Cubic Pell Equation

John D Mangual

On Math.StackExchange I learned we can solve Pell's Equation purely from Pigeonhole Principle. Let's try[1]

$$x^2 - 17y^2 = 1$$

#1 Using Pigeonhole, there are infinely many pairs (x, y) with

$$x^2 - 17y^2 \leq 2\sqrt{17}$$

This stems from attempting to use the Euclidean algorithm to find the GCD of $\sqrt{17}$ and 1:

$$\sqrt{17} = 4 \times 1 + (\sqrt{17} - 4)$$

[1] Here is also

The number $\sqrt{17}-4$ is the remainder when we use the division algorithm. But this is getting ahead of ourselves.

The 18 multiples of $\sqrt{17}$ starting from 0 can be put into groups:

$$0, \sqrt{17}, 2\sqrt{17}, \ldots, 10\sqrt{17}$$

How do I compute the best integer approximations, I might square these:

$$0, 17, 68, \ldots, 4913$$

In the second case $68 = 8 \times 8 + 4$ so that $2\sqrt{7} - 8 < 1$. And one more:

$$9 \times 17 = 153 = 12 \times 12 + 9 \longrightarrow 3\sqrt{17} - 12 < 1$$

I know I shouldn't generalize, but probably we can take any multiple of $\sqrt{17}$ and find a number very close to it. One more:

$$10 \times 10 \times 17 = 1700 = 41 \times 41 + 19 \longrightarrow 10\sqrt{17} - 19 < 1$$

I forgot that in this case we get very lucky $4^2 - 17 \times 1^2 = -1$

I wanted to solve $x^2 - 17y^2 = 1$ (with $+1$ instead of -1)

Can we find two numbers (p, q) which give a very small remainder and $q < 10$?

$$0 < q\sqrt{17} - p < \frac{1}{10}$$

I think our initial guess still works. I hate when I get it on the first try. Not dramatic enough.

$$\sqrt{17} - 4 = \frac{(\sqrt{17} - 4)(\sqrt{17} + 4)}{\sqrt{17} + 4} = \frac{1}{\sqrt{17} + 4} < \frac{1}{8}$$

And worse of all it looks correct because like I said:

$$4^2 - 17 \times 1^2 = 1 \textbf{ not } -1$$

Technical point: in the words of Bill Clinton we have to meditate of the meaning of the word "is" ...

I just realized our example is not good enough. I asked for $\frac{1}{10}$ and not $\frac{1}{8}$. I went and looked at a calculator:

$$8\sqrt{17} = 32.984845\ldots \longrightarrow -8\sqrt{17} + 32 < \frac{1}{10}$$

What's funny about that…even if we asked $0 \leq q \leq 10$ we found a $q = -8$ which is out of our range[2]. This is why we can use absolute value sign:

$$\left|8\sqrt{17} - 32\right| < \frac{1}{10}$$

If we were really good, we'd do all the steps without a calculator. With a slide rule or something.

Lastly how bad is the error?

$$33 \times 33 - 8 \times 8 \times 17 = 1089 - 1088 = 1$$

[2] Acceptable just not what I originally had in mind

Solving Pell Equation with Pigeonhole

Let's try to approximate $\sqrt{19}$ as a fraction. We can list multiples of this number and see which one is nearest a whole number:

$$0, \sqrt{19}, 2\sqrt{19}, 3\sqrt{19}, \dots 10\sqrt{19}$$

This is kind of like interlacing the perfect squares $\square = \{1, 4, 9, 16, \dots\}$ and $19 \times \square$:

0, $1, 4, 9, 16,$ **19**, $25, 36, 49, 64,$ **76**, $81, 100, 121, 144, 169,$ **171**, $196, 225, 256$ $289,$ **304**, $324, 361, 400, 441,$ **475**, $484, 529, 576, 625, 676,$ **684**, $729, 784, 841,$ $900,$ **931**, $961, 1024, 1089, 1156,$ **1216**, $1225, 1296, 1369, 1444, 1521,$ **1539**

Interleaving these two squences of numbers, we can see nont of them are next to a square:

$$x^2 - 19y^2 \neq 1$$

So far. How are we going to generate an answer if none of these small numbers work?

$4^2 - 19 \times 1^2 = -3$

$31^2 - 19 \times 7^2 = 30$

We have no guarantee these differences should be small, but pigeonhole-principle has found us infinitely many.

Once we see that $0 < \sqrt{19} - 4 < 1$, let's save ourselves some time by just multiplying by this number instead.

$$\sqrt{19} - 4 = \frac{(\sqrt{19} - 4)(\sqrt{19} + 4)}{\sqrt{19} + 4} = \frac{3}{\sqrt{19} + 4} > \frac{1}{3}$$

So if I multiply this number by 4 I get a new solution slightly larger than 1.

$$3(\sqrt{19} - 4) - 1 = 3\sqrt{19} - 13$$

In fact $4^2 \times 19 - 17^2 = 15$ which is rather large but still less than 19.

