Quaternions and Arithmetic

Colloquium, UCSD, October 27, 2005

This talk is available from www.math.mcgill.ca/goren
Quaternions came from Hamilton after his really good work had been done; and, though beautifully ingenious, have been an un-mixed evil to those who have touched them in any way, including Maxwell. – Lord Kelvin, 1892.
We beg to differ.
Hamilton’s quaternions \( \mathbb{H} \)

\[
\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k, \quad i^2 = j^2 = -1, \quad ij = k = -ji
\]

For \( x = a + bi + cj + dk \), we let

\[
\text{Norm}(x) = a^2 + b^2 + c^2 + d^2, \quad \text{Tr}(x) = 2a.
\]

This is a division algebra, \( x^{-1} = (\text{Tr}(x) - x)/\text{Norm}(x) \). In fact, the normed division algebras over \( \mathbb{R} \) are precisely

<table>
<thead>
<tr>
<th>dim</th>
<th>properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{R} )</td>
<td>1 assoc., comm., ordered</td>
</tr>
<tr>
<td>( \mathbb{C} )</td>
<td>2 assoc., comm.</td>
</tr>
<tr>
<td>( \mathbb{H} )</td>
<td>4 assoc.</td>
</tr>
<tr>
<td>( \mathbb{O} )</td>
<td>8</td>
</tr>
</tbody>
</table>
Classical motivation:

- **Physics**
  Generalization of the then new powerful complex numbers. Couples of real numbers to be replaced by triples (can’t), quadruples (can). Today, subsumed by Clifford algebras.

- **Topology**
  \{Quaternions of norm 1\} \cong S^3, so \(S^3\) is a topological group. The other div. alg. give top. groups \(S^0, S^1, S^7\) (H−space). No other spheres are top. groups \(\Leftrightarrow\)
  no other normed division algebras over \(\mathbb{R}\).
• Euclidean geometry and engineering
  \{\text{Trace zero, norm 1 quaternions}\} \cong S^2. \text{ The quaternions of norm 1 act by } x \ast v = x^{-1}vx. \text{ This gives a double cover } S^3 = \text{Spin}(3) \to SO_3. \text{ This is an efficient way to describe rotations. Used in spacecraft attitude control, etc.}

• Arithmetic
  \textbf{Lagrange: Every natural number is a sum of 4 squares.}
  \[\text{Norm}(x) \cdot \text{Norm}(y) = \text{Norm}(xy) \quad (\text{Euler})\]
  \text{Apply to } x, y \in \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k \text{ to reduce the proof to the case of prime numbers.}
Bhargava-Conway-Schneeberger: a quadratic form represents all natural numbers if and only if it represents $1, 2, \ldots, 15$. 
How often is a number a sum of squares?

A modular form of level $\Gamma_1(N)$ and weight $k$ is a holomorphic function

$$f : \mathcal{H} \rightarrow \mathbb{C}, \quad f(\gamma \tau) = (c\tau + d)^k f(\tau),$$

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}), \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}$$

Since $f(\tau + 1) = f\left(\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \tau\right) = f(\tau)$, the modular form $f$ has $q$-expansion

$$f(\tau) = \sum_{n \in \mathbb{Z}} a_n q^n, \quad q = \exp(2\pi i \tau).$$

In fact, such Fourier expansions can be carried at other “cusps” and we require that in all of them $a_n = 0$ for $n < 0$. If also $a_0 = 0$ we call $f$ a cusp form.
**Eisenstein series**

\[
E_{2k}(\tau) = c \cdot \sum_{(n,m) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(m\tau + n)^{2k}}
\]

\[
= \zeta(1 - 2k) + \sum_{n=1}^{\infty} \sigma_{2k-1}(n)q^n,
\]

\[
\sigma_r(n) = \sum_{d|n} d^r. \text{ This is a modular form on } \text{SL}_2(\mathbb{Z}) \text{ of weight } 2k.
\]

**Theta series of a quadratic form**

\[
q(x_1, \ldots, x_r) = \frac{1}{2} x^t A x,
\]

where \( A \) is integral symmetric positive definite with even entries on the diagonal. The level \( N(A) \) of \( A \) is defined as the minimal integer \( N \) such that \( NA^{-1} \) is integral.
Theorem. The theta series

\[ \sum_{n=0}^{\infty} a_q(n) \cdot q^n, \quad a_q(n) = \#\{(x_1, \ldots, x_r) \in \mathbb{Z}^n : q(x_1, \ldots, x_r) = n\} \]

is a modular form of weight \( r/2 \) and level \( N(A) \).

In particular, if

\[ q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2 = \frac{1}{2} x^t \begin{pmatrix} 2 & 2 & 2 & 2 \end{pmatrix} x \]

we get a modular form of level 2. It is obviously not a cusp form.
Two options

• **Particular quadratic form:** identify the modular form (for fixed level and weight this is a finite dimensional vector space). Find explicit answer. One gets $a(n) = \begin{cases} 4 \sum_{d|n} d & n \text{ odd} \\ 24 \sum_{d|n,d \text{ odd}} d & n \text{ even}. \end{cases}$

• **General quadratic form:** estimate coefficients.

