COMBINATORICA
Akadémiai Kiadó - Springer-Verlag

COMBINATORICA **12** (3) (1992) 275–285

CUBIC RAMANUJAN GRAPHS

PATRICK CHIU

Received September 6, 1989
Revised June 30, 1991

A fimily of cubic Ramanujan graph is explicitly constructed. They are realized as Cayley graphs of a certain free group acting on the 3-regular tree; this group is obtained from a definite quaternion algebra that splits at the prime 2 and has a maximal order of class number 1.

1. Introduction

A k-regular graph is called a Ramanujan graph if its second largest eigenvalue (in absolute value) with respect to the adjacency matrix Δ is less than or equal to $2\sqrt{k-1}$. In their paper *Ramanujan Graphs* [9], Lubotzky, Phillips, and Sarnak describe a number of extremal properties which Ramanujan graphs possess, and explicitly construct a family of Ramanujan graphs $X^{p,q}$ for each prime $\equiv 1 \pmod 4$. According to the above authors, for $p \equiv 3 \pmod 4$, all one has to do is modify the set S to be the set of $p+1$ elements (up to $\pm$) $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ with $N(\alpha) = p$ and $\alpha \equiv i + j + k \pmod 2$. Then the same proof as in the case $p \equiv 1 \pmod 4$ gives the result that the Cayley graph of $PGL(2, \mathbb{Z}/q\mathbb{Z})$ relative to S is a $(p+1)$-regular Ramanujan graph of order $q(q^2-1)$ if $\left(\frac{p}{q}\right) = -1$ and of order $q(q^2-1)/2$ if $\left(\frac{p}{q}\right) = 1$. This paper will treat the remaining case of $p=2$. Margulis [12] constructs essentially the same graphs as LPS [9] and mentions, without an explicit description, the construction for the case $p=2$. Using a generalization of the LPS [9] construction, we will give an explicit construction of cubic Ramanujan graphs.

The heart of the problem has to do with the Hamiltonian quaternion algebra $\mathbf{H}$ not splitting at the prime 2. In order to realize the graphs and carry out the spectral analysis arguments, one must use more general quaternion algebras. More precisely, the desired algebra must be definite, split at the prime 2, and have a maximal order of class number 1. Before delving into the theory of quaternion algebras, we first give a simple description of how to make graphs $X^{2,q}$.

AMS Subject Classification code (1991): 05 C 35

2. Construction of $X^{2,q}$

Let $\mathbf{D}$ be the quaternion algebra defined as follows. It is generated by the basis $[1,\omega,\Omega,\omega\Omega]$ over $\mathbb{Q}$ with the relations: $\omega^2=-2$, $\Omega^2=-13$, and $\omega\Omega+\Omega\omega=0$. Hence an element α in $\mathbf{D}$ may be represented as $\alpha = a_0 + a_1\omega + a_2\Omega + a_3\omega\Omega$, $a_i \in \mathbb{Q}$. Consider the following set S of 3 elements $\{\omega,\rho,\bar{\rho}\}$, where $\rho=(2+\omega+\omega\Omega)/4$, $\bar{\rho}=(2-\omega-\omega\Omega)/4$. Let $q\neq 2$, 13 be a prime such that $\sqrt{-2}$ and $\sqrt{13}$ belong in $\mathbb{Z}/q\mathbb{Z}$ (i.e. $x^2\equiv -2 \pmod q$ and $x^2\equiv 13 \pmod q$ are solvable). Then we may work with matrices in $PGL(2,\mathbb{Z}/q\mathbb{Z})$ by identifying the basis elements 1, ω, Ω, $\omega\Omega$ with

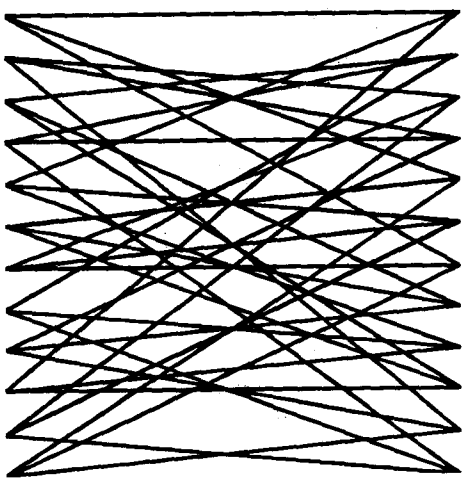
$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}\sqrt{-2}&0\\0&-\sqrt{-2}\end{pmatrix},\begin{pmatrix}0&\sqrt{13}\\-\sqrt{13}&0\end{pmatrix},\begin{pmatrix}0&\sqrt{-26}\\\sqrt{-26}&0\end{pmatrix}.$$

