Extracting the First Prime Greater than m

Henry Shin

May 1, 2026

Abstract

For an integer $m \geq 3$, define

$$d = \gcd\big((m!)^{m!} - 1, (2m)!\big), \qquad t = \frac{d^d}{\gcd(d^d, d!)}.$$

Let a be the largest nonnegative integer such that $d^a \mid t$. We prove that

$$\frac{d}{\gcd\left(t/d^a, d\right)}$$

is the smallest prime greater than m. The construction has two stages: first d isolates exactly the primes in the interval $(m, 2m)$, and then the factorial $d!$ distinguishes the smallest of those primes by giving it the largest valuation.

Introduction

This problem was mentioned to me on IRC. The following argument explains why the construction works: one stage isolates a finite set of primes, and the other uses factorial valuations to distinguish its smallest member.

There are two separate filters in the formula. The first filter is

$$d = \gcd\big((m!)^{m!} - 1, (2m)!\big).$$

The factor $(2m)!$ prevents primes larger than $2m$ from appearing, while the congruence condition modulo $(m!)^{m!} - 1$ prevents primes at most m from appearing. What remains is precisely the set of primes strictly between m and $2m$.

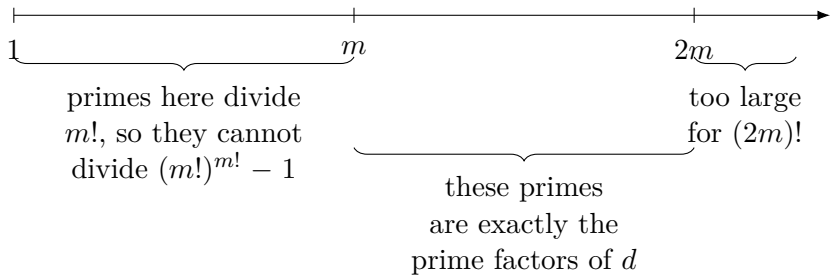


Figure 1: The first gcd filters primes according to their position relative to m.

The second filter is more subtle. Once d has been shown to be a squarefree product

$$d = p_1 p_2 \cdots p_k, \qquad m < p_1 < p_2 < \cdots < p_k < 2m,$$

the number d^d gives each prime factor p_i the same exponent d. Dividing by $\gcd(d^d, d!)$ subtracts the exponent with which p_i appears in $d!$. Smaller primes appear more often in $d!$, so the smallest prime p_1 is the one whose exponent is reduced the most. The definition of a then removes the common remaining power of d, and the final gcd detects which primes are still present. Exactly one prime has disappeared: p_1.

Statement

Theorem 1. *Let $m \geq 3$ be an integer. Define*

$$d = \gcd\big((m!)^{m!} - 1, (2m)!\big),$$

$$t = \frac{d^d}{\gcd(d^d, d!)}.$$

Let a be the largest nonnegative integer such that $d^a \mid t$. Then

$$\frac{d}{\gcd\left(\dfrac{t}{d^a}, d\right)}$$

is the smallest prime greater than m.

Proof

For a prime p and a positive integer N, write $\nu_p(N)$ for the exponent of p in the prime factorization of N.

We shall use Bertrand's postulate in the following form: for every integer $n > 1$, there is a prime p such that

$$n < p < 2n.$$

For completeness, an elementary proof of this fact is included in the appendix.

Lemma 1 (The first gcd)**.** *Let*

$$\mathcal{P}_m = \{p : \ p \text{ is prime and } m < p < 2m\}.$$

Then

$$d = \prod_{p \in \mathcal{P}_m} p.$$

In particular, d is squarefree and $d \neq 1$.

Proof. First suppose that a prime p divides d. Since $p \mid (2m)!$, we have $p \leq 2m$. On the other hand, $p \nmid m!$, because if $p \mid m!$, then

$$(m!)^{m!} - 1 \equiv -1 \pmod{p},$$

which is incompatible with $p \mid d$. Therefore $p > m$. Since $m \geq 3$, the endpoint $2m$ is composite, so $p \neq 2m$. Hence

$$m < p < 2m.$$

Thus every prime divisor of d lies in $\mathcal{P}_m$.

Conversely, let $p \in \mathcal{P}_m$. We prove that $p \mid d$. Since $p > m$, the prime p does not divide $m!$. Hence Fermat's little theorem gives

$$(m!)^{p-1} \equiv 1 \pmod{p}.$$

It remains to know that the exponent $m!$ is compatible with this congruence.

Except for the small case $(m, p) = (3, 5)$, one has

$$p - 1 \mid m!.$$

Indeed, write

$$p - 1 = 2q, \qquad q = \frac{p-1}{2}.$$

If $p = 5$, then $m = 3$ or $m = 4$. The case $m = 4$ gives $4 = p - 1 \mid 4!$, while the case $m = 3$ is the exceptional case just mentioned. If $p > 5$, then $q \geq 3$, and from $p < 2m$ we get $q < m$. Thus 2 and q are distinct factors occurring in $m!$, so

$$p - 1 = 2q \mid m!.$$

Therefore, outside the exceptional case,

$$(m!)^{m!} \equiv 1 \pmod{p}.$$

In the exceptional case $(m, p) = (3, 5)$, we have $m! = 6 \equiv 1 \pmod{5}$, so again

$$(m!)^{m!} \equiv 1 \pmod{p}.$$

Thus in every case $p \mid (m!)^{m!} - 1$.

