# The Leech Lattice

Balázs Elek

Cornell University,
Department of Mathematics

November 8, 2016

Consider the equation

$$0^2 + 1^2 + 2^2 + \ldots + n^2 = m^2.$$

How many solutions does it have?

Okay,

$$0^2 + 1^2 = 1^2.$$

Édouard Lucas in 1875, tried some more numbers and found that

$$0^2 + 1^2 + 2^2 + \ldots + 24^2 = 4900 = 70^2.$$

Then conjectured that there are no other solutions. G.N. Watson proved in 1919 that the conjecture was true.

If we remember that

$$0^2 + 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

then we are trying to find integer points on an elliptic curve, which is still not easy, but there is a way to do it.

Let's talk about Lorentzian $n$-space $\mathbb{R}^{n+1,1}$. This is $\mathbb{R}^{n+2}$ with the inner product

$$x \cdot y = \left( \sum_{i=0}^{n} x_i y_i \right) - x_{n+1} y_{n+1}.$$

Let $\Lambda$ be a lattice in $\mathbb{R}^{n+1,1}$. We say $\Lambda$ is

- **integral** if $x \cdot y \in \mathbb{Z}$ for all $x, y \in \Lambda$,
- **unimodular** if there is a $\mathbb{Z}$-basis $v^0, \ldots v,^{n+1}$ such that the determinant of the matrix $(v^i \cdot v^j)_{i,j=0}^{n+1}$ is $\pm 1$,
- **even** if $x \cdot x \in 2\mathbb{Z}$ for all $x \in \Lambda$, and **odd** otherwise.

It turns out that the classification of integral unimodular lattices in $\mathbb{R}^{n+1,1}$ is easy (this is a really difficult problem in $\mathbb{R}^n$), there is a unique odd one $I_{n+1,1}$ in any dimension and there is a unique even one $II_{n+1,1}$ when $n+1 \equiv 1 \mod 8$. More explicitly,

$$I_{n+1,1} = \left\{ x = (x_0, \ldots x_{n+1}) \in \mathbb{R}^{n+1,1} : x_i \in \mathbb{Z} \right\}$$

$$II_{n+1,1} = \left\{ x = (x_0, \ldots x_{n+1}) \in \mathbb{R}^{n+1,1} : x_i \in \mathbb{Z}, x \cdot x \in 2\mathbb{Z} \right\}$$

$$\bigcup \left\{ x = (x_0, \ldots x_{n+1}) \in \mathbb{R}^{n+1,1} : x_i \in \mathbb{Z} + \frac{1}{2}, x \cdot x \in 2\mathbb{Z} \right\}$$

One of the cool things about the lattices $I_{n+1,1}$ and $II_{n+1,1}$ is that they can have isotropic/lightlike vectors, like

$$u = (1, 1, 1, 1, 1, 1, 1, 1, 1, 3) \in I_{9,1}.$$

Since $u \cdot u = 0$, $u \in u^{\perp}$, so $\frac{u^{\perp} \cap I_{9,1}}{u}$ is an integral unimodular lattice in $R^8$ (called the $E_8$ lattice).

What is really special about $II_{25,1}$ in particular is that here the vector

$$w = (0, 1, 2, \ldots, 23, 24, 70)$$

is lightlike. The lattice

$$\Lambda_{24} = \frac{w^{\perp} \cap II_{25,1}}{w}$$

is the Leech lattice.

Let's talk about packing spheres.

This is the **hexagonal close packing** of 2-spheres.

We would like to know what is the most efficient way of packing spheres (in arbitrary dimensions). This is a question people probably asked when they started doing mathematics.

Here is how far we got:

1. In the beginning of mathematics, people discover the 1-dimensional statement.

Here is how far we got:

1. In the beginning of mathematics, people discover the 1-dimensional statement.
2. In 1940, László Fejes Tóth proves that in 2 dimensions, the density of the hexagonal packing $\frac{\pi}{\sqrt{12}}$ is the highest that can be attained.

