MA330
Sathaye

Better Division Algorithm

Given below is a convenient version of the well known Euclidean algorithm which is easy to use and gives several useful conclusions fast.

This version is from a Mathematical section of a work on Astronomy by an astronomer Āryabhaṭa from India in the fifth century. The suggested working presented here differs from the traditional commentaries, but seems consistent with the original (very cryptic) description.

Let us say we have to calculate the gcd of the numbers $a = 414$ and $b = 189$. We also wish to solve the equation $ax - by = s$ in integers.

The work consists of three steps represented by the three matrices given below. I will explain the work further down.

$$A = \begin{pmatrix} \textit{steps} & a_i & q_i \\ \hline 0 & 414 & * \\ 1 & 189 & 2 \\ 2 & 36 & 5 \\ 3 & 9 & 4 \\ 4 & 0 & * \end{pmatrix} \quad B = \begin{pmatrix} \textit{steps} & x_i & a_i & q_i \\ \hline 0 & 11 & 414 & \\ 1 & 5 & 189 & 2 \\ 2 & 1 & 36 & 5 \\ 3 & 0 & 9 & 4 \\ 4 & 1 & 0 & \end{pmatrix} \quad C = \begin{pmatrix} \textit{steps} & t_i & x_i & a_i & q_i \\ \hline 0 & 46 & 11 & 414 & * \\ 1 & 21 & 5 & 189 & 2 \\ 2 & 4 & 1 & 36 & 5 \\ 3 & 1 & 0 & 9 & 4 \\ 4 & 0 & 1 & 0 & * \end{pmatrix}$$

Here are the details:

1. The matrix A represents the basic algorithm of calculating successive remainders a_i (similar to Euclid's algorithm), except for the extra record of the quotients q_i. You start with the two numbers on top. Call them a_0, a_1 in our notation. Divide the upper number a_0 by the one below a_1 and write the remainder a_2 below. The quotient q_1 is recorded to the right of a_1.

   You continue until you get a 0 in the a_i column. Here $a_4 = 0$. The steps are numbered as $0, 1, 2, 3, 4$ for convenience of notation. We let n be the last step number (here $n = 4$). The $\gcd(a_0, a_1)$ is then given by $a_{n-1} = a_3 = 9$.

2. The matrix B is obtained inserting a column of x_i, but starting from the bottom. Thus we set $x_4 = 1$ at the bottom. Also the entry above is $x_3 = 0$. These are always fixed as $1, 0$ in order.

   To calculate the next x_i above, the formula is

   $$x_{i-1} = x_i q_i + x_{i+1}.$$

   Thus,

   $$x_2 = x_3 q_3 + x_4 = (0)(4) + 1 = 1.$$

   Similarly, $x_1 = x_2 q_2 + x_3 = (1)(5) + 0 = 5$.

   The array B is the main tool to write the $\gcd(a_0, a_1) = 9$ as a combination of a_0, a_1.

   We claim and note the important property called x-identity:

   $$\det \begin{pmatrix} x_i & a_i \\ x_{i+1} & a_{i+1} \end{pmatrix} = \pm \gcd(a_0, a_1). \qquad \textbf{HW1}$$

   This can be proved by **decreasing induction** starting from $i = n - 1$ down to 0.

3. The matrix C is obtained by a process similar to the one in B, except you start with $t_n = 0$ and $t_{n-1} = 1$. This explains the bottom two numbers $t_4 = 0$ and $t_3 = 1$.

   We use a similar rule as in the case of B, namely:

   $$t_{i-1} = t_i q_i + t_{i+1}.$$

   We claim and note the similar t-identity:

   $$\det \begin{pmatrix} t_i & a_i \\ t_{i+1} & a_{i+1} \end{pmatrix} = 0. \qquad \textbf{HW2}$$

   This also can be proved by **decreasing induction** starting from $i = n - 1$ down to 0.

