Is $e^{\pi \sqrt{163}}$ odd or even?

(Workshop on ‘Harmonic Analysis on symmetric spaces’
I.S.I. Bangalore : 9th July 2004)

B.Sury

$e^{\pi \sqrt{163}} = 262537412640768743.9999999999992\ldots$

The object of this talk is to ‘explain’ this amazing fact. The explanation
involves $SL(2, \mathbb{Z})$, elliptic curves, modular forms, class field theory and Artin’s
reciprocity, among other things.

1 Quadratic forms

We shall consider only positive definite, binary quadratic forms over $\mathbb{Z}$. Any
such form looks like $f(x, y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$; it takes only
values > 0 except when $x = y = 0$.

Two forms $f$ and $g$ are said to be equivalent (according to Gauss) if \( \exists A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL(2, \mathbb{Z}) \) such that $f(x, y) = g(px + qy, rx + sy)$. Obviously, equivalent forms represent the same values. Indeed, this is the reason for the
definition of equivalence. One defines the discriminant of $f$ to be disc($f$) = $b^2 - 4ac$. Further, $f$ is said to be primitive if $(a, b, c) = 1$.

Note that if $f$ is +ve-definite, the discriminant $D$ must be < 0 (because
$4a(ax^2 + bxy + cy^2) = (2ax + by)^2 - Dy^2$ represents +ve as well as -ve
numbers if $D > 0$.)

One has:

**Theorem 1.1** For any $D < 0$, there are only finitely many classes of primi-
tive, +ve definite forms of discriminant $D$. [This is the class number $h(D)$ of the field $Q(\sqrt{D})$; an isomorphism is obtained by sending $f(x, y)$ to the ideal $a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}$].

This is proved by means of reduction theory. The idea is to show that each form is equivalent to a unique ‘reduced’ form. ‘Reduced’ forms can be computed - there are even algorithms which can be implemented in a computer which can determine $h(D)$ and even the $h(D)$ reduced forms of discriminant $D$.

A primitive, +ve definite, binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is said to be reduced if $|b| \leq a \leq c$ and $b \geq 0$ if either $a = c$ or $|b| = a$. These clearly imply

$$0 < a \leq \sqrt{\frac{|D|}{3}}.$$  

For example, the only reduced form of discriminant $D = -4$ is $x^2 + y^2$.

The only two reduced forms of discriminant $D = -20$ are $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$.

The group $SL(2, \mathbb{Z})$ is a discrete subgroup of $SL(2, \mathbb{R})$ such that the quotient space $SL(2, \mathbb{Z}) \backslash SL(2, \mathbb{R})$ is non-compact, but has a finite $SL(2, \mathbb{R})$-invariant measure. Reduction theory for $SL(2, \mathbb{Z})$ is (roughly) to find a complement to $SL(2, \mathbb{Z})$ in $SL(2, \mathbb{R})$; a ‘nice’ complement is called a fundamental domain. Viewing the upper half-plane $h$ as the quotient space $SL(2, \mathbb{R})/SO(2)$,

$$\{ z \in h : \text{Im}(z) \geq \sqrt{3}/2, \ |Re(z)| \leq 1/2 \}$$

is (the image in $h$) of a fundamental domain (see the accompanying figure):
Fundamental domains can be very useful in many ways; for example, they give even a presentation for $SL(2, \mathbb{Z})$. In this case, such a domain is written in terms of the Iwasawa decomposition of $SL(2, \mathbb{R})$. One has $SL(2, \mathbb{R}) = \mathcal{KAN}$ in the usual way. The, reduction theory for $SL(2, \mathbb{Z})$ says $SL(2, \mathbb{R}) = \mathcal{KAN}/_2\mathcal{N}_2 SL(2, \mathbb{Z})$. Here $A_i = \{diag(a_1, a_2) \in SL(2, \mathbb{R}): a_i > 0 \text{ and } \frac{a_1}{a_2} \leq t\}$ and $N_u = \{(\begin{array}{cc} 1 & x \\ 0 & 1 \end{array}) \in N : |x| \leq u\}$.

What does this have to with quadratic forms? Well, $GL(2, \mathbb{R})$ acts on the space $\mathcal{S}$ of $+ve$-definite, binary quadratic forms as follows: Each $P \in \mathcal{S}$ can be represented by a $+ve$-definite, symmetric matrix. For $g \in GL(2, \mathbb{R})$, $^tgp \in \mathcal{S}$. This action is transitive and the isotropy at $I \in \mathcal{S}$ is $O(2)$. In other words, $\mathcal{S}$ can be identified with $GL(2, \mathbb{R})/O(2)$ i.e. $\mathcal{S} = \{^tgg : g \in GL(2, \mathbb{R})\}$. In general, this works for $+ve$-definite quadratic forms in $n$ variables.

