29.1.

Davenport on counting cubic rings.

Recall. Given a cubic ring $au^3 + bu^2v$, $cuv^2 + dv^3$, its Hessian is

$$-\frac{1}{4}\det\begin{bmatrix} \frac{\partial^2 f}{\partial u^2} & \frac{\partial^2 f}{\partial u \partial v} \\ \frac{\partial^2 f}{\partial u \partial v} & \frac{\partial^2 f}{\partial v^2} \end{bmatrix} = Au^2 + Buv + Cv^2,$$

$$A = b^2 - 3ac$$

$$B = bc - 9ad$$

$$C = c^2 - 3bd.$$

We have $\mathrm{Disc}(H(f)) = -3\,\mathrm{Disc}(f)$, and a commutative diagram

$$\begin{tikzcd} BCF \arrow[r, "SL_2(\mathbb{Z})"] \arrow[d, "H"] & BCF \arrow[d, "H"] \\ BQF \arrow[r, "SL_2(\mathbb{Z})"] & BQF \end{tikzcd}$$

Highbrow proof. Let $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{\partial x}{\partial u} & \frac{\partial x}{\partial v} \\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v} \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$ with the matrix in $SL_2(\mathbb{Z})$,

and $h(x,y) = f(u,v)$.

Then,
$$H(h) = \begin{bmatrix} \frac{\partial x}{\partial u} & \frac{\partial y}{\partial u} \\ \frac{\partial x}{\partial v} & \frac{\partial y}{\partial v} \end{bmatrix} \begin{bmatrix} \frac{\partial^2 f}{\partial u^2} & \frac{\partial^2 f}{\partial u \partial v} \\ \frac{\partial^2 f}{\partial u \partial v} & \frac{\partial^2 f}{\partial v^2} \end{bmatrix} \begin{bmatrix} \frac{\partial x}{\partial u} & \frac{\partial x}{\partial v} \\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v} \end{bmatrix}$$

$\in SL_2(\mathbb{Z})$.

29.2.

Def. A binary cubic form is reduced if its Hessian is.
i.e. if $-A < B \le A < C$

or $0 \le B \le A = C$.

Proposition. Every BCF is equivalent to a unique reduced BCF.
(Immediate!)

We want to count BCFs of positive discriminant, for which the Hessians have negative discriminant.

Prop. Suppose f is a BCF with $\mathrm{disc}(f) > 1$.
Then $\mathrm{Aut}(f) \in \pm I$.

Proof. If $g \in \mathrm{Aut}(f)$, then g must fix its Hessian.
And, $\mathrm{Disc}(H(f)) \le -3$, so use what we know.

Note also that $f \circ -I = -f$.
So $\mathrm{Aut}(f)$ must be trivial.

Proposition. Every class of $SL_2(\mathbb{Z})$-equivalent irred. CF can be represented by exactly one reduced form with $a > 0$, apart from possible exceptions when $A = C$ and $B = 0$ or $A = B = C$.

29.3. Prop.

Suppose $|B| \le A \le C$ and $0 \le D \le X$.

Then: $|a| < X^{1/4}$, $|b| < 2X^{1/4}$, $|ad| < X^{1/2}$, $|bc| < 4X^{1/2}$,

$|ac^3| < 8X$, $|b^3 d| < 8X$, $c^2 |bc - 9ad| < 4X$.

Proof. Write down some identities.

$$9Ca^2 - 3Bab + Ab^2 = A^2$$
$$Cc^2 - 3Bcd + 9Ad^2 = C^2.$$

Have $B^2 \le AC$, so in above,

$|(\text{middle term})| \le$ GM of others

$\le$ AM of others,

so:

$$9Ca^2 + Ab^2 \le 2A^2$$
$$Cc^2 + 9Ad^2 \le 2C^2.$$

So, $|a| < AC^{-1/2}$, $|b| < 2A^{1/2}$, $|c| < 2C^{1/2}$, $|d| < CA^{-1/2}$.

We also have $A \le C$ and

$AC \le \frac{1}{3}(4AC - B^2) = D \le X$ so we get the first four.

Also, $|bc - 9ad| = |B| \le A$, get ~~some~~ the rest of the inequalities that way.

