Lecture 4: Wilson’s theorem

Here are the connections $p = 13$ or $p = 29$ as well as the ones for the 2000'th prime.

The Sieve of Erasthostenes

Here is the filled in sieve

The Ulam spiral
b) Let \( p_k \) be the largest of the primes not greater than \( n! + 1 \). Then \( p_{k+1} \) is larger than \( n! + n \).

**Remark:** There are also infinitely many primes of the form \( p = 4n + 1 \). For those primes \(-1\) is a square modulo \( p \). Assume there are only finitely many. Any prime divisor \( p \) of \((p^2 \cdots p_k) + 1\) we know that \(-1\) is a square. It can be shown that this implies that \( p \) is of the form \( 4n + 1 \).

**Fermat’s little theorem**

1) Fermat’s theorem is true for \( a = 0 \) and \( a = 1 \) because \( a^p - a = 0 \) both for \( a = 0 \) and \( a = 1 \).

2) The difference between \( a^{p+1} - a \) and \( a^p - a \) is \( (a + 1)^p - a^p - 1 \).

3) We have

\[
(a + 1)^p - a^p - 1 = \left( \begin{array}{c}
p \\ 2 \end{array} \right) a^{p-2} + \ldots + \left( \begin{array}{c}
p \\ p-1 \end{array} \right) a
\]

so that \((a + 1)^p - a^p - 1\) is a sum of terms which include \( \left( \begin{array}{c}
p \\ m \end{array} \right) \). If each is divisible by \( p \), then \((a + 1)^p - a^p - 1\) is.

4) 

\[
p \cdot (p - 1) \cdots (p - m + 1) \over m \cdot (m - 1) \cdots 1
\]

is divisible by \( p \) because the denominator terms can not cancel with the prime \( p \) because each term is smaller than \( p \).

**Prime numbers**

1. Primes of the form \( 4n + 3 \).

a) \( 4p_1p_2\ldots p_k - 1 \) is of the form \( 4n + 3 \) because it leaves rest 3 when divided by 4.

b) \( 4p_1p_2\ldots p_k - 1 \) can not be a prime because it is larger than any of the \( p_k \) because by a) it would be a prime of the form \( 4n + 3 \).

c) \( 4p_1p_2\ldots p_k - 1 \) can not have a factor of the form \( 4n + 3 \) because this factor would have to be one of the \( p_k \).

2. Arbitrary large gaps of primes