As in LPS [9], one forms the Cayley graph $X^{2,q}$ of $PGL(2,\mathbb{Z}/q\mathbb{Z})$ relative to the set S given above. Hence,

$$S=\left\{\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}2+\sqrt{-2}&\sqrt{-26}\\\sqrt{-26}&2-\sqrt{-2}\end{pmatrix},\begin{pmatrix}2-\sqrt{-2}&-\sqrt{-26}\\-\sqrt{-26}&2+\sqrt{-2}\end{pmatrix}\right\}.$$

These graphs are Ramanujan. If the Legendre symbol $\left(\frac{2}{q}\right)=-1$, the graph is bipartite with the two partitions of the set of $q(q^2-1)$ vertices corresponding to the set of matrices whose determinant is a square (mod q) and the set of matrices whose determinant is not. If $\left(\frac{2}{q}\right)^{-1}$ a connected graph is formed with $PSL(2,\mathbb{Z}/q\mathbb{Z})$ and it has $q(q^2-1)/2$ vertices but is not bipartite.

Example. *The smallest such Ramanujan graph $X^{2,3}$ is shown below. Its eigenvalue computed via numerical methods is* 2.414, *which is less than the defining bound for cubic Ramanujan graphs of* $2\sqrt{2}=2.828$.



$X(2,3)$

3. General Quaternion Algebras

This section summarizes the necessary theory which will be used later to construct the family $X^{2,q}$. For details and proofs, refer to Eichler [3], [4] and Vigneras [18]. In general, a quaternion algebra $\mathbf{D}$ is an algebra generated by four elements $[1,\omega,\Omega,\omega\Omega]$ over a field k satisfying $\omega\Omega+\Omega\omega=0$, $\omega^2=s$, $\Omega^2=t$, with $s,t\in k$. The conjugate of an element $\alpha=a_0+a_1\omega+a_2\Omega+a_3\omega\Omega$, $a_i\in k$, denoted by $\overline{\alpha}$, is $a_0-a_1\omega-a_2\Omega-a_3\omega\Omega$. The norm of α is $N(\alpha)=\alpha\overline{\alpha}=a_0^2-sa_1^2-ta_2^2+sta_3^2$, and the algebra is called definite or indefinite according to whether its norm is a definite or indefinite quadratic form.

A quaternion algebra is said to *split* over a field extension L of k if $\mathbf{D}\otimes L$ is isomorphic to the matrix algebra $\mathrm{Mat}(2,L)$. Let k_p be the p-adic completion of k, then the quaternion algebra $\mathbf{D}_p=\mathbf{D}\otimes k_p$ will split over k_p (or "$\mathbf{D}$ splits at p") for almost all primes p. The following is a useful technical lemma.

Lemma 3.1. *Let $\mathbf{D}$ be a quaternion algebra described above. Then*
(a) *$\mathbf{D}$ splits at p if and only if there are zero divisors in $\mathbf{D}_p$.*
(b) *$\mathbf{D}$ splits at p only if p divides the discriminant $-16s^2t^2$.*
(c) *If $\mathbf{D}$ is definite, then $\mathbf{D}$ splits at all but an odd number of primes.* ∎

We will also need a notion of factorization. As in classical algebraic number theory, factorization in terms of ideals sheds light on the factorization of numbers. Ideals for quaternion algebras are defined through certain subrings called orders: an *order* is a rank 4 module over the integers (rational or p-adic depending on the context) consisting of 1 and elements of the algebra whose norms are integral. Every order is contained in a maximal order. A *right ideal* for the order $\mathbf{T}$ is a module M satisfying $M\mathbf{T}=M$. Left ideals are defined similarly. If N and M are respectively left and right ideals for the *same* order $\mathbf{T}$, then the product of these two ideals is well-defined and denoted by MN.

Example. *Setting $s=t=-1$ in above, we get the familiar Hamiltonian quaternion algebra $\mathbf{H}$. Define $\mathbf{H}(\mathbb{Z})=\mathbb{Z}+\mathbb{Z}i+\mathbb{Z}j+\mathbb{Z}k$, then $\mathbf{H}(\mathbb{Z})$ is an order. It is contained in the maximal order $\mathbf{T}=\mathbb{Z}\sigma+\mathbb{Z}i+\mathbb{Z}j+\mathbb{Z}k$, where $\sigma=(1+i+j+k)/2$.*

Because the ring is noncommutative and the ideals cannot be freely multiplied, the factorization theory is much more complicated than that of classical algebraic number theory. However, some combinatorical results may be extracted which will serve our purposes.

