Bertrand's Postulate

James Bang

November 23, 2019

1 Introduction

A **Prime Number** p is any positive integer for which, given two integers a, b with $p \mid ab$, then we have either $p \mid a$ or $p \mid b$ (or both). Across $\mathbb{Z}^+$, it can be thought as any number greater than 1 which has only two factors, 1 and itself. For many, the sequence of prime numbers show no obvious pattern and often thought to be almost random; however, while there are no simple local patterns, there are in fact many properties regarding their distribution which are striking by nature.

One of these properties is known as **Bertrand's Postulate,** which states that for any positive integer $n \geq 2$, there exists a prime number p for which $n < p < 2n$, i.e. there must always be a prime number between n and $2n$ for each $n \geq 2$. Equivalently, this means if the primes were arranged in ascending order $p_1 < p_2 < \ldots$, then we must have $p_{n+1} < 2 \cdot p_n$ (why is this true?). This handout explores Bertrand's Postulate, its proofs and generalisations, and its role in solving Olympiad mathematical problems.

2 A few weaker bounds

Proving distribution-related properties about prime numbers is generally very difficult, and require very clever ideas. Hence, it may be worth exploring some weaker results than Bertrand's Postulate.

2.1 Bound from Euclid's Infinitude of Primes

Problem 2.1

For each $n \geq 2$, there exists a prime number p such that

$$n \leq p \leq n! + 1.$$

Essentially, this result follows from **Euclid's Infinitude of Primes** result. Suppose there is only a finite number of primes $p_1 < p_2 < \cdots < p_k$ for some k: then the number $P = p_1 p_2 \ldots p_k + 1$ has a prime factor which is not any of the p_i, which is a contradiction.

Now, how does this relate to our bound above? Consider the number $n! + 1$ – this number, as per Euclid's proof, has no prime factor which is $\leq n$ since all such primes divide $n!$ and thus not $n! + 1$. However, $n! + 1$ also has a prime factorisation, and thus has a prime factor p. This p satisfies $n \leq p \leq n! + 1$, and thus we are done. $\square$

This proof can obviously be strengthened by not multiplying all of $1, 2, \ldots, n$, and only multiplying the prime numbers below n. However, even when removing excess terms, this result is far from acceptable compared to Bertrand's: we define the **primordial** $n\# = \prod_{p \leq n} p$: then, a consequence of the Prime

Number Theorem states $n\# \sim e^n$, which gives the best possible bounds along these lines as there exists a prime p satisfying
$$n < p < (e + o(1))^n.$$
The right side is still exponential in n, and thus this leaves a lot to be strengthened for the linear bound as per Bertrand's Postulate.

2.2 Erdös' Quadratic Bound

Problem 2.2

For each $n \geq 2$, there exists a prime number p such that
$$n \leq p \leq n^2.$$

Erdös' idea for obtaining such a quadratic bound was to bound a binomial coefficient $\binom{n^2}{n}$: this is a good idea, since the binomial coefficient is rather large but is divisible only by primes at most n^2, much smaller than the coefficient. By bounding the coefficient, we can find a contradiction that it is much smaller than it should be.

Proof. Define the **Prime Counting Function** $\pi(x)$ as the number of primes that exist which are at most x, i.e. $\pi(x) = \sum_{p \leq x} 1$. We assume the statement is false for some $n \geq 9$ (the smaller cases which may be checked by hand): this assumption gives $\pi(n^2) = \pi(n)$ since there are no primes between n and n^2. We also have $\pi(n) < \frac{n}{2}$ by an obvious induction (or just notice that the only even prime is 2, and lots of odd numbers are not prime anyway).

Lower Bound for $\binom{n^2}{n}$. We have
$$\binom{n^2}{n} = \frac{n^2(n^2-1)\dots(n^2-n+1)}{n(n-1)\dots(1)} = \frac{n^2}{n} \cdot \frac{n^2-1}{n-1} \cdot \dots \cdot \frac{n^2-n+1}{1} > \frac{n^2}{n} \cdot \frac{n^2}{n} \cdot \dots \cdot \frac{n^2}{n} = n^n,$$
because adding the same number to the numerator and denominator decreases it.