Here is how far we got:

1. In the beginning of mathematics, people discover the 1-dimensional statement.
2. In 1940, László Fejes Tóth proves that in 2 dimensions, the density of the hexagonal packing $\frac{\pi}{\sqrt{12}}$ is the highest that can be attained.
3. In 1998, Thomas Hales proved that in dimension 3, the hexagonal close packing is the best.

Here is how far we got:

1. In the beginning of mathematics, people discover the 1-dimensional statement.
2. In 1940, László Fejes Tóth proves that in 2 dimensions, the density of the hexagonal packing $\frac{\pi}{\sqrt{12}}$ is the highest that can be attained.
3. In 1998, Thomas Hales proved that in dimension 3, the hexagonal close packing is the best.
4. In 2016, Maryna Viazovska and collaborators proved that the $E_8$ lattice packing is the densest possible in 8 dimensions, and $\Lambda_{24}$ is the densest packing in 24 dimensions.

So this problems seems to be really hard, maybe we should assume that we are packing our spheres so that their centers are at the points of a lattice, this is somewhat easier, but it still took

1. the first person to consider the problem to solve it in dimension 1,

So this problems seems to be really hard, maybe we should assume that we are packing our spheres so that their centers are at the points of a lattice, this is somewhat easier, but it still took

1. the first person to consider the problem to solve it in dimension 1,
2. Lagrange to do dimension 2,

So this problems seems to be really hard, maybe we should assume that we are packing our spheres so that their centers are at the points of a lattice, this is somewhat easier, but it still took

1. the first person to consider the problem to solve it in dimension 1,
2. Lagrange to do dimension 2,
3. Gauss to do dimension 3,

So this problems seems to be really hard, maybe we should assume that we are packing our spheres so that their centers are at the points of a lattice, this is somewhat easier, but it still took

1. the first person to consider the problem to solve it in dimension 1,
2. Lagrange to do dimension 2,
3. Gauss to do dimension 3,
4. Viazovska et al. to do dimensions 8 and 24.

To this day, we only know the optimal lattice packings in dimensions $\leq 8$, 16 and 24.

Here is a picture summarizing how good sphere packings are in different dimensions:

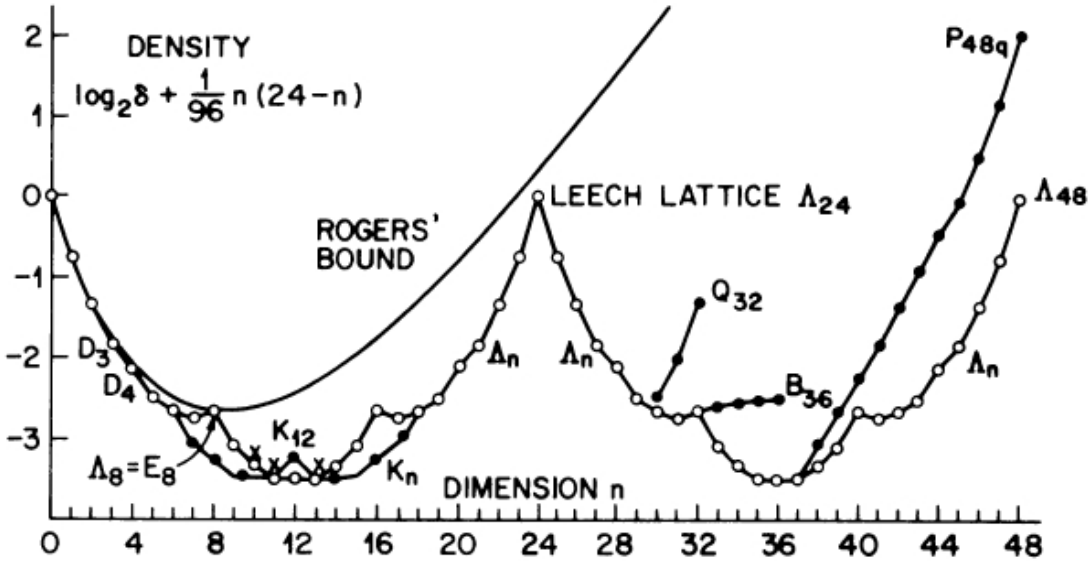


Figure 1.5. The densest sphere packings known in dimensions $n \leq 48$.

