

Bertrand's Postulate

Jonathan L.F. King
 University of Florida, Gainesville FL 32611-2082, USA
 squash@ufl.edu
 Webpage <http://squash.1gainesville.com/>
 17 November, 2017 (at 02:49)

Background. Proofs are from Shoup, from Wikipedia and from my notes.

The superscript ‘ \oplus ’. An inequality OTForm

$\forall_{\text{large } n}: f(n) \leq 5^{\oplus} \cdot h(n)$ means

$$\forall \mathbf{U} > 5, \quad \forall_{\text{large } n}: f(n) \leq \mathbf{U} \cdot h(n).$$

Similarly, $\forall_{\text{large } n}: f(n) \geq [\frac{1}{3}]^{\ominus} \cdot h(n)$ means

$$\forall_{\text{positive } \mathbf{L}} < \frac{1}{3}, \quad \forall_{\text{large } n}: f(n) \geq \mathbf{L} \cdot h(n).$$

Notice that \mathbf{U} and \mathbf{L} are quantified *before* n .

Clumps. For p prime, let $\text{Divlog}_p(1500)$ denote the maximum natnum L st. $p^L \mid 1500$. Another notation for this is $p^L \parallel 1500$. So $\text{Divlog}_5(1500) = 3$.

For a non-zero integer B , the “ p -clump of B ”, $\text{Clm}_p(B)$, is the largest power of p which divides B . So $\text{Clm}_5(1500)$ is 125, and $\text{Clm}_2(1500) = 4$.

Evidently $\text{Clm}_p(B) = p^{\text{Divlog}_p(B)}$; and B 's clumps multiplied-together make B .

1: Lemma. Fix a prime p and natnum K . Then

$$\text{Divlog}_p(K!) = \sum_{j=1}^{\infty} \left\lfloor \frac{K}{p^j} \right\rfloor. \quad (\text{Exercise})$$

2: Prop'n. $\forall \alpha \in \mathbb{R}: [2\alpha] - 2[\alpha]$ is zero or one. \diamond

We denote the set of prime numbers by \mathbb{P} . Below, “ p ” ranges over the prime numbers. All following definitions are for real x , although usually x will be an integer.

First the “Product Of Primess”,

$$\text{PrOP}(N) := \prod_{p: p \leq x} p.$$

Its logarithm is the famous *Chebyshev theta fnc*:

$$\vartheta(x) := \log(\text{PrOP}(N)) = \sum_{p: p \leq x} \log(p).$$

Generalizing PrOP. When S is a set of reals, let $\text{PrOP}(S)$ mean the product of the primes in S .

3: PowFour Lemma. For each $x \geq 1$: $\text{PrOP}(x) < 4^x$.
 in other words: $\vartheta(x) < \log(4) \cdot x$, \diamond

Proof. WLOG, x is an integer N .

$$\begin{aligned} \text{CASE: } N = 1 & : \text{PrOP}(1) = 1 < 4^1. \\ \text{CASE: } N = 2 & : \text{PrOP}(2) = 2 < 4^2. \\ \text{CASE: } N > 2 \text{ and } N \text{ is even} & \end{aligned}$$

$$\begin{aligned} \text{PrOP}(N) &= \text{PrOP}(N-1), \text{ since } N \text{ isn't prime,} \\ &< 4^{N-1}, \text{ by induction,} \end{aligned}$$

which is less than 4^N .

$N > 2$ and N is odd Write $N := [2H + 1]$. Induction gives (since $1+H < N$) that

$$\text{PrOP}([1 .. 1+H]) < 4^{1+H},$$

so our goal is to show that

$$???: \quad \text{PrOP}((1+H .. N]) \stackrel{?}{\leq} 4^H.$$

Flipping a coin N times, the number of coin-flip sequences is (letting j, k range over \mathbb{N})

$$\begin{aligned} [1 + 1]^N &= \sum_{j+k=N} \binom{N}{j, k} \\ &\geq \binom{N}{H, 1+H} + \binom{N}{1+H, H} = 2 \cdot \binom{N}{H}. \end{aligned}$$

Divide by 2, then exchange sides, to get $\binom{N}{H} \leq 4^H$.

