Pell’s Equation and Ramsey Theory

Andrew D Smith
University College Dublin

5 October 2024

10:00-11:00 Modular Arithmetic, Infinite Descent and Pell's Equation.

A Problem with Remainders and Powers

(a) Find all positive integers n for which $17^n - 1$ is divisible by 10.

(b) Find all positive integers n for which $17^n + 1$ is divisible by 10.

Idea of solution: Calculate powers of 17 and look at the last digit:

n	0	1	2	3	4	5	6	7
17^n	1	17	289	4913	83521	1419857	24137569	410338673

Note that $17^n - 1$ is divisible by 10 if the last digit of 17^n is 1. This happens for $n = 0, 4$ and (we conjecture) whenever n is a multiple of 4.

Also $17^n + 1$ is divisible by 10 if the last digit of 17^n is 9. This happens for $n = 2, 6$ and (we conjecture) whenever n is twice an odd number.

How would you prove this?

International Maths Olympiad 1964 Problem 1

(a) Find all positive integers n for which $2^n - 1$ is divisible by 7;

(b) Prove that there is no positive integer n for which $2^n + 1$ is divisible by 7

Idea of solution: For $n = 0, 1, 2 \ldots$ let $2^n \pmod 7$ denote the remainder of 2^n on division by 7.

n	0	1	2	3	4	5	6	7	8	9	10
2^n	1	2	4	8	16	32	64	128	256	512	1024
$2^n \pmod 7$	1	2	4	1	2	4	1	2	4	1	2

If $2^n - 1$ is divisible by 7, then $2^n \pmod 7 = 1$. We conjecture this happens whenever n is a multiple of 3.

If $2^n + 1$ is divisible by 7, then $2^n \pmod 7 = 6$. We conjecture this never happens.

How do you prove this pattern?

Here is something you might be able to prove:

Lemma: Let $n \geq 0$ be a positive integer and a be any integer. Then $2^n + a$ is divisible by 7 if any only if $2^{n+3} + a$ is divisible by 7.

Proof: The difference is:

$$2^{n+3} + a - (2^n + a) = (2^3 - 1)2^n = 7 \times 2^n$$

which is a multiple of 7.

Can you see how to prove the conjectures by induction now?

Pell's Equation with $d = 2$

We are interested in finding positive integers a, b such that

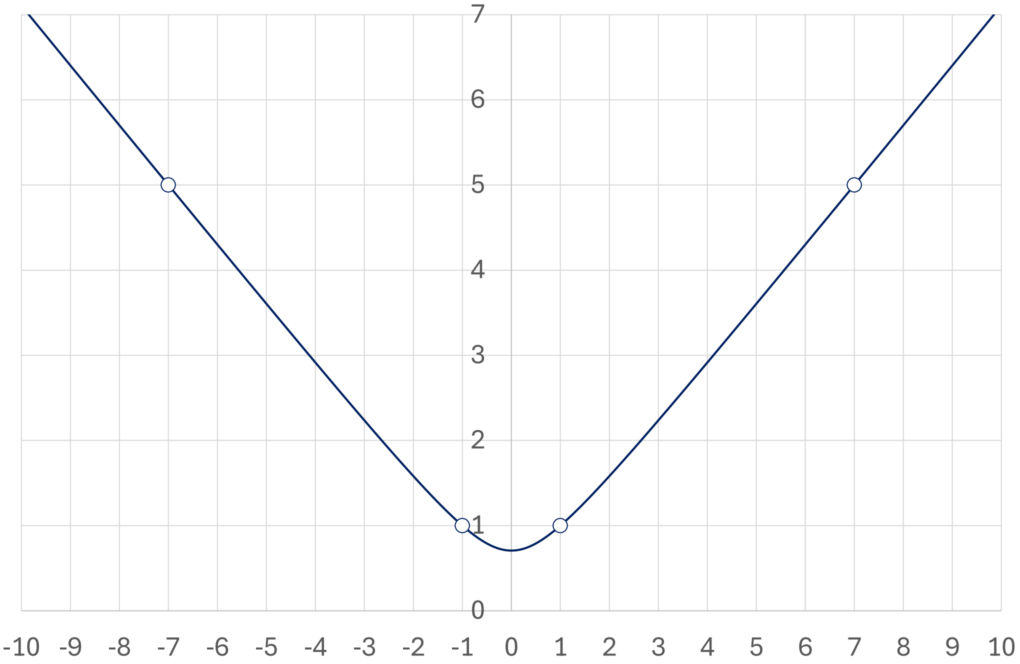
$$\frac{x}{y} \approx \sqrt{2}$$

As x and y are integers, so $x^2 - 2y^2$ is an integer. For good approximations x/y to $\sqrt{2}$ we look for solutions to:

$$x^2 - 2y^2 = r$$

where r is a small integer. If $r = 1$ this is an example of *Pell's Equation* while if $r = -1$ this is an example of *Negative Pell's Equation.*