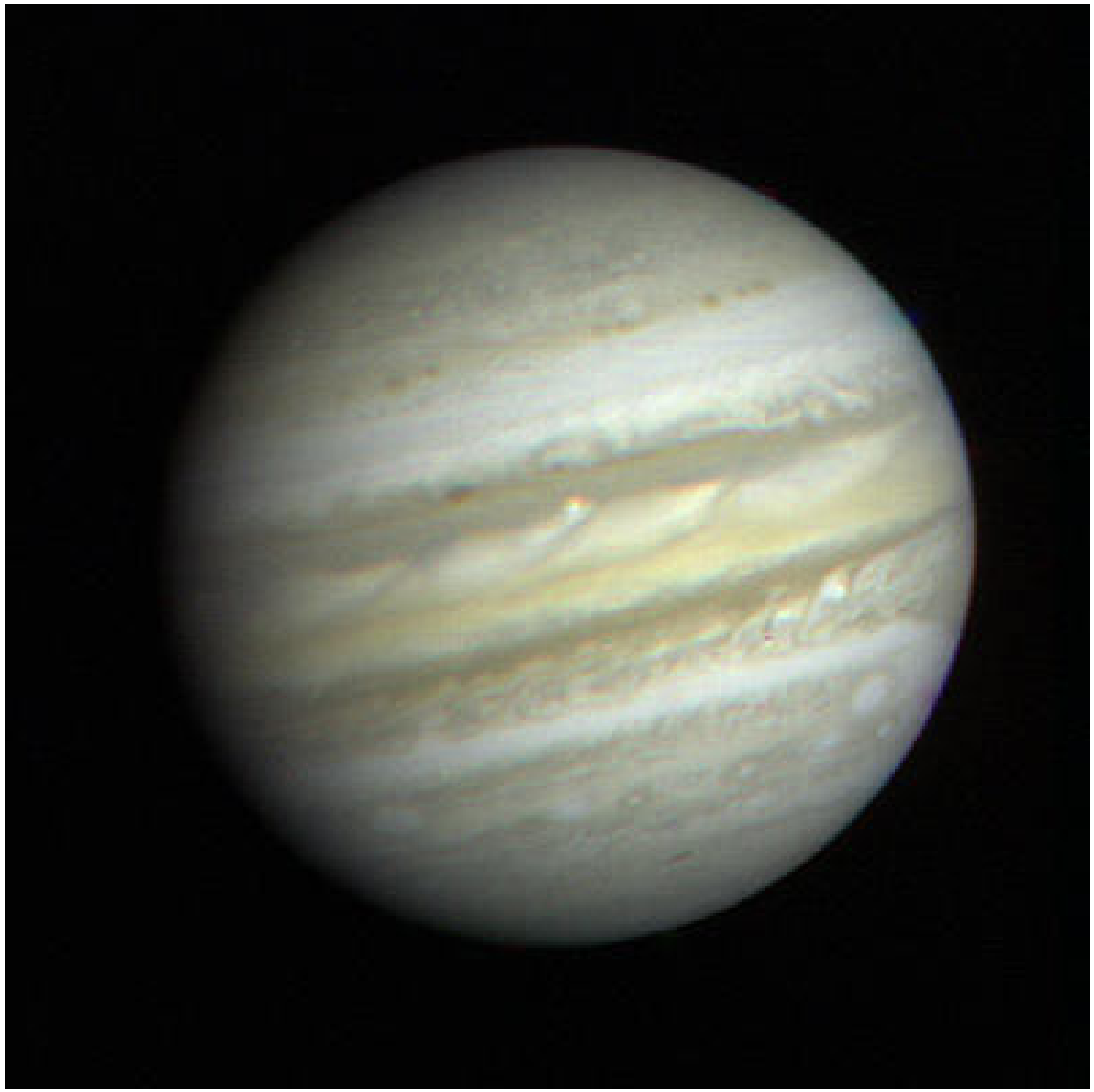
where $\delta$ is the "center density" (the actual density $\Delta$ divided by the volume of the unit sphere in dimension $n$).

