Lecture 3: Riemann's Hypothesis, Part 1

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

Proof: $p_1, \dots, p_n$ distinct primes.

Let $N = p_1 \cdots p_n + 1$

$= q_1 \cdots q_m$ (product of primes q_i)

If $q_1 = p_i$ some i then

$$p_i \mid N \text{ and } p_i \mid N-1$$

so $p_i \mid \gcd(N, N-1) = 1$, a contradiction.

So q_1 is a new prime.

We thus have a "gadget" that produces new primes, so there must be infinitely many.

Ex: $2+1 = 3$, $2\cdot 3+1 = 7$, prim
$2\cdot 3\cdot 5+1 = 31$ prime
$2\cdot 3\cdot 5\cdot 7+1 = 211$ prime
$2\cdot 3\cdot 5\cdot 7\cdot 11+1 = 2311$ prime
$2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1 = 59\times 509$
↑ ↗ new primes

Project? "Primorial Primes"

Question: Do you think there are infinitely many primes of the form

$$p_1 p_2 \cdots p_n + 1$$

where $p_i = i$th prime? Is it prob. prime for $n = 1, 2, 3, 4, 5, 11, 75, 171, 172, 384, 457, 616, 643, \dots$?

Hint: Sage code `is_pseudoprime` `prime_range`
See Caldwell & Gallot
conj: Yes

Joke (Lenstra): only many composites.

$p_1 \cdots p_n$ and do not add 1.

The Prime Sieve:

Algorithm to list all primes $\leq n$.

INPUT: $n \geq 2$.

OUTPUT: All primes $p \leq n$.

1. $X = [3, 5, \ldots,]$ odds $\leq n$
   $P = [2]$ = primes found so far
2. p = first elt. of X.
   if $p \geq \sqrt{n}$ return $P + X$
   otherwise append p to P.
3. Replace X by elts in X not a mult. of p, then go to 2.

Example: Primes up to $n=30$

2 3 5 7 ~~9~~ 11 13 ~~15~~ 17 19 ~~21~~ 23 ~~25~~ ~~27~~ 29

→ and circle the rest.

Read quote (from book, pg 1).

"There are two facts ..." – Don Zagier, 1975.

Turn on projector and do Sage demo.