Some Highlights along a Path to Elliptic Curves

Part 4: Solving a Cubic Equation

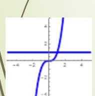
Steven J. Wilson, Fall 2016

Outline of the Series

1. The World of Algebraic Curves
2. Conic Sections and Rational Points
3. Projective Geometry and Bezout's Theorem
4. **Solving a Cubic Equation**
5. Exploring Cubic Curves
6. Rational Points on Elliptic Curves

Simple Cubic Equations

- Solve $x^3 - 6x^2 = 0$.
  - By factoring: $x^2(x-6) = 0$, so $x = 0 \text{ (twice)}, 6$
- Solve $x^3 - 6x = 0$.
  - By factoring: $x(x^2 - 6) = 0$, so $x = 0, \pm\sqrt{6}$
- Solve $x^3 - 6x^2 + 6x = 0$.
  - By factoring: $x(x^2 - 6x + 6) = 0$
  - Then with quadratic formula: $x = 0, 3 \pm \sqrt{3}$
- Solve $x^3 - 1 = 0$.
  - We get $x^3 = 1$ so $x = \sqrt[3]{1} = 1$. But what's wrong?
  - Corollary of the Fundamental Theorem of Algebra says 3 solutions.
  - Bezout's Theorem says 3 solutions.



Cube Roots of Unity, Algebraically

- Solve $x^3 - 1 = 0$.
  - By factoring: $(x-1)(x^2+x+1)=0$
  - Then with quadratic formula: $x = 1, -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$
- The value $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ is important.
- Note $\omega^2 = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^2 = \frac{1}{4} - \frac{\sqrt{3}}{2}i + \frac{3}{4}i^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$

$$\omega^3 = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \frac{1}{4} - \frac{3}{4}i^2 = 1$$

- So three solutions are $x = \omega, \omega^2, \omega^3$.

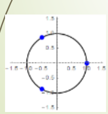
Cube Roots of Unity, With Trig

- Solve $x^3 - 1 = 0$.
  - We have: $x^3 = 1 = 1(\cos 0 + i \sin 0)$
- Then by (a corollary of) DeMoivre's Theorem:

$$x = \left[1(\cos 0 + i \sin 0)\right]^{1/3}$$

$$= 1^{1/3}\left(\cos\frac{0+2k\pi}{3} + i \sin\frac{0+2k\pi}{3}\right)$$

- So the 3 solutions are:



$$1(\cos 0 + i \sin 0) = 1$$

$$1\left(\cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i = \omega$$

$$1\left(\cos\frac{4\pi}{3} + i \sin\frac{4\pi}{3}\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i = \omega^2$$

Other Cube Roots

- Solve $x^3 - 40 = 0$.
  - We have: $x^3 = 40 = 40(\cos 0 + i \sin 0)$
- Then by (a corollary of) DeMoivre's Theorem:

$$x = \left[40(\cos 0 + i \sin 0)\right]^{1/3}$$

$$= \sqrt[3]{40}\left(\cos\frac{0+2k\pi}{3} + i \sin\frac{0+2k\pi}{3}\right)$$

- So the 3 solutions are:

$$\sqrt[3]{40}(\cos 0 + i \sin 0) = \sqrt[3]{40}$$

$$\sqrt[3]{40}\left(\cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}\right) = \sqrt[3]{40}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \omega\sqrt[3]{40}$$

$$\sqrt[3]{40}\left(\cos\frac{4\pi}{3} + i \sin\frac{4\pi}{3}\right) = \sqrt[3]{40}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = \omega^2\sqrt[3]{40}$$