The *norm* of an ideal is defined to be the principal ideal generated by the g.c.d. of the norms over all elements in the ideal.

Theorem 3.2. (Eichler [3]): *Suppose $\mathbf{D}_p$ splits over k_p and $\mathbf{T}_p$ is a maximal order in $\mathbf{D}_p$, then the number of right integral ideals of $\mathbf{T}_p$ having norm (p^k) is*

$$1+p+p^2+\ldots+p^k.$$

Moreover, each of these ideals may be represented canonically as principal ideals $(u)=u\mathbf{T}_p$, with

$$u=\begin{pmatrix} p^{k_1} & m \\ 0 & p^{k_2}\end{pmatrix},\ \text{where } k_1+k_2=k \text{ and } 0\le m<p^{k_2}.$$ ∎

The *class number* of an order is the number of inequivalent right (or left — it turns out to be the same number) ideals of the order, where two ideals M and N are equivalent if $M = \alpha N$, for some $\alpha \in \mathbf{D}^*$. The next result is the class number formula.

Theorem 3.3. (Eichler [4]): *Let* $\mathbf{D}$ *be a definite quaternion algebra,* $\mathbf{T}$ *a maximal order of* $\mathbf{D}$. *Then the class number of right (or left) ideals of* $\mathbf{T}$ *is*

$$h = \frac{1}{12}\prod_{p|\delta}(p-1) + \frac{1}{4}\prod_{p|\delta}\left(1 - \left(\frac{-4}{p}\right)\right) + \frac{1}{3}\prod_{p|\delta}\left(1 - \left(\frac{-3}{p}\right)\right),$$

where δ *is the product of all the primes* p *for which* $\mathbf{D}$ *does not split at* p, *and* $\left(\frac{n}{p}\right)$ *is Kronecker's extension of the Legendre symbol.* ∎

Remark. Thus in general $h > 1$. The only definite quaternion algebras with $h = 1$ and splitting at 2 are those with $\delta = 3, 5, 7, 13$. Should $h = 1$, then all ideals are principal and may be written as $(u) = u\mathbf{T}$, for some $u \in \mathbf{D}^*$.

Example. In the above example, $\mathbf{H}$ with the maximal order $\mathbf{T}$ has class number 1 by theorem 3.3. It is also known to have an Euclidean algorithm, so there is a very complete theory of factorization: every element may be factored into elements whose norms are prime. For general quaternion algebras, however, there may not be an Euclidean algorithm and the factorization question becomes more delicate.

There is also a theory of the zeta function, see Eichler [3]. The zeta function of an order $\mathbf{T}$ is defined as

$$\zeta(s) = \sum_{n \geq 1} \frac{a_n}{n^{2s}},$$

where a_n is the number of right integral ideals for $\mathbf{T}$ with norm (n). It may be written as an Euler product

$$\zeta(s) = \prod_p \left(\sum_{k \geq 0} \frac{a_{p^k}}{(p^k)^{2s}} \right),$$

where a_{p^k} is the number of right p-adic integral ideals of $\mathbf{T}_p$ with norm (p^k). The fact that this Euler product exists is equivalent to the fact that there is a $1-1$ correspondence between global integral ideals of norm (p^k) and local p-adic integral ideals of norm (p^k). Granted this, from theorem 3.2 the following is immediate:

Proposition 3.4. *Let* $\mathbf{D}$ *be a quaternion algebra of class number* 1 *which splits at* p, *and let* $\mathbf{T}$ *be a maximal order of* $\mathbf{D}$. *Then there exist* $1+p+\ldots+p^k$ *elements, unique up to units, of norm* p^k.

4. The Cubic Tree

In this section, we give in detail the main result of this paper: the construction of the cubic tree that will be used to realize the Ramanujan graphs $X^{2,q}$ in the subsequent section.

Consider the quaternion algebra $\mathbf{D}$ over $\mathbb{Q}$ given by $s=-2$ and $t=-13$. It is definite with norm $N(\alpha)=a_0^2+2a_1^2+13a_2^2+26a_3^2$.