Each prime in $(1+H .. N]$ divides $\binom{N}{H}$, so

$$\text{PrOP}((1+H .. N]) \mid \binom{N}{H}.$$

Since $\binom{N}{H}$ is positive, $\text{PrOP}((1+H .. N]) \leq \binom{N}{H}$. Hence (??). \diamond

Prime-number Thm and related results

Use $\pi(x)$ for the number of primes in $[1, x]$. We'll estimate it in terms of $\frac{x}{\log(x)}$. Differentiating this latter gives:

4: The fnc $x \mapsto \frac{x}{\log(x)}$ is strictly-increasing on the $[e, \infty)$ interval.

5: Chebyshev's Theorem. For each posint $n \geq 2$:

$$??a: \quad \pi(n) \geq \frac{\log(2)}{2} \cdot \frac{n}{\log(n)}.$$

Conversely, for each real $U > \log(4)$:

$$??b: \quad \forall_{\text{large } x} : \quad \pi(x) \leq U \cdot \frac{x}{\log(x)}.$$

Proof of (??a). Sound-bite: Produce a big integer B all of whose clumps are small. Since the clumps multiply to B , and they are small, there must be many clumps. Hence many small primes divide B . So many small primes exist. Thus $\pi(x)$ must be big.

Even n : Write $2N := n$. Let $B := \binom{2N}{N, N}$. Easily

$$B \geq 2^N.$$

Let \mathbf{T} denote the number of distinct primes which divide B ; each such $p \leq 2N$, so

$$6: \quad \pi(2N) \geq \mathbf{T}.$$

Lower-binding \mathbf{T} . Evidently $\text{Divlog}_p\left(\binom{2N}{N, N}\right)$ equals $\text{Divlog}_p([2N]!) - 2 \cdot \text{Divlog}_p(N!)$. By (??), then,

$$\begin{aligned} \text{Divlog}_p(B) &= \sum_{j=1}^{\infty} \left\lfloor \frac{2N}{p^j} \right\rfloor - 2 \sum_{j=1}^{\infty} \left\lfloor \frac{N}{p^j} \right\rfloor \\ &= \sum_{j=1}^L \left[\left\lfloor \frac{2N}{p^j} \right\rfloor - 2 \left\lfloor \frac{N}{p^j} \right\rfloor \right], \end{aligned}$$

where L is $\lfloor \log_p(2N) \rfloor$. By (??), each summand is either 1 or 0. Thus $\log_p(2N) \geq \text{Divlog}_p(B)$. So

$$7: \quad 2N \geq \text{Clm}_p(B),$$

since $p^{\text{Divlog}_p(B)}$ is $\text{Clm}_p(B)$. Multiplying the B -clumps together gives B , so $[2N]^{\mathbf{T}} \geq B$. Hence $[2N]^{\mathbf{T}} \geq 2^N$. Consequently $\mathbf{T} \cdot \log(2N) \geq \log(2) \cdot N$. Dividing yields (note $N > 0$, so $\log(2N) \neq 0$)

$$\mathbf{T} \geq \frac{\log(2)}{2} \cdot \frac{2N}{\log(2N)} \stackrel{\text{def}}{=} \frac{\log(2)}{2} \cdot \frac{n}{\log(n)}.$$

Courtesy (??), this is the desired (??a).

Odd $n \geq 3$: Since $n+1$ is even, thus not prime,

$$\pi(n) = \pi(n+1) \geq \frac{\log(2)}{2} \cdot \frac{n+1}{\log(n+1)}.$$

Now use (??). ♦

Proof of (??b). We will use Thm ??, below, being careful not to argue circularly.