The General Cubic Equation

- The **general cubic equation** has the form $ax^3+bx^2+cx+d=0$
- Divide by leading coefficient: $x^3+\frac{b}{a}x^2+\frac{c}{a}x+\frac{d}{a}=0$
- But $\left(x+\frac{b}{3a}\right)^3=x^3+\frac{b}{a}x^2+\frac{b^2}{3a^2}x+\frac{b^3}{27a^3}$
- Therefore $\left(x+\frac{b}{3a}\right)^3+\left(\frac{c}{a}-\frac{b^2}{3a^2}\right)x+\left(\frac{d}{a}-\frac{b^3}{27a^3}\right)=0$

$$\left(x+\frac{b}{3a}\right)^3+\left(\frac{3ac-b^2}{3a^2}\right)x+\left(\frac{27a^2d-b^3}{27a^3}\right)=0$$

$$\left(x+\frac{b}{3a}\right)^3+\left(\frac{3ac-b^2}{3a^2}\right)\left(x+\frac{b}{3a}\right)+\left(\frac{27a^2d+2b^3-9abc}{27a^3}\right)=0$$

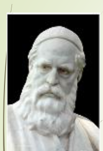
- Which has the form: $\left(x+\frac{b}{3a}\right)^3+p\left(x+\frac{b}{3a}\right)+q=0$
- A **reduced cubic equation** has the form $x^3+px+q=0$.

Controversy

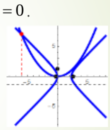



- 1515: Del Ferro solved a cubic lacking a quadratic term. He died in 1526, after sharing the solution with his pupil Fior.
- 1535: Tartaglia announces he has solved a cubic (lacking a linear term). Fior does not believe him, and challenges Tartaglia to a contest. Shortly before the contest, Tartaglia finds another solution to a cubic (lacking a quadratic term). Tartaglia wins the contest.
- 1539: Cardano gets the cubic solution from Tartaglia, but (according to Tartaglia) is pledged to secrecy.
- Cardano's pupil Ferrari solves the quartic.
- 1543: Cardano & Ferrari see the cubic solution in the papers of Del Ferro.
- 1545: Cardano publishes the solutions of both the cubic and the quartic, crediting Tartaglia, Ferrari, del Ferro, and others. Tartaglia accuses Cardano of plagiarism.
- 1547-1548: Ferrari challenges Tartaglia to a contest, Ferrari wins and Tartaglia is discredited.

Solving a Cubic Geometrically



- Omar Khayyam (1070) "constructed" solutions of all types of cubic equations using intersecting conic sections.
- Example: Solve $x^3-26x+60=0$.
- Graph: $\begin{cases} y=\dfrac{x^2}{\sqrt{26}} \\ y^2=x\left(x-\dfrac{60}{26}\right)\end{cases}$



$x=-6$

- Why does it work? Substitute: $\left(\frac{x^2}{\sqrt{26}}\right)^2=x^2-\frac{60}{26}x$

$$x^4=26x^2-60x$$

$$x^4-26x^2+60x=0$$

$$x(x^3-26x+60)=0$$

Reduced Cubic, Algebraically

- Solve: $x^3 - 26x + 60 = 0$
- Suppose a solution of two terms, that is: $x = u + v$
- Then $(u+v)^3 - 26(u+v) + 60 = 0$

  $u^3 + (3uv - 26)(u+v) + v^3 + 60 = 0$
- Choose $v = \frac{26}{3u}$, so that several terms drop out.
- Then $u^3 + v^3 + 60 = 0$

  $u^3 + \left(\frac{26}{3u}\right)^3 + 60 = 0$

  $27u^6 + 1620u^3 + 17576 = 0$
- This is quadratic in u^3. So

$$u^3 = \frac{-1620 \pm \sqrt{1620^2 - 4(27)17576}}{2(27)} = -30 \pm \frac{82}{9}\sqrt{3}$$

Reduced Cubic, Algebraically

- Solve: $x^3 - 26x + 60 = 0$
- Suppose a solution of two terms, that is: $x = u + v$

- Since $u^3 = -30 \pm \frac{82}{9}\sqrt{3}$
- We use $u = \sqrt[3]{-30 + \frac{82}{9}\sqrt{3}} \approx -2.42265$
- and $v = \sqrt[3]{-30 - \frac{82}{9}\sqrt{3}} \approx -3.57735$
- Solutions:

