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

B.Sury

Stat-Math Unit
Indian Statistical Institute
Bangalore 560059, India
sury@isibang.ac.in

The title is just a bit of persiflage as $e^{\pi\sqrt{163}}$ is not an integer but then ......

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

The object here is to 'explain' this amazing fact. The explanation involves $SL(2, \mathbf{Z})$, 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 $\mathbf{Z}$. Any such form looks like $f(x,y) = ax^2 + bxy + cy^2$ with $a,b,c \in \mathbf{Z}$; it takes only values > 0 except when $x = y = 0$.

Two forms f and g are said to be equivalent (according to Gauss) if $\exists\ A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL(2,(\mathbf{Z})$ 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 $\operatorname{disc}(f) = b^2 - 4ac$. Further, f is said to be primitive if $(a,b,c) = 1$.

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

One has:

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

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

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

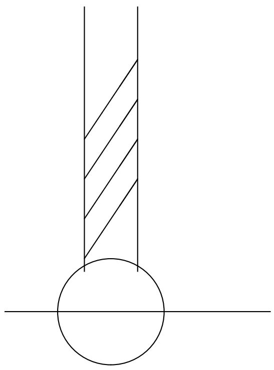
For example, the only reduced form of discriminant $D = -4$ is $x^2 + y^2$.

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

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

$$\{z \in \mathbf{H} : \mathrm{Im}(z) \geq \sqrt{3}/2, \mid Re(z) \mid \leq 1/2\}$$

is (the image in $\mathbf{H}$) of a fundamental domain (figure below) :



Fundamental domains can be very useful in many ways; for example, they give even a presentation for $SL(2, \mathbf{Z})$. In this case, such a domain is written in terms of the Iwasawa decomposition of $SL(2, \mathbf{R})$. One has $SL(2, \mathbf{R}) = KAN$ in the usual way. The, reduction theory for $SL(2, \mathbf{Z})$ says $SL(2, \mathbf{R}) = KA_{\frac{2}{\sqrt{3}}} N_{\frac{1}{2}} SL(2, \mathbf{Z})$. Here $A_t = \{diag(a_1, a_2) \in SL(2, \mathbf{R}) : a_i > 0 \text{ and } \frac{a_1}{a_2} \leq t\}$ and $N_u = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N : |x| \leq u\}$.

What does this have to with quadratic forms? Well, $GL(2, \mathbf{R})$ acts on the space S of +ve-definite, binary quadratic forms as follows: Each $P \in S$ can be representated by a +ve-definite, symmetric matrix. For $g \in GL(2, \mathbf{R})$, ${}^t gPg \in S$. This action is transitive and the isotropy at $I \in S$ is $O(2)$. In other words, S can be identified with $GL(2, \mathbf{R})/O(2)$ i.e. $S = \{{}^t gg : g \in GL(2, \mathbf{R})\}$. 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 $SL(2, \mathbf{Z})$ to show that each +ve definite, binary quadratic form is equivalent to a unique reduced form.
Indeed, writing $f = {}^t gg$ and $g = kan\gamma$, ${}^t gg = {}^t \gamma {}^t na^2 n\gamma$ with $n \in U_{1/2}$ and $a^2 \in A_{4/3}$; so ${}^t na^2 n$ 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 $p \equiv 1 \bmod 4$ is expressible as a sum of two squares. Since $(p-1)! \equiv -1 \bmod p$ and since $(p-1)/2$ is even, it follows that $(\frac{p-1}{2}!)^2 \equiv -1 \bmod p$ i.e.,

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

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.

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,

$$(\frac{3}{p}) = 1 \Leftrightarrow p \equiv \pm 1 \ mod\ 12.$$

$$(\frac{5}{p}) = 1 \Leftrightarrow p \equiv \pm 1, \pm 11 \ mod\ 20.$$

$$(\frac{7}{p}) = 1 \Leftrightarrow p \equiv \pm 1, \pm 3, \pm 9 \ mod\ 28.$$

The quadratic reciprocity law (QRL) says:

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

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

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 $\mathbf{Q}$, in terms of congruences. Here p splits completely in
$Q(\alpha)$ if the minimal polynomial of α over $\mathbf{Q}$ splits into linear factors when viewed modulo p.
For e.g. in $\mathbf{Q}(e^{2\pi i/n})$, a prime p splits completely $\Leftrightarrow p \equiv 1 \text{ mod } n$. In any finite extension field K of $\mathbf{Q}$, one can do algebra as in $\mathbf{Z}$ and $\mathbf{Q}$, 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 $K = \mathbf{Q}(\sqrt{D})$ 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 $\mathbf{Q}(\sqrt{-14})$ is $\mathbf{Q}(\sqrt{-14})(\sqrt{2\sqrt{2}-1})$. One has:

Theorem 2.1 *Let $n > 0$ be square-free and $\not\equiv 3 \ mod \ 4$. 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 $\mathbf{Q}(\sqrt{-n})$.*

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

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 $\mathbf{Q}(\sqrt{-n})$. Indeed, if $L = \mathbf{Q}(\sqrt{-n})(\alpha)$ is the Hilbert class field (actually the ring class field of $\mathbf{Z}[\sqrt{-n}]$ and $f_n(X)$ is the minimal polynomial of α (where $\alpha \in \mathcal{O}_L$), then for a prime $p \neq 2$ with $p \not| n, p \not| disc.f_n$, we have:

$$p = x^2 + ny^2 \Leftrightarrow (\frac{-n}{p}) = 1 \text{ and } f_n(x) \equiv 0 \ mod \ p \text{ for some } x \in \mathbf{Z}.$$

As before, there is an analogous version for $n \equiv 3 \pmod 4$.

