Assorted NT

Stuyvesant Senior Math Team

Aditya Pahuja

August 14, 2025

Contents

0 Introduction

This is a (pretty large) superset of the lesson I gave in class the week before the AMC A exam. The content I went over in class was section 1 and part of section 2, so plenty of extra things to read if you hunger for knowledge.

Also, blue text is always a link.

1 Multiplicative functions

A function $f(n)$ whose domain is positive integers is called an **arithmetic function**. Of interest to us are a special subset called **multiplicative functions**, which satisfy the relation $f(a)f(b) = f(ab)$ whenever a and b are **relatively prime** positive integers, and have $f(1) = 1$.

If the multiplicativeness relation holds for all positive integers, then f is said to be **completely multiplicative**. (Make sure that these are distinct in your head; otherwise, **you will get things very wrong**.)

> **Remark 1.1.** From the definition, you can infer that $f(1)f(a) = f(a)$ and thus $f(1) = 0$ or $f(1) = 1$; however, the former forces $f(a) = 0$ for all a. For this reason, some authors explicitly omit the zero function when discussing multiplicative functions, since it's basically just an annoying special case.

1.1 The big three multiplicative functions

The three most common multiplicative functions (especially at the AMC level) are $\tau(n)$, the number of divisors of n; $\sigma(n)$, the sum of the divisors of n; and $\varphi(n)$, the number of positive integers less than n and relatively prime to n. In this section, we will establish their multiplicativeness as well as determine explicit closed forms to compute them.

In what follows, we take $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ to be the prime factorization of n. We'll present the first one in the form of a walkthrough:

Example 1.1 (The number of divisors)

The number-of-divisors function $\tau(n)$ is multiplicative, and

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1).$$

Walkthrough. This is actually a counting problem masquerading as a number-theoretic one.

(a) Suppose d is a divisor of n. Since its prime factors are a subset of the prime factors of n, we can say that $d = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$. How are e_i and f_i related?

(b) Based on **(a)**, how many possible values can each f_i take?

(c) Conclude the formula for $\tau(n)$.

Now, we verify that $\tau(n)$ is multiplicative. One common way to prove that τ is multiplicative is to show that

$$\tau(n) = \tau(p_1^{e_1})\tau(p_2^{e_2}) \cdots \tau(p_k^{e_k})$$

for any n; this is nice because it lets us ignore anything that's not a prime power.

(d) Consider an arbitrary function $f\colon \mathbb{N} \to \mathbb{C}$. (We use $\mathbb{N}$ to mean “positive integers.”) Prove that if
$$f(n) = f(p_1^{e_1})f(p_2^{e_2})\cdots f(p_k^{e_k})$$
for any n, then f is multiplicative.

(e) What is $\tau(p^e)$ when p is prime, using the formula?

(f) Conclude that the relation we want to prove is in fact true.

Of course, in this case, you can also directly show that $\tau(m)\tau(n) = \tau(mn)$ just from the formula.

The other two functions are similar, so we'll just present their proofs.

Theorem 1.2 (The sum of divisors)**.** The sum-of-divisors function $\sigma(n)$ is multiplicative, with its closed form given by
$$\sigma(n) = \left(\frac{p_1^{e_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{e_2+1}-1}{p_2-1}\right)\cdots\left(\frac{p_k^{e_k+1}-1}{p_k-1}\right).$$

Proof. We will prove both parts in one fell swoop by inducting on k (which is the number of distinct prime factors of n).

First, suppose $k = 1$. Then n is just a prime power, so its prime factors are 1, p_1, p_1^2, $\dots$, $p_1^{e_1}$. Their sum is therefore
$$1 + p_1 + p_1^2 + \cdots + p_1^{e_1} = \frac{p_1^{e_1+1}-1}{p_1-1}$$
by geometric series.

Now, suppose the claim is true for some positive integer k. Then, consider a number with $k+1$ distinct prime factors. Write it as $n \cdot q^f$, where n has k distinct prime factors (so q is prime), and look at set of its divisors. If some d divides n, then we can see that
$$d, dq, dq^2, \dots, dq^f$$
are all divisors of $n \cdot q^f$. Moreover, each d corresponds to a unique set of $f+1$ divisors (that is, none of the divisors are over- or under-counted).

