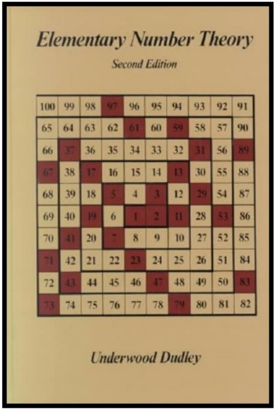
Elementary Number Theory

Section 22. Formulas for Primes—Proofs of Theorems



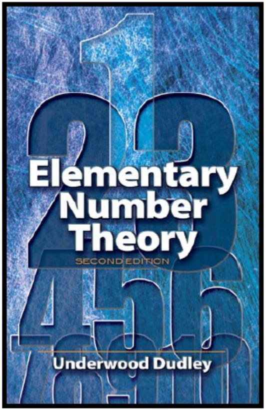


Table of contents

1. Theorem 22.A
2. Theorem 22.C
3. Theorem 22.1
4. Lemma 22.E
5. Lemma 22.F
6. Theorem 22.2. Bertrand's Theorem
7. Theorem 22.3

Theorem 22.A

Theorem 22.A. An arithmetic progression of prime numbers must be finite in length.

Proof. Suppose the arithmetic progression is given by the function $f(n) = an + b$. Let p be prime and suppose $p \nmid a$, so that $(a, p) = 1$. So by Lemma 5.2 there is (exactly one) integer r such that $ax \equiv -b \pmod{p}$. Then $a(r + kp) + b \equiv ar + b \equiv 0 \pmod{p}$ for all $k \in \{0, 1, 2, \ldots\}$. So every pth term in the sequence is divisible by p (that is, $ar + b$ is divisible by p, $ar + b + p$ is divisible by p, $ar + b + 2p$ is divisible by p, etc.).

Theorem 22.A

Theorem 22.A. An arithmetic progression of prime numbers must be finite in length.

Proof. Suppose the arithmetic progression is given by the function $f(n) = an + b$. Let p be prime and suppose $p \nmid a$, so that $(a, p) = 1$. So by Lemma 5.2 there is (exactly one) integer r such that $ax \equiv -b \pmod{p}$. Then $a(r + kp) + b \equiv ar + b \equiv 0 \pmod{p}$ for all $k \in \{0, 1, 2, \ldots\}$. So every pth term in the sequence is divisible by p (that is, $ar + b$ is divisible by p, $ar + b + p$ is divisible by p, $ar + b + 2p$ is divisible by p, etc.). Since one of these multiples of p must be in the sequence (and hence p-terms later the sequence repeats a multiple of p), then the sequence cannot consist of only primes (any multiple of p greater then p is not prime). That is, the arithmetic progression of primes must be finite in length, as claimed. □

Theorem 22.A

Theorem 22.A. An arithmetic progression of prime numbers must be finite in length.

Proof. Suppose the arithmetic progression is given by the function $f(n) = an + b$. Let p be prime and suppose $p \nmid a$, so that $(a, p) = 1$. So by Lemma 5.2 there is (exactly one) integer r such that $ax \equiv -b \pmod{p}$. Then $a(r + kp) + b \equiv ar + b \equiv 0 \pmod{p}$ for all $k \in \{0, 1, 2, \ldots\}$. So every pth term in the sequence is divisible by p (that is, $ar + b$ is divisible by p, $ar + b + p$ is divisible by p, $ar + b + 2p$ is divisible by p, etc.). Since one of these multiples of p must be in the sequence (and hence p-terms later the sequence repeats a multiple of p), then the sequence cannot consist of only primes (any multiple of p greater then p is not prime). That is, the arithmetic progression of primes must be finite in length, as claimed. □

Theorem 22.C

Theorem 22.C. If $f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_2 n^2 + a_1 n + a_0$ is a polynomial function with integer coefficients, and if r is such that $f(r) \equiv 0 \pmod{p}$ for some p, then $f(r + mp) \equiv f(r) \equiv 0 \pmod{p}$ for all $m \in \mathbb{N}$. That is, no polynomial can have only prime values.

Proof. Notice that we cannot have $f(r) \in \{-1, 0, 1\}$ for all $r \in \mathbb{N}$, unless f is a constant function (and constant functions don't count as polynomial functions). So there is $r \in \mathbb{N}$ such that $f(r) \notin \{-1, 0, 1\}$. For p a prime divisor of such $f(r)$, we have $f(r) \equiv 0 \pmod{p}$.

Theorem 22.C

Theorem 22.C. If $f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_2 n^2 + a_1 n + a_0$ is a polynomial function with integer coefficients, and if r is such that $f(r) \equiv 0 \pmod{p}$ for some p, then $f(r + mp) \equiv f(r) \equiv 0 \pmod{p}$ for all $m \in \mathbb{N}$. That is, no polynomial can have only prime values.