  $u + v = -6$

  $u\omega + v\omega^2 = 3 + i$

  $u\omega^2 + v\omega = 3 - i$

Unanswered Questions

- Since $u^3 = -30 \pm \frac{82}{9}\sqrt{3}$
- We use $u = \sqrt[3]{-30 + \frac{82}{9}\sqrt{3}} \approx -2.42265$
- and $v = \sqrt[3]{-30 - \frac{82}{9}\sqrt{3}} \approx -3.57735$
- Solutions: $u + v = -6$, $u\omega + v\omega^2 = 3 + i$, $u\omega^2 + v\omega = 3 - i$

- How do we know u^3 and v^3 are conjugates?
- How do we know $u\omega + v\omega^2$ and $u\omega^2 + v\omega$ are also solutions?
- What if the radicand of the square root in the formula for u^3 is negative, causing us to get cube roots of nonreal numbers?
- Can we simplify $\sqrt[3]{-30 + \frac{82}{9}\sqrt{3}}$ without using decimal approximations?

Cardano's Formula

- When substituting $x=u+v$ into $x^3+px+q=0$, we get: $(u+v)^3+p(u+v)+q=0$
- or: $u^3+v^3+(3uv+p)(u+v)+q=0$, so use: $v=\frac{-p}{3u}$
- Then $u^3+\left(\frac{-p}{3u}\right)^3+q=0$ becomes $27u^6+27qu^3-p^3=0$
- And quadratic formula gives:

$$u^3=\frac{-27q\pm\sqrt{27^2q^2-4(27)(-p^3)}}{2(27)}=\frac{-q}{2}\pm\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}$$

- So

$$x=\sqrt[3]{\frac{-q}{2}+\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{\frac{-q}{2}-\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

Conjugates?

How do we know u^3 and v^3 are conjugates?

- Note that:

$$\left(\frac{-q}{2}+\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)\left(\frac{-q}{2}-\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)=\frac{q^2}{4}-\left(\frac{q^2}{4}+\frac{p^3}{27}\right)=\left(\frac{-p}{3}\right)^3$$

- But $v=\frac{-p}{3u}$ implies $u^3v^3=\left(\frac{-p}{3}\right)^3$,
- so choosing $u^3=\frac{-q}{2}+\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}$
- implies $v^3=\frac{-q}{2}-\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}$.

The Other Solutions?

- How do we know $u\omega+v\omega^2$ and $u\omega^2+v\omega$ are also solutions?

$$\begin{aligned}
x^3+px+q&=(u\omega+v\omega^2)^3+p(u\omega+v\omega^2)+q\\
&=u^3\omega^3+3u^2v\omega^4+3uv^2\omega^5+v^3\omega^6+pu\omega+pv\omega^2+q\\
&=u^3+3u^2v\omega+3uv^2\omega^2+v^3+pu\omega+pv\omega^2+q\\
&=u^3+v^3+(3uv+p)(u\omega+v\omega^2)+q\\
&=u^3+v^3+q\\
&=u^3+v^3+(3uv+p)(u+v)+q\\
&=(u+v)^3+p(u+v)+q\\
&=0
\end{aligned}$$

- Similarly for $u\omega^2+v\omega$.

Discriminants

- Cardano said: $x=\sqrt[3]{\frac{-q}{2}+\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{\frac{-q}{2}-\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$
- The quantity $\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3$ determines the solution types.
- The **discriminant** is defined as $\Delta=-108\left[\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3\right]=-27q^2-4p^3$

Radicands of Square Roots	Discriminant	Radicands of Cube Roots	Solutions of Cubic Equation
Positive	Negative	Real	1 real, 2 nonreal
Zero	Zero	Real, equal	2 real (1 repeated)
Negative	Positive	Nonreal	3 real

- Real solutions from nonreal radicands was the actual catalyst for the development of complex numbers, by Bombelli (1572).

Cube Roots of Nonreal Numbers?