Upper Bound for $\binom{n^2}{n}$. It is obvious from the expansion that $\binom{n^2}{n}$ only has primes $p < n^2$, since any larger prime cannot divide $n^2 - k$ for any $k = 0, 1, \dots, n-1$.

Recall **Legendre's Formula,** which states that
$$\nu_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor,$$
where the **p-adic valuation** $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ is defined by
$$\nu_p(n) = \begin{cases} \alpha, & \text{if } \alpha \in \mathbb{Z} : \ p^\alpha \mid n, \ p^{\alpha+1} \nmid n \\ +\infty, & \text{if } n = 0. \end{cases}$$

Also, we have $\lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \in \{0, 1\}$ (which can be checked quite easily by hand) and thus is at most 1. Hence, using the above, we have
$$\nu_p \binom{n^2}{n} = \nu_p((n^2)!) - \nu_p(n!) - \nu_p((n^2-n)!) = \sum_{k=1}^{\lfloor \log_p(n^2) \rfloor} \left(\left\lfloor \frac{n^2}{p^k} \right\rfloor - \left\lfloor \frac{n^2-n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor \right) \leq \lfloor \log_p(n^2) \rfloor.$$

Hence, we have

$$\binom{n^2}{n} = \sum_{1\le p\le n^2} p^{\nu_p\binom{2n}{n}} < \sum_{1\le p\le n^2} p^{\log_p(n^2)} = \sum_{1\le p\le n^2} n^2 = (n^2)^{\pi(n^2)} = (n^2)^{\pi(n)} \le (n^2)^{n/2} = n^n.$$

It follows that we have established two contradicting bounds, $n^n > \binom{2n}{n} > n^n$, and thus the contradiction yields the desired result. $\square$

This quadratic bound of $n \le p \le n^2$ is a much better generalisation of the previous bound $n \le p \le n!+1$ or even the $n \le p \le (e+o(1))^n$, as we now have a polynomial bound. However, this is still quite inferior to Bertrand's Postulate which gives a linear bound. So, how exactly do we prove Bertrand's Postulate?

3 Proof of Bertrand's Postulate

Fortunately, a lot of the theory from Erdös' proof of the quadratic bound translates to the proof of Bertrand's Theorem[1]. However, instead of bounding the coefficient $\binom{n^2}{n}$, we consider the coefficient $\binom{2n}{n}$: heuristically, this would lead a better bound, because the size of the coefficient is much larger than the possible primes which can divide this coefficient.

Problem 3.0

For each $n \ge 2$, there exists a prime number p such that

$$n < p < 2n.$$

Proof. As before, we split the proof into a contradicting lower bound and upper bound for $\binom{2n}{n}$. This also only proves Bertrand's Postulate for $n \ge 128$; however, this is not a problem since we may merely find a sequence of primes, for example $3, 5, 7, 13, 23, 43, 83$, where each prime is less than twice its predecessor.

Lower Bound for $\binom{2n}{n}$. Recall the very well known **Binomial Expansion**

$$4^n = 2^{2n} = \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{2n}{2n},$$

and it is well known that the central binomial coefficient $\binom{2n}{n}$ is the largest out of them all, and furthermore it is also trivially greater than the sum $\binom{2n}{0} + \binom{2n}{2n} = 2$. Hence, we get the trivial lower bound,

$$4^n = \left(\binom{2n}{0} + \binom{2n}{2n}\right) + \binom{2n}{1} + \binom{2n}{2} + \cdots + \binom{2n}{2n-1} < 2n\binom{2n}{n} \implies \boxed{\binom{2n}{n} > \frac{4^n}{2n}.}$$

Upper Bound for $\binom{2n}{n}$. Recall by Legendre's Formula as before, that

$$\nu_p\binom{2n}{n} = \nu_p\left(\frac{(2n)!}{(n!)^2}\right) = \sum_{k\ge1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - \left\lfloor\frac{n}{p^k}\right\rfloor - \left\lfloor\frac{n}{p^k}\right\rfloor\right) = \sum_{k\ge1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right).$$

Lemma ($\diamondsuit$): Let $n \ge 3$ and p is prime. Then, we have

(a) $p^{\nu_p\binom{2n}{n}} \le 2n$,

(b) If $p > \sqrt{2n}$, then $\nu_p\binom{2n}{n} \le 1$;

(c) If $\frac{2n}{3} < p \le n$, then $p \nmid \binom{2n}{n}$ (and thus $\nu_p\binom{2n}{n} = 0$).