4. As described above, we have $\gcd(414, 189) = 9$. From the x-identity above, we have

   $$\det \begin{pmatrix} x_0 & a_0 \\ x_1 & a_1 \end{pmatrix} = 11(189) - 5(414) = \pm 9.$$

   A simple check of the units digit shows the RHS to be $+9$.

   Moreover, it is easy to deduce that

   $$(x_0 + st_0)(a_1) - (x_1 + st_1)(a_0) = \pm \gcd(a_0, a_1) \qquad \textbf{HW3}$$

   for **any value of s**.

   Naturally, the sign is the same as determined by using the x-identity.

5. In our example, this becomes

   $$(11 + 46s)189 - (5 + 21s)414 = 9$$

   for any value of s.

6. The top two numbers t_0, t_1 are also useful, namely

   $$t_0 = \frac{a_0}{d} \text{ and } t_1 = \frac{a_1}{d}$$

   where $d = \gcd(a_0, a_1)$. Prove this! **HW4**

   Thus $t_0 = a_0/d = 414/9 = 46$ and $t_1 = a_1/d = 189/9 = 21$ respectively. Thus the $\operatorname{lcm}(a_0, a_1) = t_0 t_1 d$

7. Now we solve the main problem that Āryabhaṭa wanted to solve: "How to write a desired integer w as $w = x_0 a_1 - x_1 a_0$ for some integers x_0, x_1 and moreover, how to find all possible values of x_0, x_1 which satisfy this condition?"

   We have three methods.

8. **Method 1.** First, we remark that the desired w must be a multiple of d, since both a_0, a_1 are a multiple of d.

   Thus write $w = md$ and note that we do have a relation $\epsilon d = x_0 a_1 - x_1 a_0$ where $\epsilon = \pm 1$. This gives us a desired relation:

   $$w = (\epsilon m x_0)\, a_1 - (\epsilon m x_1)\, a_0$$

.

Using the most general solution above, we can even write:

$$w = (\epsilon m(x_0 + st_0))\, a_1 - (\epsilon m(x_1 + st_1))\, a_0$$

.

We can choose suitable values of s so that the coefficients of a_0 and a_1 are both positive (or negative) as desired and moreover their absolute values are minimal.

See details below.

For our example, we have $\epsilon = 1$ and we get

$$(46s + 11m)189 - (21s + 5m)414 = 9m.$$

Thus if $w = 54$ we set $m = 6$ and

$$(46s + 66)189 - (21s + 30m)414 = 54.$$

To find minimal positive solutions we may set $s = -1$ to yield $(20)189 - (9)414 = 54$. The most general solution will become $(46s + 20)189 - (21s + 9)(414) = 54$.

If, on the other hand, we desire a solution of the form $w = X(414) - Y(189) = 54$ then we may take $s = -1$ to get

$$(-26)(189) - (-12)(414) = 12(414) - 26(189) = 54.$$

This gives a new general solution:

$$w = (46s + 12)(414) - (21s + 26)(189) = 54.$$

Method 2. Here, we redo the process for finding x_i by choosing suitable x_n, x_{n-1} so that

$$w = x_{n-1}a_n - x_n a_{n-1} = x_{n-1}0 - x_n d = -x_n d.$$

Thus, we can take $x_{n-1} = 0$ and $x_n = m$.

Then we can repeat the original process so that we get our desired solution for the expression of w.

9. **Original Method 3.** The original algorithm said that we need not go to the $a_n = 0$, but may lift the solution from any convenient step (cleverly imagined!)

   For instance, for $w = 54$, we start by setting $x_3 = -1, x_2 = 2$. The lifting process then gives: $x_1 = x_2q_2 + x_3 = (2)(6) + (-1) = 9$ and $x_0 = x_1q_1 + x_2 = (9)(2) + 2 = 20$.

   We then have $(20)(189) - (9)(414) = 54$ as desired. The general solution is still $(46s+20)(189) - (21s + 9)(414)$. We may have to modify the signs as before.

10. First homework on this discussion is to provide proofs for the various statements marked as **(HW)**above. These should be written out and submitted. They would be more appreciated, if typed.

    Problems based on the above algorithms will be announced as a separate homework later.