Proof. Notice that we cannot have $f(r) \in \{-1, 0, 1\}$ for all $r \in \mathbb{N}$, unless f is a constant function (and constant functions don't count as polynomial functions). So there is $r \in \mathbb{N}$ such that $f(r) \notin \{-1, 0, 1\}$. For p a prime divisor of such $f(r)$, we have $f(r) \equiv 0 \pmod{p}$. Notice that by the Binomial Theorem $(r + mp)^N = \sum_{i=0}^{N} \binom{N}{i} r^{N-i}(mp)^i \equiv r^N \pmod{p}$, so

$$f(r+mp) = a_k(r+mp)^k + a_{k-1}(r+mp)^{k-1} + \cdots + a_2(r+mp)^2 + a_1(r+mp) + a_0$$

$$\equiv a_k r^k + a_{k-1} r^{k-1} + \cdots + a_2 r^2 + a_1 r + a_0 \equiv f(r) \pmod{p}.$$

So, as with arithmetic progressions, every pth term in the sequence is divisible by p, and so is not prime. Hence, no polynomial can have only prime values, as claimed □

Theorem 22.C

Theorem 22.C. If $f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_2 n^2 + a_1 n + a_0$ is a polynomial function with integer coefficients, and if r is such that $f(r) \equiv 0 \pmod{p}$ for some p, then $f(r + mp) \equiv f(r) \equiv 0 \pmod{p}$ for all $m \in \mathbb{N}$. That is, no polynomial can have only prime values.

Proof. Notice that we cannot have $f(r) \in \{-1, 0, 1\}$ for all $r \in \mathbb{N}$, unless f is a constant function (and constant functions don't count as polynomial functions). So there is $r \in \mathbb{N}$ such that $f(r) \not\in \{-1, 0, 1\}$. For p a prime divisor of such $f(r)$, we have $f(r) \equiv 0 \pmod{p}$. Notice that by the Binomial Theorem $(r + mp)^N = \sum_{i=0}^{N} \binom{N}{i} r^{N-i} (mp)^i \equiv r^N \pmod{p}$, so

$$f(r+mp) = a_k(r+mp)^k + a_{k-1}(r+mp)^{k-1} + \cdots + a_2(r+mp)^2 + a_1(r+mp) + a_0$$

$$\equiv a_k r^k + a_{k-1} r^{k-1} + \cdots + a_2 r^2 + a_1 r + a_0 \equiv f(r) \pmod{p}.$$

So, as with arithmetic progressions, every pth term in the sequence is divisible by p, and so is not prime. Hence, no polynomial can have only prime values, as claimed □

Theorem 22.1

Theorem 22.1. There is a real number θ such that $[\theta^{3^n}]$ is a prime for all $n \in \mathbb{N}$.

Proof. Let p_1 be any prime greater than integer A given in Theorem 2.2.D. Define a sequence of prime numbers recursively for $n = 1, 2, \ldots$ where p_{n+1} satisfies $p_n^3 < p_{n+1} < (p_n + 1)^3 - 1$. Notice that such p_{n+1} always exists by Theorem 2.2.D. Let $u_n = p_n^{3^{-n}}$ and $v_n = (p_n + 1)^{3^{-n}}$ for $n = 1, 2, \ldots$. Since $p_{n+1} > p_n^3$ and 3^{-n-1} is a positive exponent, then $p_{n+1}^{3^{-n-1}} > (p_n^3)^{3^{-n-1}}$ and so as n increases, u_n increases because:

$$u_{n+1} = p_{n+1}^{3^{-n-1}} > (p_n^3)^{3^{-n-1}} = p_n^{3^{-n}} = u_n.$$

Theorem 22.1

Theorem 22.1. There is a real number θ such that $[\theta^{3^n}]$ is a prime for all $n \in \mathbb{N}$.

Proof. Let p_1 be any prime greater than integer A given in Theorem 2.2.D. Define a sequence of prime numbers recursively for $n = 1, 2, \ldots$ where p_{n+1} satisfies $p_n^3 < p_{n+1} < (p_n + 1)^3 - 1$. Notice that such p_{n+1} always exists by Theorem 2.2.D. Let $u_n = p_n^{3^{-n}}$ and $v_n = (p_n + 1)^{3^{-n}}$ for $n = 1, 2, \ldots$. Since $p_{n+1} > p_n^3$ and 3^{-n-1} is a positive exponent, then $p_{n+1}^{3^{-n-1}} > (p_n^3)^{3^{-n-1}}$ and so as n increases, u_n increases because:

$$u_{n+1} = p_{n+1}^{3^{-n-1}} > (p_n^3)^{3^{-n-1}} = p_n^{3^{-n}} = u_n.$$

Similarly, since $p_{n+1} < (p_n + 1)^3 - 1$ and 3^{-n-1} is a positive exponent, then $(p_{n+1} + 1)^{3^{-n-1}} < ((p_n + 1)^3 - 1 + 1)^{3^{-n-1}}$ and so as n increases then v_n decreases because:

$$v_{n+1} = (p_{n+1} + 1)^{3^{-n-1}} < ((p_n + 1)^3 - 1 + 1)^{3^{-n-1}} = (p_n + 1)^{3^{-n}} = v_n.$$