- If the radicand of the square root is negative, then
  $u^3=\frac{-q}{2}+\sqrt{\left(\frac{-q}{2}\right)^2+\left(\frac{p}{3}\right)^3}=\frac{-q}{2}+i\sqrt{-\frac{q^2}{4}-\frac{p^3}{27}}$
- Then rewrite the complex value in trigonometric form.
  $r^2=\frac{q^2}{4}+\left(-\frac{q^2}{4}-\frac{p^3}{27}\right)=-\frac{p^3}{27}$ $\qquad \cos\theta=\frac{a}{r}=\frac{-q}{2}\sqrt{\frac{27}{-p^3}}=\frac{3q}{2p}\sqrt{\frac{3}{-p}}$
- So

$$u^3=\sqrt{\frac{-p^3}{27}}\left[\cos\left(\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)\right)+i\sin\left(\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)\right)\right]$$

$$u=\sqrt{\frac{-p}{3}}\left[\cos\left(\frac{1}{3}\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)\right)+i\sin\left(\frac{1}{3}\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)\right)\right]$$

$$v=\sqrt{\frac{-p}{3}}\left[\cos\left(\frac{1}{3}\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)\right)-i\sin\left(\frac{1}{3}\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)\right)\right]$$

$$x=u+v=2\sqrt{\frac{-p}{3}}\left[\cos\left(\frac{1}{3}\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)\right)\right]$$

$$x=2\sqrt{\frac{-p}{3}}\left[\cos\left(\frac{1}{3}\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)+120^\circ k\right)\right]$$

Due to Viete (1540-1603), Published 1615

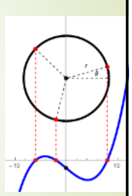
Example using a Trig Solution

- Solve $x^3-52x-96=0$.
- Using $p=-52$ and $q=-96$
- Then $x=2\sqrt{\frac{-p}{3}}\left[\cos\left(\frac{1}{3}\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)+120^\circ k\right)\right]$

$$=2\sqrt{\frac{52}{3}}\left[\cos\left(\frac{1}{3}\cos^{-1}\left(\frac{3(96)}{2(52)}\sqrt{\frac{3}{52}}\right)+120^\circ k\right)\right]$$

$$=\begin{cases} 8.3267\cos 16.10^\circ=8 \\ 8.3267\cos 136.10^\circ=-6 \\ 8.3267\cos 256.10^\circ=-2 \end{cases}$$

- Solutions involving decimal approximations may not be completely satisfying.



$r=2\sqrt{\frac{-p}{3}}$

$\theta=\frac{1}{3}\cos^{-1}\left(\frac{3q}{2p}\sqrt{\frac{3}{-p}}\right)$

Nested Radicals

- Can we simplify $\sqrt[3]{-30+\frac{82}{9}\sqrt{3}}$ without using decimal approximations?
- Recall from trigonometry:

$$\sin 15^\circ = \sin\left(45^\circ - 30^\circ\right) = \sin 45^\circ \cos 30^\circ - \cos 45^\circ \cos 30^\circ = \frac{\sqrt{6}-\sqrt{2}}{4}$$

$$\sin 15^\circ = \sin\left(\frac{30^\circ}{2}\right) = +\sqrt{\frac{1-\cos 30^\circ}{2}} = \sqrt{\frac{1-\frac{\sqrt{3}}{2}}{2}} = \frac{\sqrt{2-\sqrt{3}}}{2}$$

- And $\frac{\sqrt{6}-\sqrt{2}}{4} \approx 0.2588190451 \approx \frac{\sqrt{2-\sqrt{3}}}{2}$
- Are they really equal? How can we tell?

$$\frac{\sqrt{6}-\sqrt{2}}{4} = \sin 15^\circ = \frac{\sqrt{2-\sqrt{3}}}{2}$$

Converting Radical Forms

- How can we convert from one form to the other?
- One direction is easy:

$$\frac{\sqrt{6}-\sqrt{2}}{4} = \sqrt{\left(\frac{\sqrt{6}-\sqrt{2}}{4}\right)^2} = \sqrt{\frac{6-2\sqrt{12}+2}{16}} = \sqrt{\frac{8-4\sqrt{3}}{16}} = \frac{\sqrt{2-\sqrt{3}}}{2}$$

- But the nested form is generally not simpler. Can we denest a radical?