This means that, by splitting the divisors of $n \cdot q^f$ into groups based on the largest power of q dividing them, $\sigma(n \cdot q^f)$ looks like
$$\sigma(n) + q\sigma(n) + q^2\sigma(n) + \cdots + q^f\sigma(n) = \sigma(n)\cdot\frac{q^{f+1}-1}{q-1} = \sigma(n)\sigma(q^f).$$

Induction now lets us conclude that σ follows the claimed formula, and
$$\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2})\cdots\sigma(p_k^{e_k}),$$
i.e. σ is multiplicative. $\square$

Theorem 1.3 (The φ function)**.** Let $\varphi(n)$ be the number of positive integers less than n and relatively prime to n, as usual. Then, $\varphi(n)$ is multiplicative and

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Proof. We'll count $\varphi(n)$ using the principle of inclusion-exclusion.

(a) We have n numbers.

(b) Of these, $\frac{n}{p_1}$ are multiples of p_1, $\frac{n}{p_2}$ are multiples of p_2, and so on; we want to not count these (since we're hunting for numbers coprime to n).

(c) Then, $\frac{n}{p_i p_j}$ are multiples of p_i and p_j, which are overcounted in (b), so we add these back for all i and j.

(d) Now, we need to subtract off multiples of three primes, of which there are $\frac{n}{p_a p_b p_c}$, summed over all (a, b, c).

And so on. You get the picture. This means we end up with

$$n\left(1 - \sum_{1 \le m_1 \le k} \frac{1}{p_{m_1}} + \sum_{1 \le m_1 < m_2 \le k} \frac{1}{p_{m_1} p_{m_2}} - \sum_{1 \le m_1 < m_2 < m_3 \le k} \frac{1}{p_{m_1} p_{m_2} p_{m_3}} + \cdots\right).$$

It turns out that the thing in the parentheses factors exactly how we want, so the final result is indeed

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

If the factorization feels like it came out of nowhere, write out all eight terms for $k = 3$ and see what happens.

The multiplicativeness then follows immediately from the formula. □

Exercise 1.2. Compute $\tau(1434)$, $\sigma(561)$, and $\varphi(1984)$.

Again, I cannot stress enough: **make sure your arguments are relatively prime** when you use multiplicativeness; none of the functions above are completely multiplicative.

Here are some extra multiplicative functions, just for more variety in your palate.

Example 1.3 (More multiplicative functions)

The following are completely multiplicative:

- The identity function $\mathrm{id}(n) = n$.
- The Dirichlet identity function $\delta(n) = \left\lfloor \frac{1}{n} \right\rfloor$ (aka $\delta(1) = 1$, $\delta(n) = 0$ for $n > 1$).
- The constant function $\mathrm{uno}(n)$, which is defined as $\mathrm{uno}(n) = 1$ for all n.

The following are multiplicative, but not completely:

- The Möbius function, defined as $\mu(n) = 0$ if n is divisible by the square of a prime, and $\mu(n) = (-1)^k$ if $n = p_1 p_2 \cdots p_k$.
- The sum of the rth powers of the divisors of n for any $r \in \mathbb{C}$. (What do $r = 0$ and $r = 1$ give you?)

1.2 Generating more multiplicative functions

Sometimes, you will be asked to compute a sum over all divisors of n, such as

$$\sum_{d|n} \varphi(d).$$

It turns out that such constructs are very well-behaved under some circumstances:

Theorem 1.4. Let f and g be multiplicative functions. Then, the function

$$\sum_{d|n} f(d)g\left(\frac{n}{d}\right),$$

denoted $f * g$, is also multiplicative (in particular, not the zero function).

Proof. Let m and n be relatively prime. Then,

$$(f * g)(mn) = h(mn) = \sum_{d|n} f(d)g\left(\frac{mn}{d}\right).$$

We can then write $d = ab$ where $a \mid m$ and $b \mid n$ and $\gcd(a,b) = \gcd(m/a, n/b) = 1$ due to the "relatively prime" hypothesis, so

$$h(mn) = \sum_{d|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) = \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right)$$

which is indeed just $h(m)h(n)$.

