

# Week 1.

## Admin

- OH Th/Fr 4 PM in MS 3919
- or by appointment
- HW 1 due next Thursday at 11:59PM  
late submissions by following Monday at 11:59PM  
(not super strict)
- . collaboration allowed and encouraged, but  
cite all sources  
peers, slackexchange, textbooks, etc.
- Prof. Elman and I will fix the  
Canvas / Gradescope issue.

# Eudid-Euler theorem

First, the relevant definitions:

Def. A Mersenne prime is a prime number of the form  $2^n - 1$ .

(cf. OEIS A000668)

Rmk. By If w 1 #1, this forces  $n$  to be prime.

e.g.  $3 = 2^2 - 1$ ,  $7 = 2^3 - 1$ ,  $31 = 2^5 - 1$ ,  $127 = 2^7 - 1$

Rmk. The Lucas-Lehmer primality test determines primality of  $n = 2^p - 1$  in  $O(p^3) = O((\log n)^3)$ . For general  $n$ , the AKS test is  $O((\log n)^6)$ .

Def. Let  $n \geq 1$  an integer. We say  $n$  is

perfect if  $n = \sum_{\substack{d|n \\ d \neq n}} d$

(cf. OEIS A000396)

e.g.  $6 = 1 + 2 + 3$ ,  $28 = 1 + 2 + 4 + 7 + 14$

Thm. (Euclid-Euler).

$\approx 300 \text{ BCE}$  Euclid. If  $M_p = 2^p - 1$  is prime then  
Alexandria  $\frac{1}{2} M_p (M_p + 1)$  is perfect.

$\approx 1700 \text{ CE}$  Euler, Swiss If  $n$  is perfect and even,  
then we can find a Mersenne prime  
 $M_p$  so that

$$n = \frac{1}{2} M_p (M_p + 1)$$

This is a correspondence between Mersenne primes and perfect numbers.

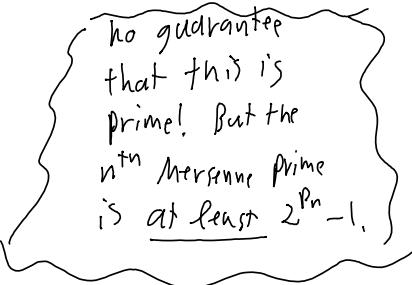
Rmk. By the prime number theorem (hard!), the  
 $n^{\text{th}}$  prime  $p_n$  is roughly  $n \log(n)$ .

Hence, the  $n^{\text{th}}$  even perfect number is at least

$$\frac{1}{2} (2^{p_n} - 1) (2^{p_n} - 2) \approx \left(2^{n \log(n)}\right)^2$$

$$= 4^{n \log(n)}$$

$$\approx h^n$$

  
no guarantee  
that this is  
prime! But the  
 $n^{\text{th}}$  Mersenne prime  
is at least  $2^{p_n} - 1$ .

Pf. We introduce the divisor function

$$\text{Def. } \sigma: \mathbb{Z}^{\geq 1} \longrightarrow \mathbb{Z}^{\geq 1}$$

$$n \longmapsto \sum_{d|n} d$$

Then  $n$  perfect  $\Leftrightarrow \sigma(n) = 2n$ ,

Lemma. If  $n$  and  $m$  are relatively prime  
then  $\sigma(nm) = \sigma(n)\sigma(m)$ .

We call  $\sigma$  a "multiplicative arithmetic function".

Pf. of lemma. Consider  $\sigma(nm)$ . What are the  
divisors of  $nm$ ?

If  $q$  has divisors:

$$1, 2, 3, 4, 6, 9, 36$$

$$2^{0,0}, 2^{1,0}, 2^{0,1}, 2^{2,0}, 2^{1,1}, 2^{0,3}, 2^{2,3}$$

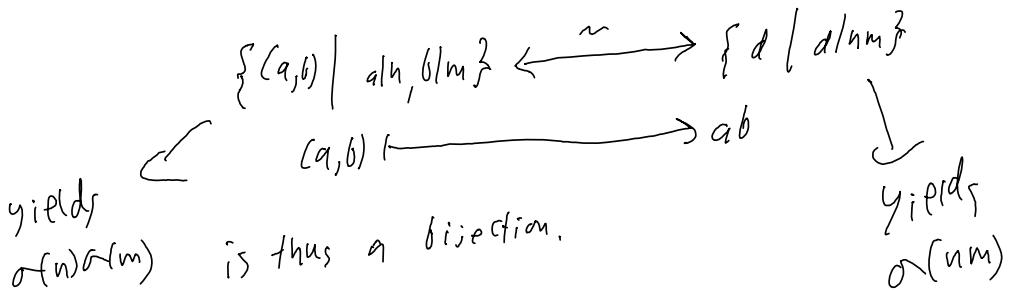
Let  $d|nm$ . Write  $d = \prod_{i=1}^l p_i^{e_i}$ . Then