Theorem 22.1

Theorem 22.1. There is a real number θ such that $[\theta^{3^n}]$ is a prime for all $n \in \mathbb{N}$.

Proof. Let p_1 be any prime greater than integer A given in Theorem 2.2.D. Define a sequence of prime numbers recursively for $n = 1, 2, \ldots$ where p_{n+1} satisfies $p_n^3 < p_{n+1} < (p_n + 1)^3 - 1$. Notice that such p_{n+1} always exists by Theorem 2.2.D. Let $u_n = p_n^{3^{-n}}$ and $v_n = (p_n + 1)^{3^{-n}}$ for $n = 1, 2, \ldots$. Since $p_{n+1} > p_n^3$ and 3^{-n-1} is a positive exponent, then $p_{n+1}^{3^{-n-1}} > (p_n^3)^{3^{-n-1}}$ and so as n increases, u_n increases because:

$$u_{n+1} = p_{n+1}^{3^{-n-1}} > (p_n^3)^{3^{-n-1}} = p_n^{3^{-n}} = u_n.$$

Similarly, since $p_{n+1} < (p_n + 1)^3 - 1$ and 3^{-n-1} is a positive exponent, then $(p_{n+1} + 1)^{3^{-n-1}} < ((p_n + 1)^3 - 1 + 1)^{3^{-n-1}}$ and so as n increases then v_n decreases because:

$$v_{n+1} = (p_{n+1} + 1)^{3^{-n-1}} < ((p_n + 1)^3 - 1 + 1)^{3^{-n-1}} = (p_n + 1)^{3^{-n}} = v_n.$$

Theorem 22.1 (continued)

Theorem 22.1. There is a real number θ such that $[\theta^{3^n}]$ is a prime for all $n \in \mathbb{N}$.

Proof (continued). Now $u_n = p_n^{3^{-n}} < (p_n + 1)^{3^{-n}} = v_n$, so we now have $u_n < v_n < v_{n-1} < \cdots < v_1$. So $u_n < v_1$ for all $n \in \mathbb{N}$. That is, $\{u_n\}$ is an increasing sequence (and hence nondecreasing) of real numbers that is bounded above by v_1. So by Lemma 22.A, $\{u_n\}$ has a limit, say $\lim_{n\to\infty} u_n = \theta$. Similarly, $v_n > u_n > u_{n-1} > \cdots > u_1$, so we also have $v_n > u_1$ for all $n \in \mathbb{N}$. That is, $\{v_n\}$ is a decreasing sequence (and hence nonincreasing) of real numbers that is bounded below by u_1. So by Lemma 22.B, $\{v_n\}$ has a limit, say $\lim_{n\to\infty} v_n = \varphi$. Since $\{u_n\}$ increases and $\{v_n\}$ decreases, we have $u_n < \theta \le \varphi < v_n$ for all $n \in \mathbb{N}$. Thus $u_n^{3^n} < \theta^{3^n} \le \varphi^{3^n} < v_n^{3^n}$ for all $n \in \mathbb{N}$. Since $u_n^{3^n} = p_n$ and $v_n^{3^n} = p_n + 1$, then we have $p_n < \theta^{3^n} < p_n + 1$. So θ^{3^n} lies between two consecutive *integers*, and hence $[\theta^{3^n}] = p_n$. That is, $[\theta^{3^n}]$ is prime for all $n \in \mathbb{N}$, as claimed. □

Theorem 22.1 (continued)

Theorem 22.1. There is a real number θ such that $[\theta^{3^n}]$ is a prime for all $n \in \mathbb{N}$.

