The Extended Euclidean Algorithm
March 2017

1 Making change

Theorem 1. *Let d be the greatest common divisor of the positive integers a and b. Then there are integers x and y such that*

$$ax + by = d. \tag{1}$$

Proof. Coming soon □

The is Bezout's Theorem. In everyday language it says that in a country with just two kinds of bills, worth \$$a$ and \$$b$ you can only hope to make change for amounts that are a multiple of \$$d$. Bezout's Theorem says you can in fact do \$$d$. Then it's easy to see how to do any multiple of \$$d$. smallest amount.

2 The extended Euclidean algorithm

Bezout's Theorem says that two integers exist. Here's an algorithm that finds them explicitly. We'll discuss it by working through an example for $a = 100$ and $b = 73$ to discover that the greatest common divisor is 1 and that

$$(100)(-27) + (73)(37) = 1\ .$$

Here is the computation, in a table.

step	R	r	x	y	q
0			1	0	
1	100	73	0	1	
2	73	27	1	-1	1
3	27	19	-2	3	2
4	19	8	3	-4	1
5	8	3	-8	11	2
6	3	2	19	-26	2
7	2	1	-27	37	1
8	1	0			

Here's how it's done.

- Fill rows 0 and 1 as in the example.
- To fill the next row:
  - Copy r to R (in the next row)
  - Do some long division, Divide R by r and find the quotient q and remainder r:

    $$R = r \times q + \text{ remainder.}$$

  - Put the quotient in column q.
  - Put the remainder in column r.
  - Let

    $$x = x \uparrow\uparrow -q \times x \uparrow$$

    where the $\uparrow$ means take the value from the previous row.
  - Let

    $$y = y \uparrow\uparrow -q \times y \uparrow$$

- When $r = 0$ you're done.

Note that in every row

$$ax + by = r.$$

so r in the row right before it's 0 is the greatest common divisor d of a and b.

3 Fibonacci

Experiment with Bezout's Theorem for consecutive Fibonacci numbers. What about Fibonacci numbers two apart?

4 A geometric research problem