Notes on the Euclidean algorithm

Consider trying to find integer solutions to $6x + 15y = 3$ and $6x + 15y = 4$. The first equation has an integer solution $3(-2) + 15(1) = 3$. For the second equation we can factor out a 3 and we have $3(2x + 5y) = 4$. If there was a solution, that is integers x^* and y^* with $6x^* + 15y^* = 4$ then, dividing by 3 we get $2x^* + 5y^* = \frac{4}{3}$. Since $2, 5, x^*, y^*$ are integers so is $2x^* + 5y^*$ and we then would have that $\frac{4}{3}$ is an integer, which is nonsense. So there is no integer solution to $6x + 15y = 4$. Consider in general $6x + 15 = c$. If we divide the left side by 3, the left side is an integer so we see we get a similar contradiction unless the right side c is a multiple of 3. When c is a multiple of 3, say $c = 3h$ then multiplying the first solution by h we have $3(-2h) + 15(1 \cdot h) = (3 \cdot -2 + 15 \cdot 1)h = 3h = c$.

Our aim is to show that the ideas of the previous example work in general. Given positive integers a, b, c we have an integer solution to $ax + by = c$ if and only if c is a multiple of the greatest common divisor of a and b. In addition we will describe the Euclidean algorithm, which uses the simple idea of the proof to compute the greatest common divisor and a solution.

The greatest common divisor is a familiar notion from basic arithmetic. Formally, we say that a positive integer c is a *common divisor* of a and b if $c|a$ and $c|b$ (i.e., c divides a and c divides b). Then c is a *greatest common divisor* of a and b, written $c = \gcd(a, b)$, if it is larger than every other common divisor. In fact, for any other common divisor d, we have $d|c$. Note that $c|a$ (c divides a) means that there exists an integer k such that $ck = a$.

We need to use the division algorithm, which is essentially the familiar idea of division from elementary arithmetic. For simplicity assume that $a \geq b \geq 0$. Then we can divide a by b and get a quotient q and a remainder r with the nonnegative remainder strictly less than b. (Technically there is a little to show this formally. We will omit these details.) That is we can find integers q and r with $0 \leq r < b$ so that $a = qb + r$.

The key to the Euclidean algorithm and the proof is the fact that $\gcd(a, b) = \gcd(b, r)$. Then for the algorithm we make a recursive call with b and r and for the proof we apply induction with b and r, finding $b = q'b + r'$.

We will first assume $\gcd(a, b) = \gcd(b, r)$ and use it to prove the theorem about integral solutions. Later will will give the simple proof that $\gcd(a, b) = \gcd(b, r)$.

Theorem: Let $a \geq b$ and c be non-negative integers. There in an integer solution to $ax + by = c$ if and only if c is a multiple of the greatest common divisor of a and b.

Proof: Let $g = \gcd(a, b)$.

We first prove 'only if'. That is, we need to show that if there is an integer solution that c is a multiple of g. There exist integers h_a, h_b with $a = gh_a$ and $b = gh_b$ since g divides a and b. If x^*, y^* are integers such that $ax^* + by^* = c$ then substituting we get $g(h_a x^* + h_b y^*) = (gh_a)x^* + (gh_b)y^* = ax^* + by^* = c$. Since $h_a x^* + h_b y^*$ is an integer, c is a multiple of g.

For 'if' we need to prove that if c is a multiple of g then there exist integers x^*, y^* such that $ax^* + by^* = c$. Note first that if c is a multiple of g then $c = gh$ for some integer h. Then if we have integers x', y' with $ax' + by' = g$ we have $a(x'h) = b(y'h) = (ax' + by')h = gh = c$. Thus it is enough to show that there is an integer solution to $ax + by = g$. We use induction on b. When $b = 0$, $g = a$ and we have the trivial solution $g \cdot 1 = g$. By the division algorithm there are integers q, r with $0 \leq r < b$ such that $a = qb + r$. Since $g = \gcd(a, b) = \gcd(b, r)$ and $b > r$, by induction there exist integers x', y' such that $bx' + ry' = g$. Then using $r = a - qb$ we have $g = bx' + ry' = bx' + (a - qb)y' = ay' + b(x' - qy')$ and hence $ax^* + by^* = g$ with $x^* = y'$ and $y^* = x' - qy'$. □

We used the following lemma in the proof so we need to prove the lemma too.