Also, since $f(1) = g(1) = 1$, $h(1) = f(1)g(1) = 1$, too, so h is not the zero function. □

Warning 1.5 — Even if f and g are completely multiplicative, $f * g$ need not be. For example, $\mathrm{id} * \mathrm{uno} = \tau$, which is not completely multiplicative even though id and uno both are.

As a silly application of Theorem 1.4, we can now establish that $\sigma(n)$ is multiplicative directly, since

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \mathrm{id}(d)\,\mathrm{uno}\left(\frac{n}{d}\right)$$

Exercise 1.4. Show similarly that $\tau(n)$ is multiplicative, too.

A couple of example problems are now in order.

Example 1.5

Given a positive integer n, compute

$$\sum_{d|n} \varphi(d).$$

Walkthrough. There are multiple ways to attack this (combinatorial proofs are popular), but we can just close our eyes and bash using Theorem 1.4.

(a) How can the sum be written as

$$\sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

for multiplicative functions f and g?

(b) Compute the sum when n is a prime power (this should be pretty easy).

(c) Conclude by considering the prime factorization of n.

Just for fun, I will also outline a short combinatorial proof:

(d) Let $n = 15$ for a moment. Write out the fractions $\frac{1}{15}, \frac{2}{15}, \ldots, \frac{15}{15}$, and then simplify all of them.

(e) For each $d \mid 15$, many fractions have denominator d?

(f) Generalize the previous two steps to arbitrary n, and conclude by summing over all d.

The main upshot of Theorem 1.4 is that if we know f is multiplicative, we have a good handle on anything that looks like

$$g(n) = \sum_{d|n} f(d).$$

However, sometimes, we know g and would like to recover f. To do this, we use the following:

Example 1.6 (Möbius inversion formula)
Suppose that f and g are *any* (not necessarily multiplicative!) arithmetic functions satisfying

$$g(n) = \sum_{d|n} f(d).$$

Then,

$$f(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right),$$

where $\mu(n)$ is the Möbius function from Example 1.3.

Walkthrough. We can actually do this purely using properties of the $*$ operation.

(a) Show that $*$ is associative: given functions f, g, and h, prove that

$$(f * g) * h = f * (g * h).$$

(b) What is the identity function under $*$? That is, which function $\mathbf{I}(n)$ satisfies

$$f * \mathbf{I} = \mathbf{I} * f = f?$$

(c) Show that uno(n) and $\mu(n)$ are inverses under $*$ by verifying that

$$\text{uno} * \mu = \mu * \text{uno} = \mathbf{I}.$$

(d) Rephrase the two given equations using the $*$ operation, and figure out why they're equivalent because of the claims made in the previous three parts.

This problem mainly relies on the fact that the set of arithmetic functions is (almost) a group when equipped with the $*$ operation: the operation is associative, and there's an identity function $\mathbf{I}$. In an actual group, we can also always find an inverse for each element (in other words, if the arithmetic functions with $*$ were a group, then we could always find an f^{-1} so that $f * f^{-1} = \mathbf{I}$). However, in this case, some functions, like the zero function, doesn't have an inverse:

$$\mathbf{0} * f = \mathbf{0}$$

for any f, where $\mathbf{0}$ denotes the function that is 0 everywhere. If we were to remove the functions that don't have an inverse, then we have a pretty nice algebraic system to play around with, as witnessed in this problem.

Question: Which functions have inverses under $*$?

Another silly example, because why not?

Example 1.7 (Shortlist 1989)

Define a sequence $(a_n)_{n\geq 1}$ by

$$\sum_{d|n} a_d = 2^n.$$

Show that n divides a_n.

Walkthrough. This pretty much directly collapses upon Möbius inversion.

(a) Show that

$$a_n = \sum_{d|n} \mu(d) 2^{n/d}.$$

(b) Write out the prime factorization of n and bash. It may help to write out a few test values of n first.