Also, $3^2 \times 19 - 13^2 = 2$

$$1421^2 - 19 \times 326^2 = 3$$

$$4^2 - 19 \times 1^2 = 3$$

Are these enough to solve Pell's equation?

$$\frac{1421 - 326\sqrt{19}}{4 - \sqrt{19}} \times \frac{4 + \sqrt{19}}{4 + \sqrt{19}} = \frac{\text{complicated number}}{-3}$$

For some reason 3 seems to be a common remainder for $\sqrt{19}$

- (1,4)
- (14,61)
- (326, 1421)
- (4759, 20744)

This algorithm is really slow since I am tediously[3] checking that

$$0 < \left| q\sqrt{19} - p \right| < \frac{1}{N}$$

[3] A more judicious use of Pigenhole uses **renormalization** but I think we have demonstrated that $p^2 - 19q^2 = 3$ has infinitely many solutions. Next we check for solutions which are give the same remainder upon division by 19. These will divide into each other and return a solution to the Pell equation $p^2 - 19q^2 = 1$.

Really slow algorithm for solving Pell equation in some cases. Solves $p^2 - 19q^2 = 3$ a lot.

```
sol = []

for N in 1 + np.arange(1000):

    q = 1
    while( q*np.sqrt(19) % 1 > 1.0/N):
        q += 1
    p = int(q*np.sqrt(19) // 1)

    if (q,p) not in sol:
        sol += [(q,p)]
        print q, p, q*q*19 - p*p
```

Really slow algorithm for solving Pell equation in some cases. Solves $p^2 - 19q^2 = 3$ a lot.

1	4	3
3	13	2
14	61	3
53	231	10
92	401	15
131	571	18
170	741	19
209	911	18
248	1081	15
287	1251	10
326	1421	3
1017	4433	2

Algorithm gets really slow after that…Sorry!

Faster for solving Pell equation in some cases.

```
# subtractive Euclidean algorithm

x = (0,1)
y = (1,0)

f = lambda x:  x[1] + np.sqrt(19)* x[0]

for t in range(15):
    k = 0
    while( f(y) - f(x)> 0 and k < 10 ):
        y = ( y[0] - x[0], y[1] - x[1] )
        k += 1

    print y, 19*y[0]**2 - y[1]**2
    x,y = y,x
```

Faster for solving Pell equation in some cases.

```
(       1,        -4)   3
(      -2,         9)  -5
(       3,       -13)   2
(     -11,        48)  -5
(      14,       -61)   3
(     -39,       170)  -1
(     326,     -1421)   3
(    -691,      3012)  -5
(    1017,     -4433)   2
(   -3742,     16311)  -5
(   4759,     -20744)   3
(  -13260,     57799)  -1
(  110839,   -483136)   3
(-234938,   1024071)  -5
(  345777, -1507207)   2
```

Finding units of $\mathbb{Z}[\sqrt[3]{2}]$ vis Pigeonhole

There's no continued fraction algorithm for cube roots. Some people think $\sqrt[3]{2}$ is a sequence that never repeats[4] – but nobody knows for sure.

Hale and Trotter print out the first 1000 digits (they fit neatly on a page), the paper is from the 1970's and the numbers are type-written. I don't know how they got a computer to do all of that... I can do it on my laptop with some effort.

There is a continued fraction algorithm due to Brun, which starts from the vector $(1, \sqrt[3]{2}, \sqrt[3]{4})$ and leads to approximate vectors in $\mathbb{Z}^3$ (up to a proportionate factor).

In a comuter simulation, the algorithm began repeating after 19 steps

[4] Think about that... how we we know a sequence avoids not just any pattern but all patterns. That seems like a rather odd thing.

but how do we know our Euclidean algorithm finished?