29.4.

Lemma 2. The number of cubic forms with integral coeffs and $a > 0$, which are reduced with $|B| = A$ or $A = C$ is

$$O(X^{3/4} \log X).$$

Half of the proof. Suppose $|B| = A$.

Then $$bc - 9ad = \pm (b^2 - 3ac)$$

so $\pm d$ is determined by a, b, c.

\# of possible b: $\ll X^{1/4}$

\# of a and c: Use $|a| < X^{1/4}$ and $|ac^3| < 8X$.

Sum of $$\sum_{a=1}^{\lfloor X^{1/4} \rfloor} 2 \left(\frac{8X}{a} \right)^{1/3} + 1$$

$$\sim 4X^{1/3} \int_{t=1}^{X^{1/4}} \frac{1}{t^{1/3}} \, dt$$

$$= 4X^{1/3} \left[\frac{t^{2/3}}{2/3} \right]_1^{X^{1/4}} < 3X^{1/3} \cdot X^{2/12} = 6X^{1/2}.$$

Lemma 3. # Reducible cubic forms with $a > 0$ with $|B| \leq A \leq C$ (like "reduced", but less restrictive)

and $0 \leq D \leq X$ is $\ll X^{3/4 + \varepsilon}$.

Moral. Most of them live in the cusp.

(See also BST, Lemma 21.)

30.1.

The Davenport - Heilbronn correspondence.

We've set up a correspondence

$$\begin{tikzcd} \mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{BCF}(\mathbb{Z}) \arrow[r, leftrightarrow] & \text{cubic rings} \\ \text{irreducible} \arrow[r] & \text{integral domain} \\ \text{~~has nilpote~~ disc} = 0 \arrow[r, leftrightarrow] & \text{has nilpotents.} \end{tikzcd}$$

(discriminant preserving)

We've also counted $\mathrm{SL}_2(\mathbb{Z})$-orbits on $\mathrm{BCF}(\mathbb{Z})$.

(Note: $\mathrm{GL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \sqcup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mathrm{SL}_2(\mathbb{Z})$,
so twice as many unless $f\circ\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in f\circ \mathrm{SL}_2(\mathbb{Z})$.

Prop. Let R be ~~a~~ a cubic ring which is an integral domain. Then R is an order in a cubic field.

Proof. (Hasty) Suppose to the contrary $R \ni w$, where w ~~contains~~ ~~a~~ satisfies a quadratic polynomial, and is not in $\mathbb{Z}$.

Then $w^2 = aw + b$,
so $\left(w - \frac{a}{2}\right)^2 = b + \frac{a^2}{4}$.

Slightly cheating. But write $2w - a$.

So, WLOG $w^2 = b$. (and $w \notin \mathbb{Z}$.)

Since $R \neq \mathbb{Z} \oplus \mathbb{Z}w$, R contains some θ not in $\mathbb{Z} \oplus \mathbb{Z}w$.

We have $w \cdot \theta = d + ew + f\theta$, for some $d, e, f \in \mathbb{Q}$.)
(This involves linear algebra over $\mathbb{Q}$.)

$w(\theta - e) = d + f\theta$, so

WLOG (again!) $w \cdot \theta = d + f\theta$.

Then, $w^2\theta = w[d + f\theta] = wd + f[d + f\theta]$
$= b\theta$, so $d = 0$.

$w \cdot \theta = f\theta$, so $(w - f)\theta = 0$. Done.

30, 2 = 31.1.

~~The key proposition.~~

<u>Def</u>. A cubic ring R is <u>nonmaximal</u> <u>at</u> p if it is contained in another cubic ring R' with index a multiple of p.

<u>Fact / exercise</u>. <u>TFAE</u>.

(1) R is nonmaximal at p.

(2) $R \subseteq R'$ with $[R' : R]$ a <u>power</u> of p.

(3) $R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is nonmaximal as a cubic ring over $\mathbb{Z}_p$.

We'll omit the proof. You can get $(1) \longleftrightarrow (2)$ without going through (3).

So assume $[R' : R]$ is a power of p.

