The Extended Euclidean Algorithm

Andreas Klappenecker

September 22, 2002

The Euclidean algorithm for the computation of the greatest common divisor of two integers is one of the oldest algorithms known to us. This algorithm was described by Euclid in Book VII of his *Elements*, which was written about 300BC. In modern formulation, this algorithm can be stated as follows:

Algorithm 1 (Euclidean Algorithm)

Input: Integers $a > b \geq 0$.
Output: The greatest common divisor of a and b.
  while $b \neq 0$ **do**
    $(a, b) := (b, a \bmod b)$;
  od;
  return a.

The algorithm terminates after a finite number of iterations, since b is replaced in each iteration by the remainder $r = a \bmod b$, which is a non-negative integer that is strictly smaller than b. Therefore, the algorithm terminates after at most b iterations.

We show now that the algorithm is correct. We denote by $\langle a, b\rangle$ the set $\{ax + by \,|\, x, y \in \mathbf{Z}\}$; this set is called the ideal generated by a and b in the ring of integers. Notice that if $\langle a, b\rangle$ contains the integers c and d, then $\langle c, d\rangle$ is a subset of $\langle a, b\rangle$.

Lemma 1 *If* $b \neq 0$, *then* $\langle a, b\rangle = \langle b, a \bmod b\rangle$.

Proof. The ideal $\langle a, b\rangle$ contains the remainder $r = a \bmod b$, since $r = a - qb$ with $q = \lfloor a/b \rfloor$. Thus, if $b \neq 0$ then the ideal $\langle b, a \bmod b\rangle$ is a subset of $\langle a, b\rangle$.

On the other hand, a is an element of the ideal $\langle b, a \bmod b\rangle$, since $a = qb + r$. Therefore, $\langle a, b\rangle$ is contained in the ideal $\langle b, a \bmod b\rangle$. It follows that the ideals $\langle a, b\rangle$ and $\langle b, a \bmod b\rangle$ are the same. $\square$

The lemma shows that the ideal generated by the values of the variables a and b in Algorithm 1 is an invariant of the loop. Suppose that the variable a in Algorithm 1 contains the value g when the algorithm terminates, then $\langle a, b\rangle = \langle g, 0\rangle$. It follows that a and b are multiples of g, hence g is a common divisor of a and b. On the other hand, g can be expressed in the form $g = ax + by$. Therefore, each common divisor of a and b divides g, hence $g = \gcd(a, b)$. This proves that Algorithm 1 is correct.

Extension. The correctness proof of Algorithm 1 showed that there exist integers r and s such that $\gcd(a, b) = ar + bs$. We want to extend the Euclidean algorithm to determine r and s.

Each iteration in the Euclidean algorithm replaces (a, b) by $(b, a \bmod b)$. We can formulate this as a matrix multiplication:

$$(b, a \bmod b) = (a, b)\begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}, \quad \text{with} \quad q = \lfloor a/b \rfloor.$$

Suppose that the algorithm terminates after k iterations, then the operations performed on (a, b) can be summarized in matrix notation by

$$(\gcd(a, b), 0) = (a, b)\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}.$$

The product of the quotient matrices $\left(\begin{smallmatrix} 0 & 1 \\ 1 & -q_i \end{smallmatrix}\right)$ gives a 2×2 matrix such that

$$(\gcd(a, b), 0) = (a, b)\begin{pmatrix} r & u \\ s & v \end{pmatrix},$$

and the first column of the resulting matrix gives the desired integers r and s.

The idea of the extended Euclidean algorithm is to keep track of the product of the quotient matrices along with the remainder computation. For example, the Euclidean algorithm computes the greatest common divisor of 15 and 6 by the following swap and remainder steps $(15, 6) \to (6, 3) \to (3, 0)$. The extended Euclidean algorithm performs these steps in matrix formulation, and records the product of the quotient matrices as follows:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 15 & 6 \end{pmatrix} \xrightarrow{\left(\begin{smallmatrix} 0 & 1 \\ 1 & -2 \end{smallmatrix}\right)} \begin{pmatrix} 0 & 1 \\ 1 & -2 \\ 6 & 3 \end{pmatrix} \xrightarrow{\left(\begin{smallmatrix} 0 & 1 \\ 1 & -2 \end{smallmatrix}\right)} \begin{pmatrix} 1 & -2 \\ -2 & 5 \\ 3 & 0 \end{pmatrix}.$$

The left column of the last matrix contains integers $r = 1, s = -2$, and $g = 3$ so that $g = ar + bs = 15 \times 1 + 6 \times (-2) = \gcd(15, 6)$. We use matrices in the formulation of the extended Euclidean algorithm for easier mnemonics:

Algorithm 2 (Extended Euclidean Algorithm)

Input: Integers $a > b \geq 0$.
Output: Integers (g, r, s) such that $\gcd(a, b) = g = ar + bs$.

$$\begin{pmatrix} r & u \\ s & v \\ a & b \end{pmatrix} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ a & b \end{pmatrix};$$

while $b \neq 0$ **do**

$q := \lfloor a/b \rfloor$;

$$\begin{pmatrix} r & u \\ s & v \\ a & b \end{pmatrix} := \begin{pmatrix} r & u \\ s & v \\ a & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix};$$

od;

return (a, r, s).