Proof (continued). Now $u_n = p_n^{3^{-n}} < (p_n + 1)^{3^{-n}} = v_n$, so we now have $u_n < v_n < v_{n-1} < \cdots < v_1$. So $u_n < v_1$ for all $n \in \mathbb{N}$. That is, $\{u_n\}$ is an increasing sequence (and hence nondecreasing) of real numbers that is bounded above by v_1. So by Lemma 22.A, $\{u_n\}$ has a limit, say $\lim_{n\to\infty} u_n = \theta$. Similarly, $v_n > u_n > u_{n-1} > \cdots > u_1$, so we also have $v_n > u_1$ for all $n \in \mathbb{N}$. That is, $\{v_n\}$ is a decreasing sequence (and hence nonincreasing) of real numbers that is bounded below by u_1. So by Lemma 22.B, $\{v_n\}$ has a limit, say $\lim_{n\to\infty} v_n = \varphi$. Since $\{u_n\}$ increases and $\{v_n\}$ decreases, we have $u_n < \theta \le \varphi < v_n$ for all $n \in \mathbb{N}$. Thus $u_n^{3^n} < \theta^{3^n} \le \varphi^{3^n} < v_n^{3^n}$ for all $n \in \mathbb{N}$. Since $u_n^{3^n} = p_n$ and $v_n^{3^n} = p_n + 1$, then we have $p_n < \theta^{3^n} < p_n + 1$. So θ^{3^n} lies between two consecutive *integers*, and hence $[\theta^{3^n}] = p_n$. That is, $[\theta^{3^n}]$ is prime for all $n \in \mathbb{N}$, as claimed. □

Lemma 22.E

Lemma 22.E. For $n \geq 2$, we have $\prod_{p \leq n} p \leq 2^{2n}$ where p is prime.

Proof. First, observe that by the Binomial Theorem,

$$2^{2m+1} = (1+1)^{2m+1} = 1 + \binom{2m+1}{1} + \binom{2m}{2} + \cdots + \binom{2m+1}{m} + \binom{2m+1}{m+1}$$

$$+ \cdots + \binom{2m+1}{2m} + 1 \geq \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2\binom{2m+1}{m},$$

and so $2^{2m} \geq \binom{2m+1}{m} = \frac{(2m+1)(2M)\cdots(m+2)}{m(m-1)\cdots(2)(1)}$.

Lemma 22.E

Lemma 22.E. For $n \geq 2$, we have $\prod_{p \leq n} p \leq 2^{2n}$ where p is prime.

Proof. First, observe that by the Binomial Theorem,

$$2^{2m+1} = (1+1)^{2m+1} = 1 + \binom{2m+1}{1} + \binom{2m}{2} + \cdots + \binom{2m+1}{m} + \binom{2m+1}{m+1}$$

$$+ \cdots + \binom{2m+1}{2m} + 1 \geq \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2\binom{2m+1}{m},$$

and so $2^{2m} \geq \binom{2m+1}{m} = \dfrac{(2m+1)(2M)\cdots(m+2)}{m(m-1)\cdots(2)(1)}$. Now $\binom{2m+1}{m}$ is divisible by each prime p such that $m+1 < p \leq 2m+1$, so

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m} \leq 2^{2m}. \qquad (*)$$

Lemma 22.E

Lemma 22.E. For $n \geq 2$, we have $\prod_{p \leq n} p \leq 2^{2n}$ where p is prime.

Proof. First, observe that by the Binomial Theorem,

$$2^{2m+1} = (1+1)^{2m+1} = 1 + \binom{2m+1}{1} + \binom{2m}{2} + \cdots + \binom{2m+1}{m} + \binom{2m+1}{m+1}$$

$$+ \cdots + \binom{2m+1}{2m} + 1 \geq \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2\binom{2m+1}{m},$$

and so $2^{2m} \geq \binom{2m+1}{m} = \frac{(2m+1)(2M)\cdots(m+2)}{m(m-1)\cdots(2)(1)}$. Now $\binom{2m+1}{m}$ is divisible by each prime p such that $m+1 < p \leq 2m+1$, so

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m} \leq 2^{2m}. \qquad (*)$$

Lemma 22.E (continued 1)

Lemma 22.E. For $n \geq 2$, we have $\prod_{p \leq n} p \leq 2^{2n}$ where p is prime.

Proof (continued). We now prove the claim by induction. The claim holds for $n = 2$ since $\prod_{p \leq 2} p = 2 \leq 4 = 2^{2(2)}$, so the base case is established. For the induction hypothesis, suppose the claim holds for all $n \leq k$. If k is odd, then $k+1$ is even and

$$\begin{aligned} \prod_{p \leq k+1} p &= \prod_{p \leq k} p \leq 2^{2k} \text{ by the induction hypothesis} \\ &\leq 2^{2(k+1)}, \end{aligned}$$

and the induction step holds when k is odd.

Lemma 22.E (continued 2)

Lemma 22.E. For $n \geq 2$, we have $\prod_{p \leq n} p \leq 2^{2n}$ where p is prime.