If you want to do some extra reading on this topic, the relevant keywords are "Dirichlet convolution" — that's the name of the $*$ operation we've been talking about.

2 Factorials(Factorials − 1)(Factorials − 2)...

There are about two main theorems relating to factorials.

Theorem 2.1 (Wilson)**.** Let $p > 1$ be an integer. Then

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

if and only if p is prime.

Proof. First, suppose p is prime. Then, we have the following claim:

Claim 2.2 — The only numbers that are their own inverse modulo p are ± 1.

Proof. We want to solve $x^2 \equiv 1 \pmod{p}$, which means $p \mid x^2 - 1$. This implies that $p \mid x+1$ or $p \mid x-1$ as desired. □

Now, consider the $\frac{p+1}{2}$ (unordered) pairs of inverses modulo p. Each number appears exactly once among these pairs, except for 1 and $p-1$, which appear twice. This means the product of everything except ± 1 is 1 because we're multiplying a bunch of pairs of inverses together, and then multiplying by $1 \cdot (p-1)$ shows that

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

On the other hand, suppose that p is composite. We can then find $1 < a \le b \le p-1$ such that $ab = p$. If a and b are distinct, we are immediately done since $ab \mid (p-1)!$. If $a = b$ (i.e. p is the square of a prime), then suppose that $p = k^2$ for prime k. If $k > 2$, then k and $2k$ are both less than p, hence

$$k^2 \mid 2k^2 \mid (p-1)!,$$

and if $k = 2$, we can verify by hand that

$$3! \equiv 2 \not\equiv -1 \pmod{4},$$

so no composite p satisfies the relation. □

The main thing you want to take away from Wilson's theorem is that it's very strong; if you wanted to check whether a number n is prime, you could in principle compute $(n-1)!$ and look at it mod n. In fact, this is the basis of some prime-counting formulas, such as Willans' formula: letting $\pi(n)$ be the number of primes that are at most n, we have

$$\pi(n) = \left\lfloor \frac{n}{2} + \frac{1}{2} \sum_{k=0}^{n-1} \cos\left(\frac{k! - k}{k+1}\pi\right) \right\rfloor$$

for each integer $n \ge 1$. Of course, because of the growth of factorials, this is kind of ridiculous to compute, but the existence of a precise formula purely due to Wilson's theorem is nice in its own right.

Example 2.1

Let p be a prime that is $1 \pmod 4$. Show that $x^2 \equiv -1 \pmod p$ has an integer solution x.

Walkthrough. The idea here is to use Wilson to manually construct an x.

(a) What does Wilson give you for free?

(b) Pair terms in $(p-1)!$ to create something that looks similar to a square.

(c) You should have a bunch of factor pairs that look like $k(p-k) \equiv -k^2 \pmod p$. How many -1s can you peel off from these pairs?

(d) Remove all the -1s and rejoice, for you have found x.

The other theorem has to do with the greatest prime power dividing $n!$:

Theorem 2.3 (Legendre)**.** For any positive integer n and prime p,

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - s_p(n)}{p-1},$$

where $\nu_p(N)$ is the largest integer e such that $p^e \mid N$ and $s_p(n)$ is the sum of the digits of n in base p.

Exercise 2.2 (Mandatory if you haven't seen ν_p before)**.** Show that, for all primes p, $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ and $\nu_p(x/y) = \nu_p(x) - \nu_p(y)$ for integers x and y. You may notice that this allows you to extend ν_p to nonzero rational numbers, which we will talk about later in the year.

Proof. For the first part, we count the prime powers as follows: add 1 for each multiple of p that is at most n, then add 1 for each multiple of p^2 (since these need to be counted twice), then add 1 for each multiple of p^3 (since these need to be counted thrice), and so on. Symbolically, this is exactly what the sum says, since $\lfloor \frac{n}{k} \rfloor$ is the number of multiples of k that are at most n.

The second part is pretty nice and therefore reserved for you as one of the practice problems. □

The biggest benefit of the second form of Legendre's formula is that it makes binomial coefficients about a kajillion times nicer to work with. For example:

Example 2.3

Show that $\binom{2k}{k}$ is always even for $k \geq 1$.

