Lecture 6: Lamé's theorem

Being an algorithm, we are entitled to ask what the complexity of Euclid's algorithm is, thus applying modern ideas to those of antiquity. What is surprising is that to do this we shall apply some ideas from the thirteenth century — the Fibonacci numbers. This application is the first mathematical application of these numbers.

The Fibonacci numbers

In his book, *Liber Abaci*, Fibonacci posed the following puzzle:

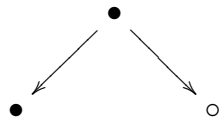
> A certain man put a pair of rabbits in a place surrounded on all sides by a wall. How many pairs of rabbits can be produced from that pair in a year if it is supposed that every month each pair begets a new pair which from the second month on becomes productive?

These are obviously mathematical rabbits rather than real ones so let me spell out the rules more explicitly:

Rule 1: The problem begins with one pair of immature rabbits.[1]
Rule 2: Each immature pair of rabbits takes one month to mature.
Rule 3: Each mature pair of rabbits produces a new immature pair at the end of a month.
Rule 4: The rabbits are immortal.

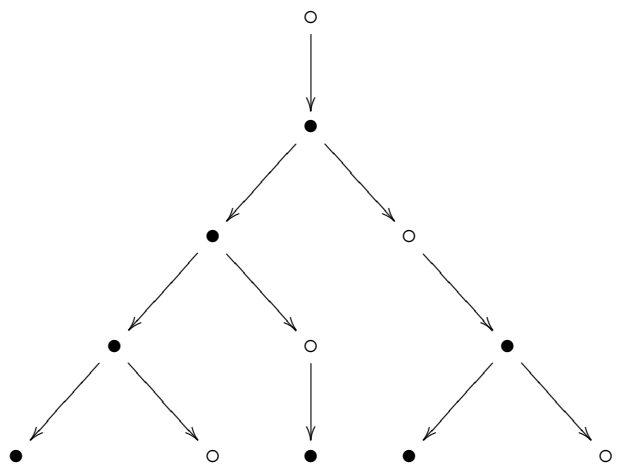
The important point is that we must solve the problem using the rules we have been given. To do this, I am going to draw a picture. I will represent an immature pair of rabbits by ∘ and a mature pair by •. Rule 2 will be represented by

and Rule 3 will be represented by



Rule 1 tells us that we start with ∘. Applying the rules we obtain the following picture for the first 4 months.

[1]Fibonacci himself seems to have assumed that the starting pair was already mature but we shan't.



We start with 1 pair and at the end of the first month we still have 1 pair, at the end of the second month 2 pairs, at the end of the third month 3 pairs, and at the end of the fourth month 5 pairs. I shall write this $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, and so on.

There is an apparent pattern in the sequence of numbers $1, 1, 2, 3, 5, \ldots$ after the first two terms in the sequence each number is the sum of the previous two. Let's check that we are not just seeing things. Suppose that the number of immature pairs of rabbits at a given time t is I_t and the number of mature pairs is M_t. Then using our rules at time $t + 1$ we have that $M_{t+1} = M_t + I_t$ and $I_{t+1} = M_t$. Thus

$$F_{t+1} = 2M_t + I_t.$$

Similarly

$$F_{t+2} = 3M_t + 2I_t.$$

It is now easy to check that

$$F_{t+2} = F_{t+1} + F_t.$$

The sequence of numbers such that $F_1 = 1$, $F_2 = 1$ and satisfying the rule $F_{t+2} = F_{t+1} + F_t$ is called the *Fibonacci sequence*. We have that

$$F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, F_7 = 13, F_8 = 21,$$

$$F_9 = 34, F_{10} = 55, F_{11} = 89, F_{12} = 144, F_{13} = 233.$$

Fibonacci numbers arise in the most diverse situations: famously, in *phyllotaxis*[2] which is the study of how leaves and petals are arranged on plants.

Finding a formula: empirical results

We shall now look for a formula that will enable us to calculate F_n directly. To begin, we'll follow an idea due to the astronomer Jonannes Kepler, and look at the behaviour of the fractions $\frac{F_{n+1}}{F_n}$ as n gets bigger and bigger. I have tabulated some calculations below.

$\frac{F_2}{F_1}$	$\frac{F_3}{F_2}$	$\frac{F_4}{F_3}$	$\frac{F_5}{F_4}$	$\frac{F_6}{F_5}$	$\frac{F_7}{F_6}$	$\frac{F_8}{F_7}$	$\frac{F_{15}}{F_{14}}$
1	2	$1 \cdot 5$	$1 \cdot 6$	$1 \cdot 625$	$1 \cdot 615$	$1 \cdot 619$	$1 \cdot 6180$

These ratios seem to be going somewhere; the question is: where? Notice that

$$\frac{F_{n+1}}{F_n} = \frac{F_n + F_{n-1}}{F_n} = 1 + \frac{F_{n-1}}{F_n} = 1 + \frac{1}{\frac{F_n}{F_{n-1}}}.$$

But for very large n we suspect that $\frac{F_{n+1}}{F_n}$ and $\frac{F_n}{F_{n-1}}$ will be almost the same. We therefore need to find the positive solution x to

$$x = 1 + \frac{1}{x}.$$

Thus x is a number that when you take its reciprocal[3] and add 1 you get x back again. This problem is really a quadratic equation in disguise

$$x^2 = x + 1 \text{ or more usually } x^2 - x - 1 = 0.$$

I never remember formulae but I do remember methods. The method I'll use to solve this quadratic equation is called *completing the square*. Look first at $x^2 - x$; that is, we ignore for the moment the constant term. This is equal to $(x - \frac{1}{2})^2 - \frac{1}{4}$. Substituting this into our original equation we get

$$(x - \frac{1}{2})^2 - \frac{1}{4} = 1.$$

This equation can now be solved very simply to give us

$$x = \frac{1 \pm \sqrt{5}}{2}.$$

That is

$$\phi = \frac{1 + \sqrt{5}}{2} \text{ and } \bar{\phi} = \frac{1 - \sqrt{5}}{2}.$$

[2]This is made of two Greek words: *phyllo* meaning leaf and *taxis* meaning arrangement.