Proof (continued). If k is even, say $k = 2m$, then

$$\begin{aligned} \prod_{p \leq k+1} p &= \left(\prod_{p \leq m+1} p \right) \left(\prod_{m+1 < p \leq 2m+1} p \right) \\ &\leq 2^{2(m+1)} 2^{2m} \text{ by the induction hypothesis and } (*) \\ &= 2^{4m+2} = 2^{2(2m+1)} = 2^{2(k+1)}, \end{aligned}$$

and the induction step holds when k is even. So by induction, the claim holds for all $n \geq 2$. □

Lemma 22.F

Lemma 22.F. For $n \geq 1$, we have $\binom{2n}{n} \geq \frac{2^{2n}}{2n}$.

Proof. We prove the claim by induction. For the base case, with $n = 1$ we have $\binom{2n}{n} = \binom{2}{1} = 2 = \frac{4}{2} = \frac{2^{2(1)}}{2(1)} = \frac{2^{2n}}{2n}$. For the induction hypothesis, suppose the claim holds for $n = k$ so that $\binom{2k}{k} \geq \frac{2^{2k}}{2k}$.

Lemma 22.F

Lemma 22.F. For $n \geq 1$, we have $\binom{2n}{n} \geq \frac{2^{2n}}{2n}$.

Proof. We prove the claim by induction. For the base case, with $n = 1$ we have $\binom{2n}{n} = \binom{2}{1} = 2 = \frac{4}{2} = \frac{2^{2(1)}}{2(1)} = \frac{2^{2n}}{2n}$. For the induction hypothesis, suppose the claim holds for $n = k$ so that $\binom{2k}{k} \geq \frac{2^{2k}}{2k}$. With $n = k + 1$ we have

$$\begin{aligned}\binom{2(k+1)}{k+1} &= \binom{2k+2}{k+1} = \frac{(2k+2)!}{(k+1)!(k+1)!} = \frac{(2k+2)(2k+1)(2k)!}{(k+1)^2 k!k!} \\ &= \frac{2(k+1)(2k+1)}{(k+1)^2}\frac{(2k)!}{k!k!} = \frac{2(k+1)(2k+1)}{(k+1)^2}\binom{2k}{k} \\ &\geq \frac{2(k+1)(2k+1)}{(k+1)^2}\frac{2^{2k}}{2k} \text{ by the induction hypothesis}\end{aligned}$$

Lemma 22.F

Lemma 22.F. For $n \geq 1$, we have $\binom{2n}{n} \geq \frac{2^{2n}}{2n}$.

Proof. We prove the claim by induction. For the base case, with $n = 1$ we have $\binom{2n}{n} = \binom{2}{1} = 2 = \frac{4}{2} = \frac{2^{2(1)}}{2(1)} = \frac{2^{2n}}{2n}$. For the induction hypothesis, suppose the claim holds for $n = k$ so that $\binom{2k}{k} \geq \frac{2^{2k}}{2k}$. With $n = k + 1$ we have

$$
\begin{aligned}
\binom{2(k+1)}{k+1} &= \binom{2k+2}{k+1} = \frac{(2k+2)!}{(k+1)!(k+1)!} = \frac{(2k+2)(2k+1)(2k)!}{(k+1)^2 k!k!} \\
&= \frac{2(k+1)(2k+1)}{(k+1)^2}\frac{(2k)!}{k!k!} = \frac{2(k+1)(2k+1)}{(k+1)^2}\binom{2k}{k} \\
&\geq \frac{2(k+1)(2k+1)}{(k+1)^2}\frac{2^{2k}}{2k} \text{ by the induction hypothesis}
\end{aligned}
$$

Lemma 22.F (continued)

Lemma 22.F. For $n \geq 1$, we have $\binom{2n}{n} \geq \frac{2^{2n}}{2n}$.

Proof (continued). ...

$$\begin{aligned}\binom{2(k+1)}{k+1} &\geq \frac{2(k+1)(2k+1)}{(k+1)^2}\frac{2^{2k}}{2k} \\ &= \frac{2k+1}{k+1}\frac{2^{2k+1}}{2k} = \frac{(2k+2)(2k+1)}{(2k+2)(k+1)}\frac{2^{2k+1}}{2k} \\ &= \frac{2(k+1)}{k+1}\frac{2k+1}{2k}\frac{2^{2k+1}}{2k+2} \geq \frac{2^{2(k+1)}}{2(k+1)},\end{aligned}$$

so the induction step is established. Hence, the claim holds by induction for all $n \in \mathbb{N}$. □

Theorem 22.2. Bertrand's Theorem

Theorem 22.2. Bertrand's Theorem.
For all integers $n \geq 2$, there is a prime p such that $n < p < 2n$.