Now, by "elementary divisors" there is a basis $\langle 1, w, \theta \rangle$ of R for which

$$R' = \mathbb{Z} + \mathbb{Z}(w/p^i) + \mathbb{Z}(\theta/p^j) \qquad *$$

for some i, j. WLOG $i \geq j$ and $i \geq 1$.

<u>Lemma</u>. (BST, Lemma 13)

If R is nonmaximal at p, there is a $\mathbb{Z}$-basis $\langle 1, w, \theta \rangle$ of R s.t. at least one of the following is true.

(1) $\mathbb{Z} + \mathbb{Z}(w/p) + \mathbb{Z}\theta$ is a ring.

(2) $\mathbb{Z} + \mathbb{Z}(w/p) + \mathbb{Z}(\theta/p)$ is a ring.

<u>Proof</u>. Go back to above. If $i = 1$, done, so assume $i > 1$.

<u>Normalize</u> the <u>basis</u> $(*)$ for R'. (i.e. $\frac{w}{p^i} \cdot \frac{\theta}{p^j} \in \mathbb{Z}$.)

Write out

$$w\theta = n$$
$$w^2 = m - bw + a\theta$$
$$\theta^2 = l - dw + c\theta$$

and demand that (*) gives a ring:

$$\frac{w\theta}{p^{i+j}} = \frac{n}{p^{i+j}}$$

$$\left(\frac{w}{p^i}\right)^2 = \frac{m}{p^{2i}} - b \cdot \frac{w}{p^{2i}} + a \cdot \frac{\theta}{p^{2i}}$$

$$\left(\frac{\theta}{p^j}\right)^2 = \frac{l}{p^{2j}} - d \cdot \frac{w}{p^{2j}} + c \cdot \frac{\theta}{p^{2j}}$$

We must have: $\frac{c\theta}{p^{2j}}$ is an integer multiple of $\frac{\theta}{p^j}$,

hence $c \equiv 0 \pmod{p^j}$

similarly $b \equiv 0 \pmod{p^i}$

Also $\frac{a\theta}{p^{2i}}$ is an integer multiple of $\frac{\theta}{p^j}$, so

$a \equiv 0 \pmod{p^{2i-j}}$

(assuming $2i - j \geq 0$)

similarly $d \equiv 0 \pmod{p^{2j-i}}$.

These conditions are equivalent to $\langle 1, w/p^i, \theta/p^j \rangle$ being a ring.

If $j = 0$, may replace $(i, 0)$ with $(1, 0)$.

If $j > 0$, may replace (i, j) with $(i-j, 0)$

or with $(i-j+1, 1)$.

So get $(1,0)$ or $(1,1)$ as desired.

7. ~ 51.5.

So what do we get in the end?

Prop. If $au^3 + bu^2v + cuv^2 + dv^3$ corresponds to a cubic ring nonmaximal at p, then it is $GL_2(\mathbb{Z})$-equivalent to a form for which either.

(1: (1,1) case) $p \mid a$, $p \mid b$, $p \mid c$, $p \mid d$, or

(2: (1,0) case) $p^2 \mid a$, $p \mid b$.

Exercise. Compute the cubic rings R corresponding to $7u^3 + 7u^2v + 7uv^2 + 7v^3$

$49u^3 + 7u^2v + uv^2 + v^3$

and for each find $R' \supseteq R$ with $[R' : R]$ a power of p.

Exercise. Let R be the cubic form corresponding to 0. Let m be any integer. Find R' with $m \mid [R' : R]$.

If time (doubtful) Talk about how this is used, how to prove D-H etc.

More parametrizations and counting theorems.

How to count quartic fields?

We <u>wish</u> the following was true.

<u>Non-Theorem</u>. There is a bijection

$$\text{Binary Quartic Forms}\Big/GL_2(\mathbb{Z}) \longleftrightarrow \text{Quartic Rings}.$$

The issue is that the $GL_2(\mathbb{Z})$ action isn't enough. Different orbits can give the same ring.

Indeed: Look over $\mathbb{C}$.

$$\{\text{nondegen. quartic forms}\}\Big/GL_2(\mathbb{C}) \overset{?}{\longleftrightarrow} \begin{array}{l}\text{quartic rings}/\mathbb{C}\\ \text{with no nilpotents.}\end{array}$$

The RHS is $\mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}$.
i.e. only one of them.

