MCS 260 S13 WILL

Instructor: Roy Lowman
Email: rmlowman@math.uic.edu
Web page: http://www.math.uic.edu/~rmlowman

How to solve a problem using a computer.

Example: Given m, n are positive integers,
Find $\gcd(m, n)$

Here is one approach:

1. Study the problem. Make sure you completely understand it.

2. Find a solution to a special case.
   e.g. $\gcd(6,12) = ?$
3. generalize the steps so they can work for any valid input.
4. Write the solution in the form of an algorithm that can easily be implemented on a computer.
5. Test the algorithm.
6. Write computer program to implement the algorithm and test it.
7. Test the algorithm and Computer program again ...
8. More testing.

$\gcd(m, n) = ?$

Grade School gcd: find $\gcd(8, 12) = ?$

divisors of 8 and 12

8 : 1, 2, ~~3~~, 4, ~~5~~, ~~6~~, ~~7~~ 8, ~~9~~, ~~10~~, ~~11~~ ...

12 : 1, 2, 3, 4, ~~5~~, 6, ~~7~~, ~~8~~, ~~9~~, ~~10~~, ~~11~~ 12, ~~13~~, ~~14~~, ~~15~~, ...

Common divisors: 1, 2, 4

greatest common divisor

i.e. $\gcd(8, 12) = 4$

Note:

- 4 is a divisor of 8 bcs 8/4 has remainder = 0

$$4\overline{)8}\quad 2,\ -8,\ 0 = \text{rem}$$

- 6 is not a divisor of 8 bcs 8/6 has remainder = 2 (ie. keep subtracting 6 and left with 2)

- Integers larger than 8 are never divisors of 8 because the remainder is always 8

ex $9\overline{)8}\ 0,\ -0,\ 8 = \text{Rem} \neq 0$ $\quad 10\overline{)8}\ 0,\ -0,\ 8 = \text{rem} \neq 0$ $\quad \cdots$ $\quad 99\overline{)8}\ 0,\ -0,\ 8 = \text{rem}$

• all integers greater than zero are divisors of 0.

ex $\frac{0}{1} \Rightarrow 1\overline{)0}$; $\frac{0}{2} \Rightarrow 2\overline{)0}$ ... $\frac{0}{99} \Rightarrow 99\overline{)0}$

0 = rem 0 = rem 0 = rem

• This gives a useful result:

$$\gcd(1,0) = 1 \;,\; \gcd(2,0) = 2 \;,\; \ldots \;\boxed{\gcd(n,0) = n}$$

Now test the algorithm on some larger numbers.

$\gcd(137652 \;,\; 9287632) = ?$ Yuk!

Obviously the above algorithm will not work for numbers this large.

⇒ Need a different algorithm.

Euclids Algorithm

$\gcd(8, 12)$ remainder of $8/12 = 8$

written rem = 8 mod 12
or just $r = 8 \% 12$

$$12 \overline{)\,8\,}\ 0$$
$$\underline{-\,0}$$
$$8 = \text{rem}$$

$= \gcd(12, 8)$ $\quad r = 12 \% 8 = 4$

$= \gcd(8, 4)$ $\quad r = 8 \% 4 = 0$

$= \gcd(4, 0)$

$= \underline{\underline{4}}$

Now generalize the pattern for any positive integers m and n.

given m, n find $\gcd(m, n) = ?$

$\gcd(m, n)$ $\quad r = m \bmod n$, $m_1 = n$, $n_1 = r$

$\gcd(m_1, n_1)$ $\quad r_1 = m_1 \bmod n_1$, $m_2 = n_1$, $n_2 = r_1$

$\gcd(m_2, n_2)$ $\quad r_2 = m_2 \bmod n_2$, $m_3 = n_2$, $n_3 = r_2$

$\gcd(m_3, n_3)$

Repeat ... while $n_i != 0$

If $n_i = 0$ then return m_i

ie when $\gcd(m_i, n_i) = \gcd(m_i, 0)$ return m_i

Now write the algorithm in a more compact <u>functional</u> form:

```
gcd(m, n)
    while(n != 0)
        r = m % n
        m = n
        n = r
    return m
```

This is called Pseudo Code.

Now you can test the Algorithm

1. With a walk-Thru: Make a table of values to test the algorithm on several special cases like gcd(8, 12) = 4.
2. Write a simple computer program to test the algorithm.