Proposition 4.1.
(a) $\mathbf{D}$ *splits at the prime* 2.
(b) $\mathbf{D}$ *has class number* 1 *for right ideals of a maximal order.*

Proof. (a) By lemma 3.1(a), it suffices to find a zero divisor in $\mathbf{D}_2=\mathbf{D}\otimes\mathbb{Q}_2$. Since $\alpha\overline{\alpha}=N(\alpha)$, solving the equation $a_0^2+2a_1^2+13a_2^2+26a_3^2=0$ nontrivially in the 2-adics $\mathbb{Q}_2$ would imply the existence of a zero divisor. Now a 2-adic integer z is a square if $z\equiv 1 \mod 8$. Hence there exists $\xi\in\mathbb{Q}_2$ such that $\xi^2=-15$. Then $(\xi,1,1,0)$ is a solution.

(b) The discriminant of $\mathbf{D}$ is $-16\cdot 2^2\cdot 13^2$. Since $\mathbf{D}$ splits at 2, it must split at every prime except 13 (using lemma 3.1(b) and (c)). Hence $\delta=13$ and the class number formula of theorem 3.3 yields $h=1$. ∎

Next we look for an order $\mathbf{T}$ containing the 3 elements (up to units) of norm 2 furnished by Proposition 3.4. The obvious order is $\mathbb{Z}[1,\omega,\Omega,\omega\Omega]$, but the only element up to units of norm 2 is ω. The remedy is to extend this order by adjoining the element $\rho=(2+\omega+\omega\Omega)/4$. Then this new $\mathbb{Z}$-module $\mathbf{T}=\mathbb{Z}[1,\omega,\Omega,\rho]$ is an order, as easily verified, and a little computation shows that $\mathbf{T}$ is in fact maximal. Since the only units in $\mathbf{T}$ are ± 1, the three sought after elements are $\{\omega,\rho,\overline{\rho}\}$.

The cubic tree will be realized as the Cayley graph of a free group generated by $\{\omega,\rho,\overline{\rho}\}$ in the projective space $\mathbf{D}^*/Z(\mathbf{D})^*$. (Here $Z(\mathbf{D})$ denotes the center of $\mathbf{D}$, which consists of the scalars.) More precisely, let Λ' be the set of $\alpha\in\mathbf{T}$ with $N(\alpha)=2^k$. Identify α and β if $\pm 2^\nu\alpha=\beta$ for some $\nu\in\mathbb{Z}$, and let Λ be the set of equivalence classes. The main result proved in this paper is:

Lemma 4.2. *The Cayley graph of* Λ *is a* 3*-regular tree.*

Proof. Let Γ be the subgroup of Λ generated by the equivalence classes $\{\omega,\rho,\overline{\rho}\}$. *A priori*, Γ may not be all of Λ. Our approach is to show that Γ acts freely and transitively on the well-known cubic tree $PGL(2,\mathbb{Q}_2)/PGL(2,\mathbb{Z}_2)$. Moreover, $\{\omega,\rho,\overline{\rho}\}$ is precisely the set of elements which take each vertex to all three of its neighbors. Therefore, Γ is a free group with basis $\{\omega,\rho,\overline{\rho}\}$, so that $\Gamma=\Lambda$, and the Cayley graph of Γ is a cubic tree. For a treatment on the theory of trees, see Serre's *Trees* [17].

From now on, let G and U denote $PGL(2,\mathbb{Q}_2)$ and $PGL(2,\mathbb{Z}_2)$, respectively. As the reader may verify, the cubic tree G/U may be realized by choosing for the vertex set the set of coset representatives

$$\begin{pmatrix} 2^{l_1} & n \\ & 2^{l_2} \end{pmatrix}/U, \text{ where } 0\le l_1, l_2; 0\le n<2^{l_2}.$$

The distance from this vertex to the identity I/U is given by l_1+l_2, and two vertices are adjacent if they are at a distance 1 part.

On the other hand, the group Γ may be identified as elements in G. First, we view the order $\mathbf{T}$ as a local object $\mathbf{T}_2 = \mathbf{T} \otimes \mathbb{Q}_2$ in $\mathbf{D}_2 \cong \mathrm{Mat}(2, \mathbb{Q}_2)$. Since a maximal order is isomorphic to $\mathrm{Mat}(2, \mathbb{Z}_2)$, there exists an isomorphism

$$\psi : \mathbf{D}_2 \to \mathrm{Mat}(2, \mathbb{Q}_2)$$

such that $\psi(\mathbf{T}_2) = \mathrm{Mat}(2, \mathbb{Z}_2)$. Using the canonical forms for local ideals in theorem 3.2, each element $[\alpha]$ in Γ with $N(\alpha) = 2^k$ may be represented uniquely as