Proof. ASSUME that for some $n \in \mathbb{N}$ there are no primes p such that $n < p < 2n$ or, equivalently, such that $n < p \leq 2n$. For this value of n, let

$$N = \binom{2n}{n} = \frac{(2n)(2n-1)(2n-2)\cdots(n+1)}{n(n-1)(n-2)\cdots(2)(1)}.$$

Theorem 22.2. Bertrand's Theorem

Theorem 22.2. Bertrand's Theorem.
For all integers $n \geq 2$, there is a prime p such that $n < p < 2n$.

Proof. ASSUME that for some $n \in \mathbb{N}$ there are no primes p such that $n < p < 2n$ or, equivalently, such that $n < p \leq 2n$. For this value of n, let

$$N = \binom{2n}{n} = \frac{(2n)(2n-1)(2n-2)\cdots(n+1)}{n(n-1)(n-2)\cdots(2)(1)}.$$

So if $2n/3 < p \leq n$, then p is a factor of the denominator, and since $2p > 4n/3 \geq n+1$, then $2p$ is a factor of the numerator. The two p's cancel and, since $3p > 2n$, there are no more factors of p in the numerator. Thus all prime divisors of N are at most $2n/3$, so that by Lemma 22.E

$$\prod_{p \mid N} \leq \prod_{p \leq 2n/3} p \leq 2^{2(2n/3)} = 2^{4n/3}. \qquad (*)$$

Theorem 22.2. Bertrand's Theorem

Theorem 22.2. Bertrand's Theorem.
For all integers $n \geq 2$, there is a prime p such that $n < p < 2n$.

Proof. ASSUME that for some $n \in \mathbb{N}$ there are no primes p such that $n < p < 2n$ or, equivalently, such that $n < p \leq 2n$. For this value of n, let

$$N = \binom{2n}{n} = \frac{(2n)(2n-1)(2n-2)\cdots(n+1)}{n(n-1)(n-2)\cdots(2)(1)}.$$

So if $2n/3 < p \leq n$, then p is a factor of the denominator, and since $2p > 4n/3 \geq n+1$, then $2p$ is a factor of the numerator. The two p's cancel and, since $3p > 2n$, there are no more factors of p in the numerator. Thus all prime divisors of N are at most $2n/3$, so that by Lemma 22.E

$$\prod_{p \mid N} \leq \prod_{p \leq 2n/3} p \leq 2^{2(2n/3)} = 2^{4n/3}. \qquad (*)$$

Theorem 22.2. Bertrand's Theorem (continued 1)

Theorem 22.2. Bertrand's Theorem.
For all integers $n \geq 2$, there is a prime p such that $n < p < 2n$.

Proof (continued). By Lemma 21.4, each prime power in the prime-power decomposition of $N = \binom{2n}{n}$ is at most $2n$. So, if p appears in the prime-power decomposition of N to a power greater than 1, then $p^2 \leq 2n$ (in fact if p^k is in the prime-power decomposition then $p^k \leq 2n$, but we only need the case $k = 2$ since if $p^k \leq 2n$, where $k \geq 2$, then also $p^2 \leq 2n$) and so $p \leq \sqrt{2n}$. There are at most $\sqrt{2n}$ such primes, and since each prime power is at most $2n$, so their total contribution to the prime-power decomposition is at most $(2n)^{\sqrt{2n}}$. All of the other primes appear to the power 1 and, from $(*)$, their product is at most $2^{4n/3}$. That is, the prime divisors of N that appear to the power 1 in the prime-power decomposition of N are bounded by $2^{4n/3}$, and those that appear to a power greater than 1 have a product bounded by $(2n)^{\sqrt{2n}}$.

Theorem 22.2. Bertrand's Theorem (continued 1)

Theorem 22.2. Bertrand's Theorem.
For all integers $n \geq 2$, there is a prime p such that $n < p < 2n$.

Proof (continued). By Lemma 21.4, each prime power in the prime-power decomposition of $N = \binom{2n}{n}$ is at most $2n$. So, if p appears in the prime-power decomposition of N to a power greater than 1, then $p^2 \leq 2n$ (in fact if p^k is in the prime-power decomposition then $p^k \leq 2n$, but we only need the case $k = 2$ since if $p^k \leq 2n$, where $k \geq 2$, then also $p^2 \leq 2n$) and so $p \leq \sqrt{2n}$. There are at most $\sqrt{2n}$ such primes, and since each prime power is at most $2n$, so their total contribution to the prime-power decomposition is at most $(2n)^{\sqrt{2n}}$. All of the other primes appear to the power 1 and, from $(*)$, their product is at most $2^{4n/3}$. That is, the prime divisors of N that appear to the power 1 in the prime-power decomposition of N are bounded by $2^{4n/3}$, and those that appear to a power greater than 1 have a product bounded by $(2n)^{\sqrt{2n}}$.

Theorem 22.2. Bertrand's Theorem (continued 2)

Theorem 22.2. Bertrand's Theorem.
For all integers $n \geq 2$, there is a prime p such that $n < p < 2n$.