$p_i^{e_i}|nm$  for all  $i$ . In this case, as  $n$   
and  $m$  are coprime,  $p_i^{e_i}|n$  or  $p_i^{e_i}|m$   
(c.f. Euclid's lemma or FTA).

$$\text{So } d = \left( \prod_{\substack{p_i|n \\ p_i \neq 1}} p_i^{e_i} \right) \left( \prod_{\substack{p_j|m \\ p_j \neq 1}} p_j^{e_j} \right)$$

factor of  $n$       factor of  $m$

$$\text{so } d = ab \text{ for } a|n, b|m.$$



$$\sigma(nm) = \sum_{d|nm} d$$

$$\sigma(n)\sigma(m) = \left( \sum_{a|n} a \right) \left( \sum_{b|m} b \right)$$

$$= \sum_{\substack{a|n \\ b|m}} ab$$

$$\text{and } \sum_{d|nm} d = \sum_{\substack{a|n \\ b|m}} ab \text{ by the above}$$

bijection, proving the lemma.  $\square$

Back to the theorem, first,

Euclid. Let  $n = \frac{1}{2} M_p (M_p + 1)$  where

$M_p = 2^p - 1$  is a Mersenne prime.

$$\text{Then } n = \frac{1}{2} (2^p - 1)(2^p)$$

$$= (2^p - 1) 2^{p-1}$$

$2^p - 1$  is odd, hence coprime to  $2^{p-1}$ .

$$\sigma(n) = \sigma(2^p - 1) \sigma(2^{p-1})$$

$$\cdot \sigma(2^{p-1}) = \sum_{i=0}^{p-1} 2^i = 2^p - 1$$

$$\cdot \sigma(2^p - 1) = 1 + (2^p - 1) \quad \text{as } 2^p - 1 \text{ is prime.}$$

$$\therefore \sigma(n) = 2^p (2^p - 1)$$

$$= 2 \cdot 2^{p-1} (2^p - 1)$$

$$= 2n$$

Thus,  $n$  is perfect. D

Euler, Let  $n$  be perfect. Write  
 $n = 2^R m$  for  $m$  odd.

As  $n$  is even,  $R \geq 1$ .

$2n = \sigma(n)$  by perfection.

$$= \sigma(2^R) \sigma(m)$$

$$= \left( \sum_{i=0}^R 2^i \right) \sigma(m)$$

$$= (2^{R+1} - 1) \sigma(m)$$

Hence,  $2^{R+1} - 1 \mid 2n$  and

$$\sigma(m) = \frac{2n}{2^{R+1} - 1}$$

$$= \frac{2^{R+1} m}{2^{R+1} - 1}$$

$2^{R+1} - 1$  is odd, hence coprime to  $2^{R+1}$ ,  
so in fact  $2^{R+1} - 1 \mid m$ .

$$\text{Let } l = \frac{m}{2^{R+1} - 1}.$$

We have  $l \mid m$ .

Hence,

$$\sigma(m) = \sum_{d|m} d$$

$$\begin{aligned} &\geq \ell + m \\ &= \ell + (2^{k+1} - 1)\ell \\ &= 2^{k+1}\ell \\ &= \frac{2^{k+1}m}{2^{k+1} - 1} \\ &= \sigma(m) \end{aligned}$$

Hence,  $\swarrow$  must have been equality, so

the only divisors of  $m$  are  
 $\ell$  and  $m$ . Thus,  $m$  is prime  
and  $\ell = 1$ .

$$1 = \ell = \frac{m}{2^{k+1} - 1}, \text{ so } m = 2^{k+1} - 1 \text{ is prime.}$$

In conclusion,

$$n = \frac{1}{2} \sigma(m) (2^{k+1} - 1)$$

$$= \frac{1}{2} (2^{k+1}) (2^{k+1} - 1)$$

$$= \frac{1}{2} M_{k+1} (M_{k+1} + 1) \text{ as desired.}$$

□

Questions,

- Are there odd perfect numbers?
- Are there infinitely many even perfect numbers?

Equivalently, are there infinitely many

Mersenne primes?

GIMPS (Great internet Mersenne prime search)

searches for large Mersenne primes. Due to  
the speed of Mersenne tests like Lucas-Lehmer,  
these are the largest known primes.

Stats.

- Oct. 2020 -  $2^{82,589,433} - 1$  is the largest known prime.
- Sep 2008 - A UCLA team found a 13 million digit prime, the first w/ more than 10 million digits, and won \$100,000 from the EFF.  
 $2^{43,112,608}$

This can be contributed to via Prime95,  
a CPU benchmarking tool.