It is easy to use the above identification and the reduction theory statement for $SL(2, \mathbb{Z})$ to show that each $+ve$ definite, binary quadratic form is equivalent to a unique reduced form.

Indeed, writing $f = ^tgg$ and $g = kan\gamma$, $^tgg = ^t\gamma^ta^2n\gamma$ with $n \in U_{1/2}$ and $a^2 \in A_{4/3}$; so $^t\gamma an^2\gamma$ is a reduced form equivalent to $f$.

To see how useful this is, let us prove a beautiful discovery of Fermat, viz., that any prime number $p \equiv 1 \mod 4$ is expressible as a sum of two squares. Since $(p - 1)! \equiv -1 \mod p$ and since $(p - 1)/2$ is even, it follows that

$$((\frac{p-1}{2})!)^2 + 1 = pq$$

for some natural number $q$. Now the form $px^2 + 2(\frac{p-1}{2})!xy + qy^2$ is $+ve$ definite and has discriminant $-4$. Now, the only reduced form of discriminant $-4$ is $x^2 + y^2$ as it is trivial to see. Since each form is equivalent to a reduced form (by reduction theory), the forms $px^2 + 2(\frac{p-1}{2})!xy + qy^2$ and $x^2 + y^2$ must be equivalent. As the former form has $p$ as the value at $(1,0)$, the latter also takes the value $p$ for some integers $x, y$. 

3
2 Class field theory/Reciprocity

One way to motivate reciprocity is as follows.

A prime $p \neq 2$ is of the form $x^2 + y^2 \Leftrightarrow (-\frac{1}{p}) = 1$ (i.e., $-1$ is a square mod $p$).

A prime $p \neq 2$ is of the form $x^2 + 27y^2 \Leftrightarrow 2$ is a cube mod $p$ and $p \equiv 1 \mod 3$.

A prime $p \neq 2$ is of the form $x^2 + 64y^2 \Leftrightarrow 2$ is a 4th power mod $p$ and $-1$ is a square mod $p$.

The point of quadratic reciprocity is that one can express a condition of the form $(\frac{a}{p}) = 1$ in terms of congruences for $p$. For instance,

\[
\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \mod 12.
\]
\[
\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 11 \mod 20.
\]
\[
\left(\frac{7}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 3, \pm 9 \mod 28.
\]

The quadratic reciprocity law (QRL) says:

$p \neq q$ odd primes \(\Rightarrow\)

\[
\left(\frac{p}{q}\right) = 1 \Leftrightarrow q \equiv \pm d^2 \mod 4p \text{ for some odd } d.
\]

Abelian class field theory and Artin’s reciprocity law in particular - QRL corresponds to the special case of quadratic extensions - tells us when a prime $p$ splits completely in a finite abelian extension of $\mathbb{Q}$, in terms of congruences. Here $p$ splits completely in $Q(\alpha)$ if the minimal polynomial of $\alpha$ over $Q$ splits into linear factors when viewed modulo $p$.

For e.g. in $Q(e^{2\pi i/n})$, a prime $p$ splits completely $\Leftrightarrow p \equiv 1 \mod n$. In any finite extension field $K$ of $Q$, one can do algebra as in $\mathbb{Z}$ and $Q$, excepting the fact that unique factorisation is absent, in general. Fortunately, a finite
group (called the class group of \( K \)) measures the deviation from this property holding good.

For \( K = \mathbb{Q}(\sqrt{D}) \) with \( D < 0 \), the order \( h(D) \) of the class group of \( K \) gives the number of +ve-definite, primitive, reduced, binary, quadratic forms.

Class Field Theory has two parts - one consists of the reciprocity law and the other is an existence theorem of a certain field called the Hilbert class field corresponding to any field \( K \). The latter is the maximal, unramified, abelian extension of \( K \). For example, the Hilbert class field of \( \mathbb{Q}(\sqrt{-14}) \) is \( \mathbb{Q}(\sqrt{-14})(\sqrt{2\sqrt{2} - 1}) \). One has:

**Theorem 2.1** Let \( n > 0 \) be square-free and \( \equiv 3 \mod 4 \). Then, an odd prime \( p \) can be expressed as \( x^2 + ny^2 \) if, and only if, \( p \) splits completely in the Hilbert class field of \( \mathbb{Q}(\sqrt{-n}) \).

**Remark** There is an analogous version when \( n \equiv 3(4) \). In that case one looks at primes \( p \) expressible as \( x^2 + xy + (1+n)4y^2 \) and one considers the so-called ring class field of \( \mathbb{Z}[(\sqrt{-n})] \).

