

## Multiplicative functions

MATH2068 Number Theory & Cryptography  
Week 5 Lecture 1

University of Sydney  
NSW 2006  
Australia

25th August 2008



## Definition and examples

Definition: A function  $f$  defined on the positive integers is said to be *multiplicative* if  $f(mn) = f(m)f(n)$  whenever  $\gcd(m, n) = 1$ .

Examples:

- ▶ The Euler phi function,  $\phi$ .  
 $\phi(n) = \#\{k \in \mathbb{N} \mid k < n \text{ and } \gcd(k, n) = 1\}$ .
- ▶ The “number of divisors” function,  $\tau$ .  
 $\tau(n) = \#\{k \in \mathbb{N} \mid k|n\}$ .
- ▶ The “sum of divisors” function,  $\sigma$ .  
 $\sigma(n) = \sum_{k|n} k$ .
- ▶ The Möbius function,  $\mu$ .  
We will meet this in a week or two.

## Revision



**Lemma:** If  $a|mn$  and  $\gcd(a, m) = 1$  then  $a|n$ .

$\gcd(a, m) = 1$  implies that  $1 = ra + sm$  for some  $r, s \in \mathbb{Z}$ ;  
so  $n = ran + smn$ .

Both terms on RHS are multiples of  $a$ ; so  $a|n$ .

**Lemma:** If  $a|m$  and  $b|m$  and  $\gcd(a, b) = 1$ , then  $ab|m$ .

$a|m$  implies gives  $m = an$  for some  $n \in \mathbb{Z}$ .

So we have  $b|an$  and  $\gcd(a, b) = 1$ .

So  $b|n$  (by above lemma); i.e.  $n = bk$  for some  $k$ .

So  $m = an = abk$ , a multiple of  $ab$ .

## Taking out a common factor



Obviously  $a|b$  iff  $ka|kb$  (for all  $a, b, k \in \mathbb{Z}^+$ ). (\*)

The following is Question 3 of Tutorial 4

**Proposition:** If  $k, m, n \in \mathbb{Z}^+$ , then  $\gcd(km, kn) = k \gcd(m, n)$ .

Proof: Let  $d = \gcd(m, n)$  and  $e = \gcd(km, kn)$ .

Since  $k|km$  and  $k|kn$  it follows that  $k|e$ .

So  $e = ke'$  for some  $e' \in \mathbb{N}$ .

Now  $e|km$  gives  $ke'|km$ , and  $e'|m$  (by (\*)).

Similarly  $e'|n$ , and so  $e'|\gcd(m, n) = d$ .

So  $e|kd$ , by (\*).

But  $d|m$  and  $d|n$  gives  $kd|km$  and  $kd|kn$ . Hence  $kd|e$ .

So  $e = kd$ , as required.

## A special case



This is what we just proved:

**Proposition:** *If  $k, m, n \in \mathbb{Z}^+$ , then  $\gcd(km, kn) = k \gcd(m, n)$ .*

Writing  $a = km$  and  $b = kn$  gives the following reformulation.

**Proposition:** *If  $k|a$  and  $k|b$  then  $\gcd(a, b) = k \gcd(a/k, b/k)$ .*

In particular, we can apply this with  $k = \gcd(a, b)$ .

The hypotheses  $k|a$  and  $k|b$  do hold when  $k = \gcd(a, b)$ .

The conclusion is that  $k = \gcd(a, b) = k \gcd(a/k, b/k)$ .

So  $\gcd(a/k, b/k) = 1$ .

**Proposition:** *If  $k = \gcd(a, b)$  then  $\gcd(a/k, b/k) = 1$ .*

## gcd's of more than two numbers



Let  $a, b, c \in \mathbb{N}$ , and let  $g = \gcd(\gcd(a, b), c)$ .

It is not hard to shown that

- ▶  $g|a$  and  $g|b$  and  $g|c$ , and
- ▶ if  $k \in \mathbb{N}$  satisfies  $k|a$  and  $k|b$  and  $k|c$ , then  $k|g$ .