Proof (continued). Thus $N = \binom{2n}{n} \leq 2^{4/3}(2n)^{\sqrt{2n}}$. By Lemma 22.F, $\binom{2n}{n} \geq \frac{2^{2n}}{2n}$, so we now have $\frac{2^{2n}}{2n} \leq 2^{4n/3}(2n)^{\sqrt{2n}}$. Taking logarithms of this inequality (remember, the log function is increasing and so preserves inequalities), we get $2n \log 2 - \log 2n \leq (4n/3) \log 2 + \sqrt{2n} \log 2n$, or

$$(2n/3) \log 2 \leq (\sqrt{2n} + 1) \log 2n \leq (\sqrt{2n} + \sqrt{2n}) \log 2n = 2\sqrt{2}\sqrt{n} \log 2n,$$

or $\sqrt{n} \leq \frac{2\sqrt{2} \log 2n}{\log 2}$.

Theorem 22.2. Bertrand's Theorem (continued 3)

Theorem 22.2. Bertrand's Theorem.
For all integers $n \geq 2$, there is a prime p such that $n < p < 2n$.

Proof (continued). $\ldots \sqrt{n} \leq \dfrac{2\sqrt{2}\log 2n}{\log 2}$. But $\sqrt{n}$ increases more rapidly that $\log 2n$, then this inequality if false for n sufficiently large. In fact, we can numerically verify that for $n > 2787$ the inequality is false, and we have CONTRADICTION. So the assumption that there are no primes p such that $n < p < 2n$ is false for $n > 2787$, and so the claim holds provided $n > 2787$. By Note 22.C, we see that the claim holds for $n \leq 9973$, and hence the claim holds for all $n \in \mathbb{N}$, as needed. □

Theorem 22.3

Theorem 22.3. There exists a real number θ such that $[2^\theta]$, $[2^{2^\theta}]$, $[2^{2^{2^\theta}}]$, ... are all prime.

Proof. Let p_1 be any prime, and for $n \in \mathbb{N}$ let p_{n+1} be a prime such that $2^{p_2} < p_{n+1} < 2^{p_n+1}$; notice that such a p_{n+1} exists by Theorem 22.2. Let $u_n = \log^{(n)} p_n$ and $v_n = \log^{(n)} \log^{(n)}(p_n + 1)$, where the function $\log^{(n)}$ is defined recursively as: $\log^{(1)} k = \log_2 k$ and $\log^{(n)} k = \log_2(\log^{(n-1)} k)$. Since $2^{p_2} < p_{n+1} < 2^{p_n+1}$, we have by taking logarithms base 2 that

$$\log_2 2^{p_2} < \log_2 p_{n+1} < \log_2 2^{p_n+1} \text{ or } p_n < \log_2 p_{n+1} < p_n + 1.$$

Theorem 22.3

Theorem 22.3. There exists a real number θ such that $[2^\theta]$, $[2^{2^\theta}]$, $[2^{2^{2^\theta}}]$, ... are all prime.

Proof. Let p_1 be any prime, and for $n \in \mathbb{N}$ let p_{n+1} be a prime such that $2^{p_2} < p_{n+1} < 2^{p_n+1}$; notice that such a p_{n+1} exists by Theorem 22.2. Let $u_n = \log^{(n)} p_n$ and $v_n = \log^{(n)} \log^{(n)}(p_n + 1)$, where the function $\log^{(n)}$ is defined recursively as: $\log^{(1)} k = \log_2 k$ and $\log^{(n)} k = \log_2(\log^{(n-1)} k)$. Since $2^{p_2} < p_{n+1} < 2^{p_n+1}$, we have by taking logarithms base 2 that

$$\log_2 2^{p_2} < \log_2 p_{n+1} < \log_2 2^{p_n+1} \text{ or } p_n < \log_2 p_{n+1} < p_n + 1.$$

Since $p_{n+1} + 1 \leq 2^{p_n+1}$ (because $p_{n+1} < 2^{p_n+1}$) then we have

$$p_n < \log^{(1)} p_{n+1} < \log^{(1)}(p_{n+1} + 1) \leq \log^{(1)}(2^{p_n+1}) = p_n + 1.$$

Taking logarithms base 2 of this inequality n times gives

$$\log^{(n)} p_n < \log^{(n+1)} p_{n+1} < \log^{(n+1)}(p_{n+1} + 1) \leq \log^{(n)}(p_n + 1)$$

or $u_n < u_{n+1} < v_{n+1} \leq v_n$.

Theorem 22.3

Theorem 22.3. There exists a real number θ such that $[2^\theta]$, $[2^{2^\theta}]$, $[2^{2^{2^\theta}}]$, ... are all prime.