Of course, \( (\frac{-n}{p}) = 1 \) implies that \( p \) divides \( x^2 + ny^2 \) for some integers \( x, y \). Unlike the case of \( n = 1 \) (and the cases \( n = 2, 3, 4, 7 \)), there are many (as many as \( h(-4n) \)) reduced forms (among which is the form \( x^2 + ny^2 \)) and the condition \( (\frac{-n}{p}) = 1 \) only implies that \( p \) is represented by one of these forms.

When do we know that \( p \) is represented by \( x^2 + ny^2 \) itself?

Now, the previous theorem can be used to determine the primes expressible in the form \( x^2 + ny^2 \) provided one can determine the Hilbert class field of \( \mathbb{Q}(\sqrt{-n}) \). Indeed, if \( L = \mathbb{Q}(\sqrt{-n})(\alpha) \) is the Hilbert class field (actually the ring class field of \( \mathbb{Z}[\sqrt{-n}] \) and \( f_n(X) \) is the minimal polynomial of \( \alpha \) (where \( \alpha \in \mathcal{O}_L \)), then for a prime \( p \neq 2 \) with \( p \nmid n, p \nmid \text{disc} f_n \), we have:

\[
p = x^2 + ny^2 \iff (\frac{-n}{p}) = 1 \text{ and } f_n(x) \equiv 0 \mod p \text{ for some } x \in \mathbb{Z}.
\]

As before, there is an analogous version for \( n \equiv 3 \pmod 4 \).
3 The modular function

For \( \tau \in h \), the upper half-plane, consider the lattice \( \mathbb{Z} + \mathbb{Z} \tau \) and the functions

\[
g_2(\tau) = 60 \sum_{m,n} \frac{1}{(m+n\tau)^4} \left( \frac{(2\pi)^4}{12} \left( 1 + \sum_{n=1}^{\infty} \sigma_3(n) e^{2\pi i n\tau} \right) \right)
\]

\[
g_3(\tau) = 140 \sum_{m,n} \frac{1}{(m+n\tau)^6} \left( \frac{(2\pi)^6}{12} \left( 1 + \sum_{n=1}^{\infty} \sigma_5(n) e^{2\pi i n\tau} \right) \right).
\]

[Note that \( p'(z)^2 = 4p(z)^3 - g_2(\tau) p(z) - g_3(\tau) \) where the Weierstrass \( p \)-function on \( \mathbb{Z} + \mathbb{Z} \tau \) is given by \( p(z) = \frac{1}{z^2} + \sum \frac{1}{(z-w)^2} - \frac{1}{w^2} \).]

It can be shown that \( \Delta(\tau) \overset{d}{=} g_2(\tau)^3 - 27g_3(\tau)^2 \neq 0 \). The elliptic modular function \( j : h \to \mathbb{C} \) is defined by

\[
j(\tau) = 12^3 \cdot \frac{g_2(\tau)^3}{\Delta(\tau)}.
\]

The adjective ‘modular’ accompanies the \( j \)-function because of the invariance property:

\[
j(\tau) = j(\tau') \Leftrightarrow \tau' \in SL(2, \mathbb{Z})(\tau) \overset{d}{=} \left\{ \frac{a\tau + b}{c\tau + d} : \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL(2, \mathbb{Z}) \right\}.
\]

In fact, we have:

**Theorem 3.1** (i) \( j \) is holomorphic on \( h \).
(ii) \( j \) has the invariance property above.
(iii) \( j : h \to \mathbb{C} \) is onto.

The proof of (iii) needs the fundamental domain of \( SL(2, \mathbb{Z}) \) we referred to earlier.
That fact that \( p \) satisfies the equation \( (p')^2 = 4p^3 - g_2p - g_3 \) implies, by the above theorem, that the \( j \)-function, gives an isomorphism from the set \( SL(2, \mathbb{Z}) \backslash h \) to the set all ‘complex elliptic curves’ \( \mathbb{C}/\mathbb{Z} + \mathbb{Z} \tau \).
In fact, one has bijective correspondences between:

(i) lattices \( L = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C} \) upto scalar multiplication,
(ii) complex elliptic curves \( \mathbb{C}/L \) upto isomorphism,
(iii) the numbers \( j(\tau) \), and
(iv) Riemann surfaces of genus 1 upto complex analytic isomorphism.

As a matter of fact, \( SL(2, \mathbb{Z})\backslash h \) is the (coarse) moduli space of elliptic curves over \( \mathbb{C} \).

In general, various subgroups of \( SL(2, \mathbb{Z}) \) describe other moduli problems for elliptic curves. This description has been vastly exploited by Shimura et al. in modern number theory.