[1]because, guess what, this proof is also due to Erdös.

Proof. Denote $\nu_p\binom{2n}{n}$ for ν_p for convenience. For (a), it is easy to see that $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0,1\}$, and furthermore if $x < 1/2$ then it must be equal to zero. Hence, the summand

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor = 0$$

for each k with $2n < p^k$, or equivalently $k > \log_p(2n)$. Hence, we have

$$\nu_p = \sum_{k\geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right) = \sum_{k\geq 1}^{\lfloor \log_p(2n) \rfloor} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right) \leq \lfloor \log_p(2n) \rfloor \leq \log_p(2n),$$

whence $p^{\nu_p} \leq 2n$. To prove (b), notice that $\sqrt{2n} < p$ implies $p^2 > 2n$, and so by (a) we have $s \leq 1$. To prove (c), notice that $2n/3 < p < 2n$ means $p^2 > 2n$, and hence $\nu_p = \left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor$. However, we have $1 \leq n/p < 3/2$, and it becomes a routine computation to show that $\nu_p = 2 - 2(1) = 0$. $\square$

Lemma ($\heartsuit$)**:** Let $n \geq 2$. Then

$$n\# = \prod_{p\leq n} p < 4^n.$$

Proof. Obviously this is weaker than the $(e + o(1))^n$ bound given by the Prime Number Theorem, but an elementary solution exists to this lemma. We proceed by strong induction over n: for $n = 2$, we have $n\# = 2 < 2^2 = 4$, and hence this holds for the base case.

Suppose, by strong induction, that for some $N \geq 2$, this statement is true for every $k \leq N$. To show for $N + 1$:

- If $N + 1$ is not prime, then we have $(N + 1)\# = N\# < 4^N < 4^{N+1}$, and the inductive step has been completed.

- If $N + 1$ is prime, then it must be odd (since $N \geq 2$). Let $N + 1 = 2M + 1$ for some integer M, so

  $$\prod_{M+1<p\leq 2M+1} p \mid \binom{2M+1}{M+1};$$

  hence, we have

  $$(N+1)\# = \prod_{p\leq 2M+1} p = \left(\prod_{1\leq p\leq M+1} p \right) \times \left(\prod_{M+1<q\leq 2M+1} q \right) < \left(4^{M+1}\right) \times \binom{2M}{M+1}$$

  where we have used the inductive hypothesis for $M + 1$, and also used $\prod_{M+1<p\leq 2M} p \leq \binom{2M}{M+1}$. However, we also have

  $$2^{2M+1} = \binom{2M+1}{0} + \binom{2M+1}{1} + \cdots + \binom{2M+1}{2M+1} < \binom{2M+1}{M} + \binom{2M+1}{M+1} = 2\binom{2M+1}{M+1}$$

  $$\implies \binom{2M+1}{M+1} < 2^{2M},$$

  and thus

  $$(N+1)\# \ll 4^{M+1} \cdot 2^{2M} = 4^{2M+1} = 4^{N+1},$$

  and the inductive step has been completed. Hence, the initial statement $n\# < 4^n$, is true for all $n \geq 2$ by mathematical induction. $\square$

Now, we can prove Bertrand's Postulate. Suppose there are no primes $n < p < 2n$ for some integer n. This means $\nu_p\binom{2n}{n} = 0$ for each $n \le p \le 2n$; thus, all prime factors must be at most n. We decompose $\binom{2n}{n}$ into its prime factors:

$$\binom{2n}{n} = \prod_{p\le n} p^{\nu_p} = \prod_{p\le 2n/3} p^{\nu_p},$$

where the second inequality follows by (c) from $\diamondsuit$ since $\nu_p = 0$ for $2n/3 < p \le n$. Furthermore, since we had $\nu_p \le 1$ for each $p > 2n$, we can further express this product as

$$\binom{2n}{n} \le \prod_{p\le\sqrt{2n}} p^{\nu_p} \cdot \prod_{\sqrt{2n}<p<2n/3} p.$$