Walkthrough. This is a one-shot kill with Legendre.

(a) What do you want to show, in terms of ν_2?

(b) What does Legendre tell you about $\nu_2\left(\binom{2k}{k}\right)$?

(c) Why does this imply **(a)**?

This is is a decent bit less annoying than using the floor function version of the formula (try it and see!).

3 More ad-hoc problems

These are generally just problems with a more "weird" flavor. Expect to do algebra — things like factoring and pushing symbols around tend to be helpful. Not much theory here, so I'm just going to show a couple of examples.

Example 3.1 (2019 AMC 12A/24)
For how many positive integers n between 1 and 50, inclusive, is

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

an integer?

Walkthrough. One of the weird things about working with integers is that you can sometimes find combinatorial interpretations of things (for a really funny story, see USAMO 2016/2).

(a) Find a combinatorial interpretation for

$$\frac{(n^2)!}{(n!)^{n+1}}.$$

Now, we are given that

$$\frac{(n^2-1)!}{(n!)^n} = \frac{(n^2)!}{(n!)^{n+1}} \cdot \frac{n!}{n^2}$$

is an integer. This leaves us with two cases to consider: either $\frac{n!}{n^2}$ is an integer, or it isn't.

(b) First, if $\frac{n!}{n^2}$ is an integer, then obviously that value of n works. For which n is $n!$ divisible by n^2? Be very careful: this step is where most people sillied this problem.

(c) Show that the other cases don't work, and extract the answer.

Example 3.2 (NIMO 15.8, by Justin Stevens)
Find the prime factors of 67208001, given that 23 is one.

Walkthrough. While this is pretty short, I think it's pretty instructive.

(a) Why is this number suspicious? Before continuing, stare at it for a couple of minutes and try to understand what's so special.

(b) Answer to the previous clue: you can write it as

$$x^6 + x^5 + x^3 + 1$$

where $x = 20$. Try factoring this polynomial; you get a root for free by checking rational roots, and the resulting quintic should also factor cleanly.

(c) If you did everything right, you should now be able to extract the prime factors with the knowledge that 23 is one of them. As a check, their sum is 881.

4 Assorted Practice Problems (ft. many NIMOs)

Again, expect to do a lot of algebra.

Problem 4.1 (GLIME 2023/5)
Evaluate
$$\sum_{n=1}^{18} \left\lfloor \frac{n^3 - n}{9} \right\rfloor.$$

Problem 4.2 (NIMO 6.3, by Kevin Sun)
Find the integer $n \geq 48$ for which the number of trailing zeros in the decimal representation of $n!$ is exactly $n - 48$.

Problem 4.3 (NIMO 20.5, by Michael Tang)
For positive integers n, let $s(n)$ be the sum of the digits of n. Over all four-digit positive integers n, which value of n maximizes the ratio $\frac{s(n)}{n}$?

Problem 4.4
Prove that for any integer $n \geq 1$,
$$\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d) \right)^2$$

Problem 4.5 (NIMO 14.5, by Evan Chen)
Find the largest integer n for which 2^n divides
$$\binom{2}{1}\binom{4}{2}\binom{6}{3}\cdots\binom{128}{64}.$$

★ **Problem 4.6** (Legendre, second form)
Show that
$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Problem 4.7 (NIMO Summer 2017.15, by David Altizio)
For all positive integers n, denote by $\sigma(n)$ the sum of the positive divisors of n and $\nu_p(n)$ the largest power of p which divides n. Compute the largest positive integer k such that 5^k divides
$$\sum_{d|N} \nu_3(d!)(-1)^{\sigma(d)},$$
where $N = 6^{1999}$.

Problem 4.8 (NIMO 27.5, by Mehtaab Sawhney)

Find the number of integers n with $1 \le n \le 100$ for which $n - \varphi(n)$ is prime.

