1-21-2019

The Extended Euclidean Algorithm

The **Extended Euclidean Algorithm** finds a linear combination of m and n equal to (m, n). I'll begin by reviewing the **Euclidean algorithm**, on which the extended algorithm is based.

The Euclidean algorithm is an efficient way of computing the greatest common divisor of two numbers. It also provides a way of finding numbers a, b, such that

$$(x, y) = ax + by.$$

The Euclidean Algorithm. Take $m, n > 0$. Define

$$r_0 = m, \quad r_1 = n.$$

Then recursively define r_k using the Division Algorithm:

$$r_{k-2} = qr_{k-1} + r_k, \quad \text{where} \quad 0 \le r_k < r_{k-1}.$$

The inequality $0 \le r_k < r_{k-1}$ shows that the r_k's form a decreasing sequence of nonnegative integers. It follows that the algorithm must terminate.

For instance, to cmpute $(1914, 899)$:

$$\begin{aligned} 1914 &= 2 \cdot 899 + 116 \\ 899 &= 7 \cdot 116 + 87 \\ 116 &= 1 \cdot 87 + 29 \\ 87 &= 3 \cdot 29 + 0 \end{aligned}$$

We usually write this in tabular form:

1914	-
899	2
116	7
87	1
29	3

The greatest common divisor is the last nonzero remainder: $(1914, 899) = 29$.

According to an earlier result, the greatest common divisor 29 must be a linear combination $a \cdot 1914 + b \cdot 899$. Here's a tedious way to find integers a and b which work. Simply work backwards through the equations above, *treating the r_k's as if they were variables.*

$$29 = 116 + (-1) \cdot 87 \quad \text{and} \quad 87 = 899 + (-7) \cdot 116.$$

Substituting for 87 in the first equation,

$$29 = 116 + (-1) \cdot [899 + (-7) \cdot 116] = (-1) \cdot 899 + 8 \cdot 116.$$

But

$$116 = 1914 + (-2) \cdot 899.$$

Substituting for 116, I find that

$$29 = (-1) \cdot 899 + 8 \cdot [1914 + (-2) \cdot 899] = 8 \cdot 1914 + (-17) \cdot 899.$$

I've written the greatest common divisor 29 as a linear combination of the original numbers 1914 and 899.

While you can use this back-substitution approach to write the greatest common divisor as a linear combination of the original numbers, it's rather tedious. Here's a better way. I'll write it more formally, since the steps are a little complicated.

I proved the next result earlier, but the proof below will actually give an algorithm which constructs a linear combination. It is called a *backward recurrence*, and is due to S. P. Glasby [1]. It will look a little complicated, but you'll see that it's really easy to use in practice.

Theorem. (**Extended Euclidean Algorithm**) (a, b) is a linear combination of a and b: For some integers s and t,

$$(a, b) = sa + tb.$$

Warning: s and t are not unique.

Proof. (a, b) is only defined if at least one of a, b is nonzero. If $a \neq 0$, $(a, 0) = a$ and $a = 1 \cdot a + 0 \cdot 0$. This proves the result if one of the numbers is 0, so I may as well assume both are nonzero. Moreover, since $(a, b) = (|a|, |b|)$, I can assume both numbers are positive.

Suppose $a \geq b$. Apply the Euclidean Algorithm to $a_0 = a$ and $a_1 = b$, and suppose that a_n is the last *nonzero* remainder:

$$\begin{aligned}
a_0 &= a_1 q_1 + a_2, \quad \text{where} \quad 0 \leq a_2 < a_1 \\
a_1 &= a_2 q_2 + a_3, \quad \text{where} \quad 0 \leq a_3 < a_2 \\
&\vdots \\
a_k &= a_{k+1} q_{k+1} + a_{k+2}, \quad \text{where} \quad 0 \leq a_{k+2} < a_{k+1} \\
&\vdots \\
a_{n-1} &= a_n q_n + 0.
\end{aligned}$$

I'm going to define a sequence of numbers y_n, y_{n-1}, $\ldots y_1$, y_0. They will be constructed recursively, starting with y_n, y_{n-1} and working downward to y_0. (This is why this is called a *backward recurrence*.)