[3]The *reciprocal of a number* x *is* $\frac{1}{x}$.

The number ϕ is called *the golden ratio*, about which more nonsense has been written than any other number. Observe that

$$\phi^2 = \phi + 1 \text{ and } \bar{\phi}^2 = \bar{\phi} + 1$$

and that

$$\phi + \bar{\phi} = 1 \text{ and } \phi\bar{\phi} = -1.$$

Let's go back and see if this calculation makes sense. First we calculate ϕ and we get

$$\phi = 1 \cdot 618033988\ldots$$

I compute

$$\frac{F_{20}}{F_{19}} = \frac{6765}{4181} = 1 \cdot 618033963$$

on my pocket calculator. This is pretty close.

Binet's formula

$$\boxed{F_n = \tfrac{1}{\sqrt{5}}\left(\phi^n - \bar{\phi}^n\right).}$$

There are a number of different proofs of this formula. In the exercises, I shall let you prove it by induction. Here I shall give a direct proof using what are called *generating functions*, a very important technique in number theory. It's convenient to define $F_0 = 0$.

Put

$$F(z) = \sum_{i=0}^{\infty} F_i z^i.$$

Then observe that

$$F(z) = z + zF(z) + z^2F(z).$$

It follows that

$$F(z) = \frac{z}{1 - z - z^2}.$$

Thus

$$F(z) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\phi z} - \frac{1}{1-\bar{\phi}z}\right).$$

We deduce that

$$F(z) = \sum_{i=0}^{\infty} \frac{1}{\sqrt{5}}(\phi^i - \bar{\phi}^i)z^i,$$

and the proof of Binet's formula follows by comparsion with the original series.

The Fibonacci numbers and Euclid's algorithm

The Fibonacci numbers and Euclid's algorithm do not on the face of it look as if they have anything to do with each other. In fact, there is a deep connection between them that we shall now uncover.

If $a = b$ then $\gcd(a, b) = a = b$. Also if $a = 0$ then $\gcd(0, b) = b$. Thus we may always assume that one number is strictly larger than the other and that neither is zero. Thus $a > b > 0$.

For notation, we put $r_0 = a$ and $r_1 = b$. We shall suppose that Euclid's algorithm terminates after *exactly* n *divisions* have been carried out. Thus we are taking as our *step* one application of the Remainder theorem.

We therefore accumulate the following calculations:

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\dots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \\ r_{n-1} &= r_n q_n + 0 \end{aligned}$$

where $0 < r_2 < r_1$, $0 < r_3 < r_2$, $\dots$, $0 < r_n < r_{n-1}$ and $r_{n+1} = 0$.

- The smallest value that the last non-zero remainder r_n can attain is 1. Now $F_2 = 1$ and so $r_n \geq F_2$.
- Now $r_{n-1} = r_n q_n$. Since $r_n < r_{n-1}$ it follows that q_n cannot be equal to 1. Thus $q_n \geq 2$. It follows that $r_{n-1} \geq 2r_n \geq 2 = F_3$.
- These two arguments get us started. Now look at

  $$r_{n-2} = r_{n-1} q_{n-1} + r_n.$$

  Since $q_{n-1} \geq 1$ we have that

  $$r_{n-2} \geq r_{n-1} + r_n \geq F_3 + F_2 = F_4.$$

- This argument can clearly be repeated going up our list of calculations. We deduce that $b = r_1 \geq F_{n+1}$.

Thus if n divisions are needed in the application of Euclid's algorithm the smaller of the two numbers whose gcd is being sought cannot be smaller than the $(n + 1)$th Fibonacci number.

Our goal is to estimate the value of n in terms of the number b.

- We have a formula for the nth Fibonacci number but it is a bit complicated. An induction argument shows that

  $$F_n > \phi^{n-2}$$

  for $n \geq 3$. See the Exercises for this.
- Thus $b \geq F_{n+1}$ implies that $b > \phi^{n-1}$.

- Take $\log_{10}$'s of both sides to get
$$\log_{10}(b) > (n-1)\log_{10}(\phi).$$
- $\log_{10}(\phi) > \frac{1}{5}$.
- Thus $\log_{10}(b) > \frac{1}{5}(n-1)$.
- If k is the number of digits in the base 10 representation of the number b, we have already shown that $k = \lfloor \log_{10}(b) \rfloor + 1$. Thus $k > \log_{10}(b)$.
- It follows that $k > \frac{1}{5}(n-1)$.
- Thus $5k \geq n$.

We have therefore proved the following.

Theorem 0.1 (Lamé)**.** *The number of divisions needed in the application of Euclid's algorithm is less than or equal to five times the number of digits in the smaller of the two numbers whose gcd is being sought.*

The point is that not only is the gcd theoretically important but it can be calculated in polynomial time.