By (??), there is a real, 1^+ , and x_0 so that $\forall x \geq x_0$: $\pi(x) \leq 1^+ \cdot \frac{\vartheta(x)}{\log(x)}$. By the PowFour Lemma, then,

$$\pi(x) \leq 1^+ \cdot \log(4) \cdot \frac{x}{\log(x)}.$$

Chebyshev's thm gives a growth rate on the n^{th} -prime p_n .

8: Theorem. Fix posreals $L \leq U$ such that $\forall_{\text{large } \ell}$:

$$L^{\ominus} \cdot \frac{\ell}{\log(\ell)} \stackrel{1\ddagger}{\leq} \pi(\ell) \stackrel{2\ddagger}{\leq} U^{\oplus} \cdot \frac{\ell}{\log(\ell)}.$$

Then $\forall_{\text{large } n}$:

$$\left[\frac{1}{U}\right]^{\ominus} \cdot n \log(n) \stackrel{1\ddagger}{\leq} p_n \stackrel{2\ddagger}{\leq} \left[\frac{1}{L}\right]^{\oplus} \cdot n \log(n).$$

Pf of (1‡). Fix a $U > U$ with $\forall_{\text{large } \ell} : \pi(\ell) \leq U \cdot \frac{\ell}{\log(\ell)}$. Taking n sufficiently large, then,

$$n \stackrel{\text{def}}{=} \pi(p_n) \leq U \cdot \frac{p_n}{\log(p_n)}.$$

Cross-multiplying gives $\frac{1}{U} \cdot n \log(p_n) \leq p_n$. But $n \leq p_n$, so $\log(n) \leq \log(p_n)$. Thus

$$\frac{1}{U} \cdot n \log(n) \leq p_n.$$

Proof of (2‡). Suppose $\forall_{\text{large } \ell} : \pi(\ell) \geq \frac{1}{5} \cdot \frac{\ell}{\log(\ell)}$. We want to establish (2‡), with the constant being 5^{\oplus} .

Define K_n by $p_n = K_n \cdot n \log(n)$. Let S be the set of n with $\boxed{K_n \geq 5.001}$. FTSOC, suppose S is infinite.

For large $n \in S$, then, $\frac{1}{5} \cdot \frac{p_n}{\log(p_n)} \leq \pi(p_n) \stackrel{\text{def}}{=} n$. So

$$\frac{1}{5} \leq \frac{\log(K_n \cdot n \log(n))}{K_n \log(n)} = \frac{\log(K_n \log(n))}{K_n \log(n)} + \frac{1}{K_n}.$$

Note that $[K_n \log(n)] \rightarrow \infty$, as $n \rightarrow \infty$, since $\{K_n\}_1^{\infty}$ is bndd below, and $\log(n) \rightarrow \infty$. Apply to each side $\limsup_{n \rightarrow \infty}$, but only for $n \in S$, to obtain that

$$\frac{1}{5} \leq \limsup_{\substack{n \rightarrow \infty \\ n \in S}} \frac{1}{K_n} \stackrel{\text{note}}{\leq} \frac{1}{5.001}.$$

This contradiction shows S must have been finite! ♦

9: Lemma. Fix a positive $\delta < 1$. Then $x^\delta = o(\frac{x}{\log(x)})$.
Consequently,

??*: $x^\delta = o(\pi(x))$.

Proof. Use l'Hôpital's rule. For (??*), note that (??a) implies $\frac{x}{\log(x)} = O(\pi(x))$. ♦

10: Asymptotic π, ϑ Thm. Indeed,

.1: $\pi(x) \geq \frac{\vartheta(x)}{\log(x)}$, for all $x > 1$.

.2: $\pi(x) \asymp \frac{\vartheta(x)}{\log(x)}$, as $x \rightarrow \infty$.