Define $y_n = 0$ and $y_{n-1} = 1$. Then define

$$y_{k-1} = q_k y_k + y_{k+1} \quad \text{for} \quad k = n-2, \ldots, 2, 1.$$

Now I claim that

$$(-1)^{n+k+1} a_{k-1} y_k + (-1)^{n+k} a_k y_{k-1} = a_n \quad \text{for} \quad 1 \leq k \leq n.$$

I will prove this by *downward* induction, starting with $k = n$ and working downward to $k = 1$.

For $k = n$, I have

$$(-1)^{2n+1} a_{n-1} y_n + (-1)^{2n} a_n y_{n-1} = -a_{n-1} y_n + a_n y_{n-1} = -a_{n-1} \cdot 0 + a_n \cdot 1 = a_n.$$

The result holds for $k = n$.

Next, suppose $1 < k < n$. Suppose the result holds for $k + 1$, i.e.

$$(-1)^{n+k+2} a_k y_{k+1} + (-1)^{n+k+1} a_{k+1} y_k = a_n.$$

I want to prove the result for k. Substitute $y_{k+1} = y_{k-1} - q_k y_k$ in the preceding equation and simplify:

$$a_n = (-1)^{n+k+2} a_k y_{k+1} + (-1)^{n+k+1} a_{k+1} y_k = (-1)^{n+k+2} a_k (y_{k-1} - q_k y_k) + (-1)^{n+k+1} a_{k+1} y_k =$$

$$(-1)^{n+k}a_k(y_{k-1}-q_ky_k)+(-1)^{n+k+1}a_{k+1}y_k=(-1)^{n+k}a_ky_{k-1}+(-1)^{n+k+1}a_kq_ky_k+(-1)^{n+k+1}a_{k+1}y_k=$$

$$(-1)^{n+k}a_ky_{k-1}+(a_kq_k+a_{k+1})(-1)^{n+k+1}y_k=(-1)^{n+k}a_ky_{k-1}+(-1)^{n+k+1}a_{k-1}y_k.$$

This proves the result for k, so the result holds for $1 \le k \le n$, by downward induction.

In particular, for $k = 1$, the result says

$$a_n=(-1)^{n+1}a_1y_0+(-1)^{n+2}a_0y_1=(-1)^{n+1}a_1y_0+(-1)^na_0y_1=\left[(-1)^ny_1\right]a_0+\left[(-1)^{n+1}y_0\right]a_1.$$

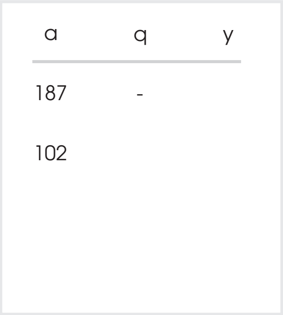
Since $a_n = (a_0, a_1)$, I've expressed (a_0, a_1) as a linear combination of a_0 and a_1. □

There are many algorithms (like the one in the proof) which produce a linear combination, but I'll call this one *the* Extended Euclidean Algorithm.

Example. Compute $(187, 102)$ and express it as a linear combination of 187 and 102.

I'll arrange this computation in the form of a table; it's just an extension of the table I used for the Euclidean algorithm.

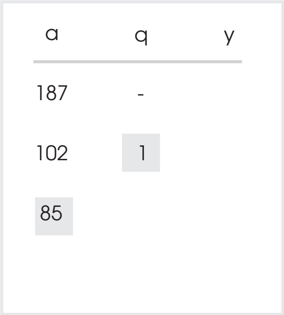
Here's how you start:



a	q	y
187	-	
102		

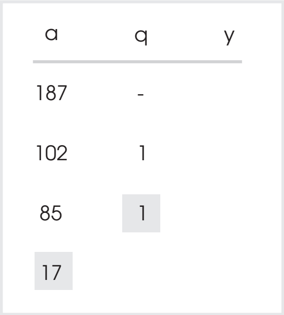
(You can save a step by putting the larger number first.)