But LHS is <u>not</u> a point.
$GL_2(\mathbb{C})$ does <u>not</u> act transitively on 4-tuples of points in $\mathbb{P}^1(\mathbb{C})$.

To get a parametrization, go back way in history.

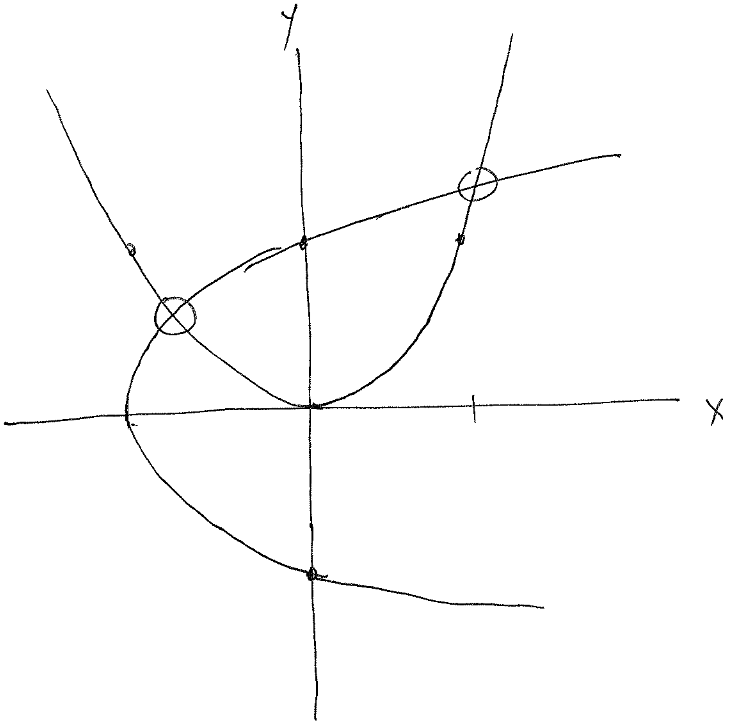
(1) <u>Solution of the quartic</u>. (Ferrari, 1522 - 1565).

(2) <u>Further back</u>. Omar Khayyam (1048 - 1131)

32.2.

Example. Find a root of $x^4 - x - 1 = 0$.

Solution. Write $y = x^2$. So, $y^2 - x - 1 = 0$,
$x = y^2 - 1$.



There they are!
We didn't write them down explicitly.
But we basically understand them.

Solutions to the quartic are given by the intersection of quadrics (i.e. conic sections).

Sol'n of the quartic. Use Galois theory.
Assume K is S_4 over $\mathbb{Q}$.

$$\begin{tikzcd}
 & \tilde{K} \arrow[dl, dash] \arrow[dd, dash] \\
K \arrow[dd, dash, "4"'] & \\
 & E \\
\mathbb{Q} \arrow[ur, dash] &
\end{tikzcd}$$

Let E be the resolvent cubic:
Corresponds to a 2-sylow subgroup of $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$, which is unique up to conjugation.

32. 3.

Prop. Let $K = \mathbb{Q}(\theta)$, where θ has conjugates $\theta', \theta'', \theta'''$.
Then, $E = \mathbb{Q}(\theta\theta' + \theta''\theta''')$.

Proof. Galois theory. Let $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ act on $\theta\theta' + \theta''\theta'''$.
Does so with stabilizer group of size 8. $(= D_4)$

Stabilizers are all $\tau \in \mathrm{Gal}(\tilde{F}/\mathbb{Q})$ sending:

$$\theta \to \theta, \quad \theta' \to \theta'$$
$$\theta \to \theta', \quad \theta' \to \theta$$
$$\theta \to \theta'', \quad \theta' \to \theta'''$$
$$\theta \to \theta''', \quad \theta' \to \theta''.$$

Prop. If $K = \mathbb{Q}(\theta)$, with
$$\theta^4 + a_3\theta^3 + a_2\theta^2 + a_1\theta + a_0 = 0,$$
can take E generated by a root of
$$x^3 - a_2x^2 + (a_1a_3 - 4a_0)x + 4a_0a_2 - a_1^2 - a_0a_3^2.$$

Proof. a_3, a_2, a_1, a_0 are all symmetric functions in $\theta, \theta', \theta'', \theta'''$:
$$(x-\theta)(x-\theta')(x-\theta'')(x-\theta''') = x^4 - [\theta + \theta' + \theta'' + \theta''']x^3 + (\text{etc.})$$

E is generated by
$$(x - [\theta\theta' + \theta''\theta'''])(x - [\theta\theta'' + \theta'\theta'''])(x - [\theta\theta''' + \theta'\theta'']).$$

Multiply out and compare.