Let's say you want to send messages through a noisy channel. That is, we want to send a binary string to someone, but there is some probability $p$ that a bit gets flipped. How can we make sure to get our message across? For instance, we could agree to send each bit three times in a row, so if we want to send $'0'$, we would send $'000'$. Then receiving $'000', '100', '010', '001'$ is interpreted as the correct result. This is summarized as using 3 bits to transmit 1 bit while being able to detect errors of at most 1 bit (not very impressive).

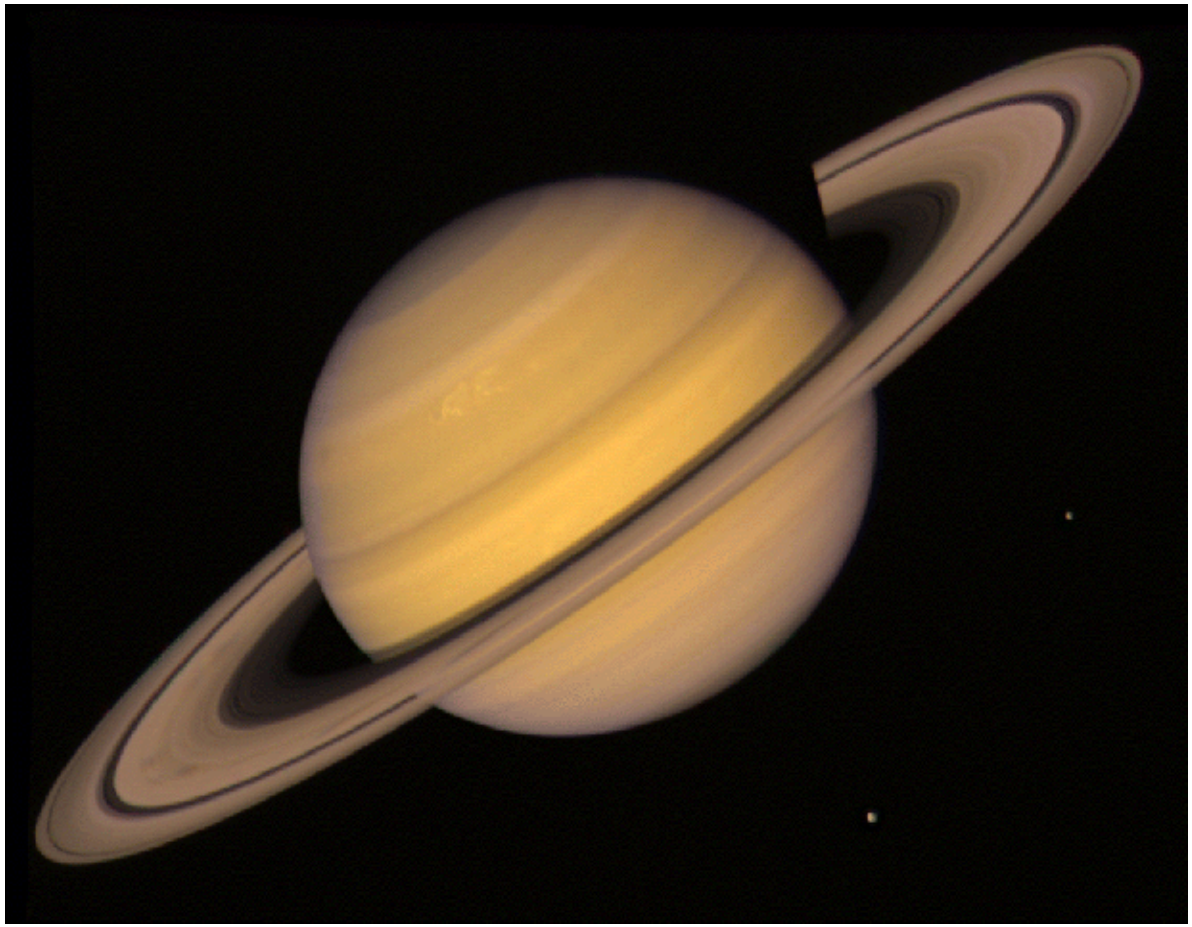
Mathematically, an **error-correcting code** is a set of codewords (vectors in a vector $V$ space over $\mathbb{F}_2$) that are easy to distinguish, even if there were somerrors introduced. Let's define the **Hamming distance** between two vectors in $V$ as the number of coordinates where they differ. If we let $d$ to be the minimal distance between our codewords in our code, we can stick spheres of radius $\rho = \frac{1}{2}(d-1)$ at the points, and if we land in any of the vectors in that sphere after signal transmission, we have received the correct message. That is, the code can correct $\rho$ bits of errors.

