Math 4400
Week 7 - Thursday.
Big primes and perfect numbers.

Theorem (Euclid): There are infinitely many prime numbers.

Proof: Suppose there are only finitely many primes, $p_1, \dots, p_K$. ← complete list of all primes.

Let $n = p_1 p_2 \cdots p_K + 1$.

So there is an i s.t. $p_i \mid n$.

But $n \equiv 1 \bmod p_i$ ↘ $n \equiv 0 \bmod p_i$

But $0 \not\equiv 1 \bmod p_i$! Contradiction.

Some fun with perfect numbers and Mersenne primes

Definition: A positive integer n is <u>perfect</u> if it equals the sum of its proper divisors, i.e. if

$$\sum_{\substack{d \mid n \\ d \neq n}} d = n$$

Example: $6 = 3 + 2 + 1$ is perfect.

Theorem (Euler): An <u>even</u> number n is perfect if and only if

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

such that $2^\ell - 1$ is prime.

Example: $\ell = 2 \rightsquigarrow 2^2 - 1 = 3$ prime $\rightsquigarrow$ $6 = 2^{2-1}(2^2-1)$ is perfect

$\ell = 3 \rightsquigarrow 2^3 - 1 = 7$ prime $\rightsquigarrow$ $28 = 2^{3-1}(2^3-1)$ is perfect

$28 = 1 + 2 + 4 + 7 + 14$

$\ell = 4 \rightsquigarrow 2^4 - 1 = 15$ not prime — $8 \cdot 15 = 120$ not perfect.

(check this!)

Open problem: Are there any odd perfect #s?
(Know there are none $\leq 10^{1500}$).

Definition: A prime number of the form $2^\ell - 1$ is called a Mersenne prime.

Note: $(2^a - 1)(1 + 2^a + 2^{2a} + 2^{3a} + \dots + 2^{(b-1)a}) = 2^{ab} - 1$.

So if $2^\ell - 1$ is prime then ℓ must also be prime!

⚠ But ℓ prime $\not\Rightarrow$ $2^\ell - 1$ is prime

$2^{11} - 1 = 2047 = 23 \cdot 89$.

On worksheet – Lucas-Lehmer test; a good way to check if $2^\ell - 1$ is prime.

Very special!

The largest prime number known

$$2^{82,589,983} - 1$$

(almost 25 million digits!!!).

... back to even perfect numbers.

How to prove Euler's theorem?

Idea: use the function

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

e.g. $\sigma(6) = 1+2+3+6 = 12$.

So n is perfect if and only if $\sigma(n) = 2n$

Example: If $2^\ell - 1 = M_\ell$ is prime

$n = 2^{\ell-1} M_\ell$

then divisors of n are

$1, M_\ell, 2, 2M_\ell, \ldots, 2^{\ell-1}, 2^{\ell-1}M_\ell$.

so $\sigma(n) = (1 + 2 + \ldots + 2^{\ell-1})(1 + M_\ell)$

$= (2^\ell - 1)(1 + \underbrace{2^\ell - 1}_{M_\ell})$

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

$= 2n.$

How to show these are the only even perfect numbers?

$$\sigma(p^k) = 1 + p + \dots + p^k = \frac{p^{k+1}-1}{p-1}$$

if p is prime.

↖ Like ϕ, but even easier to check.

$\sigma(ab) = \sigma(a)\sigma(b)$ if $\gcd(a,b) = 1$

Let n be an even perfect number.

$$n = 2^{l-1}r \qquad r \text{ odd}, \quad l \geq 2$$

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

because n is perfect → $2n = (2^l - 1)\sigma(r)$

$$2^l r = (2^l - 1)\sigma(r)$$

In particular $\underbrace{(2^l-1)}_{\text{odd}} \mid 2^l r$

so $(2^l - 1) \mid r$ ⇝ can rewrite

$$n = 2^{l-1}r = 2^{l-1}(2^l - 1)s.$$

Remains to show $s=1$ and 2^l-1 is prime.

One more clever argument then shows
$s=1$ and 2^l-1 is prime —
see p. 61 in the book!