1) Coeff. of “basic” Eisenstein series of weight $k$ grow like $n^{k-1}$. Show little cancelation in the Eisenstein part.

2) Deligne (Ramanujan’s conjecture): The coefficients of cusp forms of weight $k$ grow like $\sigma_0(n) \cdot n^{(k-1)/2}$.

Using this we see that $a_q(n) = O(n) \rightarrow \infty$ for 4 squares.
Deuring’s quaternions $B_{p,\infty}$

$K$ = field, char($K$) $\neq 2$.

The quaternion algebra $\left(\frac{a,b}{K}\right)$ is the central simple algebra

$$K \oplus Ki \oplus Kj \oplus Kk, \quad i^2 = a, \ j^2 = b, \ ij = -ji = k.$$ 

Example, $K = \mathbb{R}$. Then $\mathbb{H} \cong \left(\frac{-1,-1}{K}\right)$ and $M_2(\mathbb{R}) \cong \left(\frac{1,1}{K}\right)$. No others!

Example, $K = \mathbb{Q}_p$. Then there are again only two quaternion algebras, one of which is $M_2(\mathbb{Q}_p)$ and the other is a division algebra.
Theorem. Let $B$ be a quaternion algebra over $\mathbb{Q}$. $B$ is uniquely determined by $\{B \otimes_{\mathbb{Q}} \mathbb{Q}_p : p \leq \infty\}$. For a (finite) even number of $p \leq \infty$ we have $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ ramified, i.e. $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \not\cong M_2(\mathbb{Q}_p)$.

An order in a quaternion algebra over $\mathbb{Q}$ is a subring, of rank 4 over $\mathbb{Z}$. Every order is contained in a maximal order.

Example: in the rational Hamilton quaternions $\left(\frac{-1}{\mathbb{Q}}, \frac{-1}{\mathbb{Q}}\right)$ the order $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$ is not maximal. A maximal order is obtained by adding $\frac{1+i+j+k}{2}$.
Elliptic curves and Deuring’s quaternions

**Elliptic curve:** homogeneous non-singular cubic $f(x, y, z) = 0$ in $\mathbb{P}^2$, with a chosen point.

An elliptic curve is a commutative algebraic group (addition given by the secant method).

$\text{End}(E)$ is a ring with no zero divisors and for any elliptic curve $E'$, $\text{Hom}(E, E')$ is a right module.
Classification:

- if $\text{char}(K) = 0$ then $\text{End}(E) \otimes \mathbb{Q} \cong \begin{cases} \mathbb{Q} \\ \mathbb{Q}(\sqrt{-d}) \end{cases}$

- if $\text{char}(K) = p$ then $\text{End}(E) \otimes \mathbb{Q} \cong \begin{cases} \mathbb{Q} \\ \mathbb{Q}(\sqrt{-d}) \\ B_{p,\infty} \end{cases}$

An elliptic curve with $\text{End}(E) \otimes \mathbb{Q} \cong B_{p,\infty}$ is called supersingular. It is known that $\text{End}(E)$ is a maximal order in $B_{p,\infty}$. There are finitely many such elliptic curves up to isomorphism. Fix one, say $E$. 
Deuring: there is a canonical bijection between supersingular elliptic curves and right projective rank 1 modules for $\text{End}(E)$. One sends $E'$ to $\text{Hom}(E, E')$.

In this manner, quaternion algebras provide new information on elliptic curves.
Singular moduli

Let $E_s$ (resp. $E'_t$) be the finitely many elliptic curves over $\mathbb{C}$ such that End($E_s$) (resp. End($E'_t$)) has endomorphism ring which is the maximal order $R_d$ (resp. $R_{d'}$) of $\mathbb{Q}(\sqrt{-d})$ (resp. $\mathbb{Q}(\sqrt{-d'})$).

Each elliptic curve is isomorphic to $\mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$, where $\tau \in \text{SL}_2(\mathbb{Z}) \backslash \mathfrak{H}$ is uniquely determined. There is a modular form of weight 0, namely a modular function

$$j : \text{SL}_2(\mathbb{Z}) \backslash \mathfrak{H} \overset{\sim}{\longrightarrow} \mathbb{C}, \quad j(q) = \frac{1}{q} + 744 + 196884q + \ldots$$

Gross-Zagier. There is an explicit formula for the integer

$$\prod_{s,t} (j(E_s) - j(E'_t)).$$
The numbers $j(E_i)$, called singular moduli, are of central importance in number theory, because they classify elliptic curves and allow generation of abelian extensions of $\mathbb{Q}(\sqrt{-d})$. (Hilbert’s 12th problem).