$$[\alpha] = \left[\begin{pmatrix} 2^{k_1} & m \\ & 2^{k_2} \end{pmatrix} e \right],$$

where $k_1 + k_2 = k$, $0 \le k_1, k_2$; $0 \le m < 2^{k_2}$, and e is a unit in U. This gives a natural action on the tree G/U; it acts on the vertices by

$$\begin{aligned} [\alpha] \left(\begin{pmatrix} 2^{l_1} & n \\ & 2^{l_2} \end{pmatrix} /U \right) &= \begin{pmatrix} 2^{k_1} & m \\ & 2^{k_2} \end{pmatrix} \begin{pmatrix} 2^{l_1} & n \\ & 2^{l_2} \end{pmatrix} /U \\ &= \begin{pmatrix} 2^{k_1+l_1} & 2^{k_1} n + 2^{l_2} m \\ & 2^{k_2+l_2} \end{pmatrix} /U \\ &= \begin{pmatrix} 2^{j_1} & h \\ & 2^{j_2} \end{pmatrix} /U, \end{aligned}$$

for some $0 \le j_1$, j_2 and $0 \le h < 2^{j_2}$. This action is well-defined because everything is projective.

With this explicit formulation, it is easy to see that Γ acts freely, transitively, and the elements

$$\left[\begin{pmatrix} 1 & 0 \\ & 2 \end{pmatrix} e_1 \right], \left[\begin{pmatrix} 1 & 1 \\ & 2 \end{pmatrix} e_2 \right], \left[\begin{pmatrix} 2 & 0 \\ & 1 \end{pmatrix} e_3 \right]$$

(where $e_i \in U$) corresponding in some order to $[\omega]$, $[\rho]$, $[\overline{\rho}]$ are the elements which take each vertex of the tree to all three of its neighboring vertices. ∎

5. Properties of $X^{2,q}$

The key is constructing the global tree Λ. The importance of Λ being a global object is that it brings us back to the study of the rational integers. Essentially, Λ consists of elements from the order $\mathbf{T} = \mathbb{Z}[1, \omega, \Omega, \rho]$ of norm 2^k (up to equivalence); that is, integral solutions to the equation $a_0^2 + a_0 a_3 + 2a_1^2 + a_1 a_3 + 13a_2^2 + 2a_3^2 = 2^k$. To relate the graphs $X^{2,q}$ of Section 2 to the cubic tree and to prove that they are Ramanujan graphs use ideas very similar to those of proposition 3.3 and theorem 4.1 of LPS [9]. We briefly sketch the arguments. A little care must be taken, however, to set up the problem since the quadratic form for the norm is different and poses a subtlety that will require the work of Rankin [14] to be added to our already long list of ingredients which we have cited but not gone into in depth.

First of all, we want *finite* graphs. For each prime $q \neq 2$ or 13, subgroups $\Lambda(q)$ of finite index in Λ may be defined as the kernel of the homomorphism

$$\varphi : \Lambda \to T(\mathbb{Z}/q\mathbb{Z})^* / Z(\mathbf{D})^*,$$

where $t(\mathbb{Z}/q\mathbb{Z}) = \{\alpha = a_0 + a_1\omega + a_2\Omega + a_3\rho | a_i \in \mathbb{Z}/q\mathbb{Z}\}$, $Z(\mathbf{D})$ is the center of scalars, and

$$[\alpha] \to (\alpha \bmod q)Z(\mathbf{D})^*.$$

The analogue of proposition 3.3 in LPS [9] is

Proposition 5.1.

$$\text{Image } \varphi = \begin{cases} PGL(2, \mathbb{Z}/q\mathbb{Z}) & \text{if } \left(\frac{2}{q}\right) = -1 \\ PSL(2, \mathbb{Z}/q\mathbb{Z}) & \text{if } \left(\frac{2}{q}\right) = 1. \end{cases}$$