Proof. When $p \leq x$, necessarily $\log(p) \leq \log(x)$. So

$$\vartheta(x) \leq \sum_{p \in (1..x]} \log(x) = \log(x) \cdot \pi(x).$$

Because of (??1), ISTFix a posreal ε and show

$$[1 + \varepsilon] \frac{\vartheta(x)}{\log(x)} \stackrel{?}{\geq} [1 - o(1)] \cdot \pi(x),$$

to establish the (??2) asymptotics. Rewritten, our goal is

$$[1 + \varepsilon] \cdot \frac{\vartheta(x)}{\log(x)} \stackrel{?}{\geq} \pi(x) - o(\pi(x)).$$

So fix a positive $\delta < 1$ and set $\mathbf{L} := x^\delta$. Thus

$$\vartheta(x) \geq \sum_{p \in (\mathbf{L}..x]} \log(\mathbf{L}) = \delta \log(x) \cdot [\pi(x) - \pi(\mathbf{L})].$$

Hence $\frac{1}{\delta} \cdot \frac{\vartheta(x)}{\log(x)} \geq \pi(x) - \pi(\mathbf{L})$. Therefore, we need but show that $\pi(\mathbf{L})$ is $o(\pi(x))$. But $\pi(\mathbf{L}) \leq \mathbf{L} = x^\delta$. And (??*) is our knight in shining armor. ♦

11: Coro. There is a positive constant C so that

$$\forall_{\text{large } n}: C \cdot n \leq \vartheta(n).$$

Proof. Combine (??2) with (??a). ♦

The n^{th} **harmonic number** is $H_n := \sum_{j=1}^n \frac{1}{j}$, for n a posint. Easily,

†: $\forall n: H_n \geq H_{n-1} \geq \log(n) \geq H_n - 1$.

‡: $\forall x > 0: x \geq \log(1 + x)$.

Euler proved that $\sum_p \frac{1}{p} = \infty$. His argument essentially shows (??), below.

12: Thm. For N a posint: $\sum_{p: p \leq N} \frac{1}{p-1} \geq \log \log(N)$.

Hence, $\sum_{p \leq N} \frac{1}{p} \geq \log \log(N) - O(1)$. ♦

Proof. Each $n \leq N$ is some product of $p_j^{e_j}$, over primes $p_j \leq N$. So $\frac{1}{n}$ has form $\prod_{p \leq N} \frac{1}{p^{e(n)}}$. Thus

$$H_N \leq \prod_{p \leq N} \left[1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots \right].$$

And $1 + \frac{1}{p} + \frac{1}{p^2} + \dots = \frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p-1}$. By (†), then, $\log \log(N) \leq \log(H_N) \leq \sum_{p \leq N} \log(1 + \frac{1}{p-1})$. Hence

$$\log \log(N) \stackrel{\text{by } (\ddagger)}{\leq} \sum_{p \leq N} \left[\frac{1}{p-1} \right].$$

Shoup's proof of Bertrand's postulate

Let $\mathbf{T}_n := \pi(2n) - \pi(n)$. The PNT suggests that $\mathbf{T}_n \approx \frac{n}{\log(2n)}$. We will show this weaker stmt.

13: Bertrand's Density Postulate. For each posint N :

??†: $\mathbf{T}_N \geq \frac{1}{3} \cdot \frac{N}{\log(2N)}$.

Rem. It will suffice to produce a constant $\mathbf{U} > \frac{1}{3}$ st.

??‡: $\mathbf{T}_N \geq \mathbf{U} \cdot \frac{N}{\log(2N)} - o(\frac{N}{\log(2N)})$,

then verify (??†) for finitely many values of N . □

Proof. We use notation from (??a) and its proof.