– insert discussion here –

Table I

$\sqrt[3]{2}$

	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10
0	1	3	1	5	1	1	4	1	1	8	1	14	1	10	2	1	4	12	2	3
20	2	1	3	4	1	1	2	14	3	12	1	15	3	1	4	*a	1	1	5	1
40	1	*b	1	2	2	4	10	3	2	2	41	1	1	1	3	7	2	2	9	4
60	1	3	7	6	1	1	2	2	9	3	1	1	69	4	4	5	12	1	1	5
80	15	1	4	1	1	1	1	1	89	1	22	*c	6	2	3	1	3	2	1	1
100	5	1	3	1	8	9	1	26	1	7	1	18	6	1	*d	3	13	1	1	14
120	2	2	2	1	1	4	3	2	2	1	1	9	1	6	1	38	1	2	25	1
140	4	2	44	1	22	2	12	11	1	1	49	2	6	8	2	3	2	1	3	5
160	1	1	1	3	1	2	1	2	4	1	1	3	2	1	9	4	1	4	1	2
180	1	27	1	1	5	5	1	3	2	1	2	2	3	1	4	2	2	8	4	1
200	6	1	1	1	36	9	13	9	3	6	2	5	1	1	1	2	10	21	1	1
220	1	2	1	2	6	2	1	6	19	1	1	18	1	2	1	1	1	27	1	1
240	10	3	11	38	7	1	1	1	3	1	8	1	5	1	5	4	4	4	7	2
260	1	21	1	1	5	10	3	1	72	6	9	1	3	3	2	1	4	2	1	1
280	1	1	2	1	7	8	1	2	1	8	1	8	3	1	1	3	2	1	8	1
300	1	1	1	1	6	1	4	3	4	1	1	1	4	30	39	2	1	3	8	1
320	1	2	1	3	1	9	1	4	1	2	2	1	6	2	1	1	3	1	4	1
340	2	1	1	5	1	2	10	1	5	4	1	1	4	1	2	1	1	2	12	2
360	1	8	3	2	6	1	3	10	1	2	20	1	6	1	2	*e	2	2	1	2
380	47	1	19	2	2	1	1	1	2	1	1	3	2	8	1	18	3	5	39	1
400	2	1	1	1	1	4	1	5	2	6	3	1	1	1	4	2	1	6	1	1
420	*f	1	3	1	3	1	4	5	1	2	1	13	2	2	2	1	1	1	1	7
440	2	1	7	1	3	1	1	11	1	2	2	4	2	33	3	1	1	2	6	3
460	1	1	3	6	8	3	4	84	1	1	2	1	10	2	2	20	1	3	1	7
480	13	14	1	29	1	1	5	1	7	1	1	2	1	56	1	3	2	1	13	2
500	1	2	2	2	1	1	1	1	1	1	*g	2	4	5	1	1	1	3	1	3
520	3	1	6	1	1	6	1	71	1	9	1	2	1	11	5	1	25	1	6	67
540	2	9	6	1	5	2	15	1	2	48	2	7	1	3	1	4	21	1	1	2
560	1	27	3	26	2	1	1	2	5	7	3	*h	2	29	4	3	8	17	3	8
580	2	3	1	1	1	5	*i	1	3	4	1	4	1	1	13	1	34	1	2	7
600	1	3	3	7	1	3	1	1	4	2	69	1	3	12	34	1	2	*j	1	*k
620	4	1	1	12	3	4	2	3	1	1	1	1	1	2	1	1	6	16	1	2
640	27	2	13	4	1	1	1	3	11	1	1	3	1	53	2	15	1	1	1	1
660	1	1	2	2	1	1	3	3	1	9	1	1	10	3	1	1	2	1	2	2
680	1	10	9	1	2	5	1	2	2	1	1	2	4	7	1	5	1	1	1	1
700	4	2	25	16	5	4	1	3	2	3	13	1	49	6	2	5	1	1	2	7
720	3	2	1	1	1	4	1	1	1	5	1	2	1	2	1	1	1	1	2	2
740	4	1	2	1	10	5	4	8	10	2	4	1	1	1	4	1	41	1	3	1
760	56	3	1	1	3	1	3	1	5	6	6	3	1	2	1	1	1	12	1	10
780	2	1	1	1	1	50	5	1	2	6	5	1	2	5	6	5	2	77	1	4
800	2	1	1	1	1	1	4	2	1	2	1	1	1	1	1	6	2	1	1	7
820	1	5	1	1	1	1	2	2	1	1	5	2	1	5	1	1	1	4	1	2
840	17	1	20	7	4	2	1	1	1	2	1	4	7	3	4	3	3	5	31	1
860	1	2	2	6	1	1	1	1	1	1	1	1	6	1	6	1	1	23	20	1
880	22	16	4	2	1	3	2	1	1	2	5	5	1	1	15	3	1	1	2	1
900	1	1	4	2	1	2	23	6	10	3	2	3	6	2	1	1	1	1	1	1
920	4	3	2	1	2	1	4	10	7	1	1	1	1	3	3	2	*m	1	1	11
940	2	6	1	4	1	2	2	9	3	1	1	3	22	4	1	93	1	3	1	4
960	2	1	2	3	2	1	2	11	1	1	3	1	2	1	28	23	4	11	1	9
980	1	4	3	1	6	1	2	1	12	2	6	19	1	4	4	2	1	1	1	1

a = 534 b = 121 c = 186 d = 372 e = 186 f = 220

g = 255 h = 7451 i = 113 j = 151 k = 4941 m = 108

References

(1) Math.StackExchange **What is your favorite application of the Pigeonhole Principle?** http://math.stackexchange.com/q/62565/4997

(2) Serge Lang, Hale Trottr **Continued fractions for some algebraic numbers.** https://eudml.org/doc/151239