Relation to quaternion algebras: If $p$ divides $\prod_{s,t}(j(E_s) - j(E'_t))$ then it means that some $E_s$ and $E'_t$ become isomorphic modulo (a prime above) $p$. This implies that their reduction is a supersingular elliptic curve. The problem becomes algebraic: into which maximal orders of $B_{p,\infty}$ can one embed simultaneously $R_d$ and $R_{d'}$. 
Supersingular graphs (Lubotzky-Philips-Sarnak, Pizer, Mestre, Osterlé, Serre, . . . )

Pick a prime $\ell \neq p$ and construct the (directed) supersingular graph $\mathcal{G}_p(\ell)$.

- **Vertices:** supersingular elliptic curves.

- **Edges:** $E$ is connected to $E'$ if there is an isogeny $f : E \to E'$ of degree $\ell$. (But we really only care about the kernel of $f$).

This graph has degree $\ell + 1$ and is essentially symmetric.
Ramanujan graphs

Expanders. Let $G$ be a $k$-regular connected graph with $n$ vertices and with adjacency matrix $A$ and combinatorial Laplacian

$$\Delta = kI_n - A,$$

whose eigenvalues are $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_{n-1} \leq 2k$.

$\frac{1}{k} \Delta(f)(v)$ is $f(v)$ minus the average of $f$ on the neighbors of $v$.

The expansion coefficient is

$$h(G) = \min \left\{ \frac{|\partial S|}{|S|} : |S| \leq n/2 \right\} \leq 1 \quad \text{or} \quad \frac{n + 1}{n - 1}.$$

One is interested in getting a large $h(G)$. 
Tanner, Alon-Milman: \[
\frac{2\lambda_1}{k+2\lambda_1} \leq h(G) \leq \sqrt{2k\lambda_1}.
\]

To have a graph in which information spreads rapidly/ random walk converges quickly, one looks for a graph with a large \(\lambda_1\). Those have many technological and mathematical applications.

Alon-Boppana: \(\lim \inf \mu_1(G) \geq 2\sqrt{k-1}\), where \(k - \mu_1 = \lambda_1\) is the second largest eigenvalue of \(A\), and where the limit is over all \(k\)-regular graphs of size growing to infinity.

Thus, asymptotically, the best family of expanding graphs of a fixed degree \(d\) will satisfy the Alon-Boppana bound.

A graph \(G\) is called a Ramanujan graph if \(\mu_1(G) \leq 2\sqrt{k-1}\).
A $k$-regular infinite tree $\mathcal{T}$ is the ideal expander. One can show that $h(\mathcal{T}) = k - 1$. The idea now is to find subgroups $\Gamma$ of the automorphism group of a tree that does not identify vertices that are “very close” to each other. Arithmetic enters first in finding such subgroups $\Gamma$. 
• Two distinct primes $p \neq \ell$.

• An $\ell + 1$ regular tree $\mathcal{T}$ could be viewed as the Bruhat-Tits tree for the group $GL_2(\mathbb{Q}_\ell)$ and in particular, we have

$$PGL_2(\mathbb{Q}_\ell) \subseteq \text{Aut}(\mathcal{T}).$$

• $\mathcal{O}$ = maximal order of $B_{p,\infty}$. Then the group of units of norm 1 of $\mathcal{O}[\ell^{-1}]^\times$ maps into $B_{p,\infty} \otimes \mathbb{Q}_\ell = M_2(\mathbb{Q}_\ell)$ and gives a subgroup $\Gamma$ of $\text{Aut}(\mathcal{T})$ of the kind we want. In fact,

$$\Gamma \backslash \mathcal{T} \cong \mathcal{G}^p(\ell).$$
The Ramanujan property.

\[ \Gamma \backslash \mathcal{T} = \text{moduli space of supersingular elliptic curves} \quad \Gamma_0(p) \backslash \mathcal{H} = \text{moduli space for elliptic curves + additional data} \]

<table>
<thead>
<tr>
<th>Quaternionic modular forms (=) sections of line bundles (=) functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modular forms (=) sections of line bundles</td>
</tr>
</tbody>
</table>

Hecke operators \(T_\ell \sim\) averaging operators \(\sim\) Adjacency matrices \(G^p(\ell)\)

<table>
<thead>
<tr>
<th>System of eigenvalues of (T_\ell) acting on functions with integral zero</th>
</tr>
</thead>
<tbody>
<tr>
<td>System of eigenvalues for (T_\ell) acting on cusp forms; given by the coeff. (a_\ell) in (q)-exp.</td>
</tr>
</tbody>
</table>

The bound on the eigenvalues of the adjacency matrix of \(G^p(\ell)\) is thus given by the Ramanujan bound on the \(\ell\)-th Fourier coefficient of elliptic modular forms.
Generalization: Quaternion algebras over totally real fields


A. Cayley compared the quaternions to a pocket map “... which contained everything but had to be unfolded into another form before it could be understood.”