Proof of Bertrand’s Postulate

UW Math Circle – Advanced Group
Session 10 (5 December 2013)

Theorem (Bertrand’s postulate / Chebyshev’s theorem). For all positive integers \(n\), there is a prime between \(n\) and \(2n\), inclusively.

We will prove Bertrand’s postulate by carefully analyzing central binomial coefficients. In particular, we will examine the prime factors of these numbers and see that beyond a lower bound of 468, Bertrand’s postulate must hold.

Definition. The central binomial coefficients are defined as

\[
C_n = \binom{2n}{n}.
\]

So \(C_1 = 2\), \(C_2 = 6\), etc.

Lemma 1. For all integers \(n > 0\),

\[
C_n \geq \frac{4^n}{2n}.
\]

Proof.

\[
4^n = (1 + 1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} = 2 + \sum_{k=1}^{2n-1} \binom{2n}{k} \leq 2 + (2n-1) \binom{2n}{n} \leq 2n \binom{2n}{n}.
\]

Lemma 2. For any integer \(n\), none of the prime powers in the prime factorization of \(C_n\) exceed \(2n\).

Proof. The number of times a prime \(p\) occurs in \(n!\) – denote this by \(\nu_p(n)\) – is \(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots\).

Notice that the term \(\left\lfloor \frac{n}{p^k} \right\rfloor\) is 0 if \(p^k > n\).

Now,

\[
\nu_p(C_n) = \nu_p((2n)!) - 2\nu_p(n!) = \left(\left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor \right) + \left(\left\lfloor \frac{2n}{p^2} \right\rfloor - 2 \left\lfloor \frac{n}{p^2} \right\rfloor \right) + \left(\left\lfloor \frac{2n}{p^3} \right\rfloor - 2 \left\lfloor \frac{n}{p^3} \right\rfloor \right) + \ldots
\]

If \(p^k > 2n\), then the term \(\left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)\); else, this term is at most 1 (by the general fact that \(|a+b| - |a| - |b|\) is 0 or 1). Therefore, \(\nu_p(C_n)\) is at most the largest \(k\) such that \(p^k \leq 2n\), and \(p^{\nu_p(C_n)} \leq 2n\).
Lemma 3. For any integer \( n \), if a prime \( p \neq 2 \) is between \( \frac{2n}{3} \) and \( n \), then \( p \) does not appear in the prime factorization of \( C_n \).

Proof. If \( \frac{2n}{3} < p < n \), then \( \left\lfloor \frac{2n}{p} \right\rfloor = 2 \). If \( n > 4 \), then \( p^k > 2n \) for \( k \geq 2 \). This is also easy to verify for \( n \leq 4 \).

Definition. Define the primorial function \( x\# \) to be the product of all primes not greater than \( x \) (define \( 1\# = 1 \)).

Lemma 4. \( n\# < 4^n \) for all \( n \geq 1 \).

Proof. We show this by induction. The cases \( n = 1, 2 \) work.

Now assume \( k\# < 4^k \) for all \( k < n \). If \( n \) is not prime, then \( n\# = (n-1)\# \) and so \( n\# = (n-1)\# < 4^{n-1} < 4^n \).

Now we wish to show the inductive case for \( n \) prime. Since \( n > 2 \), it is odd and we may write \( n = 2m + 1 \).

Notice that \( \binom{2m+1}{n} \) is divisible by all prime numbers greater than \( n+1 \) and less than or equal to \( 2n+1 \), that is, it is divisible by \( (2n+1)\#/((n+1)\#) \).

But also observe that
\[
\binom{2m+1}{m} < \binom{2m+1}{0} + \binom{2m+1}{1} + \ldots + \binom{2m+1}{m-1} + \binom{2m+1}{m} = 2^{2m+1} = 4^m.
\]

Thus we have shown \( (2n+1)\#/((n+1)\#) < 4^n \). By the inductive hypothesis \( (n+1)\# \leq 4^{n+1} \). So, \( (2n+1)\# \leq 4^n \cdot 4^{n+1} = 4^{2n+1} \).

Theorem (Bertrand's postulate / Chebyshev's theorem). For all positive integers \( n \), there is a prime between \( n \) and \( 2n \), inclusively.

Proof. Suppose to the contrary that there exists \( n \) such that there is no prime between \( n \) and \( 2n \). Consider the prime factors of \( C_n \). Clearly none of them are greater than \( 2n \). In fact, none of them are greater than or equal to \( n \), since there are no primes between \( n \) and \( 2n \). Now, by Lemma 3, none of them are greater than \( \frac{2n}{3} \).

We may assume \( n > 4 \) (and check by hand that \( 1, 2, 3, 4 \) are not counterexamples), so \( \sqrt{2n} < \frac{2n}{3} \).

We can divide the prime factors of \( C_n \) into two groups: those that are between \( \sqrt{2n} \) and \( \frac{2n}{3} \) and those that are less than \( \sqrt{2n} \).

\[
n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k},
\]

Call the left product \( P_1 \) and the right product \( P_2 \).

By Lemma 2, none of the terms in \( P_1 \) exceeds \( 2n \), so \( P_1 \leq 2n\sqrt{2n} \).

Now observe that the primes in \( P_2 \) must all have exponent 1: if \( p > \sqrt{2n} \), then \( p^2 > 2n \), and the exponent could not be 2 or greater by Lemma 2. It follows that \( P_2 \leq \left( \frac{2n}{3} \right)! \leq 4^{2n/3} \).
Finally, by Lemma 1, we get

\[ \frac{4^n}{2n} \leq C_n = P_1 P_2 \leq (2n)^{\sqrt{2n}} 4^{2n/3}. \]

This can be shown to be true for \( n = 1, 2, \ldots, 467 \), but false for \( n \geq 468 \).

So we have shown that there is no such \( n \) greater than 467. To show that there are no counterexamples less than 468, it suffices to exhibit a sequence of primes beginning from 2 and ending greater than 467 such that each prime is no more than twice the previous one. Here is such a sequence:

\[ 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631. \]