For instance, complex spaces like \( \Gamma_0(N)\backslash h \) have algebraic models over \( \mathbb{Q} \) called Shimura varieties. The Taniyama-Shimura-Weil conjecture (which implies Fermat’s Last Theorem) says that any elliptic curve over \( \mathbb{Q} \) admits a surjective, algebraic map defined over \( \mathbb{Q} \) from a projectivised model of \( \Gamma_0(N)\backslash h \) onto it. The point of this is that functions on \( \Gamma_0(N)\backslash h \) or even on \( SL(2, \mathbb{Z})\backslash h \) with nice analytic properties are essentially modular forms and conjectures like Taniyama-Shimura-Weil and, more generally, those which come under the so-called Langlands Program say essentially that ‘geometric objects over \( \mathbb{Q} \) come from modular forms’.

As \( j : h \to \mathbb{C} \) is \( SL(2, \mathbb{Z}) \) - invariant, one has \( j(\tau + 1) = j(\tau) \). So \( j(\tau) \) is a holomorphic function in the variable \( q = e^{2\pi i\tau} \), in the region \( 0 < |q| < 1 \).

Thus, \( j(\tau) = \sum_{n=-\infty}^{\infty} c_n q^n \) is a Laurent expansion i.e., all but finitely many \( c_n (n < 0) \) vanish.

In fact, \( j(\tau) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n q^n \) with \( c_n \in \mathbb{Z} \) \( \forall \) \( n \). (\( c_1 = 196884, c_2 = 21493760, c_3 = 864299970 \) etc.) We shall keep this \( q \)-expansion of \( j \) in mind.
4 Complex multiplication

We defined the $j$-function on $\mathbb{H}$. One can think of $j$ as a function on lattices $\mathbb{Z} + \mathbb{Z}\tau$. In particular, if $\mathcal{O}$ is an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$, it can be viewed as a lattice in $\mathbb{C}$. In fact, any proper, fractional $\mathcal{O}$-ideal $I$ can be 2-generated i.e, is a free $\mathbb{Z}$-module of rank 2 i.e., is a lattice in $\mathbb{C}$. Then, it makes sense to talk about $j(I)$. Using basic properties of elliptic functions, it is quite easy to show:

**Proposition:** $j(I)$ is an algebraic number of degree $\leq$ class number of $\mathcal{O}$. In fact, a much stronger result holds and, it is :

**The First main theorem of Complex multiplication :**

Let $\mathcal{O}$ be an order in an imaginary quadratic field $K$. Let $I \subset \mathcal{O}$ be a factional $\mathcal{O}$-ideal. Then, $j(I)$ is an algebraic integer and $K(j(I))$ is the Hilbert (ring) class field of $\mathcal{O}$.

In particular, $K(j(\mathcal{O}_K))$ is the Hilbert class field of $K$. We have almost come back where we started from. Indeed, it only remains to explain the ‘za’ of things now:\footnote{A friend had confessed long ago that in his primary school, he understood the tables but it took him a long time to understand the meaning of ‘za’ in ‘two two za four’!}

A Corollary of the above theorem is:

**Proposition:** Let $\mathcal{O}, K$ be as above and let $I_1, \ldots, I_h$ be the ideal classes of $\mathcal{O}$ (i.e., $h = [\text{Hilbert class field of } \mathcal{O} : K] = [K(j(\mathcal{O})) : K]$). Then, $\prod_{i=1}^{h} (X - j(I_i))$ is the minimal polynomial of any $\alpha$ such that $K(\alpha) = \text{Hilbert class field of } \mathcal{O}$. Note that $\alpha$ can be any $j(I_i)$.

Applying the theorem to $j(\tau)$ for $\tau$ imaginary quadratic, it follows that $j(\tau)$ is an algebraic integer of degree $= \text{class number of } Q(\tau)$ i.e, $\exists$ integers $a_0, \ldots, a_{h-1}$ such that $j(\tau)^h + a_{h-1}j(\tau)^{h-1} + \ldots + a_0 = 0$.

Now, there are only finitely many imaginary quadratic fields $Q(\tau) = K$ which have class number 1. The largest $D$ such that $Q(\sqrt{-D})$ has class number...
1 is 163. Since $163 \equiv 3(4)$, the ring of integers is $\mathbb{Z} + \mathbb{Z}(-\frac{1+i\sqrt{163}}{2})$. Thus $j(-\frac{1+i\sqrt{163}}{2}) \in \mathbb{Z}$.

Now $j(\tau) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n q^n$ with $c_n \in \mathbb{Z}$ and

$$q = e^{2\pi i (-\frac{1+i\sqrt{163}}{2})} = -e^{-\pi\sqrt{163}}.$$ 

Thus $-e^\pi \sqrt{163} + 744 - 196884 e^{-\pi\sqrt{163}} + 21493760 e^{-2\pi\sqrt{163}} + \ldots = j(\tau) \in \mathbb{Z}$.

In other words,

$$e^{\pi\sqrt{163}} - \text{integer} = 196884 e^{-\pi\sqrt{163}} + 21493760 e^{-2\pi\sqrt{163}} \ldots \approx 0.$$ 

**VOILA !!!**