Math 680 Fall 2017

Bertrand's Postulate

Our goal is to prove the following.

Theorem (Bertrand's Postulate): For every positive integer n, there is a prime p satisfying $n < p \leq 2n$.

We remark that Bertrand's Postulate is true by inspection for $n = 1,\ 2,\ 3$ and 4, so from now on we may assume that $n \geq 5$.

To prove Bertrand's Postulate we will derive an upper bound on the integers n for which the desired property does not hold. Then it will simply be a matter of verifying Bertrand's Postulate up to that point. This approach will revolve around the binomial coefficient $\binom{2n}{n}$. Note that if there is no prime p with $n < p \leq 2n$, then any prime factor p of $\binom{2n}{n}$ necessarily satisfies $p \leq n$. We will show that even more can be said here.

Definition: Fix a prime p. Any integer m can be uniquely written as a product $m = p^e k$ where $p \nmid k$. The exponent e here is called the *order of m at p* and written $\mathrm{ord}_p(m)$.

Lemma 1: For any positive integer m and any prime p,

$$\mathrm{ord}_p(m!) = \sum_{r \geq 1} \left[\frac{m}{p^r} \right],$$

where $[\cdot]$ denotes the greatest integer function.

Proof: Fix an exponent r for the moment. The positive $n \leq m$ that are divisible by p^r are

$$p^r,\ 2p^r,\ \ldots,\ \left[\frac{m}{p^r} \right] p^r$$

and those divisible by p^{r+1} are

$$p^{r+1},\ 2p^{r+1},\ \ldots,\ \left[\frac{m}{p^{r+1}} \right] p^{r+1}.$$

Thus there are precisely $[m/p^r] - [m/p^{r+1}]$ positive $n \le m$ with $\mathrm{ord}_p(n) = r$. We now have

$$\begin{aligned}
\mathrm{ord}_p(m!) &= \sum_{n \le m} \mathrm{ord}_p(n) \\
&= \sum_{r \ge 1} \sum_{\substack{n \le m \\ \mathrm{ord}_p(n) = r}} \mathrm{ord}_p(n) \\
&= \sum_{r \ge 1} \sum_{\substack{n \le m \\ \mathrm{ord}_p(n) = r}} r \\
&= \sum_{r \ge 1} r \left([m/p^r] - [m/p^{r+1}]\right) \\
&= \sum_{r \ge 1} r[m/p^r] - \sum_{r \ge 1} r[m/p^{r+1}] \\
&= \sum_{r \ge 1} r[m/p^r] - \sum_{r \ge 1} (r-1)[m/p^r] \\
&= \sum_{r \ge 1} \left[\frac{m}{p^r}\right].
\end{aligned}$$

Lemma 2: Suppose $n \ge 5$ and p is a prime divisor of $\binom{2n}{n}$. If $p \le n$, then $p \le 2n/3$.

Proof: Suppose p is a prime divisor of $\binom{2n}{n}$ and $p \le n$. If $p > 2n/3$, then $p^2 > 4n^2/9 > 2n$ since $n \ge 5$. Hence by Lemma 1,

$$\mathrm{ord}_p\big((2n)!\big) = \sum_{r \ge 1} \left[\frac{2n}{p^r}\right] = \left[\frac{2n}{p}\right]$$

and

$$\mathrm{ord}_p(n!) = \sum_{r \ge 1} \left[\frac{n}{p^r}\right] = \left[\frac{n}{p}\right].$$

Now since $n \ge p > 2n/3$ we have $3 > 2n/p \ge 2$ and thus $2 > n/p \ge 1$, so that

$$\begin{aligned}
\mathrm{ord}_p\left(\binom{2n}{n}\right) &= \mathrm{ord}_p\left(\frac{(2n)!}{(n!)^2}\right) \\
&= \mathrm{ord}_p\big((2n)!\big) - 2\mathrm{ord}_p(n!) \\
&= \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] \\
&= 2 - 2 \\
&= 0.
\end{aligned}$$

In other words, p is not a factor of the binomial coefficient $\binom{2n}{n}$.