Proof. Let p_1 be any prime, and for $n \in \mathbb{N}$ let p_{n+1} be a prime such that $2^{p_2} < p_{n+1} < 2^{p_n+1}$; notice that such a p_{n+1} exists by Theorem 22.2. Let $u_n = \log^{(n)} p_n$ and $v_n = \log^{(n)} \log^{(n)}(p_n + 1)$, where the function $\log^{(n)}$ is defined recursively as: $\log^{(1)} k = \log_2 k$ and $\log^{(n)} k = \log_2(\log^{(n-1)} k)$. Since $2^{p_2} < p_{n+1} < 2^{p_n+1}$, we have by taking logarithms base 2 that

$$\log_2 2^{p_2} < \log_2 p_{n+1} < \log_2 2^{p_n+1} \text{ or } p_n < \log_2 p_{n+1} < p_n + 1.$$

Since $p_{n+1} + 1 \leq 2^{p_n+1}$ (because $p_{n+1} < 2^{p_n+1}$) then we have

$$p_n < \log^{(1)} p_{n+1} < \log^{(1)}(p_{n+1} + 1) \leq \log^{(1)}(2^{p_n+1}) = p_n + 1.$$

Taking logarithms base 2 of this inequality n times gives

$$\log^{(n)} p_n < \log^{(n+1)} p_{n+1} < \log^{(n+1)}(p_{n+1} + 1) \leq \log^{(n)}(p_n + 1)$$

or $u_n < u_{n+1} < v_{n+1} \leq v_n$.

Theorem 22.3 (continued)

Theorem 22.3. There exists a real number θ such that $[2^\theta]$, $[2^{2^\theta}]$, $[2^{2^{2^\theta}}]$, ... are all prime.

Proof (continued). ... $u_n < u_{n+1} < v_{n+1} \le v_n$. So sequence $\{u_n\}$ is an increasing (that is, nondecreasing) sequence which is bounded above by v_1, so that it converges by Lemma 22.A, say $\lim_{n\to\infty} u_n = \theta$. Sequence $\{v_n\}$ is a nonincreasing sequence which is bounded below below by u_1, so that it converges by Lemma 22.B, say $\lim_{n\to\infty} v_n = \varphi$. Define $\exp^{(n)} k$ recursively as: $\exp^{(1)} k = 2^k$ and $\exp^{(n)} k = 2^{\exp^{(n+1)} k}$. Since $u_n < \theta < v_n$ for all $n \in \mathbb{N}$, then $\exp^{(n)} u_n < \exp^{(n)} \theta < \exp^{(n)} v_n$, or $p_n < \exp^{(n)} < p_n + 1$. Since $\exp^{(n)} \theta$ lies between two consecutive *integers*, then $[\exp^{(n)} \theta] = p_n$. That is, $[\exp^{(n)} \theta]$ is prime for all $n \in \mathbb{N}$. Since $\exp^{(n)} k$ is defined as an iterated composition of base 2 exponential functions, then we have that each of $[2^\theta]$, $[2^{2^\theta}]$, $[2^{2^{2^\theta}}]$, ... are prime, , as claimed. □

Theorem 22.3 (continued)

Theorem 22.3. There exists a real number θ such that $[2^\theta]$, $[2^{2^\theta}]$, $[2^{2^{2^\theta}}]$, ... are all prime.

Proof (continued). ... $u_n < u_{n+1} < v_{n+1} \leq v_n$. So sequence $\{u_n\}$ is an increasing (that is, nondecreasing) sequence which is bounded above by v_1, so that it converges by Lemma 22.A, say $\lim_{n\to\infty} u_n = \theta$. Sequence $\{v_n\}$ is a nonincreasing sequence which is bounded below below by u_1, so that it converges by Lemma 22.B, say $\lim_{n\to\infty} v_n = \varphi$. Define $\exp^{(n)} k$ recursively as: $\exp^{(1)} k = 2^k$ and $\exp^{(n)} k = 2^{\exp^{(n+1)} k}$. Since $u_n < \theta < v_n$ for all $n \in \mathbb{N}$, then $\exp^{(n)} u_n < \exp^{(n)} \theta < \exp^{(n)} v_n$, or $p_n < \exp^{(n)} < p_n + 1$. Since $\exp^{(n)} \theta$ lies between two consecutive *integers*, then $[\exp^{(n)} \theta] = p_n$. That is, $[\exp^{(n)} \theta]$ is prime for all $n \in \mathbb{N}$. Since $\exp^{(n)} k$ is defined as an iterated composition of base 2 exponential functions, then we have that each of $[2^\theta]$, $[2^{2^\theta}]$, $[2^{2^{2^\theta}}]$, ... are prime, , as claimed. □