Also $p \mid (2m)!$, since $p < 2m$. Hence $p \mid d$. Moreover, because $p > m$, we have $2p > 2m$, so p occurs exactly once in $(2m)!$. Consequently p occurs exactly once in d.

We have shown that the prime divisors of d are exactly the primes in $\mathcal{P}_m$, each with exponent 1. Hence

$$d = \prod_{p \in \mathcal{P}_m} p.$$

Finally, Bertrand's postulate ensures that $\mathcal{P}_m$ is nonempty, so $d \neq 1$. □

Now list the primes in $\mathcal{P}_m$ in increasing order:

$$\mathcal{P}_m = \{p_1, p_2, \ldots, p_k\}, \qquad p_1 < p_2 < \cdots < p_k.$$

By the lemma,

$$d = p_1 p_2 \cdots p_k.$$

Here $k \geq 1$.

Lemma 2 (The exponent filter)**.** *For each i, set*

$$f_i = \nu_{p_i}(d!).$$

Then

$$f_1 > f_2 > \cdots > f_k$$

whenever $k > 1$. Consequently, if

$$t = \frac{d^d}{\gcd(d^d, d!)},$$

then the largest nonnegative integer a such that $d^a \mid t$ is

$$a = d - f_1.$$

Proof. Since $d = p_1 p_2 \cdots p_k$ is squarefree, the exponent of p_i in d^d is exactly d. Also

$$f_i = \nu_{p_i}(d!) = \left\lfloor \frac{d}{p_i} \right\rfloor + \left\lfloor \frac{d}{p_i^2} \right\rfloor + \left\lfloor \frac{d}{p_i^3} \right\rfloor + \cdots .$$

Because $p_i > m \geq 3$, we have $p_i \geq 5$, and therefore

$$f_i \leq \frac{d}{p_i} + \frac{d}{p_i^2} + \frac{d}{p_i^3} + \cdots = \frac{d}{p_i - 1} < d.$$

Hence the exponent of p_i in $\gcd(d^d, d!)$ is exactly f_i, and so

$$t = \prod_{i=1}^{k} p_i^{d - f_i}.$$

It remains to compare the numbers f_i. If $i < j$, then $p_i < p_j$, so for every positive integer r,

$$\left\lfloor \frac{d}{p_i^r} \right\rfloor \geq \left\lfloor \frac{d}{p_j^r} \right\rfloor .$$

For $r = 1$, the inequality is strict, since d/p_i and d/p_j are integers and

$$\frac{d}{p_i} > \frac{d}{p_j}.$$

Thus $f_i > f_j$. In particular,

$$f_1 > f_2 > \cdots > f_k$$

when $k > 1$.

Let

$$e_i = d - f_i.$$

Then

$$t = \prod_{i=1}^{k} p_i^{e_i},$$

and the inequalities among the f_i reverse to give

$$e_1 < e_2 < \cdots < e_k$$

when $k > 1$. Since d is squarefree, $d^a \mid t$ exactly when every exponent e_i is at least a. Therefore the largest possible a is

$$a = \min_i e_i = e_1 = d - f_1.$$

The same formula is also valid when $k = 1$, where the minimum consists of the single exponent e_1. □

We can now finish the proof of the theorem. By the preceding lemma,

$$a = d - f_1.$$

Therefore

$$\frac{t}{d^a} = \frac{\prod_{i=1}^{k} p_i^{d - f_i}}{\prod_{i=1}^{k} p_i^{d - f_1}} = \prod_{i=1}^{k} p_i^{f_1 - f_i}.$$

The exponent of p_1 in this product is 0, while for every $i > 1$, the exponent of p_i is positive. Hence

$$\gcd\left(\frac{t}{d^a}, d\right) = p_2 p_3 \cdots p_k,$$

where the empty product is interpreted as 1 when $k = 1$. It follows that

$$\frac{d}{\gcd\left(\frac{t}{d^a}, d\right)} = \frac{p_1 p_2 \cdots p_k}{p_2 p_3 \cdots p_k} = p_1.$$

By construction, p_1 is the smallest prime in the interval $(m, 2m)$. Bertrand's postulate ensures that the least prime greater than m lies in this interval. Therefore p_1 is the smallest prime greater than m, as claimed.

Appendix: Bertrand's Postulate

For completeness, we include a standard elementary proof of the form of Bertrand's postulate used above.

Lemma 3. *For every real number $x \geq 1$,*

$$\prod_{p \leq x} p < 4^x,$$

where the product is over primes $p \leq x$.