Problem 4.9 (NIMO Summer 2016.2)

Let p be a prime. It is given that there exists a unique nonconstant function $\chi : \{1, 2, \dots, p-1\} \to \{-1, 1\}$ such that $\chi(1) = 1$ and $\chi(mn) = \chi(m)\chi(n)$ for all $m, n \not\equiv 0 \pmod{p}$ (here the product mn is taken mod p). Find all positive primes p for which

$$\sum_{a=1}^{p-1} a^{\chi(a)} \equiv 0 \pmod{p}.$$

Here as usual a^{-1} denotes multiplicative inverse.

★ **Problem 4.10** (2021 AIME I/14)

For any positive integer a, $\sigma(a)$ denotes the sum of the positive integer divisors of a. Let n be the least positive integer such that $\sigma(a^n) - 1$ is divisible by 2021 for all positive integers a. Find n.

★ **Problem 4.11** (NIMO 8.6, proposed by Lewis Chen)

Let $f(n) = \varphi(n^3)^{-1}$. Compute

$$\frac{f(1) + f(3) + f(5) + \dots}{f(2) + f(4) + f(6) + \dots}.$$

Problem 4.12 (PRIMES 2019 entrance exam)

For a positive integer n, let $f(n)$ denote the smallest positive integer which neither divides n nor $n+1$. Which values can $f(n)$ take as n varies?

★ **Problem 4.13** (AMSP 2011 NT3 Exam)

Let μ be the Möbius function. For $n \ge 1$, evaluate

$$\sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor.$$

Hint, encoded by a ROT13 cipher: Erjevgr gur sybbe shapgvba nf gur fhz bs 1 bire nyy zhygvcyrf bs x gung ner ng zbfg a.

Problem 4.14 (PUMaC 2022 N8)

For $n \ge 2$, let $\omega(n)$ denote the number of distinct prime factors of n, and $\omega(1) = 0$. Compute the absolute value of

$$\sum_{n=1}^{160} (-1)^{\omega(n)} \left\lfloor \frac{160}{n} \right\rfloor.$$

Problem 4.15 (InftyDots 2018/1)

Does there exist a finite set S of primes for which the map $f\colon \mathbb{Z}_{>0} \times S \to \mathbb{Z}_{\geq 0}$ defined by

$$f(n, p) = \nu_p(n!)$$

is surjective?

Problem 4.16 (Rejected NYCTC Proposal)

Compute the number of integers k between 0 and 2024, inclusive, such that $\binom{2024}{k}$ is not a multiple of 3.

5 Solutions to Walkthroughs

5.1 Solution 1.1, The number of divisors

Observe that if $d \mid n$, then $0 \le \nu_p(d) \le \nu_p(n)$ for all prime numbers p. Thus, for each prime, there are $\nu_p(n)+1$ choices for $\nu_p(d)$, meaning

$$\tau(n) = \prod_p (\nu_p(n)+1),$$

which is equivalent to the form in the problem statement.

To see that this is multiplicative, suppose m and n are relatively prime. Then, they do not share any prime factors, so, if $p \mid mn$, then $\nu_p(mn)$ is always one of $\nu_p(m)$, $\nu_p(n)$ (and the other one is zero). This means that

$$\begin{aligned}
\tau(m)\tau(n) &= \prod_{p\mid m}(\nu_p(m)+1)\cdot\prod_{p\mid n}(\nu_p(n)+1) \\
&= \prod_{p\mid m}(\nu_p(m)+\underbrace{\nu_p(n)}_{0}+1)\cdot\prod_{p\mid n}(\nu_p(n)+\underbrace{\nu_p(m)}_{0}+1) \\
&= \prod_{p\mid m \text{ or } p\mid n}(\nu_p(m)+\nu_p(n)+1) \\
&= \prod_{p\mid mn}(\nu_p(mn)+1) = \tau(mn)
\end{aligned}$$

where the products are taken over primes.

5.2 Solution 1.5

The answer is $\boxed{n}$. We present two solutions.

Solution 1 (Dirichlet convolution). Observe that

$$f(n) = \sum_{d\mid n}\varphi(d) = \sum_{d\mid n}\varphi(n)\cdot \mathrm{uno}\left(\frac{\mathrm{n}}{\mathrm{d}}\right),$$

so, since φ and uno are multiplcative, f is also multiplicative.