The a and q columns are filled in using the Euclidean algorithm, i.e. by successive division: Divide the next-to-the-last a by the last a. The quotient goes into the q-column, and the remainder goes into the a-column.



a	q	y
187	-	
102	1	
85		

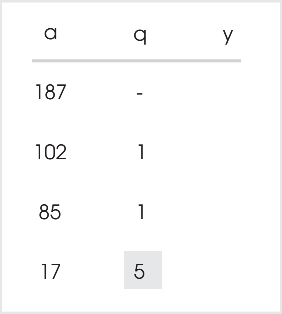
Divide 187 by 102;
Quotient 1, remainder 85.



a	q	y
187	-	
102	1	
85	1	
17		

Divide 102 by 85;
Quotient 1, remainder 17.

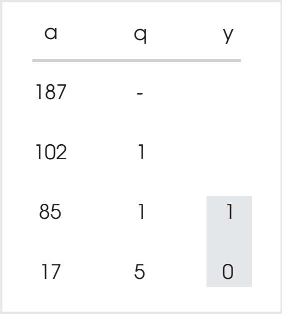
When the division comes out evenly, you stop. In this case, 85 divided by 17 is 5, with remainder 0.



a	q	y
187	-	
102	1	
85	1	
17	5	

The last entry in the a-column is the greatest common divisor. Thus, $(187, 102) = 17$.

The y-column is filled in from bottom to top. Always start with 0 for the last y and 1 for the next-to-the-last y.

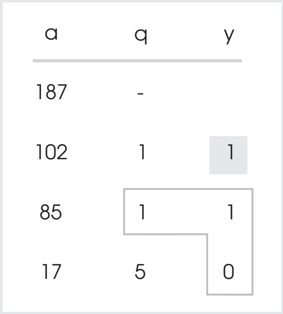


a	q	y
187	-	
102	1	
85	1	1
17	5	0

Then, working from bottom to top, fill in the y's using the rule

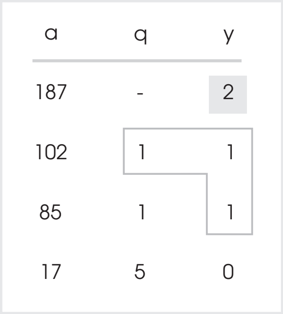
$$(\text{next } y) = (\text{last } q) \cdot (\text{last } y) + (\text{next-to-last } y).$$

It's probably easier to show than it is to explain:



a	q	y
187	-	
102	1	1
85	1	1
17	5	0

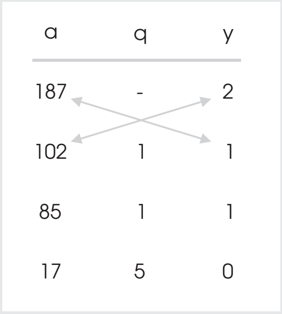
$1 \cdot 1 + 0 = 1$



a	q	y
187	-	2
102	1	1
85	1	1
17	5	0

$1 \cdot 1 + 1 = 2$

To get the linear combination, form the products diagonally and subtract one from the other:



a	q	y
187	-	2
102	1	1
85	1	1
17	5	0

Thus,

$$17 = (187, 102) = (2)(102) - (1)(187).$$

How do you know the order for the subtraction? The proof gives a formula, but the easiest thing is to pick one of the two ways, then fix it if it isn't right. If you subtract "the wrong way", you'll get a negative number. For example,

$$(1)(187) - (2)(102) = -17.$$

Since I know the greatest common divisor should be 17 — it's the last number in the a-column — I just multiply this equation by -1:

$$(-1)(187) + (2)(102) = 17.$$

This way, you don't need to memorize the exact formula. □

Example. Compute $(246, 194)$ and express it as a linear combination of 246 and 194.

246	-	52
194	1	41
52	3	11
38	1	8
14	2	3
10	1	2
4	2	1
2	2	0

Thus,

$$2 = (246, 194) = 52 \cdot 194 - 41 \cdot 246. \quad \square$$

I think this algorithm is the best for *hand* computation. For implementation on a computer, it has a drawback: You need to store all the Euclidean algorithm quotients, because you need to work your way backward up the table. There is another version of this algorithm which only requires that you save a couple of table lines at a time; it is not as good for hand computation, since you need two helper variables x and y and two multiplications at each step.

---

[1] S. P. Glasby, Extended Euclid's algorithm via backward recurrence relations, *Mathematics Magazine*, 72(3)(1999), 228–230.