We now estimate this product: for the first product, since $p^{\nu_p} \le 2n$, this is at most $(2n)^{\sqrt{2n}/2-1}$ since the number of primes $p \le \sqrt{2n}$ is at most $\frac{\sqrt{2n}}{2} - 1$ since 1 and evens are not primes. For the second product, we have

$$\prod_{\sqrt{2n}<p<2n/3} p < \prod_{p<2n/3} p = (2n/3)\# < 4^{2n/3}.$$

Hence, we have

$$\frac{2^{2n}}{2n} < \binom{2n}{n} \le (2n)^{\sqrt{2n}/2-1} \times 4^{2n/3} \implies 4^{n/3} < (2n)^{\sqrt{n}/2}.$$

After taking logs, this becomes equivalent to

$$2\sqrt{2n}\log(2) - 3\log(2n) < 0.$$

However, this inequality turns out not to hold for any $n \ge 50$, as shown in the graph below: (this can be rigorously proven using calculus, but we shall not go into this here.)

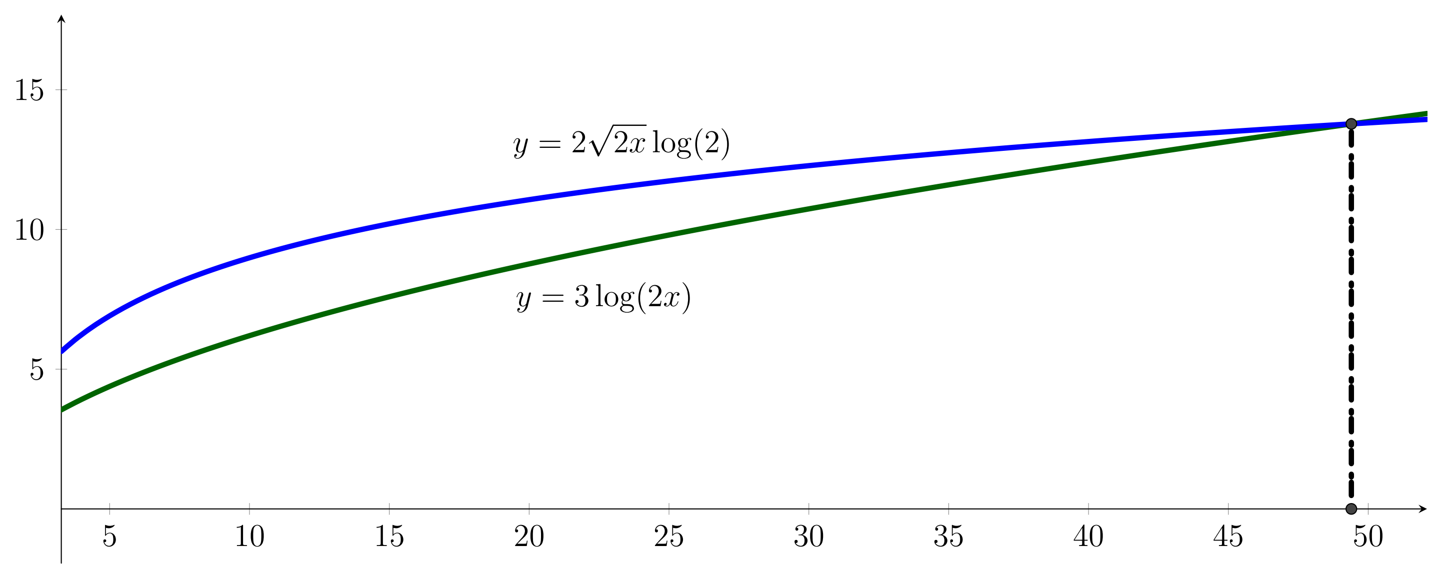

Figure 1: The inequality fails for each $n \ge 50$.

Hence, these results show Bertrand's Postulate for each $n \ge 50$. It remains to show them in the cases for $n \le 49$, which can be done by constructing a sequence of primes as done before. $\square$

4 Can Bertrand's Postulate be strengthened?

Clearly, Bertrand's Postulate is a major strengthening of the previous results we have discussed above. However, this result itself can be strengthened much more, owing to more technical mathematics: in general, as n grows extremely large, we can find many such primes between each such interval.