Here is a plot of solutions to negative Pell's equation $2y^2 = x^2 + 1$, with the integer points $(\pm 1, 1)$ and $(\pm 7, 5)$ marked. To create the graph, we looked at x in the range $-10 \leq x \leq 10$ and plotted y at small intervals of x, using the formula $y = \sqrt{\frac{1}{2}(1 + x^2)}$. There is another branch (not shown) where y is negative.



Pell's equation is famously amenable to the *method of ascent*, where we can make bigger solutions out of smaller ones.

Specifically, suppose

$$x^2 - 2y^2 = r$$

Define $x' = 3x + 4y$ and $y' = 2x + 3y$. Then

$$\begin{aligned}(x')^2 - 2(y')^2 &= (3x + 4y)^2 - 2(2x + 3y)^2 \\ &= 9x^2 + 24xy + 16y^2 - (8x^2 + 24xy + 18y^2) \\ &= x^2 - 2y^2\end{aligned}$$

This is a special case of *Brahmagupta's Identity*.

We can start with some solutions to Pell's equations, such as $1^2 - 2 \times 0^2 = 1$ and $1^2 - 2 \times 1^2 = -1$ for $r = 1$ and $r = -1$ respectively, and then apply the transformation $(x, y) \mapsto (x', y')$ repeatedly, to generate more solutions.

x	y	$x^2 - 2y^2$	x	y	$x^2 - 2y^2$
1	0	1	1	1	-1
3	2	1	7	5	-1
17	12	1	41	29	-1
99	70	1	239	169	-1
577	408	1	393	985	-1
3363	2378	1	8119	5741	-1
19601	13860	1	47321	33461	-1
114243	80782	1	275807	195025	-1

We can instead look at this in terms of rational approximations to $\sqrt{2}$. If

$$t = \frac{x}{y}$$

is an approximation, then

$$t' = \frac{x'}{y'} = \frac{3x + 4y}{2x + 3y} = \frac{3t + 4}{2t + 3}$$

is a better one. If we keep iterating, and reach a limit, then that limit must satisfy:

$$0 = (2t + 3)t - (3t + 4) = 2(t^2 - 2)$$

Question: Do all solutions to Pells Equation / Negative Pell's Equation arise from the basic solutions $(1, 0)$ and $(1, 1)$ by applying the ascent formula?

To see why the answer is *yes*, try reversing the ascent formula, to get a *descent* formula:

$$x' = 3x + 4y; \quad y' = 2x + 3y$$
$$x = 3x' - 4y'; \quad y = -2x' + 3y'$$

That reduces any integer solution to another integer solution on the same hyperbola. Eventually that reduces x to a range where we can check manually there are no further solutions.

In particular with $r = 0$ we can see that there are no solutions to $x^2 - 2y^2$ which is (another) proof that $\sqrt{2}$ is irrational.

Pell's Equation with $d = 3$

Are there solutions to $x^2 - 3y^2 = r$ for $r = 0$ or $r = \pm 1$?

We now have a different ascent / descent formula:

$$x' = 2x + 3y; \quad y' = x + 2y$$
$$x = 2x' - 3y'; \quad y = -x' + 2y'$$

As before, we have $x^2 - 3y^2 = (x')^2 - 3(y')^2$.

Exercise Use ascent / descent to show there are infinitely many integer solutions to $x^2 - 3y^2 = r$ when $r = 1$, but none when $r = 0$ or $r = -1$.

Can you think of another way to prove there are no integer solutions to $x^2 - 3y^2 = -1$, using remainders modulo 3?

Question: Where did the ascent / descent formulas come from? The maps from (x, y) to (x', y') and back again?

The origin in lost in the mists of time. Probably someone two thousand years ago tabulated the first six or seven solutions to Pell's equation by hand, and then spotted the ascent relationship between one solution and the next. Once you've guessed the formulas, then it's easy to show they work.