Proof. If $(q, 26) = 1$ and $\beta = b_0 + b_1\omega + b_2\Omega + b_3\rho$ of norm 1 (mod q) is in the image of $\varphi(\Lambda)$, then the result of Malisev[11] on the theory of quadratic diophantine equations furnishes an element (a_0, a_1, a_2, a_3) in $\mathbb{Z}^4$ such that for sufficiently large k, $a_0^2 + a_0a_3 + 2a_1^2 + a_1a_3 + 13a_2^2 + 2a_3^2 = 2^k$, $2^k \equiv 1 \pmod q$, and $a_i \equiv b_i \pmod q$ for $0 \le i \le 3$. Set $\alpha = a_0 + a_1\omega + a_2\Omega + a_3\rho$, then $\varphi(\alpha) = \beta$; and since $T(\mathbb{Z}/q\mathbb{Z})^*/Z(\mathbf{D})^*$ is clearly isomorphic to $PGL(2, \mathbb{Z}/q\mathbb{Z})$, we have shown that $PSL(2, \mathbb{Z}/q\mathbb{Z}) \subseteq \varphi(\Lambda)$. It is also clear that α is mapped into $PSL(2, \mathbb{Z}/q\mathbb{Z})$ iff $\left(\frac{2}{q}\right) = 1$, and together with the fact that $[PGL(2, \mathbb{Z}/q\mathbb{Z})\colon PSL(2, \mathbb{Z}/q\mathbb{Z})] = 2$, the proposition follows. ∎

By mapping the generators $\{\omega, \rho, \overline{\rho}\}$ to the generating matrices described in section 2, this proposition identifies the Cayley graph of the quotient group $\Lambda(q) \backslash \Lambda$ with the graph $X^{2,q}$ of section 2 constructed using matrices from $PGL(2, \mathbb{Z}/q\mathbb{Z})$ if $\left(\frac{2}{q}\right) = -1$ and from $PSL(2, \mathbb{Z}/q\mathbb{Z})$ if $\left(\frac{2}{q}\right) = 1$. Moreover, it is easy to verify that $X^{2,q}$ is bipartite iff $\left(\frac{2}{q}\right) = -1$.

In the remainder of this paper, we will show that the graphs $X^{2,q}$ are Ramanujan, and then list some additional properties of these graphs in Theorem 5.4. An element in the subgroup $\Lambda(q)$ may be written as $a_0 + qa_1\omega + qa_2\Omega + qa_3\rho$ and its norm is $a_0^2 + qa_0a_3 + 2q^2a_1^2 + q^2a_1a_3 + 13q^2a_2^2 + 2q^2a_3^2$. Denote this quadratic form by $Q(v)$ and let $r_Q(n)$ be the number of ways of writing $n = Q(v)$ with $v \in \mathbb{Z}^4$. A very special generating function for $r_Q(n)$ is

$$\Theta(z) = \sum_{v \in \mathbb{Z}^4} e^{2\pi i Q(v) z} = \sum_{n \ge 0} r_Q(n) e^{2\pi i n z}.$$

When viewed as a function of the complex variable z, it turns out that this Θ-function is a "modular form" of weight 2 and level $26q^2$, see Schoeneberg [16]. As such it may be decomposed into a linear combination of Eisenstein series and a cusp form. Let $C(n)$ denote the contribution of the n-th Fourier coefficient from the Eisenstein series and $a(n)$ the contribution from the cusp form, so that

$$r_Q(n) = C(n) + a(n). \tag{5.1}$$

The $C(n)$ part is the easier part to estimate; see Hecke [6], Ogg [13], and in particular chapter 1 of Sarnak [15]. It is of the form

$$C(n) = \sum_{d|n} dF(d), \tag{5.2}$$

where $F:\mathbb{Z}^+ \to \mathbb{C}$ is periodic with period $52q^2$.

Estimating the $a(n)$ part requires much deeper results. The work of Eichler [5] and Igusa [7] on the Ramanujan conjectures corresponding to the case of weight 2 cusp forms, plus the theory of newsforms — see Rankin [14] — which is needed because $p=2$ divides the level, yields that as $k \to \infty$, $a(2^k) = O_\varepsilon(2^{k(1/2+\varepsilon)})$ for all $\varepsilon > 0$. The argument, somewhat technical, is as follows. Let $g(z) = \sum_{n \geq 1} a(n) e^{2\pi i n z}$ denote the cusp form part of $\Theta(z)$, which is of weight 2 and level $26q^2$. Then $g(z)$ may be decomposed into a sum of an oldform and a newform, say $g(z) = g_O(z) + g_N(z)$, with the level of $g_O(z)$ decreased to an integer L_1 satisfying $L_1 < 26q^2$ and $L_1 | 26q^2$. If $L_1 > 1$, we decompose $g_O(z)$ further into another oldform and a newform, again reducing the level of the resulting oldform to L_2 with $L_2 < L_1$ and $L_2 | L_1$. After a finite number of repetitions, $g(z)$ will be broken up into