Problem 4.0

For each $\epsilon > 0$, there exists some $N = N(\epsilon)$ for which, the number of prime numbers $f(n)$ between n and $2n$ satisfies

$$f(n) \geq \left(\frac{2}{3} - \epsilon\right) \cdot \frac{n}{1 + \log_2(n)}.$$

Proof. In the proof for Bertrand's Postulate as per above, we instead write

$$\binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} p^{\nu_p} \cdot \prod_{\sqrt{2n} < p < 2n/3} p \cdot \prod_{n \leq p \leq 2n} p,$$

for which this achieves

$$\frac{4^n}{2n} \leq (2n)^{\sqrt{2n}/2 - 1} \times 4^{2n/3} \times (2n)^{f(n)}$$

since we have $p < 2n$ for each p within that interval. Hence, after logging, we instead get

$$n\log(4) - \log(2n) \leq \left(\frac{\sqrt{2n}}{2} - 1\right)\log(2n) + \frac{2n}{3}\log(4) + f(n) \cdot \log(2n)$$

$$f(n) \geq \frac{2n}{3\log(2n)}\log(2) - \frac{\sqrt{2n}}{2} \geq \left(\frac{2}{3} - \epsilon\right) \cdot \frac{n}{1 + \log_2(n)}$$

for any $\epsilon > 0$ given $n \geq N$, since the $c\sqrt{n}$ term on the right is negligible compared to the $cn/\log(n)$ term. $\square$

In particular, this statement means there are actually a lot more primes in the region than the Bertrand's Postulate which only guarantees at least one. However, the above theorems does not give too much of an effective bound as to how large N has to be given ϵ.

4.1 The Prime Number Theorem

The **Prime Number Theorem** is the statement that for a given x, we have

$$\pi(x) \sim \frac{x}{\log x}$$

where π denotes the prime-counting function (as discussed before). This statement is equivalent to the fact that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

This theorem can be used to slightly strengthen the fact proved above: we have $\pi(2x) \sim \frac{2x}{\log(2x)} \approx \frac{2x}{\log x}$, since $\log(2x) = \log x + \log 2$ and this $\log 2$ term becomes insignificant as $x \to \infty$. Hence, we obtain

$$\pi(2x) - \pi(x) \sim \frac{2x}{\log x} \sim \frac{x}{\log x} = \frac{x}{\log x},$$

which means there are about $\frac{x}{\log(x)}$ prime numbers between x and $2x$ as x approaches $+\infty$. However, the proof of the PNT is not elementary[2], and hence we shall not cover it here.

[2]It's equivalent to the fact that the Riemann Zeta function $\zeta(s)$ has no zeroes along the line $\Re(s) = 1$.

5 Example Problems

Problem 5.0

Let $n \geq 2$ be an integer. Show that the n-th **Harmonic Number**

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

is **not** an integer.

Proof. By Bertrand's Theorem, there exists some prime p for which $n/2 < p \leq n$. Notice that this implies p divides exactly one denominator of the fractions, namely $1/p$. Hence, we express

$$H_n = \frac{1}{p} + \left[1 + \frac{1}{2} + \cdots + \frac{1}{n} - \frac{1}{p}\right] = \frac{1}{p} + \frac{m}{n} = \frac{n + mp}{pn}$$

where m, n are coprime. In the bracketed part, none of the denominators are divisible by p (by assumption, since we took $1/p$ out), and hence $p \nmid n$. It follows that $p \nmid n + mp$, i.e. H_n cannot be an integer for $n \geq 2$. $\square$

Problem 5.0

Find all positive integer solutions (m, n) to the equation $n! = m^2$.

Proof. Similar to the above question, by Bertrand's Theorem, we can find a prime $n/2 < p \leq n$ when $n \geq 2$. It can easily be seen that this prime divides exactly one of the numbers $1, 2, \ldots, n$, and thus divides $n!$ exactly once. This means $n!$ cannot be a perfect square for any $n \geq 2$, since if it is a square then any exponent of the prime in the factorisation must be even.