Now Use Cardano's formula to solve that and then find $\theta, \theta', \theta'', \theta'''$ from knowing those and all symmetric functions.

32.4.

Bhargava's theorem.

Let $(\mathrm{Sym}^2 \mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ be the ~~sep~~ lattice of pairs of integral ternary quadratic forms. (= conic sections)

These are given as pairs of 3×3 symmetric matrices

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{bmatrix}, \qquad \text{(same with } b\text{'s)}$$

Corresponding to

$$[u \quad v \quad w] \begin{bmatrix} a_{11} & & \\ & \ddots & \\ & & a_{33} \end{bmatrix} \begin{bmatrix} u \\ v \\ w \end{bmatrix}$$

$$= a_{11} u^2 + 2a_{12} uv + 2a_{13} uw + \cdots$$

Note that as written we allow $a_{ij} \in \frac{1}{2}\mathbb{Z}$ for $i \neq j$.

There is an action of $GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$:

$$(g_3, g_2) \circ (A, B) = (r \cdot g_3 A g_3^T + s \cdot g_3 B g_3^T, \; t \cdot g_3 A g_3^T + u \cdot g_3 B g_3^T).$$

$$g_2 = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

So GL_3 acts by change of basis on u, v, w.

GL_2 preserves the "pencil" of conics given by A, B but switches what A and B are.

31.5.

Definition. Let Q be a quartic ring.

We say a cubic ring R is a cubic resolvent ring of R if $\mathrm{Disc}(R) = \mathrm{Disc}(Q)$, and

$$R \supseteq \{ x x' + x'' x''' : x \in R \}.$$

Caution. We haven't said what the conjugates of x are. Bhargava does a weird algebraic construction to get them

Prop. Every quartic ring has at least one cubic resolvent. If Q is the maximal order of a cubic field, it is unique.

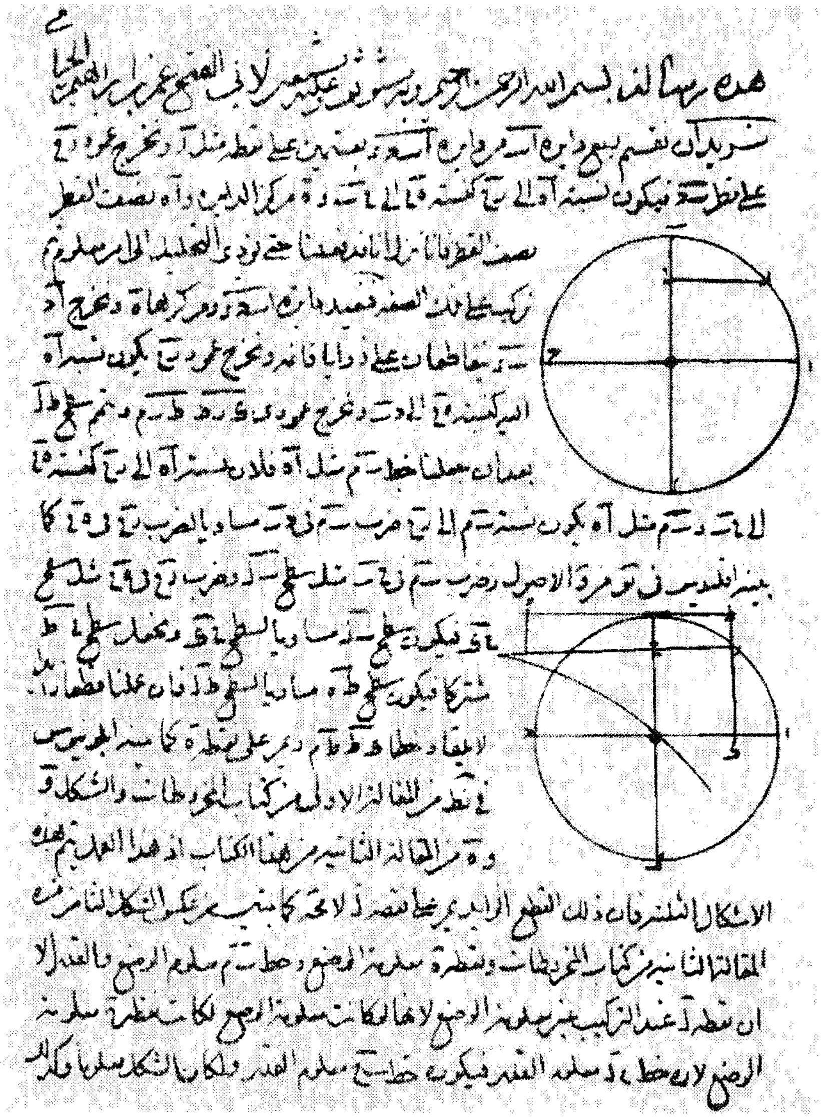
Theorem. (Bhargava, Annals, 2004)

