Week 1.

Admin

- OH Th/Fr 4PM 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, stackexchange, textbooks, etc.

- Prof. Elman and I will fix the Canvas/Gradescope issue.

Euclid - 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 Hw 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 $n = \sum_{\substack{d \mid n \\ d \neq n}} d$

(cf. OEIS A000396)

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

Thm. (Euclid - Euler).

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

≈1700 CE Swiss **Euler.** If n is perfect and <u>even</u> 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^{th} prime p_n is roughly $n \log(n)$.

Hence, the n^{th} even perfect number is <u>at least</u>

$$\frac{1}{2}(2^{p_n} - 1)(2^{p_n} - 2) \approx \left(2^{n \log(n)}\right)^2 = 4^{n \log(n)} \approx n^n$$

no guarantee that this is prime! But the n^{th} Mersenne prime is <u>at least</u> $2^{p_n} - 1$.

pf. We introduce the divisor function

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

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

Then n perfect $\iff \sigma(n) = 2n$.

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

we call σ a "multiplicative arithmetic function".

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

4.9 has diviisors!

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

$2^0 3^0, 2^1 3^0, 2^0 3^1, 2^2 3^0, 2^1 3^1, 2^0 3^2, 2^2 3^2$

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

So $d = \left(\prod_{p_i \mid n} p_i^{e_i}\right)\left(\prod_{p_j \mid m} p_j^{e_j}\right)$

(first factor: factor of n; second factor: factor of m)

So $d = ab$ for $a \mid n$, $b \mid m$.

$\{(a,b) \mid a \mid n, b \mid m\} \xleftrightarrow{\sim} \{d \mid d \mid nm\}$

$(a,b) \longmapsto ab$

yields $\sigma(n)\sigma(m)$ — is thus a bijection. — yields $\sigma(nm)$

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

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

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

and $\sum_{d \mid nm} d = \sum_{\substack{a \mid n \\ b \mid m}} ab$ by the above bijection, proving the lemma. □

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.

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}.

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

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

- $\sigma(2^p - 1) = 1 + (2^p - 1)$ as $2^p - 1$ is prime.
$= 2^p$

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

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

$= 2n$

Thus, n is perfect. □

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 $2^{R+1}-1 \mid m$.

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

We have $\ell \mid m$.

Hence,

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

$$\geq \ell + m$$

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

$$= 2^{k+1}\ell$$

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

$$= \sigma(m)$$

Hence, must have been equality, so the only divisors of m are ℓ and m. Thus, m is prime and $\ell = 1$.

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

In conclusion,

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

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

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

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 - $2^{82,589,933} - 1$ 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.

$2^{43,112,609}$

- This can be contributed to via Prime95, a CPU benchmarking tool.
- Currently there are ≈1.8 million TFLOP/S on HIMPS ≈ 1.8 quintillion $\frac{\text{floating point operations}}{\text{second}}$

Fun with arithmetic functions

Given $a : \mathbb{Z}^{\geq 1} \longrightarrow \mathbb{C}$

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

- $a = \sigma_0 \rightsquigarrow \zeta(s)\,\zeta(s-1)$
- $a = \sigma_k$ via $n \longmapsto \sum_{d \mid n} d^k$

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

- $a = \mu$ via

$n \longmapsto$
- 1 : n squarefree with an even # of prime factors
- -1 : n squarefree with an odd number of prime factors
- 0 : n has a p^2 in its factorization

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

μ is the "Möbius function"

Fact. Let a, b be arithmetic functions.

Let $c(n) = \sum_{d \mid n} a(d)\, b\left(\frac{n}{d}\right)$, called the "Dirichlet convolution" and written $c = a * b$.

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 $\sum \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$ and $\zeta(s) = \sum \frac{1}{n^s}$, we have

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

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

$a * 1 = a$ $\forall$ a arithmetic.

This yields <u>Möbius inversion</u>:

Let $b = 1 * a$. Then apply $\mu * (\sim)$ to both sides.

$$\begin{aligned} \mu * b &= \mu * 1 * a \\ &= \delta * a \\ &= a \end{aligned}$$

So $b = 1 * a \Rightarrow \mu * b = a$.

$b = 1 * a$ says $b(n) = \sum_{d \mid n} a(d)$

$\mu * b = a$ says $a(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) b(d)$

So $f(n) = \sum_{d \mid n} a(d) \Rightarrow a(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) f(d)$.

Neat facts.

The Riemann hypothesis is equivalent to

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

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

and also equivalent to, roughly speaking, $\sum_{n \le x} \mu(n) x \sqrt{x}$.

Formally, $\forall \varepsilon > 0$, $\sum_{n \le x} \mu(n) = O(x^{1/2+\varepsilon})$

i.e. $\forall \varepsilon > 0 \; \exists C_\varepsilon > 0$ s.t.

$$\sum_{n \le x} \mu(n) \le C_\varepsilon (x^{1/2+\varepsilon})$$

Rmk. If μ was random, the cancellation between the ± 1 terms would yield essentially this $\sqrt{x}$ result.