A systematic way of doing this is to use a **linear** code, i.e. an error-correcting code that is a subspace of $V$. A linear error-correcting code that is a $k$-dimensional subspace of $\mathbb{F}_2^n$ and has minimal distance $d$ is an $[n, k, d]$-code. Note that we want to minimize $n$, and maximize $k$ and $d$. Now we know this is equivalent to packing spheres efficiently.

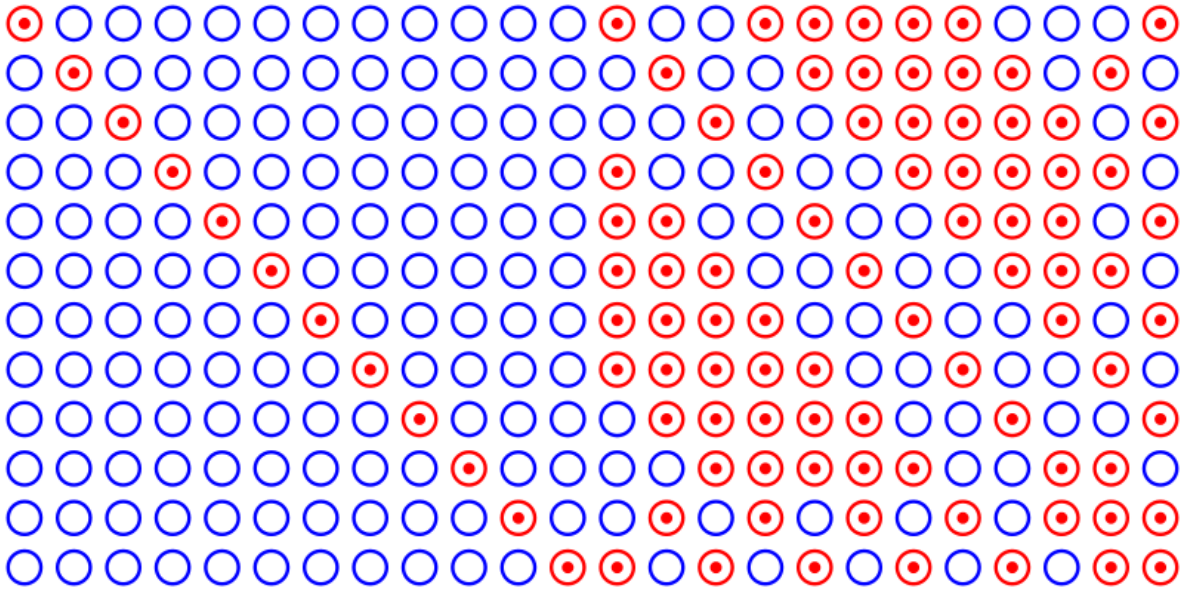
Some pictures from Voyager 1 and 2:



