Integer Divisibility

Victor Adamchik

Fall of 2005

Lecture 4 (out of seven)

Plan

1. Extended Euclidean Algorithm
2. Continued Fractions

Extended Euclidean Algorithm

Theorem (Euclidean Algorithm)

The algorithm computes a GCD of two positive integers a, b by the following chain of divisions

$$\begin{array}{rcll} a & = & b*q_1 + r_1, & 0 \le r_1 < b \\ b & = & r_1*q_2 + r_2, & 0 \le r_2 < r_1 \\ r_1 & = & r_2*q_3 + r_3, & 0 \le r_3 < r_2 \\ & \ldots & \ldots & \ldots \\ r_{k-2} & = & r_{k-1}*q_k + r_k, & 0 \le r_k < r_{k-1} \\ r_{k-1} & = & r_k*q_{k+1} + 0 & \end{array}$$

The last non-zero remainder is GCD: $\gcd(a, b) = r_k$

Exercise. Apply the Euclidean Algorithm to two real numbers. What will this procedure yield?

Theorem. $\gcd(a, b) = n*a + m*b$, where $n, m \in \mathbb{Z}$.

Question. How do you find such n, m that $gcd(a, b) = n*a + m*b$?

Let us run the algorithm to find GCD(203, 91)

$$\begin{array}{rcl} 203 & = & 2*91 + 21 \\ 91 & = & 4*21 + 7 \\ 21 & = & 3*7 + 0 \end{array}$$

Next we reverse these equations. From the first equation we have

$$21 = 203 - 2 * 91$$

From the second equation we have

$$7 = 91 - 4 * 21$$

We substitute the first equation into the second

$$7 = 91 - 4 * 21 = 91 - 4 * (203 - 2 * 91) = \mathbf{9} * 91 + (\mathbf{-4}) * 203$$

The procedure we have followed above is a bit messy because of all the back substitutions we have to make. It is possible to reduce the amount of computation involved in finding n and m by doing some auxillary computations as we go forward in the Euclidean algorithm (and no back substitutions will be necessary). This is known as the *extended Euclidean Algorithm (EEA)*.

The EEA procceeds as follows. In accordance with the Euclidean algorithm

$$\begin{array}{rcll} a & = & b * q_1 + r_1, & r_1 = a + b(-q_1) \\ b & = & r_1 * q_2 + r_2, & r_2 = b + r_1(-q_2) \\ r_1 & = & r_2 * q_3 + r_3, & r_3 = r_1 + r_2(-q_3) \\ & \ldots & \ldots & \ldots \\ r_{k-2} & = & r_{k-1} * q_k + r_k, & r_k = r_{k-2} + r_{k-1}(-q_k) \\ r_{k-1} & = & r_k * q_{k+1} + 0 & \end{array}$$

we build the matrix

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \\ r_1 & 1 & -q_1 \\ r_2 & -q_2 & 1 + q_1 q_2 \\ & \ldots & \\ r_k & n & m \end{pmatrix} \begin{array}{l} \\ \\ *(-q_1) \\ *(-q_2) \\ *(-q_3) \\ \ldots \end{array}$$

where the third row is the first row minus the second row multiplied by $-q_1$

where the fourth row is the second row minus the third row multiplied by $-q_2$ and so on.

Example. Let us run the algorithm to find GCD(123, 45)

$$\begin{aligned} 123 &= 2*45+33 \\ 45 &= 1*33+12 \\ 33 &= 2*12+9 \\ 12 &= 1*9+3 \\ 9 &= 3*3+0 \end{aligned}$$

Here is the matrix for n and m:

$$\begin{pmatrix} 123 & 1 & 0 \\ 45 & 0 & 1 \\ 33 & 1 & -2 \\ 12 & -1 & 3 \\ 9 & 3 & -8 \\ 3 & -4 & 11 \end{pmatrix} \begin{matrix} \\ *(-2) \\ *(-1) \\ *(-2) \\ *(-1) \\ \end{matrix}$$

Therefore,

$$\text{GCD}(123,45) = (\mathbf{-4}) * 123 + \mathbf{11}*45$$

Applications

Recall the ***Die Hard*** movie. Willis and Jackson are supposed to disarm a bomb by measuring exactly 4 gallons of water using only 3 and 5-gallons containers. In this section we outline the mathematrics used for solving this kind of problems.

