Conjugate numbers, irrational numbers and Pell's equation

Peter Giblin
pjgiblin@liv.ac.uk

First, an experiment, for which you'll need a calculator

Ex. 1. Work out $(2 + \sqrt{3})^n$ for $n = 1, 2, 3, 4, 5, 6, 7, 8$ to a few decimal places, and note down the answers

Ex. 2. Work out $(1 + 2\sqrt{3})^n$ for $n = 1, ..., 8$ similarly.

Do you notice anything special about the first example which is not true of the second?

For Ex.1, changing the sign, $2 - \sqrt{3} = 0.268....$
For Ex.2, changing the sign, $1 - 2\sqrt{3} = -2.46.....$

So in Ex.1, the <u>powers of $2 - \sqrt{3}$ will tend to 0</u> and the <u>powers of $2 + \sqrt{3}$ get closer and closer to whole numbers</u>

but in Ex.2, the <u>powers of $1 - 2\sqrt{3}$ get ever bigger</u> in absolute value (and alternating in sign) while the <u>powers of $1 + 2\sqrt{3}$ don't seem to be doing anything interesting</u> !

So let's look at which positive integers *a, b* satisfy $-1 < a - b\sqrt{3} < 1$, which will make powers of $a - b\sqrt{3}$ tend to 0. (Note x^n always tends to zero for large n when $-1 < x < 1$.)

For example, with a = one of the numbers 1, 2, 3,..., 8 what are the possible b?

Find solutions to
$-1 < a - b\sqrt{3} < 1$ for
$a = 1$ or 2 or....or 8
This is the same as

$$\frac{a-1}{b} < \sqrt{3} < \frac{a+1}{b}$$

a	b
1	1
2	1
3	2
4	2
5	3
6	3
6	4
7	4
8	5

$a - b\sqrt{3}$ and
$a + b\sqrt{3}$
are called **conjugate numbers.**

For each of these pairs the powers of
$a - b\sqrt{3}$ become closer and closer to zero; also the powers of
$a + b\sqrt{3}$ become closer and closer to whole numbers.

So, can we explain this strange occurrence of whole numbers?

Expand $(a + b\sqrt{3})^2$ and $(a - b\sqrt{3})^2$

$$(a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3} = A + B\sqrt{3} \text{ say}$$
$$(a - b\sqrt{3})^2 = a^2 + 3b^2 - 2ab\sqrt{3} = A - B\sqrt{3}$$

"Just change $\sqrt{3}$ to $-\sqrt{3}$ everywhere it occurs"

The same goes for $(a + b\sqrt{3})^n$ and $(a - b\sqrt{3})^n$

Indeed let $(a + b\sqrt{3})^n = A + B\sqrt{3}$. If a,b are integers then so are A, B.
Also $(a - b\sqrt{3})^n = A - B\sqrt{3}$

So $(a + b\sqrt{3})^n + (a - b\sqrt{3})^n = 2A$ and if $-1 < a - b\sqrt{3} < 1$ so $(a - b\sqrt{3})^n$ tends to 0 as n gets bigger then $(a + b\sqrt{3})^n$ must get closer to the integer 2A.

Is it ever possible for $a - b\sqrt{3} = 1$ or -1 when a, b are integers? Remember the following fact about fractions:

If $\dfrac{A}{B}$ is a fraction in its lowest terms (A, B positive integers) then the other fractions equal to this one are exactly those of the form $\dfrac{Ak}{Bk}$ for an integer k.

For example $\dfrac{4}{7}$ is in its lowest terms and all the fractions equal to this one are of the form $\dfrac{4k}{7k}$ such as $\dfrac{8}{14}, \dfrac{20}{35}$ etc.

Now suppose $\dfrac{A}{B}$ is in its lowest terms and $\left(\dfrac{A}{B}\right)^2 = N$ (N a positive integer).

Rewrite this as $\dfrac{A}{B} =$ another fraction and then use the fact above about a fraction in lowest terms equal to another fraction.

You'll find after rearrangement that $N = k^2$: N is a square number. So $\boxed{\text{the only square roots expressible as fractions are square roots of square numbers like 4,9,16, 121.}}$

It is **never** possible for $a - b\sqrt{3} = 1$ or -1 when a, b are integers, since it would imply

$$\sqrt{3} = \frac{a-1}{b} \text{ or } \sqrt{3} = \frac{a+1}{b}$$

Similarly $a + b\sqrt{3} = 1$ or -1 is impossible.

Even though $a - b\sqrt{3} = 1$ and $a + b\sqrt{3} = 1$ have no solutions in integers what about
$a^2 - 3b^2 = (a - b\sqrt{3})(a + b\sqrt{3}) = 1$? [Difference of two squares!]
Can you find some solutions?

$a = 2$, $b = 1$
$a = 7$, $b = 4$
are solutions. How could we find some more?

Well, $(2 - \sqrt{3})^n(2 + \sqrt{3})^n$ will also = 1 for any n
$n = 2$ gives the solution $a = 7$, $b = 4$:

$$1 = (2-\sqrt{3})^2(2+\sqrt{3})^2 = (7-4\sqrt{3})(7+4\sqrt{3}) = 7^2 - 4^2 \times 3$$

$n = 3$ gives the solution $a = 26$, $b = 15$
For this, work out $(2 + \sqrt{3})^3$
$n = 4$ gives the solution $a = 97$, $b = 56$
etc. This provides infinitely many solutions.

In fact for any integer $d > 0$ there are always infinitely many solutions to the "Pell equation"

$$a^2 - d\,b^2 = 1.$$

Pell's equation is important in applications to continued fractions and factoring large numbers.

Sometimes the smallest solution is quite big however: if $d = 109$ the smallest solution is

$a = 158\ 070\ 671\ 986\ 249$ [can you <u>say</u> this number?!]
$b = \quad 15\ 140\ 424\ 455\ 100$

The great number theorist Pierre de Fermat challenged his friend Bernard Frénicle de Bessy in 1657 to find the smallest solution when $d = 61$ "in order not to give you too much trouble". (It's $a = 1\ 766\ 319\ 049$, $b = 226\ 153\ 980$.)

Smallest solutions for $d = 5, 6, 7, 8$ are not hard to find and then other solutions come from using $(a + b\sqrt{d})^n$ Look up Pell's equation on Google!

Equations $a^2 - d b^2 = c$ may have no integer solutions for values of c other than 1. For example

$a^2 - 2b^2 = 3$ has no integer solutions!

(How on earth might you prove such a statement??)

whereas $a^2 - 2b^2 = 7$ has infinitely many (e.g. $a = 3$, $b = 1$).

This is part of a very big subject called the *representation of integers by means of quadratic forms.* A very weird example here is the so-called Fifteen Theorem [look it up on Google!].

Let's think about $a^2 - 2b^2 = 3$.

- Why must a^2 be odd? Why must a be odd?

- What remainder must a^2 leave when divided by 8?

  $[(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1]$

- So what remainder will $2b^2$ leave when divided by 8?

- So what remainder will b^2 give when divided by 4?

- Is this possible?