Some pictures from Voyager 1 and 2:



And here are the basis elements for the code used to receive them:

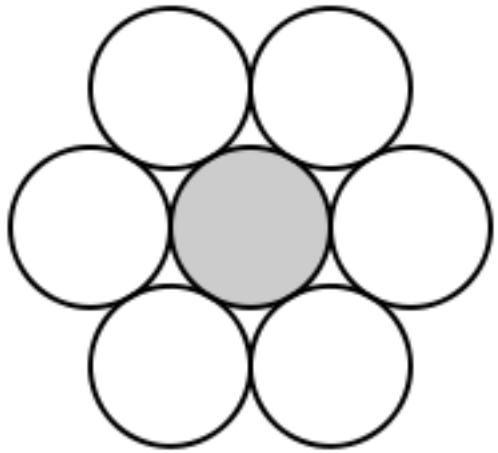


This is the **binary Golay code**. It uses 24 bits to transmit 12 bits of data, and has minimal distance 8 (so it can fix errors of up to 3 bits, pretty impressive!). By the way, the matrix above is $(I, A)$, where $A$ is the adjacency matrix of the icosahedron.

In 1964, John Leech was actually studying the Golay code packing in 24 dimensions, and (after his initial article was printed) noticed that there are holes in the packing large enough to fit more spheres (of the same size!) in, which doubles the density (and results in $\Lambda_{24}$). To his credit, it is easier to miss a 24-dimensional hole than a 3-dimensional one (these are the vectors with half-integer coordinates).

Another remarkable fact about putting these extra spheres in is that now if we look at the configuration around any given sphere (i.e. itself and its 196560 neighbors) then the spheres are locked in tightly, like the hexagonal packing of circles (but not the hexagonal close packing of spheres). The only other dimension where this tight locking happens is 8 (with the $E8$ lattice, of course).

This leads us to the topic of **kissing numbers**, the number of spheres that can touch a central sphere in a given dimension. There are apparently even harder than the packing numbers, the statements are obvious for dimensions 1 and 2:



But already in dimension 3, this is very difficult, as the 12 spheres in the hexagonal close packing have a lot of wiggle room. Newton and Gregory had a famous disagreement about this, and the first correct proof that 12 was actually the correct number was only proved in 1953. In four dimensions, 24 spheres can be easily fitted on a sphere, but there is even more room than in 3D. 24 was proven to be the correct number in 2003.

