

Apostol's Analytic Number Theory

Stefanus¹

¹ Samsung Semiconductor Inc

San Jose, CA 95134 USA

(Dated: December 29, 2016)

Abstract

Just for fun :)

Chapter 2

Problem 2.1 Find all integers n such that

$$(a) \ \varphi(n) = n/2 \qquad (b) \ \varphi(n) = \varphi(2n) \qquad (c) \ \varphi(n) = 12$$

For (a), using the definition of $\varphi(n)$, $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

$$\begin{aligned} \frac{n}{2} &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ \frac{1}{2} &= \frac{\prod_{p|n} (p-1)}{\prod_{p|n} p} \\ \prod_{p|n} p &= 2 \prod_{p|n} (p-1) \end{aligned}$$

if n is odd the LHS is odd while the RHS is even, so it can't be. If n is even the LHS only has one factor of 2 while the RHS has many so it will only work if $n = 2$.

For (b)

$$n \prod_{p|n} \left(1 - \frac{1}{p}\right) = 2n \prod_{p|2n} \left(1 - \frac{1}{p}\right)$$

If n is even then

$$\prod_{p|2n} \left(1 - \frac{1}{p}\right) = \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

and so

$$\begin{aligned} \prod_{p|n} \left(1 - \frac{1}{p}\right) &= 2 \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ &\rightarrow 1 = 2 \end{aligned}$$

which is impossible, so n has to be odd, in that case

$$\begin{aligned} \prod_{p|2n} \left(1 - \frac{1}{p}\right) &= \left(1 - \frac{1}{2}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ &= \frac{1}{2} \prod_{p|n} \left(1 - \frac{1}{p}\right) \end{aligned}$$

and therefore

$$\prod_{p|n} \left(1 - \frac{1}{p}\right) = 2 \frac{1}{2} \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ \rightarrow 1 = 1$$

and therefore $\varphi(n) = \varphi(2n)$ for all odd n .

For (c)

$$\varphi(n) = 12 = 2 \cdot 2 \cdot 3 \\ = \prod_{p|n} p^{\alpha_p} - p^{\alpha_p-1} \\ \varphi \left(\prod_{p|n} p^{\alpha_p} \right) = \prod_{p|n} p^{\alpha_p-1} (p-1)$$

the only possible solution is $n = 13$

Problem 2.2. For each of the following statements either give a proof or exhibit a counter example.

(a) If $(m, n) = 1$ then $(\varphi(m), \varphi(n)) = 1$

(b) If n is composite, then $(n, \varphi(n)) > 1$

(c) If the same primes divide m and n , then $n\varphi(m) = m\varphi(n)$

For (a) a counter example will be $(3, 4) = 1$, while $\varphi(3) = 2$, $\varphi(4) = 2$

For (b) a counter example would be $n = 15$ which means that $\varphi(15) = 8$ and $(15, 8) = 1$

For (c) I think what it means by “the same primes divide m and n ” is that $m = \prod p^{\alpha_p}$ and $n = \prod p^{\beta_p}$, so they both have the same primes but they might have different exponents for each prime, in this case $\prod_{p|n} = \prod_{p|m}$

$$n\varphi(m) = n \left(m \prod_{p|m} \left(1 - \frac{1}{p}\right) \right) \\ = m \left(n \prod_{p|n} \left(1 - \frac{1}{p}\right) \right) \\ n\varphi(m) = m\varphi(n)$$

Problem 2.3. Prove that

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}$$

Since $\mu(n)$ and $\varphi(n)$ are both multiplicative so is μ^2/φ , in that case $g(n) = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}$ is also multiplicative. To determine $g(n)$ we need only compute $g(p^\alpha)$ for prime powers

$$\begin{aligned}
g(p^\alpha) &= \sum_{d|p^\alpha} \frac{\mu^2(d)}{\varphi(d)} \\
&= \frac{\mu^2(1)}{\varphi(1)} + \frac{\mu^2(p)}{\varphi(p)} + \dots + \frac{\mu^2(p^\alpha)}{\varphi(p^\alpha)} \\
&= 1 + \frac{1}{p-1} \\
&= \frac{p}{p-1} \\
&= p^\alpha \cdot \frac{p}{p^\alpha(p-1)} \\
&\rightarrow \sum_{d|p^\alpha} \frac{\mu^2(d)}{\varphi(d)} = \frac{p^\alpha}{\varphi(p^\alpha)}
\end{aligned}$$