Thus, it suffices to compute f on prime powers. Noting that $\varphi(p^k) = p^k - p^{k-1}$ when p is prime, we have

$$\sum_{d\mid p^k}\varphi(d) = \varphi(1)+\varphi(p)+\varphi(p^2)+\cdots+\varphi(p^k) = 1+(p-1)+(p^2-p)+\cdots+(p^k-p^{k-1}),$$

whence all the the terms die except for the p^k, so $\varphi(p^k) = p^k$, which directly implies $\varphi(n) = n$ for all n by multiplicativeness.

Solution 2 (combinatorial interpretation). Consider the n fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$. Clearly, when simplified, the denominators of each of these fractions is a factor of n, so we will count the number of fractions whose denominator is d for some $d \mid n$.

> **Claim** — There are $\varphi(d)$ fractions with denominator d.

Proof. If $\frac{a}{n}$, upon being reduced, has a denominator of d, then $a = \frac{n}{d} \cdot b$ for some integer b relatively prime to d, We want to count the number of possible values of a, which entails counting the number of possible values of b, of which there are $\varphi(d)$ since $b < d$ and $\gcd(b, d) = 1$. □

Now,

$$\sum_{d|n} \varphi(d)$$

counts the number of fractions whose denominator is one of the divisors of n, but, as mentioned earlier, each fraction's denominator divides n, so the sum is equal to n, the total number of fractions.

5.3 Solution 1.6, Möbius inversion formula

We begin by establishing three facts about the Dirichlet convolution operation.

Claim — Dirichlet convolution is associative: that is,

$$(f * g) * h = f * (g * h).$$

Proof. Both sides of the equation can be written as

$$\sum_{abc=n} f(a)g(b)h(c),$$

hence they are equal. □

Claim — The identity under $*$ is the function $\delta(n)$ detailed in Example 1.3, defined as

$$\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & n > 1. \end{cases}$$

Proof. Since $*$ is commuative, we just need to check that $f * \delta = f$:

$$(f * \delta)(n) = \sum_{d|n} \delta(d) f\left(\frac{n}{d}\right) = f(n)\delta(1) + \sum_{\substack{d|n \\ d>1}} \delta(d) f\left(\frac{n}{d}\right) = f(n).$$ □

Claim — Let μ and uno be defined as in Example 1.3. Then, μ and uno are inverses under $*$.

Proof. Let f denote $\mu * \text{uno}$. Since both μ and uno are multiplicative, so is f.

Since f is multplicative, $f(1) = 1$; now assume that $n = p^k$ is a prime power. Then,

$$f(p^k) = \mu(1) + \mu(p) + \sum_{i=2}^{k} \mu(p^i) = \mu(1) + \mu(p) = 0,$$

so whenever $n > 1$, $f(n) = 0$, meaning $f \equiv \delta$. □

Now, we can finish the problem: we see that

$$g * \mu = (f * \text{uno}) * \mu = f * (\text{uno} * \mu) = f * \delta = f$$

as desired.

5.4 Solution 1.7, Shortlist 1989

By Möbius inversion,
$$a_n = \sum_{d \mid n} \mu(d) 2^{n/d}.$$
Since $\mu(d) = 0$ whenever d isn't squarefree, we may assume d is squarefree. Then, let $p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of n, as usual. We will show that $p_i^{e_i}$ divides a_n for each i.

Let S be the set of squarefree divisors of n. Then, we can partition S into two equal-size subsets: S^+, each of whose elements is divisible by p_i, and S^-, each of whose elements isn't. We then have a natural pairing between elements of S^- and S^+ given by multiplying by p_i.