The remaining dimensions only have bounds,

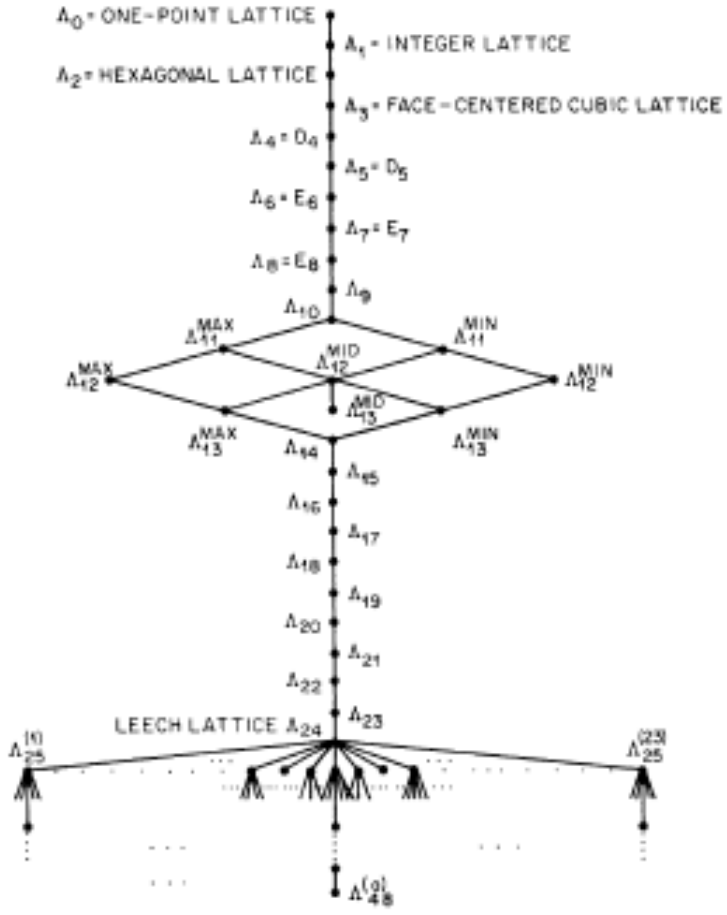
| Dim | $\geq$ | $\leq$ |
|---|---|---|
| 5 | 40 | 44 |
| 6 | 72 | 78 |
| 7 | 126 | 134 |
| 8 | 240 | 240 |
| 9 | 306 | 364 |
| 10 | 500 | 554 |
| 11 | 582 | 870 |
| 12 | 840 | 1, 357 |
| 13 | 1, 154 | 2, 069 |
| 14 | 1, 606 | 3, 183 |
| 15 | 2, 564 | 4, 866 |
| 16 | 4, 320 | 7, 355 |
| 17 | 5, 346 | 11, 072 |
| 18 | 7, 398 | 16, 572 |
| 19 | 10, 688 | 24, 812 |
| 20 | 17, 400 | 36, 764 |
| 21 | 27, 720 | 54, 584 |
| 22 | 49, 896 | 82, 340 |
| 23 | 93, 150 | 124, 416 |
| 24 | 196, 560 | 196, 560 |

The remaining dimensions only have bounds,

| Dim | $\geq$ | $\leq$ |
|---|---|---|
| 5 | 40 | 44 |
| 6 | 72 | 78 |
| 7 | 126 | 134 |
| 8 | 240 | 240 |
| 9 | 306 | 364 |
| 10 | 500 | 554 |
| 11 | 582 | 870 |
| 12 | 840 | 1, 357 |
| 13 | 1, 154 | 2, 069 |
| 14 | 1, 606 | 3, 183 |
| 15 | 2, 564 | 4, 866 |
| 16 | 4, 320 | 7, 355 |
| 17 | 5, 346 | 11, 072 |
| 18 | 7, 398 | 16, 572 |
| 19 | 10, 688 | 24, 812 |
| 20 | 17, 400 | 36, 764 |
| 21 | 27, 720 | 54, 584 |
| 22 | 49, 896 | 82, 340 |
| 23 | 93, 150 | 124, 416 |
| 24 | 196, 560 | 196, 560 |

Given the coincidences resulting in $\Lambda_{24}$, you might be surprised to hear that you *cannot fail* to make the Leech lattice if you do the most naive thing you can if you are trying to build a dense lattice packing. Let's start with dimension 1 with $\mathbb{Z} \subset \mathbb{R}$. Then in each dimension, take the lattice you got from the last dimension, and stack it in the next dimension on top of itself in a distance-minimizing way. The result is called a laminated lattice.

Strangely, there are choices involved in higher dimensions, like in this picture:



Let's talk about bosonic string theory. It turns out that strings like to have a very specific number of dimensions to wiggle in (24, of course), and if we take the torus

$$T = \mathbb{R}^{24}/\Lambda_{24},$$

consider $T/(\mathbb{Z}/2)$, and let strings wiggle in this orbifold. Borcherds showed in 1986 that this string theory has the Monster $M$ as its symmetry group. $M$ is a finite simple group with

808017424794512875886459904961710757005754368000000000

elements.