Recall from a previous handout the function

$$\Theta(x) = \sum_{\substack{p \le x \\ p \text{ prime}}} \log p.$$

Lemma 3: Assume $n \ge 5$ is such that there are no primes p satisfying $n < p \le 2n$. Then

$$\log\left(\binom{2n}{n}\right) \le \Theta(2n/3) + \sqrt{2n}\log(2n).$$

Proof: As in the proof of Lemma 2, for all primes p we have

$$\begin{aligned}
\mathrm{ord}_p\left(\binom{2n}{n}\right) &= \sum_{r\geq 1}\left[\frac{2n}{p^r}\right]-2\left[\frac{n}{p^r}\right] \\
&\leq \sum_{\substack{r\geq 1 \\ p^r\leq 2n}} 1 \\
&= \left[\frac{\log(2n)}{\log p}\right].
\end{aligned}$$

Now by hypothesis any prime p dividing $\binom{2n}{n}$ must satisfy $p \leq n$, and by Lemma 2, such a prime necessarily satisfies $p \leq 2n/3$. Therefore

$$\begin{aligned}
\log\left(\binom{2n}{n}\right) &= \sum_{\substack{p\mid\binom{2n}{n} \\ p \text{ prime}}} \mathrm{ord}_p\left(\binom{2n}{n}\right)\log p \\
&= \sum_{\substack{\mathrm{ord}_p(\binom{2n}{n})=1 \\ p \text{ prime}}} \log p + \sum_{\substack{\mathrm{ord}_p(\binom{2n}{n})>1 \\ p \text{ prime}}} \mathrm{ord}_p\left(\binom{2n}{n}\right)\log p \\
&\leq \sum_{\substack{p\leq 2n/3 \\ p \text{ prime}}} \log p + \sum_{\substack{\mathrm{ord}_p(\binom{2n}{n})>1 \\ p \text{ prime}}} \left[\frac{\log(2n)}{\log p}\right]\log p \\
&\leq \Theta(2n/3) + \sum_{\substack{p\leq\sqrt{2n} \\ p \text{ prime}}} \log(2n) \\
&\leq \Theta(2n/3) + \sqrt{2n}\log(2n).
\end{aligned}$$

Our goal now is to use the inequality in Lemma 3 to deduce an upper bound for n. We derived such bounds previously; to wit:

$$\log\left(\binom{2n}{n}\right) \geq 2n\log 2 - \log(2n+1)$$

and

$$\Theta(2n/3) \leq \frac{8n}{3}\log 2.$$

Unfortunately, when we apply these bounds to the inequality in Lemma 3, we get

$$2n\log 2 - \log(2n+1) \leq \frac{8n}{3}\log 2 + \sqrt{2n}\log(2n),$$

which doesn't imply an upper bound on n. The upshot is that we need a greater lower bound for $\log(\binom{2n}{n})$ than what we derived previously. As before, this will lead to a sharper upper bound for the theta function as well.

Lemma 4: For all positive integers n,

$$\frac{2^{2n}}{2\sqrt{n}} < \binom{2n}{n} < \frac{2^{2n}}{\sqrt{2n+1}}.$$

Proof: Consider the product

$$P_n := \prod_{i \le n} \frac{(2i-1)}{(2i)} = \frac{(2n)!}{2^{2n}(n!)^2} = \binom{2n}{n}\frac{1}{2^{2n}}.$$