We can also prove it the other way around by assuming the LHS, to do this it is easiest to use the Mobius inversion formula

$$\frac{n}{\varphi(n)} = \sum_{d|n} g(d)$$

and we want to find out what this $g(d)$ is, which is

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

The RHS is multiplicative so like above we just need to evaluate $g(p^\alpha)$ for prime powers

$$\begin{aligned}
g(p^\alpha) &= \sum_{d|p^\alpha} \frac{d}{\varphi(d)} \mu\left(\frac{p^\alpha}{d}\right) \\
&= \frac{p^{\alpha-1}}{\varphi(p^{\alpha-1})} \mu\left(\frac{p^\alpha}{p^{\alpha-1}}\right) + \frac{p^\alpha}{\varphi(p^\alpha)} \mu\left(\frac{p^\alpha}{p^\alpha}\right) \\
&= -\frac{p^{\alpha-1}}{\varphi(p^{\alpha-1})} + \frac{p^\alpha}{\varphi(p^\alpha)} \\
&= -\frac{p^\alpha}{\varphi(p^\alpha)} + \frac{p^\alpha}{\varphi(p^\alpha)} \\
&= 0
\end{aligned}$$

if $\alpha > 1$ and if $\alpha = 1$ we get

$$\begin{aligned}
g(p) &= \sum_{d|p} \frac{d}{\varphi(d)} \mu\left(\frac{p}{d}\right) \\
&= \frac{1}{\varphi(1)} \mu\left(\frac{p}{1}\right) + \frac{p}{\varphi(p)} \mu\left(\frac{p}{p}\right) \\
&= -1 + \frac{p}{\varphi(p)} \\
&= -1 + \frac{p}{p-1} \\
&= \frac{1}{p-1} \\
g(p) &= \frac{1}{\varphi(p)}
\end{aligned}$$

This means that $g(p^\alpha) = 1/\varphi(p^\alpha)$ is $\alpha = 1$ and $g(p^\alpha) = 0$ if $\alpha > 1$, in other words $g(p^\alpha) = \mu^2(p^\alpha)/\varphi(p^\alpha)$

Problem 2.4. Prove that $\varphi(n) > n/6$ for all n with at most 8 distinct prime factors.

First, let's demystify this number 8, the reason 8 is involved is because if you multiply out $(p-1)/p$ for the first eight primes we get

$$\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13} \cdot \frac{16}{17} \cdot \frac{18}{19} = \frac{55296}{323323} \sim 0.171 > \frac{1}{6}$$

but if we multiply the first nine

$$\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13} \cdot \frac{16}{17} \cdot \frac{18}{19} \cdot \frac{22}{23} = \frac{110592}{676039} \sim 0.164 < \frac{1}{6}$$

So that's how we got the eight and of course if we chose any other eight primes we will get something bigger than $55296/323323 > 1/6$ because $n/(n+1)$ converges to 1 as $n \rightarrow \infty$, *i.e.* $n/(n+1)$ gets bigger as n gets bigger.

Another reason we have to limit it to eight is because $n/(n+1) < 1$ and if we keep multiplying them we'll get a smaller and smaller number and after some point we will reach $< 1/6$.

The rest is straightforward,

$$\frac{\varphi(n)}{n} = \prod_{p|n} \frac{p-1}{p}$$

so the argument above holds

Problem 2.5. Define $\nu(1) = 0$, and for $n > 1$ let $\nu(n)$ be the number of distinct prime factors of n . Let $f = \mu * \nu$ and prove that $f(n)$ is either 0 or 1.