Proof. It suffices to prove the claim for positive integers $x = N$, since replacing x by $\lfloor x \rfloor$ can only decrease the left-hand side.

We prove the integer case by strong induction on N. The cases $N = 1, 2$ are immediate. Suppose the result is known for all positive integers smaller than N.

First let $N = 2r$. The product of the primes p with $r < p \leq 2r$ divides the binomial coefficient $\binom{2r}{r}$. Hence

$$\prod_{p \leq 2r} p = \left(\prod_{p \leq r} p\right)\left(\prod_{r < p \leq 2r} p\right) < 4^r \binom{2r}{r} \leq 4^r \cdot 4^r = 4^{2r}.$$

Now let $N = 2r + 1$. The product of the primes p with $r + 1 < p \leq 2r + 1$ divides $\binom{2r+1}{r}$. Also

$$\binom{2r+1}{r} = \frac{2r+1}{r+1}\binom{2r}{r} < 2\binom{2r}{r}.$$

The central coefficient $\binom{2r}{r}$ is at most half of the sum of all coefficients in the $2r$-th row of Pascal's triangle; indeed, the two adjacent coefficients already have sum at least $\binom{2r}{r}$. Therefore

$$2\binom{2r}{r} \leq 4^r,$$

and hence $\binom{2r+1}{r} \leq 4^r$. Using the induction hypothesis at $r + 1 < 2r + 1$, we get

$$\prod_{p \leq 2r+1} p = \left(\prod_{p \leq r+1} p\right)\left(\prod_{r+1 < p \leq 2r+1} p\right) < 4^{r+1} \cdot 4^r = 4^{2r+1}.$$

This completes the induction. □

Proposition 1 (Bertrand's postulate)**.** *For every integer $n > 1$, there is a prime p such that*

$$n < p < 2n.$$

Proof. Let

$$B_n = \binom{2n}{n}, \qquad P_n = \prod_{n<p\le 2n} p.$$

We first prove that $P_n > 1$ for $n \ge 468$. Since the central binomial coefficient is the largest coefficient in the expansion of $(1+1)^{2n}$, we have

$$B_n \ge \frac{4^n}{2n+1}.$$

Now factor B_n into primes. For a prime q, write $b_q = \nu_q(B_n)$. If $q \le \sqrt{2n}$, then each summand in

$$b_q = \sum_{r\ge 1} \left(\left\lfloor \frac{2n}{q^r} \right\rfloor - 2 \left\lfloor \frac{n}{q^r} \right\rfloor \right)$$

is at most 1, so $q^{b_q} \le 2n$. The total contribution from primes $q \le \sqrt{2n}$ is therefore at most $(2n)^{\sqrt{2n}}$.

If $\sqrt{2n} < q \le n$, then only the first summand can be nonzero. Moreover, for $2n/3 < q \le n$, one has

$$\left\lfloor \frac{2n}{q} \right\rfloor = 2, \qquad \left\lfloor \frac{n}{q} \right\rfloor = 1,$$

so such primes do not divide B_n. Hence

$$B_n \le (2n)^{\sqrt{2n}} \left(\prod_{q\le 2n/3} q \right) P_n.$$

By the previous lemma,

$$\prod_{q\le 2n/3} q < 4^{2n/3}.$$

Combining these inequalities gives

$$P_n > \frac{4^{n/3}}{(2n+1)(2n)^{\sqrt{2n}}}.$$

For $x \ge 468$, set

$$\phi(x) = \frac{x}{3}\log 4 - \log(2x+1) - \sqrt{2x}\log(2x).$$

Then

$$\phi'(x) = \frac{\log 4}{3} - \frac{2}{2x+1} - \frac{\log(2x)+2}{\sqrt{2x}}.$$

The last two terms decrease in magnitude as x increases, and a direct calculation gives

$$\phi'(468) > 0.17, \qquad \phi(468) > 0.1.$$

Thus $\phi(x) > 0$ for all $x \ge 468$. Equivalently,

$$\frac{4^{n/3}}{(2n+1)(2n)^{\sqrt{2n}}} > 1$$

for every integer $n \geq 468$. Hence $P_n > 1$, so there is a prime p with $n < p \leq 2n$. Since $2n$ is composite for $n > 1$, this prime satisfies $n < p < 2n$.

It remains only to check $2 \leq n < 468$. The following table covers all such n; in each row, the displayed number q is prime and satisfies $n < q < 2n$ throughout the indicated range.

q	range of n covered by $n < q < 2n$
3	$n = 2$
5	$3 \leq n \leq 4$
7	$5 \leq n \leq 6$
13	$7 \leq n \leq 12$
23	$13 \leq n \leq 22$
43	$23 \leq n \leq 42$
83	$43 \leq n \leq 82$
163	$83 \leq n \leq 162$
317	$163 \leq n \leq 316$
631	$317 \leq n \leq 467$

This proves Bertrand's postulate for every integer $n > 1$. □