Note that

$$\frac{(2i-1)(2i+1)}{(2i)^2} < 1$$

for all $i \ge 1$. Thus $1 > (2n+1)P_n^2$. This gives the upper bound in the lemma. On the other hand,

$$1 - \frac{1}{(2i+1)^2} < 1$$

for all $i \ge 1$, so that

$$\begin{aligned} 1 &> \prod_{i<n}\left(1 - \frac{1}{(2i+1)^2}\right) \\ &= \prod_{i<n} \frac{(2i+1)^2 - 1}{(2i+1)^2} \\ &= \prod_{i<n} \frac{(2i+1+1)(2i+1-1)}{(2i+1)^2} \\ &= \frac{4 \cdot 6 \cdots 2n}{3 \cdot 5 \cdots (2n-1)} \frac{2 \cdot 4 \cdots (2n-2)}{3 \cdot 5 \cdots (2n-1)} \\ &= \frac{1}{2}\frac{2 \cdot 4 \cdots 2n}{3 \cdot 5 \cdots (2n-1)} \frac{1}{2n} \frac{2 \cdot 4 \cdots 2n}{3 \cdot 5 \cdots (2n-1)} \\ &= \frac{1}{4nP_n^2}, \end{aligned}$$

yielding the other inequality.

Lemma 5: For all positive integers n,

$$\Theta(n) < 2n \log 2.$$

Proof: We argue as before in the handout on Chebyshev's inequalities. By Lemma 4

$$\begin{aligned} \log\left(\binom{2n}{n}\frac{1}{2}\right) &= \log\left(\binom{2n}{n}\right) - \log 2 \\ &< 2n \log 2 - \frac{1}{2}\log(2n) - \log 2 \\ &= (2n-1)\log 2 - \frac{1}{2}\log(2n). \end{aligned}$$

Since

$$\binom{2n}{n}\frac{1}{2} = \frac{(2n)!}{(n!)^2}\frac{n}{2n} = \frac{(2n-1)!}{n!(n-1)!} = \binom{2n-1}{n-1},$$

we have

$$\log\left(\binom{2n}{n}\frac{1}{2}\right) = \log\left(\binom{2n-1}{n-1}\right) \geq \sum_{\substack{n<p\leq 2n-1 \\ p \text{ prime}}} \log p = \Theta(2n-1) - \Theta(n),$$

whence

$$\Theta(2n-1) - \Theta(n) < (2n-1)\log 2 - \frac{1}{2}\log(2n).$$

We now proceed by induction. The lemma is true by inspection for 1 and 2, so suppose that $m > 2$ and the lemma is true for all integers $n < m$. If m is odd, then $m = 2n-1$ for some integer n with $m > n \geq 2$ since $m > 2$. By the above inequality and the induction hypothesis,

$$\begin{aligned}
\Theta(m) = \Theta(2n-1) &< \Theta(n) + (2n-1)\log 2 - \frac{1}{2}\log(2n) \\
&< 2n\log 2 + (2n-1)\log 2 - \frac{1}{2}\log(2n) \\
&= (4n-1)\log 2 - \frac{1}{2}\log(2n) \\
&\leq (4n-2)\log 2 \qquad (\text{since } n \geq 2) \\
&= 2m\log 2.
\end{aligned}$$

If m is even, then $m = 2n$ for some integer n with $m > n \geq 2$. By what we have already shown,

$$\begin{aligned}
\Theta(m) = \Theta(2n) &= \sum_{\substack{p\leq 2n \\ p \text{ prime}}} \log p \\
&= \sum_{\substack{p\leq 2n-1 \\ p \text{ prime}}} \log p \\
&= \Theta(2n-1) \\
&< 2(2n-1)\log 2 \\
&< 2(2n)\log 2 \\
&= 2m\log 2.
\end{aligned}$$

Proposition: Suppose $n \geq 5$ and there is no prime p with $n < p \leq 2n$. Then

$$(2n-1)\log 2 - \frac{1}{2}\log n < \frac{4n}{3}\log 2 + \sqrt{2n}\log(2n).$$

Proof: By Lemmas 3, 4 and 5

$$\begin{aligned}
(2n-1)\log 2 - \frac{1}{2}\log n &< \log\left(\binom{2n}{n}\right) \\
&\leq \Theta(2n/3) + \sqrt{2n}\log(2n) \\
&< \frac{4n}{3}\log 2 + \sqrt{2n}\log(2n).
\end{aligned}$$