3 The modular function

For $\tau \in \mathbf{H}$, the upper half-plane, consider the lattice $\mathbf{Z}+\mathbf{Z}\tau$ 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 $\mathbf{Z} + \mathbf{Z}\tau$ is given by $p(z) = \frac{1}{z^2} + \sum_w (\frac{1}{(z-w)^2} - \frac{1}{w^2})$.]

It can be shown that $\Delta(\tau) \stackrel{d}{=} g_2(\tau)^3 - 27g_3(\tau)^2 \neq 0$. The elliptic modular function $j : \mathbf{H} \to \mathbf{C}$ 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:

$$j(\tau) = j(\tau') \Leftrightarrow \tau' \in SL(2,\mathbf{Z})(\tau) \stackrel{d}{=} \left\{ \frac{a\tau + b}{c\tau + d} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbf{Z}) \right\}.$$

In fact, we have:

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

The proof of (iii) needs the fundamental domain of $SL(2, \mathbf{Z})$ we referred to earlier.
That fact that p satisfies the equation $(p')^2 = 4p^3 - g_2 p - g_3$ implies, by the above theorem, that the j-function, gives an isomorphism from the set $SL(2, \mathbf{Z}) \backslash \mathbf{H}$ to the set all 'complex elliptic curves' $\mathbf{C}/\mathbf{Z} + \mathbf{Z}\tau$.

In fact, one has bijective correspondences between :
(i) lattices $L = \mathbf{Z} + \mathbf{Z}\tau \subset \mathbf{C}$ upto scalar multiplication,
(ii) complex elliptic curves $\mathbf{C}/L$ upto isomorphism,
(iii) the numbers $j(\tau)$, and
(iv) Riemann surfaces of genus 1 upto complex analytic isomorphism.

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

In general, various subgroups of $SL(2, \mathbf{Z})$ 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 $\Gamma_0(N) \backslash \mathbf{H}$ have algebraic models over $\mathbf{Q}$ called Shimura varieties. The Taniyama-Shimura-Weil conjecture (which is proved by Wiles et al. and which implies Fermat's Last Theorem) says that *any elliptic curve over* $\mathbf{Q}$ *admits a surjective, algebraic map defined over* $\mathbf{Q}$ *from a projectivised model of* $\Gamma_0(N) \backslash \mathbf{H}$ *onto it.* The point of this is that functions on $\Gamma_0(N) \backslash \mathbf{H}$ or even on $SL(2, \mathbf{Z}) \backslash \mathbf{H}$ with nice analytic properties are essentially modular forms and conjectures like Taniyama-Shimura-Weil say essentially that 'nice geometric objects over $\mathbf{Q}$ come from modular forms'.

As $j : \mathbf{H} \to \mathbf{C}$ is $SL(2, \mathbf{Z})$ - 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, $j(\tau) = \sum\limits_{n=-\infty}^{\infty} c_n q^n$ is a Laurent expansion i.e., all but finitely many $c_n (n < 0)$ vanish.

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

4 Complex multiplication

We defined the j-function on $\mathbf{H}$. One can think of j as a function on lattices $\mathbf{Z} + \mathbf{Z}\tau$. In particular, if $\mathcal{O}$ is an order in an imaginary quadratic field $\mathbf{Q}(\sqrt{-n})$, it can be viewed as a lattice in $\mathbf{C}$. In fact, any proper, fractional $\mathcal{O}$-ideal I can be 2-generated i.e, is a free $\mathbf{Z}$-module of rank 2 i.e., is a lattice in $\mathbf{C}$. 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[1]

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 = [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 α such that $K(\alpha) =$ Hilbert class field of $\mathcal{O}$. Note that α can be any $j(I_i)$.

Applying the theorem to $j(\tau)$ for τ imaginary quadratic, it follows that $j(\tau)$ is an algebraic integer of degree = class number of $\mathbf{Q}(\tau)$ 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 $\mathbf{Q}(\tau) = K$ which have class number 1. The largest D such that $\mathbf{Q}(\sqrt{-D})$ has class number 1 is 163. Since $163 \equiv 3(4)$, the ring of integers is $\mathbf{Z} + \mathbf{Z}(\frac{-1+i\sqrt{163}}{2})$. Thus $j(\frac{-1+i\sqrt{163}}{2}) \in \mathbf{Z}$.

[1] 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'!

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

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

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

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

VOILA !!!