We call  $g$  the greatest common divisor of  $a, b$  and  $c$ .

Since the above conditions are symmetrical in  $a, b$  and  $c$ , it follows that  $\gcd(a, b, c) = \gcd(b, a, c) = \gcd(a, c, b)$ , etc..

Thus  $\gcd(\gcd(a, b), c) = \gcd(\gcd(a, c), b)$ , etc..

## Divisors of coprime products



Obviously, if  $r|m$  and  $s|n$  then  $rs|mn$ . Conversely,

**Proposition:** *If  $\gcd(m, n) = 1$  then each divisor of  $mn$  is uniquely expressible in the form  $h = rs$  with  $r|m$  and  $s|n$ . In fact,  $r = \gcd(h, m)$  and  $s = \gcd(h, n)$ .*

There are two assertions here:

- ▶ *Suppose that  $\gcd(m, n) = 1$  and  $h|mn$ . Then  $h = rs$  for some  $r, s$  with  $r|m$  and  $s|n$ .*
- ▶ *Suppose that  $\gcd(m, n) = 1$  and  $h|mn$ . If  $h = rs$  with  $r|m$  and  $s|n$  then  $r = \gcd(h, m)$  and  $s = \gcd(h, n)$ .*

## Divisors of coprime products: 1st claim



*Suppose that  $\gcd(m, n) = 1$  and  $h|mn$ . Then  $h = rs$  for some  $r, s$  with  $r|m$  and  $s|n$ .*

Proof: Let  $s = \gcd(h, n)$ . Then  $h/s, n/s$  are integers.

Now  $h|mn$  gives  $(h/s) | m(n/s)$ .

But  $\gcd(h/s, n/s) = 1$ ; so  $(h/s) | m$ .

Define  $r = h/s$ . Then  $h = rs$ , we have just shown  $r|m$ , and  $s|n$  since  $s = \gcd(h, n)$ .

## Divisors of coprime products: 2nd claim



Suppose that  $\gcd(m, n) = 1$  and  $h|mn$ . Assume also that  $h = rs$  with  $r|m$  and  $s|n$ . Then  $r = \gcd(h, m)$  and  $s = \gcd(h, n)$ .

Proof: We are given that  $h = rs$  with  $r|m$  and  $s|n$ .

Let  $d = \gcd(h, m)$ . (The aim is to prove  $d = r$ .)

Since  $r|m$  and  $r|h$  it follows that  $r|d$ .

Every divisor of  $d$  is a divisor of  $m$  and every divisor of  $s$  is a divisor of  $n$ . So every common divisor of  $d$  and  $s$  is a common divisor of  $m$  and  $n$ .

But  $\gcd(m, n) = 1$ ; so  $\gcd(d, s) = 1$ .

But now  $d|h = rs$  and  $\gcd(d, s) = 1$ ; so  $d|r$ .

Since  $r|d$  and  $d|r$  we have that  $d = r$ .

Similarly,  $\gcd(h, n) = s$ .

## Chinese Remainder Theorem



**Theorem:** If  $\gcd(m, n) = 1$  then  $k \mapsto (\text{res}_m(k), \text{res}_n(k))$  gives a 1 - 1 correspondence between  $\{k \in \mathbb{N} \mid 0 \leq k < mn\}$  and  $\{(a, b) \mid 0 \leq a < m \text{ and } 0 \leq b < n\}$ .

e.g.  $m = 2, n = 3$ :

$0 \mapsto (0, 0), 1 \mapsto (1, 1), 2 \mapsto (0, 2), 3 \mapsto (1, 0), 4 \mapsto (0, 1),$

$5 \mapsto (1, 2).$

Proof: If  $k_1$  and  $k_2$  correspond to the same pair  $(a, b)$  then

$k_1 \equiv k_2 \pmod{m}$  and  $k_1 \equiv k_2 \pmod{n}$ .

So  $m|(k_1 - k_2)$  and  $n|(k_1 - k_2)$ .

