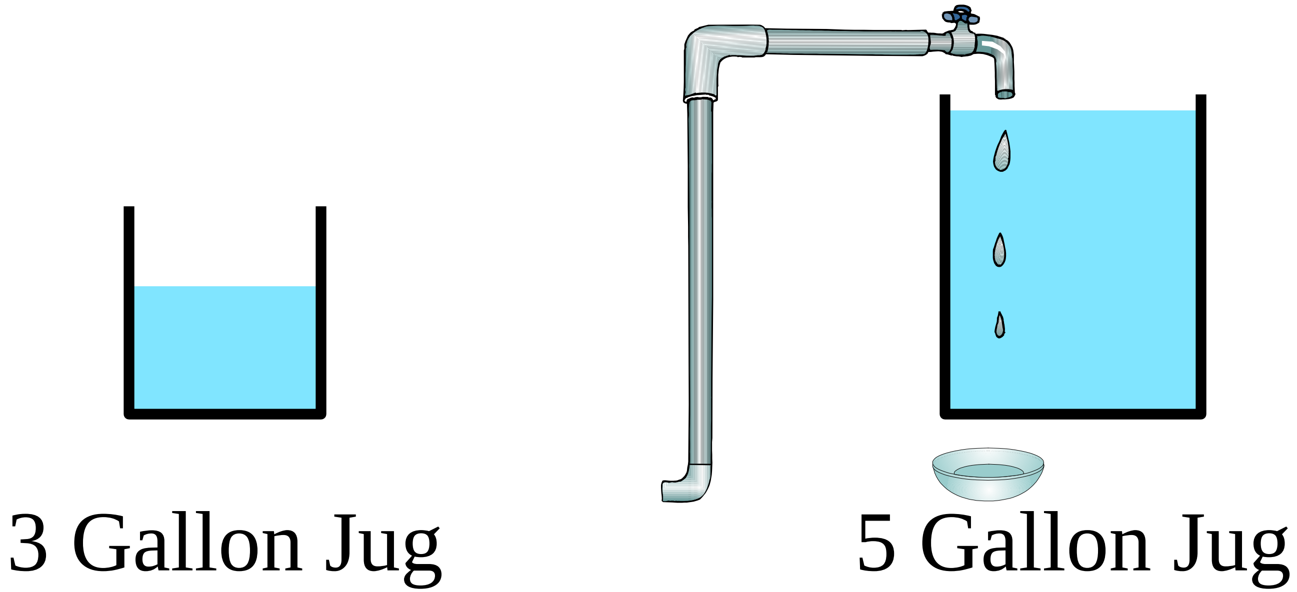
Discrete Structures I

Introduction to Number Theory

Greatest Common Divisor



Dec 28

This Lecture

- Quotient remainder theorem
- Greatest common divisor & Euclidean algorithm
- Linear combination and GCD, extended Euclidean algorithm
- Prime factorization and other applications

The Quotient-Remainder Theorem

For $b > 0$ and any a, there are *unique* numbers

$q ::= \text{quotient}(a,b)$, $r ::= \text{remainder}(a,b)$, such that

$$a = qb + r \quad \text{and} \quad 0 \le r < b.$$

We also say $q = a \text{ div } b$ and $r = a \text{ mod } b$.

When $b=2$, this says that for any a,
there is a unique q such that $a=2q$ or $a=2q+1$.

$$q = \lfloor \frac{a}{2} \rfloor$$

When $b=3$, this says that for any a,
there is a unique q such that $a=3q$ or $a=3q+1$ or $a=3q+2$.

$$q = \lfloor \frac{a}{3} \rfloor$$

The Quotient-Remainder Theorem

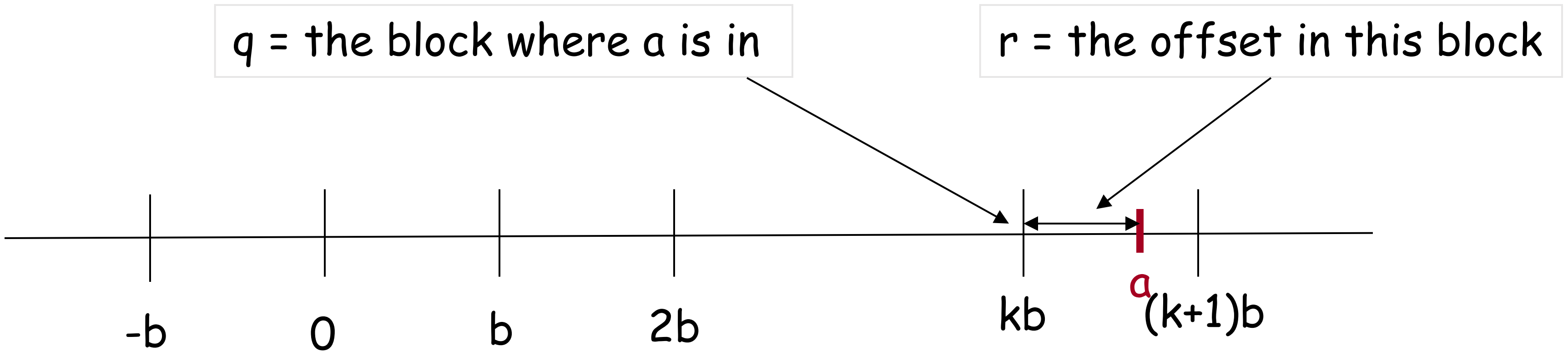
For b > 0 and any a, there are *unique* numbers

q ::= quotient(a,b), r ::= remainder(a,b), such that

$$a = qb + r \quad \text{and} \quad 0 \le r < b.$$

Given any b, we can divide the integers into many blocks of b numbers.