$$g(z) = g_O(z) + g_{N_1}(z) + g_{N_2}(z) + \ldots + g_{N_r}(z), \tag{5.3}$$

where $g_O(z)$ is an oldform of level $L_r = 1$, and each $g_{N_i}(z)$ is a newform of some level dividing $26q^2$. As a consequence of a result on newforms in Rankin [14, theorem 9.4.8], the 2^k-th Fourier coefficient of $g_{N_i}(z)$ is $O(2^{k/2})$. The more profound results of Eichler [5] and Igusa [7] tells us that the n-th Fourier coefficient of a cusp form of weight 2 and level 1 satisfies the Ramanujan bound $O_\varepsilon(n^{1/2+\varepsilon})$ for all $\varepsilon > 0$. Hence the 2^k-th Fourier coefficient of $g_O(z)$ is $O_\varepsilon(2^{k(1/2+\varepsilon)})$. Finally, equation (5.3) implies that

$$a(2^k) = O_\varepsilon(2^{k(1/2+\varepsilon)}). \tag{5.4}$$

Combining (5.1), (5.2), and (5.4), we arrive at the crucial result

$$r_Q(2^k) = \sum_{d | 2^k} dF(d) + O_\varepsilon(2^{k(1/2+\varepsilon)}). \tag{5.5}$$

By a counting argument on the quotient graph $\Lambda(q) \setminus \Lambda$, it can be shown that $r_Q(2^k)$ is equal to the trace of the operator $\frac{2}{n} H_k(\Delta)$, where $H_k(\Delta)$ is a Chebyshev polynomial in the adjacency matrix Δ defined recursively by $H_0(\Delta) = 1$, $H_1(\Delta) = \Delta$, $H_k(\Delta) = \Delta H_{k-1}(\Delta) - 2H_{k-2}(\Delta)$ for $k \geq 2$. On the other hand, writing the eigenvalues as $\lambda_j = 2\sqrt{2}\cos\Theta_j$, it follows that

$$\text{trace}\left(\frac{2}{n} H_k(\Delta)\right) = \frac{2}{n} \sum_{j=0}^{n-1} H_k(\lambda_j) = \frac{2^{k/2+1}}{n} \sum_{j=0}^{n-1} \frac{\sin(k+1)\Theta_j}{\sin\Theta_j}. \tag{5.6}$$

Equating the two different expressions (5.5) and (5.6) for the trace, we obtain

$$\sum_{d | 2^k} dF(d) + O_\varepsilon(2^{k(1/2+\varepsilon)}) = \frac{2^{k/2+1}}{n} \sum_{j=0}^{n-1} \frac{\sin(k+1)\Theta_j}{\sin\Theta_j}. \tag{5.7}$$

Next, we state the following lemma which is easily proved.

Lemma 5.2. (LPS [8]) *Let $G:\mathbb{Z}^+ \to \mathbb{C}$ be periodic and satisfy*

$$\sum_{d|p^k} dG(d) = o(p^k) \qquad \text{as } k \to \infty$$

then

$$\sum_{d|p^k} dG(d) = 0 \qquad \text{for all } k. \qquad \blacksquare$$

Applying this lemma to (5.7) and subtracting off the terms corresponding to the largest eigenvalues $\pm(p+1)$, we obtain that as $k \to \infty$, for all $\varepsilon > 0$

$$O_\varepsilon(2^{k\varepsilon}) = \begin{cases} \sum_{j=1}^{n-2} \frac{\sin(k+1)\Theta_j}{\sin\Theta_j} & \text{if } \left(\frac{p}{q}\right) = -1 \\ \sum_{j=1}^{n-1} \frac{\sin(k+1)\Theta_j}{\sin\Theta_j} & \text{if } \left(\frac{p}{q}\right) = 1. \end{cases}$$

Hence, all these remaining Θ_j are real and their corresponding eigenvalues satisfy the Ramanujan property $|\lambda_j| \le 2\sqrt{2}$. Therefore

Theorem 5.3. *The graphs $X^{2,q}$ are Ramanujan graphs.* $\blacksquare$

We also list several other extremal properties of the graphs $X^{2,q}$. These may be verified in the same manner as in LPS [9]; case ii.(c) follows from Brooks' theorem on the chromatic number of a regular graph, see Bollobás [12].

Theorem 5.4.

Case i. $\left(\frac{2}{q}\right) = -1$; *$X^{2,q}$ is of order $n = q(q^2-1)$ and is bipartite,*

(a) $\text{girth}(X^{2,q}) \ge 4\log_2 q - 2$,
(b) $\log_2 n \le \text{diam}(X^{2,q}) \le 2\log_2 n + 3$,
(c) *chromatic number* $\chi(X^{2,q}) = 2$.