Problem. You have two containers that hold 17 and 55 ounces (oz). How would you measure 1 ounce?

Solution.
Perform Euclidean algorithm, find GCD and then express it as a linear combination of 17 and 55

$$55 = 17* 3 + 4$$
$$17 = 4* 4 + 1$$

$$\text{GCD}(55,17) = 13 * 17 - 4 * 55$$

You fill a smaller container 12 times 12*17 = 204 and empty it into the larger container

$$12*17 = 204 = 3*55 + 39$$

At this stage, you have an empty smaller container and 39oz in the larger container. On the next step (13th) you fill 16 oz into the larger container, leaving 1oz in the smaller one.

Problem. Michael Klipper - our great TA - can debug any C++ code program in 10 mins and any Java program in 6 mins. If he works continiously 104 mins, how many programs can he debug?

Solution.
Write an equation

$$10*x + 6*y = 104 \quad \text{or} \quad 5*x + 3*y = 52$$

Since

$$\gcd(5, 3) = 1 = 2*3 - 1*5$$

Multiply it by 52

$$52 = 104*3 - 52*5$$

Add and subtract $15\,k$, where $k \in \mathbb{Z}$

$$52 = (104 - 5\,k)\,3 + (3\,k - 52)\,5$$

We choose k in a such manner that

$$\begin{cases} 104 - 5\,k > 0 \\ 3\,k - 52 > 0 \end{cases} \Longrightarrow \frac{52}{3} < k < \frac{104}{5}$$

This gives us three possible solutions $k = 18, 19, 20$. Therefore, he can debug $14\ \text{java} \wedge 2\,c$ OR $9\ \text{java} \wedge 5\,c$ OR $4\ \text{java} \wedge 8\,c$ programs.

■ Continued Fractions

$$\begin{array}{rcll} a & = & b*q_1 + r_1, & 0 \le r_1 < b \\ b & = & r_1*q_2 + r_2, & 0 \le r_2 < r_1 \\ r_1 & = & r_2*q_3 + r_3, & 0 \le r_3 < r_2 \\ & \ldots & \ldots & \ldots \\ r_{k-2} & = & r_{k-1}*q_k + r_k, & 0 \le r_k < r_{k-1} \\ r_{k-1} & = & r_k*q_{k+1} + 0 & \end{array}$$

From the first line we express $\frac{a}{b}$

$$\frac{a}{b} = q_1 + \frac{r_1}{b} \quad \Longrightarrow \quad \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_1}}$$

From the second line we express $\frac{b}{r_1}$

$$\frac{b}{r_1} = q_2 + \frac{r_2}{r_1} \quad \Longrightarrow \quad \frac{b}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}}$$

Substitute $\frac{b}{r_1}$ into the equation for $\frac{a}{b}$

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}}$$

One more iteration

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\frac{r_2}{r_3}}}}$$

Generally

$$\begin{aligned}
\frac{a}{b} &= q_1 + \frac{r_1}{b} \\
\frac{b}{r_1} &= q_2 + \frac{r_2}{r_1} \\
\frac{r_1}{r_2} &= q_3 + \frac{r_3}{r_2} \\
&\ldots \qquad \ldots \\
\frac{r_{k-2}}{r_{k-1}} &= q_k + \frac{r_k}{r_{k-1}} \\
\frac{r_{k-1}}{r_k} &= q_{k+1} + 0
\end{aligned}$$

We will get

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ldots + \cfrac{1}{q_{k+1}}}}}$$

This expression is called a continued fraction for a rational number. Examples,

$$\frac{37}{11} = 3 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{3}}}$$

$$\frac{21}{13} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{1}}}}}}$$

Continues fractions are used to solve quadratic equations

$$x^2 + x - 6 = 0$$

We begin with

$$x = -1 + \frac{6}{x}$$

Then express x in the right hand side by $-1 + \frac{2}{x}$:

$$x = -1 + \cfrac{6}{-1 + \frac{6}{x}}$$

We repeat this substitution again

$$x = -1 + \cfrac{6}{-1 + \cfrac{6}{-1 + \frac{6}{x}}}$$

Continuing this process, we produce an *infinite* continued fraction, that approximate one of the roots. Here is *Mathematica* section

```
ListPlot[Table[Nest[-1 + 6/# &, 1., k], {k, 1, 30}],
  PlotStyle → {Hue[0.7], PointSize[0.01]}];
```