Why would you want to know what $M$ looks like?

`http://abstrusegoose.com/96`

The prime factorization of $|M|$ is

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71,$$

so the primes dividing $|M|$ are the primes less than or equal to 31, and $41, 47, 59$, and $71$. Coincidentally, this is the same set of primes for which a certain extension of a congruence subgroup $\Gamma_0(p)^+$ has a so-called genus zero property.

Ogg noticed that these sets of primes are the same in this paper:

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
16e année, 1974/75, n° 7, 8 p.

7-01

9 décembre 1974

AUTOMORPHISMES DE COURBES MODULAIRES

par Andrew P. OGG

Soient $N$ un entier positif, et $\Gamma_0(N)$ le sous-groupe du groupe modulaire $\Gamma = SL(2, \mathbb{Z})/\pm 1$ défini par les matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $N$ divisant $c$. Alors $\Gamma_0(N)$ agit sur le demi-plan supérieur $\mathfrak{H} = \{\tau = x + iy ; \ y > 0\}$ par $\tau \longmapsto \frac{a\tau+b}{c\tau+d}$.

# And offered a reward

COROLLAIRE. - Toutes les valeurs supersingulières de $j$ sont dans $\mathbb{F}_p$ si, et seulement si, $g^+ = 0$, i. e. $g \leqslant 1$ où $X_0(p)$ est hyperelliptique avec $v = w$, i. e. $p \leqslant 31$ ou $p = 41, 47, 59, 71$.

Autrement dit, toutes les racines du polynôme de Hasse sont dans $\mathbb{F}_p$, si, et seulement si, $p$ est une de ces quinze valeurs. Notons que d'après les formules (2) et (14), la formule (15) peut être exprimée aussi sous la forme

(16) $n(w)/2$ = nombre des valeurs supersingulières de $j$ dans $\mathbb{F}_p$,

où $n(w)$ est donné par (3).

Remarque 1. - Dans sa leçon d'ouverture au Collège de France, le 14 janvier 1975, J. TITS mentionna le groupe de Fischer, "le monstre", qui, s'il existe, est un groupe simple "sporadique" d'ordre

$$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71,$$

i. e. divisible exactement par les quinze nombres premiers de la liste du corollaire. Une bouteille de Jack Daniels est offerte à celui qui expliquera cette coïncidence.

At some point after predicting the existence of $M$, Griess, Conway and Norton noticed that the minimal faithful representation of $M$ (remember, $M$ is a **finite** group) would be 196883. Of course, the minimal representation of $M$ has dimension 1.
The normalized $J$-invariant is an important modular function in number theory, and has a series (in $q = e^{2\pi i\tau}$, where $\tau \in \mathbb{C}$) expansion

$$J(\tau) = q^{-1} + 0 + 196884q + 21493760q^2.$$

McKay noticed that $196884 = 196883 + 1$, and this led to the Monstrous moonshine conjecture of Conway and Norton, connecting $M$ to modular functions. Borcherds won the Fields medal in 1998 in part for his proof of the conjecture.

[1] Baez, J. C., *My favorite number: 24* http://math.ucr.edu/home/baez/numbers/24.pdf

[2] Conway, J. H.; Sloane, N. J. A., *Sphere packings, lattices and groups.* Third edition. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 290. Springer-Verlag, New York, 1999. lxxiv+703 pp. ISBN: 0-387-98585-9 11H31 (05B40 11H06 20D08 52C07 52C17 94B75 94C30)

[3] Frenkel, Igor; Lepowsky, James; Meurman, Arne, *Vertex operator algebras and the Monster.* Pure and Applied Mathematics, 134. Academic Press, Inc., Boston, MA, 1988. liv+508 pp. ISBN: 0-12-267065-5 17B65 (17B67 20D08 81D15 81E40)