Case ii. $\left(\frac{2}{q}\right) = 1$; *$X^{2,q}$ is of order $n = q(q^2-1)/2$ and is not bipartite,*

(a) $\text{girth}(X^{2,q}) \ge 2\log_2 q$,
(b) $\log_2 n \le \text{diam}(X^{2,q}) \le 2\log_2 n + 3$,
(c) *chromatic number* $\chi(X^{2,q}) = 3$. $\blacksquare$

Remarks.

1. For practical purposes, we will show that there are many primes q such that -2 and 13 are squares in $\mathbb{Z}/q\mathbb{Z}$. We use some well-known results in number theory, see Apostol [1]. Suppose q is a prime of the form $q = 104m + 1$, $m \in \mathbb{Z}^+$. Then $\left(\frac{-2}{q}\right) = 1$ and by quadratic reciprocity $\left(\frac{13}{q}\right) = 1$, i.e. both -2 and 13 are squares in $\mathbb{Z}/q\mathbb{Z}$. Now the generalized prime number theorem for arithmetic progressions states that the number of primes q of the form $q = km + a$, $m \in \mathbb{Z}^+$ and with $(k,a) = 1$ is asymptotically $\pi(x)/\varphi(k)$, where $\pi(x) \sim x/\log x$ is the number of primes less than x,

and $\varphi(k)$ is the Euler φ-function. In our case, $\pi(x)/\varphi(k) = \pi(x)/48 \sim x/(48\log x)$, and we conclude that the desired primes can be found almost as easily as regular primes.

2. This construction provides an ε-good set of *two* elements for distributing points evenly on a sphere LPS [10], and also for the solution of the Ruziewicz problem of invariant measures on $L^\infty(S^n)$. See Sarnak [15].

3. For another approach to the proof of the Ramanujan property based on representation theory, see Lubotzky [8].

Acknowledgements. The author wishes to thank Peter Sarnak for his invaluable insights and comments.

References

[1] T. APOSTOL: *Introduction to analytic number theory*, Springer-Verlag, 1976.
[2] B. BOLLOBÁS: *Graph theory — an introductory course*, Springer-Verlag GTM 63, 1979.
[3] M. EICHLER: *Lectures on modular correspondences*, Tata Institute of Fundamental Research, Bombay, 1955–56.
[4] M. EICHLER: The basis problem for modular forms and the traces of the Hecke operators, *Modular Functions of One Variable*, Springer-Verlag Lecture Notes in Math. 320, 1973.
[5] M. EICHLER: Quaternäre quadratische Formen und die Riemannsche Vermutung für die kongruentz Zeta Funktion, *Archiv. der Math.* **V** (1954), 355–366.
[6] E. HECKE: Analytische arithmetik der positiven quadratic formen, *Collected Works*, pp. 789–898, Gottingen, 1959.
[7] J IGUSA: Fibre systems of Jacobian varieties III, *American Jnl. of Math.* **81** (1959), 453–476.
[8] A. LUBOTZKY: *Discrete groups, expanding graphs and invariant measures*, NSF-CBMS Regional Conference Lecture Notes, U. of Oklahoma, 1989.
[9] A. LUBOTZKY, R. PHILLIPS and P. SARNAK: Ramanujan graphs, *Combinatorica* **8** (1988) 261–277.
[10] A. LUBOTZKY, R. PHILLIPS and P. SARNAK: Hecke operators and distributing points on S^2, parts I and II, *Comm. Pure and Applied Math.* **39** (1986), 149–186, **40** (1987), 401–420.
[11] MALISEV: On the representation of integers by positive definite forms, *Math. Steklov* **65** (1962).
[12] G. A. MARGULIS: Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators, *Prob. of Info. Trans.* (1988) 39–46.
[13] A. OGG: *Modular forms and Dirichlet series*, W. A. Benjamin Enc., New York, 1977.
[14] R. RANKIN: *Modular forms and functions*, Cambridge University Press, 1977.
[15] P. SARNAK: *Some applications of modular forms*, Cambridge University Press, Cambridge, 1990.
[16] B. SCHOENEBERG: *Elliptic modular functions*, Springer Verlag, 1974.
[17] J. P. SERRE: *Trees*, Springer Verlag, 1980.

[18] M. VIGNERAS: *Arithmetique de algebras de quaternions*, Springer-Verlag Lecture Notes in Math. 800 1980.

Patrick Chiu

Stanford University
Stanford, CA 94305
U.S.A.
chiu@gauss.stanford.edu