Square Root Denesting Theorem (Borodin, et al, 1985)

- If the product of the radicand and its conjugate is a perfect square, then the square root of the radicand will denest.

$$\left(2-\sqrt{3}\right)\left(2+\sqrt{3}\right) = 4-3 = 1$$

Denesting a Square Root

- Assume a similar form: $\sqrt{2-\sqrt{3}} = a + b\sqrt{3}$
- Square both sides: $2-\sqrt{3} = \left(a+b\sqrt{3}\right)^2 = \left(a^2+3b^2\right) + 2ab\sqrt{3}$
- Solve the system: $\begin{cases} a^2+3b^2 = 2 \\ 2ab = -1 \end{cases}$
- Creatively: $(a^2+3b^2)(-1) = (2ab)(2)$

$$a^2+4ab+3b^2 = 0$$

$$(a+b)(a+3b) = 0 \quad \Rightarrow \quad a=-b \quad \text{or} \quad a=-3b$$

- Can use either (simpler) solution: $2(-b)(b) = -1 \quad \Rightarrow \quad b = \pm\frac{\sqrt{2}}{2}$
- So we have:

$$\sqrt{2-\sqrt{3}} = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\sqrt{3} = \frac{\sqrt{6}-\sqrt{2}}{2}$$

Denesting a Cube Root

- Denest: $u=\sqrt[3]{-30+\frac{82}{9}\sqrt{3}}\approx -2.42265$
- Assume: $\sqrt[3]{-30+\frac{82}{9}\sqrt{3}}=a+b\sqrt{3}$
- Then: $\left(a+b\sqrt{3}\right)^3=\left(a^3+9ab^2\right)+\left(3a^2b+3b^3\right)\sqrt{3}=-30+\frac{82}{9}\sqrt{3}$
- Solve: $\begin{cases} a^3+9ab^2=-30 \\ 27a^2b+27b^3=82 \end{cases}$
- Which gives: $(82)(a^3+9ab^2)=(-30)(27a^2b+27b^3)$
  $82\left(\frac{a}{b}\right)^3+810\left(\frac{a}{b}\right)^2+738\left(\frac{a}{b}\right)+810=0$
- Looking for rational zeros, we find $\frac{a}{b}=9 \;\Rightarrow\; a=9b$
- Substituting into $a^3+9ab^2=-30$ gives $810b^3=-30$ or $b=-\frac{1}{3}$
- Then $a=-3$, so $\sqrt[3]{-30+\frac{82}{9}\sqrt{3}}=-3+\frac{\sqrt{3}}{3}$

Denesting a Nonreal Radicand

- Solve $x^3-52x-96=0$.
- Using $x=u+v$ and $v=\frac{52}{3u}$ will lead to

$$u^3=\frac{2592+\sqrt{-8467200}}{54}=48+\frac{280}{9}i\sqrt{3}$$

- Assuming $u=a+bi\sqrt{3}$, then $u^3=(a^3-9ab^2)+(3a^2b-3b^3)i\sqrt{3}$
- Solving $\begin{cases} a^3-9ab^2=48 \\ 3a^2b-3b^3=\frac{280}{9} \end{cases}$
- Gives $280(a^3-9ab^2)=48(9)(3a^2b-3b^3)$
  $280\left(\frac{a}{b}\right)^3-1296\left(\frac{a}{b}\right)^2-2520\left(\frac{a}{b}\right)+1296=0 \;\Rightarrow\; \frac{a}{b}=6$
- Then $(6b)^3-9(6b)b^2=162b^3=48 \;\Rightarrow\; b=\frac{2}{3},\quad a=4$
- Therefore $\sqrt[3]{48+\frac{280}{9}i\sqrt{3}}=4+\frac{2}{3}i\sqrt{3}$ and $u+v=8$.

Challenges

- Denest $\sqrt{8+2\sqrt{15}}$
- Solve $x^3+63x-316=0$
- Solve $4x^3-79x+105=0$