For any a, there is a unique “position” for a in this line.



Clearly, given a and b, q and r are uniquely defined.

Common Divisors

c is a common divisor of a and b means $c|a$ and $c|b$.

$gcd(a,b)$ ::= the *greatest* common divisor of a and b.

Say $a=8$, $b=10$, then 1,2 are common divisors, and $gcd(8,10)=2$.

Say $a=10$, $b=30$, then 1,2,5,10 are common divisors, and $gcd(10,30)=10$.

Say $a=3$, $b=11$, then the only common divisor is 1, and $gcd(3,11)=1$.

Claim. If p is prime, and p does not divide a, then $gcd(p,a) = 1$.

Greatest Common Divisors

Given a and b, how to compute gcd(a,b)?

Can try every number,
but can we do it more efficiently?

Let's say $a>b$.

1. If $a=kb$, then $\gcd(a,b)=b$, and we are done.
2. Otherwise, by the Division Theorem, $a = qb + r$ for $r>0$.

Greatest Common Divisors

Let's say $a>b$.

1. If $a=kb$, then $gcd(a,b)=b$, and we are done.
2. Otherwise, by the Division Theorem, $a = qb + r$ for $r>0$.

$a=12, b=8 \Rightarrow 12 = 8 + 4$	$gcd(12,8) = 4$	$gcd(8,4) = 4$
$a=21, b=9 \Rightarrow 21 = 2x9 + 3$	$gcd(21,9) = 3$	$gcd(9,3) = 3$
$a=99, b=27 \Rightarrow 99 = 3x27 + 18$	$gcd(99,27) = 9$	$gcd(27,18) = 9$

Euclid: $gcd(a,b) = gcd(b,r)$!

Euclid's GCD Algorithm

a = qb + r

Euclid: gcd(a,b) = gcd(b,r)

gcd(a,b)

if b = 0, then answer = a.

else

write a = qb + r $\leftarrow$ $q = \lfloor \frac{a}{b} \rfloor$ $r = a - qb$

answer = gcd(b,r)

Example 1

```
gcd(a,b)
if b = 0, then answer = a.
else
  write a = qb + r
  answer = gcd(b,r)
```

GCD(102, 70)	102 = 70 + 32
= GCD(70, 32)	70 = 2x32 + 6
= GCD(32, 6)	32 = 5x6 + 2
= GCD(6, 2)	6 = 3x2 + 0
= GCD(2, 0)	

Return value: 2.

Example 2

```
gcd(a,b)
if b = 0, then answer = a.
else
  write a = qb + r
  answer = gcd(b,r)
```

$$
\begin{aligned}
&\ \mathrm{GCD}(252, 189) \qquad && 252 = 1\times 189 + 63 \\
&= \mathrm{GCD}(189, 63) && 189 = 3\times 63 + 0 \\
&= \mathrm{GCD}(63, 0) &&
\end{aligned}
$$

Return value: 63.

Example 3

```
gcd(a,b)
if b = 0, then answer = a.
else
  write a = qb + r
  answer = gcd(b,r)
```

GCD(662, 414)	662 = 1x414 + 248
= GCD(414, 248)	414 = 1x248 + 166
= GCD(248, 166)	248 = 1x166 + 82
= GCD(166, 82)	166 = 2x82 + 2
= GCD(82, 2)	82 = 41x2 + 0
= GCD(2, 0)	

Return value: 2.

Correctness of Euclid's GCD Algorithm

$a = qb + r$

Euclid: $\gcd(a,b) = \gcd(b,r)$

When $r = 0$:

Then $\gcd(b, r) = \gcd(b, 0) = b$ since every number divides 0.

But $a = qb$ so $\gcd(a, b) = b = \gcd(b, r)$, and we are done.

Correctness of Euclid's GCD Algorithm

$a = qb + r$

Euclid: $\gcd(a,b) = \gcd(b,r)$

When $r > 0$:

Let d be a common divisor of b, r

$\Rightarrow b = k_1 d$ and $r = k_2 d$ for some k_1, k_2.

$\Rightarrow a = qb + r = qk_1 d + k_2 d = (qk_1 + k_2)d$ => d is a divisor of a

Let d be a common divisor of a, b

$\Rightarrow a = k_3 d$ and $b = k_1 d$ for some k_1, k_3.

$\Rightarrow r = a - qb = k_3 d - qk_1 d = (k_3 - qk_1)d$ => d is a divisor of r

So d is a common factor of a, b iff d is a common factor of b, r

$\Rightarrow d = \gcd(a, b)$ iff $d = \gcd(b, r)$

How fast is Euclid's GCD Algorithm?

Naive algorithm: try every number,

Then the running time is about 2b iterations.

Euclid's algorithm:

In two iterations, the b is decreased by half. (why?)

Then the running time is about 2log(b) iterations.

Exponentially faster!!

Linear Combination vs Common Divisor

Greatest common divisor

d is a common divisor of a and b if d|a and d|b

gcd(a,b) = greatest common divisor of a and b

Smallest positive integer linear combination

d is an integer linear combination of a and b if d=sa+tb for integers s,t.

spc(a,b) = smallest positive integer linear combination of a and b

Theorem: gcd(a,b) = spc(a,b)