Extended Euclidean algorithm

We're interested in the Euclidean algorithm *gcd* to find the greatest common divisor of two integers a and b (with $a > b$).

The method is to repeat these steps:

(i) find $r = a \bmod b$; (ii) terminate if $r = 0$, returning b; (iii) set $a = b$ and $b = r$. So for example

```
60 = 4(13) + 8
13 = 1(8)  + 5
 8 = 1(5)  + 3
 5 = 1(3)  + 2
 3 = 1(2)  + 1
 2 = 2(1)  + 0
```

The numbers on each line are

```
a = q(b) + r
```

where q is the quotient (floor of a/b). Skipping the last line, each line can be rearranged as $r = a - q(b)$

```
8 = 60 - 4(13)
5 = 13 - 1(8)
3 = 8 - 1(5)
2 = 5 - 1(3)
1 = 3 - 1(2)
```

We can substitute for 2 in the last line of the second part:

$$1 = 3 - 1(2)$$

$$= 3 - 1\ [\ (5 - 1(3)\ ]$$

$$= 2(3) - 1(5)$$

We can continue in this way, substituting $3 = 8 - 1(5)$

$$= 2\ [\ 8 - 1(5)\ ]\ - 1(5)$$

$$= 2(8) - 3(5)$$

and $5 = 13 - 1(8)$

$$= 2(8) - 3\ [\ 13 - 1(8)\ ]$$

$$= 5(8) - 3(13)$$

and finally $8 = 60 - 4(13)$

$$= 5\ [\ 60 - 4(13)\ ]\ - 3(13)$$

$$= 5(60) - 23(13)$$

Remember the 1

$$1 = 5(60) - 23(13)$$

The implication of this last line is that if we're doing arithmetic mod 60, then

$$5(60) \bmod 60 = 0$$

so

$$-23(13) \bmod 60 = 1$$

and since $-23 = 37 \bmod 60$ we have finally

$$37(13) \bmod 60 = 1$$

37 is the multiplicative inverse of 13 mod 60.

general case

We imagine that we have a list like the one above from a run of the *gcd* algorithm, where we have already thrown away the last line.

```
8 = 60 - 4(13)
5 = 13 - 1(8)
3 = 8  - 1(5)
2 = 5  - 1(3)
1 = 3  - 1(2)
```

We number in reverse:

$$r_5 = a_5 - q_5 b_5$$

$$\ldots$$

$$r_1 = a_1 - q_1 b_1$$

For the case we're interested in, $r_1 = 1$ always, so let's just ignore the left-hand side for now. We have the recurrence relationships. Traversing the list from top down

$$a_n = b_{n+1}, \quad a_1 = b_2$$

$$b_n = r_{n+1}, \quad b_1 = r_2$$

The q_n notation gets a bit awkward. I would like to suppress it to just use the digit, writing n in place of q_n at the appropriate times.

However, we also have a real integer 1, which I will write as o.

Round 1: Start from

$$a_1 - q_1 b_1$$

Round 2: use the recurrence relation

$$b_2 - q_1 r_2$$

Substitute for r_2

$$b_2 - q_1 \; [\; a_2 - q_2 b_2 \;]$$

Gather terms:

$$-q_1 a_2 + (1 + q_1 q_2) b_2$$

Suppress q and write o for integer 1:

$$-1 a_2 + (o + 12) b_2$$

Round 3: use the recurrence relation

$$-1 b_3 + (o + 12) r_3$$

Substitute for r_3

$$-1 b_3 + (o + 12) \; [\; a_3 - q_3 b_3 \;]$$

Gather terms and suppress

$$(o + 12) a_3 - (1 + 3 + 123) b_3$$

Round 4: use the recurrence relation

$$(o + 12) b_4 - (1 + 3 + 123) r_4$$

Substitute for r_4

$$(o + 12) b_4 - (1 + 3 + 123)(a_4 - q_4 b_4)$$

Gather terms and suppress

$$-(1 + 3 + 123) a_4 + (o + 12 + 14 + 34 + 1234) b_4$$

Round 5: use the recurrence relation

$$-(1 + 3 + 123) b_5 + (o + 12 + 14 + 34 + 1234) r_5$$

Substitute for r_5

$$-(1+3+123)b_5 + (o+12+14+34+1234)(a_5 - q_5 b_5)$$

Gather terms

$$(o+12+14+34+1234)a_5 - \ldots$$

$$[1+3+123+5+125+145+345+12345)\ ]\ b_5$$

I cannot find a pattern for this. However, in the case of $(60, 13)$, we should be done. Recalling

```
60 = 4(13) + 8
13 = 1(8) + 5
 8 = 1(5) + 3
 5 = 1(3) + 2
 3 = 1(2) + 1
 2 = 2(1) + 0
```

Since a_5 is equal to 60 we need only the coefficient of b_5 i.e 13. But all of q_1 q_4 are 1, while $q_5 = 4$, and the encoded coefficient is

$$1+3+123+5+125+145+345+12345$$

Substituting

$$1+1+1+4+4+4+4+4 = 23$$

And we must remember the leading minus sign, so we add $60-23 = 37$, which is correct.

consolidation

Here is the list, for reference:

```
8 = 60 - 4(13)
5 = 13 - 1(8)
3 = 8  - 1(5)
2 = 5  - 1(3)
1 = 3  - 1(2)
```

As another approach, consider that we have only two coefficients at each step, one for a and one for b. Why not just compute them and save those values as we go up the chain.

Round 1: Start from

$$a_1 - q_1(b_1)$$

and then $q_1 = 1$

$$a_1 - 1(b_1)$$

Round 2: use the recurrence relation

$$b_2 - (1)(r_2)$$

$$b_2 - (1)(a_2 - q_2 b_2)$$

$$(-1)a_2 + (1 + q_2)b_2$$

and then $q_2 = 1$

$$(-1)a_2 + (2)b_2$$

Round 3: use the recurrence relation

$$(-1)b_3 + (2)r_3$$

$$(-1)b_3 + (2)(a_3 - q_3 b_3)$$

$$(2)a_3 - (1 + 2q_3)b_3$$

and then $q_3 = 1$

$$(2)a_3 - (3)b_3$$

Round 4: use the recurrence relation

$$(2)b_4 - (3)r_4$$

$$(2)b_4 - (3)(a_4 - q_4 b_4)$$

$$-(3)a_4 + (2 + 3q_4)b_4$$

and then $q_4 = 1$

$$-(3)a_4 + (5)b_4$$

Round 5: use the recurrence relation

$$-(3)b_4 + (5)r_5$$

$$-(3)b_4 + (5)(a_5 - q_5 b_5)$$

$$(5)a_5 - (3 + 5q_5)b_5$$

and then $q_5 = 4$

$$(5)a_5 - (23)b_5$$

We're almost done. The coefficient of b is $-23 = 37 \bmod 60$.

We need to find a way to program this, given a list of the values of q.