There is a canonical bijection

$$\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}) \backslash (\mathrm{Sym}^2 \mathbb{Z}^3 \otimes \mathbb{Z}^2)^* \longleftrightarrow \begin{array}{l}(Q, R) \\ Q \text{ is a quartic ring} \\ R \text{ is a cubic resolvent.}\end{array}$$

And, # of quartic fields K with $0 < |\mathrm{Disc}\, K| < X$ is

$$\sim \frac{5}{24} \prod_p (1 + p^{-2} - p^{-3} - p^{-4}) \cdot X.$$



Enter what you want to calculate or know about:

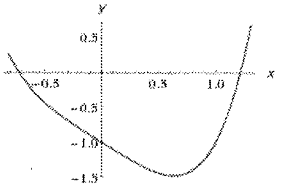
x^4 - x - 1

Examples Random

Input:

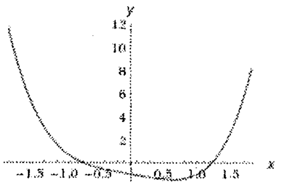
$x^4 - x - 1$

Plots:



(x from −0.5 to 1)

Enable interactivity



(x from −1.5 to 1.5)

Enable interactivity

Alternate form:

$x(x^3 - 1) - 1$

Real roots: Approximate forms Step-by-step solution

$$x = \frac{1}{2}\sqrt{\frac{\sqrt[3]{\frac{1}{2}(9+\sqrt{849})}}{3^{2/3}} - 4\sqrt[3]{\frac{2}{3(9+\sqrt{849})}}} - \frac{1}{2}\sqrt{4\sqrt[3]{\frac{2}{3(9+\sqrt{849})}} - \frac{\sqrt[3]{\frac{1}{2}(9+\sqrt{849})}}{3^{2/3}} + \frac{2}{\sqrt{\frac{\sqrt[3]{\frac{1}{2}(9+\sqrt{849})}}{3^{2/3}} - 4\sqrt[3]{\frac{2}{3(9+\sqrt{849})}}}}}$$

$$x = \frac{1}{2}\sqrt{\frac{\sqrt[3]{\frac{1}{2}(9+\sqrt{849})}}{3^{2/3}} - 4\sqrt[3]{\frac{2}{3(9+\sqrt{849})}}} + \frac{1}{2}\sqrt{4\sqrt[3]{\frac{2}{3(9+\sqrt{849})}} - \frac{\sqrt[3]{\frac{1}{2}(9+\sqrt{849})}}{3^{2/3}} + \frac{2}{\sqrt{\frac{\sqrt[3]{\frac{1}{2}(9+\sqrt{849})}}{3^{2/3}} - 4\sqrt[3]{\frac{2}{3(9+\sqrt{849})}}}}}$$

Complex roots: More digits Exact forms Step-by-step solution

$x = -0.24813 - 1.03398\, i$