Each prime $p \bullet B$ produces a clump $\text{Clm}_p := p^{\text{Divlog}_p(B)}$. Given an interval $J \subset (1..2N]$, let \bar{J} be

the product of the p -clumps over all $p \in J$. We will show that (*proof is currently omitted*)

$$\begin{aligned} \overline{(1 \dots \sqrt{2N})} &\leq [2N]^{\sqrt{2N}}; \\ \overline{(\sqrt{2N} \dots \frac{2}{3}N)} &\leq 4^{\lceil \frac{2}{3}N \rceil}; \\ \overline{(\frac{2}{3}N \dots N)} &= 1; \\ \overline{(N \dots 2N)} &\leq [2N]^{\mathbf{T}}. \end{aligned}$$

But B is the product of its clumps, so

$$[2N]^{\mathbf{T}} \cdot [2N]^{\sqrt{2N}} \cdot 4^{\lceil \frac{2}{3}N \rceil} \geq B.$$

A simple induction shows that $\binom{2n}{n} \geq \frac{1}{2^n} \cdot 4^n$. Thus

$$[2N]^{\mathbf{T}+1+\sqrt{2N}} \geq 4^{\lceil \frac{1}{3}N \rceil}.$$

So $[\mathbf{T} + 1 + \sqrt{2N}] \cdot \log(2N) \geq \log(4) \cdot \frac{1}{3}N$. Thus

$$\mathbf{T} \geq \log(4) \cdot \frac{1}{3} \frac{N}{\log(2N)} - [1 + \sqrt{2N}].$$

And this is what we needed in (??‡). ♦

Logarithmic Integral

Following Shoup, define^{♡1}

$$\text{Li}(x) := \int_2^x \frac{1}{\log(t)} dt.$$

Let's use L'Hôpital's rule to show that

$$14: \quad \text{Li}(x) \asymp \frac{x}{\log(x)}.$$

Abbrev $\log(x)$ by L . So $\frac{d}{dx} \left(\frac{x}{L} \right) = \frac{1 \cdot L - x \cdot \frac{1}{L}}{L^2} = \frac{1}{L} - \frac{1}{L^2}$. Therefore

$$\frac{\left[\frac{x}{\log(x)} \right]'}{\left[\text{Li}(x) \right]'} = \frac{\frac{1}{L} - \frac{1}{L^2}}{\frac{1}{L}} = 1 - \frac{1}{L}.$$

And $1 - \frac{1}{L} \rightarrow 0$ as $x \rightarrow \infty$. Hence l'Hôpital's yields (??).

^{♡1}Wikipedia calls this version the "Offset logarithmic integral", and uses \int_0^∞ for its "logarithmic integral".

Erdős' proof of Bertrand's postulate

Assume there is a CEX: an integer $N \geq 2$ such that there is no prime number in $(N \dots 2N)$.

If $N \in [2 \dots 2048)$, then one of the prime numbers 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259 and 2503 (each being less than twice its predecessor), call it p , will satisfy $N < p < 2N$. Therefore WLOG $N \geq 2048$.

Proof, when $N \geq 2048$. Note that

$$4^N = [1 + 1]^{2N} = \sum_{k=0}^{2N} \binom{2N}{k}.$$

Since $\binom{2N}{N}$ is the largest term in the sum, we have that

$$\frac{4^N}{2N + 1} \leq \binom{2N}{N}.$$

Define $\mathcal{R} := \mathcal{R}(p, N)$ to be highest integer x , such that p^x divides $\binom{2N}{N}$. Applying (??) to $K := 2N$ and $K := N$ yields

$$\begin{aligned} \mathcal{R} &= \text{Divlog}_p([2N]!) - 2 \cdot \text{Divlog}_p(N!) \\ &= \sum_{j=1}^{\infty} \left\lfloor \frac{2N}{p^j} \right\rfloor - 2 \sum_{j=1}^{\infty} \left\lfloor \frac{N}{p^j} \right\rfloor \\ &= \sum_{j=1}^{\infty} \left[\left\lfloor \frac{2N}{p^j} \right\rfloor - 2 \left\lfloor \frac{N}{p^j} \right\rfloor \right]. \end{aligned}$$