For $n = 1$, we trivially have $(m, n) = (1, 1)$ as the solution. $\square$

6 Problem Section

1. Is $(n + 1)!$ divisible by $\text{lcm}[1, ..., 2n]$ for $n \geq 2$?

2. Prove, using Bertrand's Theorem, that there exist infinitely many primes which are not Fibonacci numbers.

3. Let p_k be the k-th prime by size. Prove that $p_k \leq 2^{k-1}$.

4. For an integer $n > 3$, denote by $\psi(n)$ the product of all prime numbers less than n. Show that if $\psi(n) = 2n + 16$, then $n = 7$.

5. **(Austria 2008)** For every positive integer n, let $a_n = \displaystyle\sum_{k=n}^{2n} \frac{(2k+1)^n}{k}$. Show that there exists no n, for which a_n is a non-negative integer.

6. Find all prime numbers p for which $\dfrac{p^2}{1 + \frac{1}{2} + \cdots + \frac{1}{p-1}}$ is a perfect square.

7. Is it possible to split the set $X = \{1, \frac{1}{2}, \ldots, \frac{1}{n}\}$ into two disjoint sets A and B, such that the sums of the elements in each set are equal?

8. Given a prime $p \geq 13$. Can you always find integers $q, r \geq 1$ such that $1 < q < r < p+1$, such that

$$p + 1 \mid qr + 1 \quad ?$$

9. **(Estonia 1997)** Determine all positive integers n with the following property: Every integer $m > 1$ less than n and coprime to n is prime.

10. **(Greenfield)** Prove that for $n \geq 1$, the set $\{1, 2, \ldots, n\}$ can be partitioned into pairs

$$\{a_1, b_1\}, \{a_2, b_2\}, \ldots, \{a_n, b_n\}$$

such that for each $1 \leq i \leq n$, $a_i + b_i$ is a prime number.

11. Find all pair of positive integers (m, n) such that $m! = 2 \cdot (n!)^2$.

12. **(IMOSL 2000)** Determine all positive integers $n \geq 2$ that satisfy the following condition: for all a and b relatively prime to n we have $a \equiv b \pmod{n}$ if and only if $ab \equiv 1 \pmod{n}$.

13. **(APMO 1998)** Find the largest integer n such that n is divisible by all positive integers less than $\sqrt[3]{n}$.

14. **(Rioplatense 2012)** Let $a \geq 2$ and $n \geq 3$ be integers. Prove that one of the numbers $a^n + 1, a^{n+1} + 1, \ldots, a^{2n-2} + 1$ does not share any **odd** divisor greater than 1 with any of the other numbers.

15. **(MEMO 2007)** Determine all pairs (x, y) of positive integers satisfying the equation $x! + y! = x^y$.

16. **(MEMO 2017)** For an integer $n \geq 3$ we define the sequence $\alpha_1, \alpha_2, \ldots, \alpha_k$ as the sequence of exponents in the prime factorization of $n! = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where $p_1 < p_2 < \ldots < p_k$ are primes. Determine all integers $n \geq 3$ for which $\alpha_1, \alpha_2, \ldots, \alpha_k$ is a geometric progression.

17. **(Inspired by IMO 2019)** Find all pairs of positive integers (n, k), such that

$$k! = (2^n - 1)(2^n - 2)(2^n - 3) \cdots (2^n - 2^{n-1}).$$

18. **(China 2015)** Determine all integers k such that there exists infinitely many positive integers n **NOT** satisfying

$$n + k \mid \binom{2n}{n}.$$

19. **(RMM 2017)** Determine all positive integers n satisfying the following condition: for every monic polynomial P of degree at most n with integer coefficients, there exists a positive integer $k \leq n$ and $k+1$ distinct integers $x_1, x_2, \cdots, x_{k+1}$ such that

$$P(x_1) + P(x_2) + \cdots + P(x_k) = P(x_{k+1}).$$

20. Prove that every number $n > 6$ can be written as the sum of some number of **distinct** prime numbers.

21. **(USAMO 2012)** Determine which integers $n > 1$ have the property that there exists an infinite sequence $a_1, a_2, a_3, \ldots$ of nonzero integers such that the equality

$$a_k + 2a_{2k} + \ldots + na_{nk} = 0$$

holds for every positive integer k.

22. **(Serbia 2017)** Let k be a positive integer and let n be the smallest number with exactly k divisors. Given n is a cube, is it possible that k is divisible by a prime factor of the form $3j + 2$?