Tabulating those six solutions seems like a lot of work, and it would have been, especially without a calculator. But there are some short cuts, for example noticing that in solutions of $x^2 - 2y^2 = \pm 1$, the value of x must be odd, immediately cuts out half the cases. There are many more tricks like that.

Spotting the ascent / descent patterns becomes easier if you know you are looking for a linear transformation. If you've seen other problems with integer (or rational) points on quadratic curves, you might guess the form and then find the coefficients - the 2's, 3's and 4's, by trial and error.

If you already know of Brahmagupta's identity, that gives a big clue to find the ascent / descent formula. Brahmagupta's identity was known to Diophantus in the 3rd century AD. Bhaskara II used this method to solve Pell's equation around 1150. (John Pell lived in the 17th century and the attachment of his name to the equation was a mistake).

Algebraic number theorists think of forms such as $x^2 - 2y^2$ as a *norm* on the algebraic integers quadratic number field. The solution to Pell's equation are related to the group of units in that field. But that goes way beyond what we need now.

11:30-12:30 Ramsey Theory

A Problem about Creating New Integers

Two different integers u and v are written on a board. We perform a sequence of steps. At each step we do one of the following two operations:

(i) If a and b are different integers on the board, then we can write $a + b$ on the board, if it is not already there.

(ii) If a, b and c are three different integers on the board, and if an integer x satisfies $ax^2 + bx + c = 0$, then we can write x on the board, if it is not already there.

Two questions:

(a) Starting with $u = 6$ and $v = 8$, show that any integer can eventually be written on the board after a finite number of steps.

(b) (EGMO 2024 Problem 1) Determine all pairs of starting numbers (u, v) from which any integer can eventually be written on the board after a finite sequence of steps.

Solution to First Question

First step: Show we can write any even number of 26 or more. To get there, write:

$$\begin{aligned}
14 &= 6+8\\
20 &= 6+14\\
22 &= 8+14\\
26 &= 6+20\\
28 &= 6+22 = 8+20\\
30 &= 8+22
\end{aligned}$$

Then for any even $n \geq 32$ use $6 + (n-6)$.

Second Step: Show we can write any integer $x \leq -3$.

We will try to find a, b, and c already written down with:

$$0 = ax^2 + bx + c = a|x|^2 - b|x| + c$$

We only need to find one combination to make this work, so suppose c is the balancing item. Then we need $c = b|x| - a|x|^2$ to be a large even number so we know it is already written down (and c will also be a multiple of $|x|$).

Let us try taking a as small as we can, say $a = 6$. So now we are looking for b with $b|x| - a|x|^2 \geq 26$ and also $b \geq 26$, which is equivalent to:

$$b \geq \max\left\{26, \frac{26}{|x|} + 6|x|\right\}$$

Let us also make sure b is not a multiple of $|x|$. This is where we need $x \leq -3$.

Now $a = 6$ is on the board. Also b, c are on the board from the first step, as they are even and at least 26. Furthermore, $b \neq c$ as c is a multiple of $|x|$ and b is not. Then by choice of c:

$$ax^2 + bx + c = 6|x|^2 - b|x| + (b|x| - 6|x|^2) = 0$$

Therefore, we can write x on the board.

Third step: We have now written all even numbers 26 or higher, and all negative numbers up to -3 on the board.

We now show how to write any remaining integer c on the board. Choose an even number a such that

$$a \geq \max\{26, c + 3\}$$

So a is already on the board (large and even, step 1) while $c - a$ is also on the board (less than -3, second step). Finally then we can write $c = a + (c - a)$.

The conclusion is that all integers can be written on the board after finitely many steps.

Solution to Second Question See `https://www.egmo.org/egmos/egmo13/solutions.pdf`.

Number Painting Problem (Schur's Theorem)

Alice takes a list of the positive numbers from 1 to 2024 inclusive. She paints every number either red or blue.

Prove that there are positive integers x and y, not necessarily distinct, such that x, y and $x + y$ are all painted the same colour.

Solution Say a set of positive integers is *sum-free* if it contains no x, y, z with $z = x + y$, with x, y not necessarily distinct. Suppose (for a contradiction) that we can find two disjoint sum-free sets, red and blue, whose union contains $\{1, 2, 3, 4, 5\}$.