Since  $\gcd(m, n) = 1$  this gives  $k_1 \equiv k_2 \pmod{mn}$ .

So the mapping is one to one. By the pigeonhole principle it is also onto.

## Chinese Remainder Theorem and gcd's



In the CRT, if  $k \leftrightarrow (a, b)$  then  $\gcd(k, mn) = \gcd(a, m)\gcd(b, n)$ .

Let  $h = \gcd(k, mn)$ . By our "divisors of coprime products" proposition,  $h = \gcd(h, m)\gcd(h, n)$ . So we just have to prove that  $\gcd(h, m) = \gcd(a, m)$  and  $\gcd(h, n) = \gcd(b, n)$ .

Since  $k \leftrightarrow (a, b)$  we have  $k \equiv a \pmod{m}$  and  $k \equiv b \pmod{n}$ .

Now  $k \equiv a \pmod{m}$  gives  $\gcd(k, m) = \gcd(a, m)$ . (See the lemma on p. 5 of the notes for Week 1.)

But  $\gcd(k, m) = \gcd(k, \gcd(mn, m)) = \gcd(k, mn, m) = \gcd(\gcd(k, mn), m) = \gcd(h, m)$ .

So  $\gcd(a, m) = \gcd(h, m)$ , as required.

The proof that  $\gcd(b, n) = \gcd(h, n)$  is just the same.

## Multiplicativity of Euler phi



We proved this last week: if  $\gcd(m, n) = 1$  then  $\phi(mn) = \phi(m)\phi(n)$ .

Let's prove it again!

We have just shown that if  $k \leftrightarrow (a, b)$  in the CRT correspondence then  $\gcd(k, mn) = \gcd(a, m)\gcd(b, n)$ .

In particular,  $\gcd(k, mn) = 1$  if and only if  $\gcd(a, m) = 1$  and  $\gcd(b, n) = 1$ .

Therefore

(no. of  $k$  with  $\gcd(k, mn) = 1$ )

is equal to

(no. of  $a$  with  $\gcd(a, m) = 1$ )  $\times$  (no. of  $b$  with  $\gcd(b, n) = 1$ ).

That is,  $\phi(mn) = \phi(m)\phi(n)$ .



## The “number of divisors” function

For  $n \in \mathbb{Z}^+$  we define  $\tau(n) = \#\{k \in \mathbb{Z}^+ \mid k|n\}$ .

For example, the divisors of 10 are  $\{1, 2, 5, 10\}$ . So  $\tau(10) = 4$ .

By our “divisors of coprime products” proposition, if  $\gcd(m, n) = 1$  then the set

$$\{(a, b) \mid a|m \text{ and } b|n\}$$

is in one to one correspondence with

$$\{k \mid k|mn\}$$

via the function taking  $(a, b) \mapsto ab$ .

The former set has  $\tau(m)\tau(n)$  elements, the latter  $\tau(mn)$ .

So  $\tau(mn) = \tau(m)\tau(n)$  whenever  $\gcd(m, n) = 1$ .  
i.e.  $\tau$  is multiplicative.



## The “sum of divisors” function

For  $n \in \mathbb{Z}^+$  we define  $\sigma(n) = \sum_{\substack{k|n \\ k \in \mathbb{Z}^+}} k$ .

For example,  $\sigma(10) = 1 + 2 + 5 + 10 = 18$ .

By our “divisors of coprime products” proposition, if  $\gcd(m, n) = 1$  then the set

$$\{(a, b) \mid a|m \text{ and } b|n\}$$

is in one to one correspondence with

$$\{k \mid k|mn\}$$

via the function taking  $(a, b) \mapsto ab$ .

So  $\sum_{k|mn} k = \sum_{a|m} \sum_{b|n} ab = \sum_{a|m} a \sum_{b|n} b$ .

So  $\sigma(mn) = \sigma(m)\sigma(n)$  whenever  $\gcd(m, n) = 1$ .  
i.e.  $\sigma$  is multiplicative.