As the inverse of μ is $\mu^{-1} = u$, this means that

$$\begin{aligned} u * f &= (u * \mu) * \nu \\ &= I * \nu \\ u * f &= \nu \\ \rightarrow \nu(n) &= \sum_{d|n} f(d) \end{aligned}$$

ν is obviously not multiplicative since $\nu(1) \neq 1$, $\nu(pq) \neq \nu(p)\nu(q)$ but it is actually additive since $\nu(p^\alpha q^\beta) = \nu(p^\alpha) + \nu(q^\beta) = \nu(p) + \nu(q)$ where $p \neq q$ are distinct primes, so let's decompose n into its primal constituents, $n = \prod_i p_i^{\alpha_i}$

$$\begin{aligned} \nu \left(\prod_i p_i^{\alpha_i} \right) &= \sum_{d|n} f(d) \\ \sum_i \nu(p_i^{\alpha_i}) &= \sum_{d|n} f(d) \\ \sum_i \nu(p_i) &= \sum_{d|n} f(d) \end{aligned}$$

from here we can immediately see that $f(n)$ is given by

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is prime} \\ 0 & \text{otherwise} \end{cases}$$

Problem 2.6. Prove that

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

and, more generally,

$$\sum_{d^k|n} \mu(d) = \begin{cases} 0 & \text{if } m^k|n \text{ for some } m > 1 \\ 1 & \text{otherwise} \end{cases}$$

The last sum is extended over all positive divisors d of n whose k th power also divide n .

The key point here is again “multiplicative”, since $\mu(d)$ is multiplicative so is $\sum_{d^2|n} \mu(d)$ so we need to only consider $g(p^\alpha) = \sum_{d^2|p^\alpha} \mu(d)$ but note that even though the sum is over $d^2 \rightarrow \sum_{d^2|n}$, μ is only taking d , $\mu(d)$ and not $\mu(d^2)$

$$\begin{aligned} \sum_{d^2|p^\alpha} \mu(d) &= \mu(1) + \mu(p) \\ &= 1 - 1 \\ &= 0 \end{aligned}$$

The above holds if $\alpha > 1$ otherwise for $0 \leq \alpha \leq 1 \rightarrow \sum_{d^2|p^\alpha} \mu(d) = \mu(1) = +1$, in short

$$\begin{aligned} g(p^\alpha) = \sum_{d^2|p^\alpha} \mu(d) &= \begin{cases} 0 & \text{if } \alpha > 1 \\ 1 & \text{if } 0 \leq \alpha \leq 1 \end{cases} \\ &= \mu^2(p^\alpha) \end{aligned}$$

The second part follows closely, again since it is multiplicative and again note that even though the sum is over $d^k \rightarrow \sum_{d^k|n}$, μ is only taking d , $\mu(d)$ and not $\mu(d^k)$

$$\begin{aligned} \sum_{d^k|p^\alpha} \mu(d) &= \mu(1) + \mu(p) \\ &= 1 - 1 \\ &= 0 \end{aligned}$$

if $\alpha > k$ otherwise for $0 \leq \alpha \leq k \rightarrow \sum_{d^k|p^\alpha} \mu(d) = \mu(1) = +1$, the only difference now is that we can't say it is equal to $\mu^2(p^\alpha)$ because say $\alpha = k - 1 > 0 \rightarrow \mu(p^{k-1}) = 0$ but $\sum_{d^k|p^{k-1}} \mu(d) = \mu(1) = +1$

Problem 2.7. Let $\mu(p, d)$ denote the value of the Mobius function at the gcd of p and d . Prove that for every prime p we have

$$\sum_{d|n} \mu(d)\mu(p, d) = \begin{cases} 1 & \text{if } n = 1 \\ 2 & \text{if } n = p^a, a \geq 1 \\ 0 & \text{otherwise.} \end{cases}$$

The thing is the gcd (p, mn) is multiplicative as long as $(m, n) = 1$ because p is prime and once we expand m and n in their primal constituents it is evident, *i.e.* $(p, mn) = (p, m)(p, n)$, therefore $\mu(p, mn) = \mu(p, m)\mu(p, n)$

The first case is obvious $\sum_{d|1} \mu(d)\mu(p, d) = \mu(1)\mu(1) = 1$.