Lemma: If $a = qb + r$ **then** $\gcd(a, b) = \gcd(b, r)$**.**

Proof: If d divides a and b then $a = dk$ and $b = dl$ for some integers k, l. So $r = a - qb = dk - q(dl) = d(k - ql)$ and hence d divides r. Similarly if d divides b and r then $b = dl$ and $r = dj$ for some integers k, l. So $a = qb + r = q(dl) + dj = d(ql + j)$ and hence d divides a. Hence every common divisor of a and b is a common divisor or b and r and thus $\gcd(a, b) = \gcd(b, r)$. □

In the proof we found that $x^* = y'$ and $y^* = x' - qy'$ satisfy $ax^* + by^* = g$ when $bx' + ry' = g$. Simply iterating this using the q, r from the division algorithm gives us a way of finding the greatest common divisor as well as the solution to $ax + by = g$. This is called the Euclidean algorithm. We illustrate this as follows. Doing this by hand we first work down the left side using the division algorithm and then when we get to the bottom work back up the right side determining the values of the x and y using $x^* = y'$ and $y^* = x' - qy'$ where the x^*, y^* are the values one row higher than the x', y' and the q is from the row with the x^*, y^*.

For example

a_i		b_i		q_i		r_i	g	x_i	y_i
657	=	306	·	2	+	45	9	7	−15
306	=	45	·	6	+	36	9	−1	7
45	=	36	·	1	+	9	9	1	−1
36	=	9	·	4	+	0	9	0	1

So the greatest common divisor of 657 and 306 is 9 and $9 = 657 \cdot 7 + 306 \cdot -15$. Observe that at each step we have $a_i x_i + b_i y_i = 9$. And following from $g = ay' + b(x' - qy')$ above x for a given line is y for the line below and y for a given line is x for the line below minus the current q times y for the line below.

As another example

a_i		b_i		q_i		r_i	g	x_i	y_i
55	=	34	·	1	+	21	1	13	−21
34	=	21	·	1	+	13	1	−8	13
21	=	13	·	1	+	8	1	5	−8
13	=	8	·	1	+	5	1	−3	5
8	=	5	·	1	+	3	1	2	−3
5	=	3	·	1	+	2	1	−1	2
3	=	2	·	1	+	1	1	1	−1
2	=	1	·	2	+	0	1	0	1

So the greatest common divisor of 21 and 13 is 1 and $1 = 21 \cdot 5 + 13 \cdot -8$.

Note that the second example involves Fibonacci numbers. We now show that consecutive Fibonacci numbers give the worst case number of steps for the Euclidean algorithm. We will say that the number of steps for the Euclidean algorithm is the number of times that the division algorithm is used. This is the number of lines in the examples above.

Observe also that the x, y columns are also Fibonacci numbers. We see the identity $F_{k+2}F_{k-1}(-1)^k + F_{k+1}F_k(-1)^{k+1} = 1$ from the table above. This can be easily proved by induction with no reference to the Euclidean algorithm, although we will not do so here.

Lame's Theorem: If the Euclidean algorithm applied to $a > b \geq 1$ requires k steps then $b \geq F_{k+1}$ and $a \geq F_{k+2}$.

Proof: Use induction on the number of steps k. For $k = 1$ we have from $a > b \geq 1$ that $a \geq 2 = F_3$ and $b \geq 1 = F_2$. For $k \geq 2$ steps we write $a = qb + r$ and apply the algorithm to $b > r$. By induction, since we use $k - 1$ steps for $b > r$ we have $b \geq F_{(k-1)+2} = F_{k+1}$ and $r \geq F_{(k-1)+1} = F_k$. Since $q \geq 1$ we have $a = qb + r \geq b + r \geq F_{k+1} + F_k = F_{k+2}$. □

Since the number of digits in n is $\lfloor \log n \rfloor + 1$ and the k^{th} Fibonacci number is the integer closest to $\frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^k$ we can show that the number of steps in the Euclidean algorithm applied to $a \geq b$ is at most 5 times (actually $\frac{1}{\log(\frac{1+\sqrt{5}}{2})} \approx 4.785$) times the number of digits in b.