For some $s \in S^-$, consider
$$F(s) = \mu(s) 2^{n/s} + \sum (sp_i) 2^{n/(sp_i)}.$$
This pairs elements of S^- and S^+, so summing $F(s)$ over all of S^- is equal to a_n. By multiplicativeness, $\mu(s) = -\mu(sp_i)$, so
$$\begin{aligned} F(s) &= \mu(s) \left(2^{p_i^{e_i} q} - 2^{p_i^{e_i - 1} q} \right) \\ &= 2^{q p_i^{e_i - 1}} \mu(s) \cdot \left((2^q)^{p_i^{e_i} - p_i^{e_i - 1}} - 1 \right) \\ &= 2^{q p_i^{e_i - 1}} \mu(s) \cdot \left((2^q)^{\varphi(p_i^{e_i})} - 1 \right) \end{aligned}$$
where $n = q \cdot p_i^{e_i}$. If $p_i = 2$, then clearly $F(s)$ is divisible by $p_i^{e_i}$ because $p_i^{e_i - 1} > e_i$, which can be shown inductively. Otherwise $\gcd(2, p_i) = 1$, so Euler's theorem says that
$$(2^q)^{\varphi(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}},$$
so $F(s)$ is still divisible by $p_i^{e_i}$. Then,
$$a_n = \sum_{s \in S^-} F(s)$$
is divisible by each prime power dividing n, hence $n \mid a_n$.

5.5 Solution 2.1

I claim that
$$x = \left(\frac{p-1}{2} \right)!$$
is a solution to the equation. Plugging in to verify this, we have
$$\begin{aligned} x^2 &= 1^2 \cdot 2^2 \cdots \left(\frac{p-1}{2} \right)^2 \\ &\equiv (-1)^{(p-1)/2} \cdot 1(p-1) \cdot 2(p-2) \cdots \left(\frac{p-1}{2} \cdot \frac{p+1}{2} \right) \\ &= (p-1)! \equiv -1 \pmod{p}, \end{aligned}$$
where $(-1)^{(p-1)/2} = 1$ because $4 \mid p - 1$ implies $\frac{p-1}{2}$ is even.

5.6 Solution 2.3

We want to show that $\nu_2\left(\binom{2k}{k}\right)$ is nonzero. Using Legendre we have

$$\nu_2\left(\frac{(2k)!}{k!^2}\right) = (2k - s_2(2k)) - 2(k - s_2(k)) = -s_2(2k) + 2s_2(k) = s_2(k)$$

because $2k$ and k have the same sum of digits in binary. Clearly $s_2(k) > 0$ because k is not zero, so we're done.

5.7 Solution 3.1, 2019 AMC 12A/24

Observe that

$$\frac{(n^2)!}{(n!)^{n+1}}$$

counts the number of ways to put n^2 balls into n boxes without regard to the order of the boxes. For example, if we have four balls A, B, C, D, then we are counting the number of ways to pair the balls without regard to the order of the pairs, so $(AB, CD) = (CD, AB)$. Thus, this value is an integer.

Now, we see that

$$\frac{(n^2-1)!}{(n!)^n} = \frac{(n^2)!}{(n!)^{n+1}} \cdot \frac{n!}{n^2}.$$

This induces two natural cases: either n^2 divides $n!$, or it doesn't.

In the former case, the desired expression is obviously an integer. This case is also equivalent to $n \mid (n-1)!$, which, as you may have noted in the proof of Wilson's theorem, is true if and only if n is not prime and not equal to four.

In the latter case, n is either 4 or prime. If $n = 4$, then

$$\frac{15!}{(4!)^4}$$

has one too many factors of two, as

$$\nu_2(15!) - 4\nu_2(4!) = 15 - s_2(15) - 4(3) = 15 - 4 - 12 = -1 < 0,$$

so the expression isn't an integer; and if n is prime, then $\nu_n((n^2-1)! = n - 1$ while $\nu_n((n!)^n) = n$, so no primes work.

Therefore, the answer is $50 - 15 - 1 = \boxed{34}$, as there are 15 primes less than 50.

5.8 Solution 3.2, NIMO 15.8

The main idea of the problem is to notice that

$$67208001 = 20^6 + 20^5 + 20^3 + 1.$$

This factors readily as

$$(20^3 - 20 + 1)(20^2 + 1)(20 + 1) = \boxed{3 \cdot 7 \cdot 23 \cdot 347 \cdot 401}.$$