# Greatest Common Divisor

# Algorithms

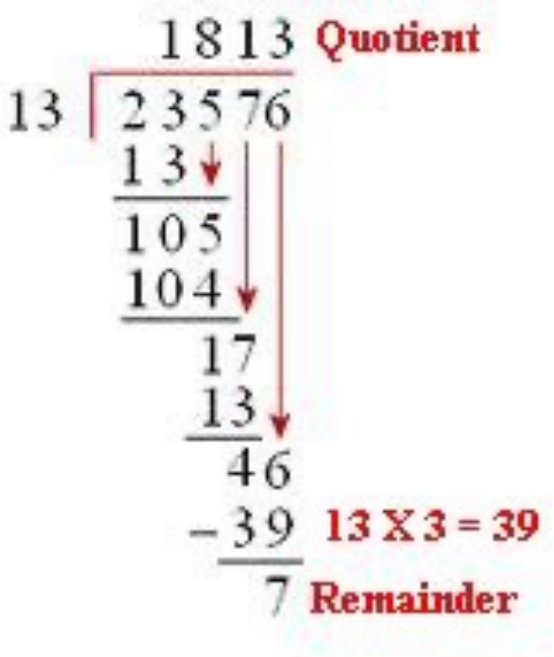
Features of algorithms

- Finiteness - there must be a finite number of steps
- Definiteness – each step must be precisely and unambiguously defined
- Input – an algorithm should have zero or more inputs
- Output – an algorithm should have one or more outputs
- Effectiveness – the algorithm should solve the required problem in a finite amount of time.

# Greatest Common Divisor (Euclid's Algorithm)

- a and b are two integers – at least one of which is greater than zero
- Consider the set of all integers that divide both *a* and *b*
- We want to find the largest element of this set
- E.g. (8, 12) = 4, (15,20)=5
- What about larger numbers? Can we construct an algorithm to find the number we are looking for?

# Greatest Common Divisor (Euclid's Algorithm)




- Long Division with remainder
  - If *a* and *b* are integers greater than zero then there is an integer *q* such that *a = b*q + r; 0<=r<=b*

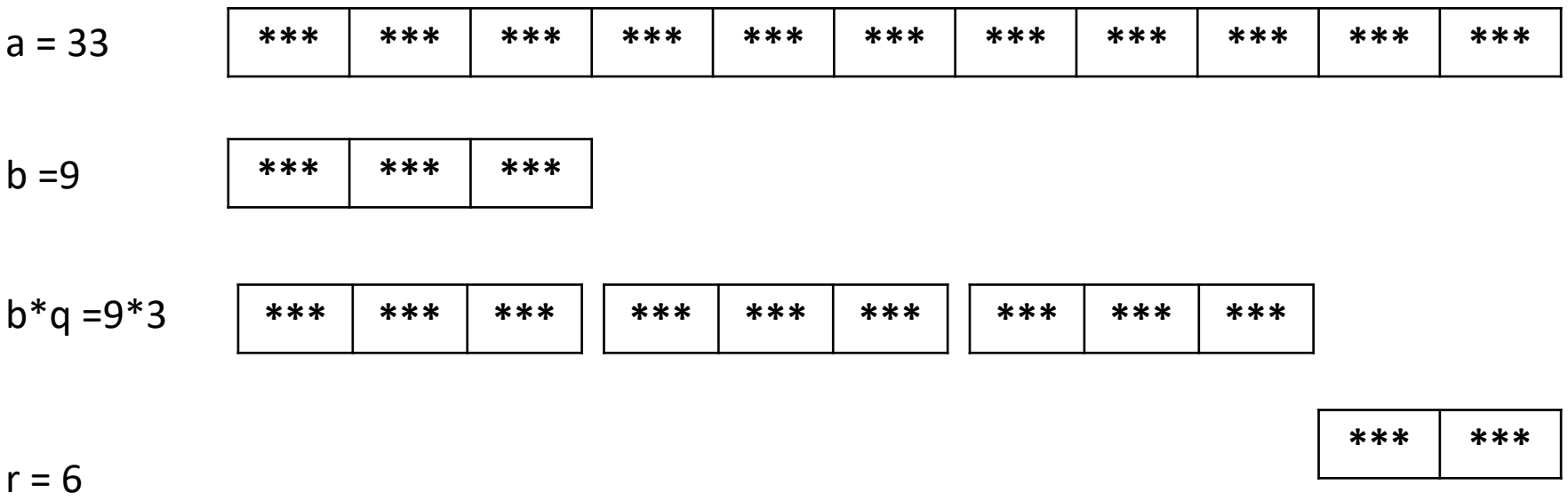
# Greatest Common Divisor (Euclid's Algorithm)

- Observation! Any number u that divides a and b also divides r (the remainder)
  - $a = bq + r$
  - $a=su,\ b=tu$
  - $r = a-bq = su – tuq = (s-tq)u$

  And conversely every number that divides both b and r also divides a`
  - $b = s'v,\ r = t'v$
  - $a = bq + r = s'vq + t'v = (s'q+t')v$

  Hence every common divisor of *a* and *b* is also a common divisor of *b* and *r* and conversely.

# GCD of 33 and 9



# Greatest Common Divisor (Euclid's Algorithm)

- This means that if we have two numbers *a* and *b* and we want to find their common divisor we can make the task easier by looking for the greatest common divisor *a* the smaller numbers *b* and the remainder *r*.
- Hang on, if the sets of common divisors are the same for the two pairs of numbers, if we apply this again can't we do the same for even smaller numbers?
- Yes we can – but can we make an algorithm out of it?

# Numerical Example

Pass 1

- a = 1143, b = 635
- 1143 = 635*1 + 508
- Set a to b and b to r

Pass 2

- a = 635, b = 508
- 635 = 508*1 + 127
- Set a to b and b to r

Pass 3

- a = 508, b 127
- 508 = 127*4 + 0
- Set a to b and b to r

a = 127, b=0  - Finished.

1143/127 = 9

635/127 = 5

# The Algorithm

```
Read a,b
r = 1;
While r>0
        r = mod(a,b)
        a = b
        b = r
EndWhile
GCD = a
```

# GCD of 33 and 9

a = 33 | *** *** *** *** *** *** *** *** *** *** ***

b =9 | *** *** ***

b*q =9*3 | *** *** *** *** *** *** *** *** ***

r = mod(a,b) = 6 | *** ***

a = b = 9 | *** *** ***

b = r = 6 | *** ***

r = mod(a,b) = 3 | ***

a = b = 6 | *** ***

b = r = 3 | ***

r = mod(a,b) = 0 #Ending conditions
a = b = 3
b= r = 0

GCD = a = 3