But each term

$$\left\lfloor \frac{2N}{p^j} \right\rfloor - 2 \left\lfloor \frac{N}{p^j} \right\rfloor$$

can either be 0 (when $\frac{N}{p^j} \bmod 1 < \frac{1}{2}$) or 1 (when $\frac{N}{p^j} \bmod 1 \geq \frac{1}{2}$). Furthermore, all terms with

$$j > \left\lfloor \frac{\log(2N)}{\log(p)} \right\rfloor$$

are 0. Therefore

$$\mathcal{R} \leq \left\lfloor \frac{\log(2N)}{\log(p)} \right\rfloor,$$

and we get:

$$\begin{aligned} p^{\mathcal{R}} &= \exp(\mathcal{R} \cdot \log(p)) \\ &\leq \exp\left(\left\lfloor \frac{\log(2N)}{\log(p)} \right\rfloor \log(p)\right) \leq 2N. \end{aligned}$$

For each $p > \sqrt{2N}$, necessarily

$$\left\lfloor \frac{\log(2N)}{\log(p)} \right\rfloor \leq 1$$

or

$$\mathcal{R} = \left\lfloor \frac{2N}{p} \right\rfloor - 2 \left\lfloor \frac{N}{p} \right\rfloor.$$

Remark that $\binom{2N}{N}$ has no prime factors p such that:

- $2N < p$, because $2N$ is the largest factor.
- $N < p \leq 2N$, because we assumed there is no such prime number.
- $\frac{2N}{3} < p \leq N$, because (since $N \geq 5$) which gives us

$$\mathcal{R} = \left\lfloor \frac{2N}{p} \right\rfloor - 2 \left\lfloor \frac{N}{p} \right\rfloor = 2 - 2 = 0.$$

Each prime factor of $\binom{2N}{N}$ is therefore not larger than $\frac{2N}{3}$.

Note that $\binom{2N}{N}$ has at most one factor of every prime $p > \sqrt{2N}$. As $p^{\mathcal{R}} \leq 2N$, the product of $p^{\mathcal{R}}$ over all other primes is at most $[2N]^{\sqrt{2N}}$. Since $\binom{2N}{N}$ is the product of $p^{\mathcal{R}}$ over all primes p , we get that

$$\begin{aligned} \frac{4^N}{2N+1} &\leq \binom{2N}{N} \leq [2N]^{\sqrt{2N}} \cdot \prod_{p \in \mathbb{P}} p^{\frac{2N}{3}} \\ &= [2N]^{\sqrt{2N}} \cdot e^{\vartheta(\frac{2N}{3})}. \end{aligned}$$

Using our lemma, $\vartheta(N) < N \cdot \log(4)$:

$$\frac{4^N}{2N+1} \leq [2N]^{\sqrt{2N}} \cdot 4^{\frac{2N}{3}}$$

Since we have $[2N+1] < [2N]^2$, automatically

$$4^{\frac{N}{3}} \leq [2N]^{2+\sqrt{2N}}.$$

Also $2 \leq \frac{\sqrt{2N}}{3}$ (since $N \geq 18$): Consequently,

$$4^{\frac{N}{3}} \leq [2N]^{\frac{4}{3}\sqrt{2N}}.$$

Taking logarithms produces

$$\sqrt{2N} \cdot \log(2) \leq 4 \cdot \log(2N).$$

Substituting 2^{2t} for $2N$:

$$\frac{2^t}{t} \leq 8.$$

This gives us $t < 6$ and the contradiction that

$$N = \frac{2^{2t}}{2} < \frac{2^{2 \cdot 6}}{2} \stackrel{\text{note}}{=} 2048.$$

Thus no counterexample to the postulate is possible. \blacklozenge

Filename: Problems/NumberTheory/bertrand_postulate.tex
As of: Wednesday 09Sep2009. Typeset: 17Nov2017 at 02:49.