Suppose without loss of generality that 1 is red. Then (as $1 + 1 = 2$), 2 must be blue, and for the same reason 4 must be red. Now neither 3 nor 5 can be red, as $1 + 3 = 4$ and $1 + 4 = 5$. So both 3 and 5 must be below.

We have a contradiction because 2, 3 and 5 are all blue, but $2 + 3 = 5$.

Further Question: Does the result still hold if Alice has three colours instead of two? How about four, five or six? What is the smallest number n of colours such that the subsets of $\{1, 2, \ldots 2024\}$ can be partitioned into n sum-free subsets?

IMO 1964 Problem 4

Seventeen people correspond by mail with one another, each one with all the rest. In their letters only three different topics are discussed. Each pair of correspondents deals with only one of these topics. Prove that there are at least three people who write to each other about the same topic.

Generalised Problem

Let $n \geq 1$ be an integer. Suppose that $3 \times n!$ people correspond with one another, each one with all the rest. In their letters, only n different topics are discussed. Prove that there are at least three people who write to each other about the same topic.

Proof: By induction on n.

If $n = 1$, then we have three people and one topic. All three people therefore write to each other about the same topic.

Now suppose that $n \geq 2$. Pick one individual, Anna. Then Anna writes to $3 \times n! - 1$ people. There must be one topic on which Anna writes to at least $3 \times (n-1)!$ people. That follows because otherwise Anna writes on n topics to at most $3 \times (n-1)! - 1$ people per topic, which can account for only $3 \times n! - n$ people, a contradiction as this is less than $3 \times n! - 1$.

Now choose a topic on which Anna writes to at least $3 \times (n-1)!$ correspondents. Call this topic X.

If two of those correspondents also write to each other on topic X, then we have three people corresponding on a common topic, that is Anna and the other two correspondents, all on topic X.

If none of these $3 \times (n-1)!$ correspondents write to each other on topic X, then those $3 \times (n-1)!$ correspondents use only $n-1$ topics between them, out of which, inductively there are three writing on a common topic.

This is a special case of *Ramsey's Theorem.*

Application to Schur's Theorem

Suppose that Alice paints the numbers from 1 to $3 \times n!$ each in one of n colours. Then Schur's theorem states that there are x, y, z, (with x and y not necessarily distinct) such that $z = x + y$ and x, y, z are the same colour.

Proof: Think instead of $3 \times n!$ correspondents with n topics. The topic on which two correspondents, a and b, write is determined by how Alice coloured $|a - b|$.

Now there are three correspondents, let's say a, b, c who correspond with each other on a common topic, by Ramsey's theorem. Label these so that $a < b < c$.

Then Alice must have coloured $b - a$, $c - b$ and $c - a$ the same colour. But as $c - a = (b - a) + (c - b)$ we now have two numbers and their sum, all of which Alice has painted the same colour.

Remark: We have proved a theorem that gives an upper bound on the so-called Schur numbers. There are smaller lists of integers than from 1 to $3 \times k!$ which cannot be painted into n sum-free subsets.

Here are some *best possible* results (the later ones obtained with a great deal of computing effort).

- The numbers $\{1, 2, 3, 4\}$ can be partitioned into two sum-free subsets, but the numbers $\{1, 2, 3, 4, 5\}$ cannot, as we have already seen.

- The numbers $\{1, 2, \ldots 13\}$ can be partitioned into three sum-free subsets, but the numbers $\{1, 2, \ldots 14\}$ cannot.

- The numbers $\{1, 2, \ldots 44\}$ can be partitioned into four sum-free subsets, but the numbers $\{1, 2, \ldots 45\}$ cannot.

- The numbers $\{1, 2, \ldots 160\}$ can be partitioned into five sum-free subsets, but the numbers $\{1, 2, \ldots 161\}$ cannot.
  See `https://arxiv.org/abs/1711.08076`.

We have already shown that the set $\{1, 2, \ldots 2160\}$ cannot be partitioned into six sum-free subsets. With a little work, our argument can be refined to show that $\{1, 2, \ldots 1958\}$ cannot be so partitioned, which implies $\{1, 2, \ldots 2024\}$ also cannot be partitioned into six sum-free subsets. But that is still not the best possible result.

Science does not currently know the smallest set $\{1, 2, \ldots S(6)\}$ that cannot be partitioned into six sum-free subsets.