Math 2200-002/Discrete Mathematics

Euclid's Algorithm with Enhancement

Given natural numbers m and n,

Definition. The *greatest common divisor* of m and n, denoted

$$gcd(mn, n)$$

is the largest natural number d such that $d|m$ and $d|n$.

Example. If $m|n$, then m is itself the gcd of m and n.

Definition. m and n are *relatively prime* if $\gcd(m, n) = 1$.

Note. If p is a prime number, then **every** natural number less than p is relatively prime to p. More generally, if n is any natural number, then either $p|n$ or else p and n are relatively prime.

Euclid's Algorithm is the following efficient method for finding $\gcd(m, n)$.

1. **Initialize.** Set $x := m$ and $y := n$ (x and y will be variables).
2. **Check.** If $x|y$, then return the value x. Otherwise.
3. **Reset.** Solve $y = xq + r$ and reset $y := x$ and $x := r$.
4. **Repeat.** Go back to **2.**

Remark. The algorithm return the gcd because *at every stage*,

$$gcd(m, n) = gcd(x, y)$$

The Enhanced Algorithm also solves the equation:

$$am + bn = gcd(m, n)$$

with inteegers a and b. The trick is to keep track of **two** equations:

$$x = am + bn \text{ and } y = cm + dn$$

at every stage of the algorithm. We will do this with a 2×2 matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

that is updated at each stage. At the end, we read off:

$$gcd(m, n) = x = am + bn \text{ from the top row of the matrix}$$

Enhanced Euclid. Given natural numbers m and n:

1. **Initialize.** Set $x := m$, $y := n$ and:
$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
2. **Check.** If $x|y$, return $x = am+bn$ from the matrix A. Otherwise:
3. **Reset.** Solve $y = xq + r$ and reset $y := x$, $x := r$ and:
$$A := \begin{bmatrix} -q & 1 \\ 1 & 0 \end{bmatrix} \cdot A$$
4. **Repeat.** Go back to **2.**

Example. Solve $a(23) + b(43) = 1$.

Set $x = 23, y = 43$ and $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Solve $43 = 23(1) + 20$.

Reset $x = 20, y = 23$ and $A = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}$.

Solve $23 = 20(1) + 3$.

Reset $x = 3, y = 20$ and $A = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}$.

Solve $20 = 3(6) + 2$.

Reset $x = 2, y = 3$ and $A = \begin{bmatrix} -6 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} -13 & 7 \\ 2 & -1 \end{bmatrix}$.

Solve $3 = 2(1) + 1$.

Reset $x = 1, y = 2$ and $A = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -13 & 7 \\ 2 & -1 \end{bmatrix} = \begin{bmatrix} 15 & -8 \\ -13 & 7 \end{bmatrix}$.

Since 1 divides 2, return:
$$1 = (15)(23) + (-8)(43)$$

Application. Consider the multiplication tables mod 7 and mod 6.

$\cdot_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$\cdot_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Note that mod 7, every row has exactly one 1 and no zeroes.
This is because 7 is a prime, and:

Application. If $\gcd(m, n) = 1$, then the equation:

$$am + bn = 1$$

solves:

$$am \equiv 1 \pmod{n}$$

which means that a and m are **reciprocals** in arithmetic mod n.

Example. Since $(15)(23) + (-8)(43) = 1$, we have:

$$(15)(23) \equiv 1 \pmod{43}$$

so 15 and 23 are reciprocals mod 43.

Corollary. If p is a prime, then mod p every number in $\{0, 1, ..., p-1\}$ other than 0 has a reciprocal.

Corollary. If p is a prime and $a \neq 0$, then every "linear equation"

$$ax \equiv b \pmod{p}$$

has a solution.

Proof. Multiply both sides by the reciprocal of a.

Proposition. If p is a prime, and $a \neq 0$ then the solution to:

$$ax \equiv b \pmod{p}$$

is unique.

Proof. Suppose $ax_1 \equiv b$ and $ax_2 \equiv b$. Then:

$$a(x_1 - x_2) \equiv 0 \pmod{p}$$

Multiplying both sides by the reciprocal of a,we get $x_1 - x_2 \equiv 0 \pmod{p}$, which says that x_1 and x_2 are the same numbers mod p.

Homework. Solve the following with integers a and b (using Euclid).

1. $45a + 57b = 3$.

2. $48a + 58b = 2$.

3. $49a + 60b = 1$.

Solve the following linear equations.

4. $49a \equiv 1 \pmod{60}$.

5. $49a \equiv 11 \pmod{60}$.

6. $48a \equiv 20 \pmod{58}$.

7. If $3a \equiv b \pmod 6$ has a solution (mod 6) and $b \neq 0$, then how many **different** solutions does it have?

8. Same as **7**. for $2a \equiv b \pmod 6$ and $4a \equiv b \pmod 6$.

9. If $\gcd(m, n) = d$ and $b \neq 0$, and if $am \equiv b \pmod n$ has a solution, then how many different solutions does it have?

10. Find a pair (a, b) of numbers mod 60 that simultaneously solve:

$$8a + 3b \equiv 1 \pmod{60} \text{ and } 5a + 8b \equiv 1 \pmod{60}$$

Hint: The inverse of a 2×2 matrix is given by:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Is this the **only** solution?