, and then try to choose $q \approx p^k$ such that $q \equiv 1 \pmod{4p}$. Works for $k > 2$ under GRH.
Unconditionally, the Linnik type theorem of Xylouris (2011) allows one to choose $q \in (p^{4.53}, p^{5.19})$ such that $q \equiv 1 \pmod{4p}$.

Second Idea

For $k > 2$, deduce from the Bombieri–Vinogradov theorem that for most $p \approx x^{1/k}$ there exists $q \approx p^k$ such that $q \equiv 1 \pmod{4p}$.

Third Idea

Apply the quadratic large sieve inequality of Heath-Brown (1995):

$$\sum_{m \leqslant M}^{*} \left| \sum_{n \leqslant N}^{*} a_n \left(\frac{n}{m} \right) \right|^2 \ll_\varepsilon (MN)^\varepsilon (M+N) \sum_{n \leqslant N}^{*} |a_n|^2.$$

Choosing the primes p and q (3 of 3)

Consider the following expression under $x \to \infty$:

$$\sum_{\substack{(1+\varepsilon/2)x<q<(1+\varepsilon)x \\ q \equiv 1 \pmod 4 \text{ is a prime}}} \left| \sum_{\substack{\sqrt[k]{x}<p<\sqrt[k]{(1+\varepsilon/2)x} \\ p \equiv 1 \pmod 4 \text{ is a prime}}} \left(\frac{p}{q}\right) \right|^2 .$$

1. By Heath-Brown's quadratic large sieve inequality, the above expression is smaller than $x^{\max(1+1/k, 2/k)+o(1)}$.
2. Assume that the required prime pair (p, q) does not exist. Then $\left(\frac{p}{q}\right)$ is never 1 in the inner sum, hence the above expression is larger than $x^{1+2/k-o(1)}$.

The two bounds contradict each other, hence the required prime pair (p, q) exists.

A combinatorial application (1 of 2)

Definition

We say that two graphs on the same vertex set are G-creating if their union (the union of their edges) contains G as a not necessarily induced subgraph. Let $H_n(G)$ and $\overline{H_n(G)}$ be the maximum number of pairwise G-creating and pairwise non-G-creating Hamiltonian paths of K_n, respectively.

Theorem

For every integer $n \geqslant 2$, we have $H_n(G)\overline{H_n(G)} \leqslant n!/2$.

Theorem

For every integer $k \geqslant 3$, we have $H_n(C_{2k}) \leqslant n^{\left(1-\frac{1}{3k}+o(1)\right)n}$.

A combinatorial application (2 of 2)

Proof.

Let $k \geqslant 3$ and $\varepsilon > 0$ be given, and let $n > 0$ be large. There exists a Ramanujan graph $X^{p,q}$ on $N = q(q^2-1)/2$ vertices such that

$$n < N < (1+\varepsilon)n \qquad \text{and} \qquad p^k < q < (1+\varepsilon)p^k.$$

By a result of Krivelevich (2012), the number of Hamiltonian cycles in $X^{p,q}$ is $N!\left(\frac{p+1}{N}\right)^N(1+o(1))^N$. Hence, trivially, $\overline{H_N(C_{2k})}$ is at least that large. It follows that

$$H_n(C_{2k}) \leqslant H_N(C_{2k}) \leqslant \frac{N!/2}{\overline{H_N(C_{2k})}} \leqslant \left(\frac{N}{p+1}\right)^N (1+o(1))^N.$$

Here $p > N^{\frac{1}{3k}}$, so that in the end

$$H_n(C_{2k}) \leqslant N^{\left(1-\frac{1}{3k}\right)N+o(N)} \leqslant n^{\left(1-\frac{1}{3k}\right)n+\varepsilon n}.$$

$\square$

Thanks for your attention!