- Currently there are  $\approx 1.8$  million TFLOP/s on  
HIMPS
- $\approx 1.8$  quintillion floating point  
operations,  
second

# Fun with arithmetic functions.

Given  $a: \mathbb{Z}^{\geq 1} \rightarrow \mathbb{C}$   
(an "arithmetic function")

We associate a "Dirichlet series"

$$\sum_{n \geq 1} \frac{a(n)}{n^s}$$

for a complex parameter  $s$ ,

e.g.,  $a(n) = 1 \rightsquigarrow \sum_{n \geq 1} \frac{1}{n^s}$ , the Riemann Zeta function

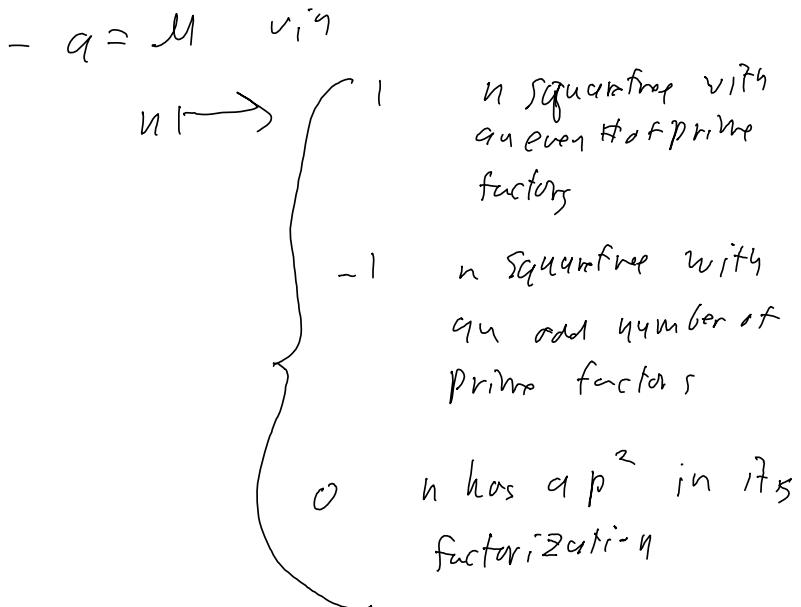
denote this  $\zeta(s)$ ,

Fact.  $\zeta(s) = \prod_{\text{prim}} \left(1 - \frac{1}{p}\right)^{-s}$

$\sim a = \sigma \rightsquigarrow \zeta(s) \zeta(s-1)$

$\sim a = \sigma_k \text{ via } n \mapsto \sum_{d|n} d^k$

$\rightsquigarrow \zeta(s) \zeta(s-k)$



$\rightsquigarrow \frac{1}{\varphi(s)}$

$M$  is the "Möbius function"

Fact. Let  $a, b$  be arithmetic functions,

Let  $c(n) = \sum_{d|n} a(d) b\left(\frac{n}{d}\right)$ , called the

"Dirichlet convolution" and written  $c = a * b$ .

$$\text{Then } \left( \sum \frac{a(n)}{n^s} \right) \left( \sum \frac{b(n)}{n^s} \right) = \sum \frac{c(n)}{n^s}$$

Corollary. As  $\sum \frac{\mu(n)}{n^s} = \frac{1}{\varphi(s)}$  and  $\varphi(s) = \sum \frac{1}{n^s}$ , we have

$$(M * 1)(n) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases} \quad \text{"Dirac delta"}$$

Let  $\delta = \mu \ast 1$ , and observe that

$a \ast 1 = a$  is a arithmetic.

This yields Möbius inversion:

Let  $b = \delta \ast a$ . Then apply  $\mu \ast (-)$  to both sides,

$$\begin{aligned}\mu \ast b &= \mu \ast 1 + g \\ &= \delta \ast a \\ &= a\end{aligned}$$

so  $b = \delta \ast a \Rightarrow \mu \ast b = a$ .

$$b = \delta \ast a \text{ says } b(n) = \sum_{d|n} a(d)$$

$$\mu \ast b = a \text{ says } a(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) b(d)$$

$$\text{so } f(n) = \sum_{d|n} a(d) \Rightarrow a(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d).$$

## Meat facts .

The Riemann hypothesis is equivalent to

$$\sigma(n) \leq H_n + \log(H_n) e^{H_n}$$

$$\text{for } H_n = \sum_{i=1}^n \frac{1}{i}$$

and also equivalent to, roughly speaking,  $\sum_{u \leq x} \mu(u) \approx \sqrt{x}$ .

formally,  $\sum_{u \leq x} \mu(u) = O(x^{1/2 + \epsilon})$

i.e.  $H \approx \sum u \approx x^{1/2 + \epsilon}$

$$\sum_{u \leq x} \mu(u) \leq C_\epsilon (x^{1/2 + \epsilon})$$

rk. If  $\mu$  was random, the cancellation between the  $\pm 1$  terms would yield essentially this  $\sqrt{x}$  result.