The second case

$$\begin{aligned} \sum_{d|p^a} \mu(d)\mu(p, d) &= \mu(1)\mu(p, 1) + \mu(p)\mu(p, p) \\ &= \mu(1)\mu(1) + \mu(p)\mu(p) \\ &= (1)(1) + (-1)(-1) \\ &= 2 \end{aligned}$$

To show the last case it's easiest to utilize the fact that $g(n) = \sum_{d|n} \mu(d)\mu(p, d)$ is multiplicative and now we just need to show $g(q^b)$, $q \neq p$ as $g(p^a)$ is already covered above

$$\begin{aligned} g(q^b) &= \sum_{d|q^b} \mu(d)\mu(p, d) = \mu(1)\mu(p, 1) + \mu(q)\mu(p, q) \\ &= \mu(1)\mu(1) + \mu(q)\mu(1) \\ &= (1)(1) + (-1)(1) \\ &= 0 \end{aligned}$$

Problem 2.8. Prove that

$$\sum_{d|n} \mu(d) \log^m d = 0$$

if $m \geq 1$ and n has more than m distinct prime factors. [*Hint:* Induction.]

To use induction we need to prove the base case, the thing is that \log is not multiplicative, so that's a bit hard. The base case should be $m = 1$ and then we go up from there to bigger m !? $\neg \setminus (^{\circ} _ o) / \neg$

But one thing I notice is that we only need to consider numbers with one power of distinct primes, *i.e.* $n = p_1 p_2 \dots p_k$ because $\mu(d)$ is zero if the powers of the primes are not zero that is

$$\begin{aligned} \sum_{d|n} \mu(d) \log^m d &= \cancel{\mu(1) \log^m(1)} + \mu(p_1) \log^m(p_1) + \dots + \mu(p_k) \log^m(p_k) + \\ &\quad \mu(p_1 p_2) \log^m(p_1 p_2) + \dots + \mu(p_{k-1} p_k) \log^m(p_{k-1} p_k) + \dots + \\ &\quad \mu(p_1 p_2 \dots p_k) \log^m(p_1 p_2 \dots p_k) \end{aligned}$$

and from the definition of $\mu(d)$ we know that if it has odd number of primes it's negative and if there are an even number of distinct primes μ is positive, therefore

$$\begin{aligned} \sum_{d|n} \mu(d) \log^m d &= -(\log^m(p_1) + \dots + \log^m(p_k)) \\ &\quad + (\log^m(p_1 p_2) + \dots + \log^m(p_{k-1} p_k)) + \\ &\quad - (\log^m(p_1 p_2 p_3) + \dots + \log^m(p_{k-2} p_{k-1} p_k)) + \\ &\quad (-1)^k \log^m(p_1 p_2 \dots p_k) \end{aligned}$$

Since log is additive we can expand them but before we do that let's denote $\log(p_k) = l_k$

$$\begin{aligned} \sum_{d|n} \mu(d) \log^m d &= - \sum_{i_1=(k|1)} l_{i_1}^m + \sum_{i_1, i_2=(k|2)} (l_{i_1} + l_{i_2})^m - \sum_{i_1, i_2, i_3=(k|3)} (l_{i_1} + l_{i_2} + l_{i_3})^m + \\ &\quad \dots + (-1)^k \sum_{i_1, i_2, \dots, i_k=(k|k)} (l_{i_1} + l_{i_2} + \dots + l_{i_k})^m \end{aligned}$$

where the notation $(k|j)$ means that all combinations of k choose j , as a concrete example, say $m = 4$, $k = 5$ which is the minimum k required

$$\begin{aligned} \sum_{d|n} \mu(d) \log^m d &= -(l_1^4 + l_2^4 + l_3^4 + l_4^4 + l_5^4) + \\ &\quad + ((l_1 + l_2)^4 + (l_1 + l_3)^4 + (l_1 + l_4)^4 + (l_1 + l_5)^4 + (l_2 + l_3)^4 + (l_2 + l_4)^4 + \\ &\quad (l_2 + l_5)^4 + (l_3 + l_4)^4 + (l_3 + l_5)^4 + (l_4 + l_5)^4) + \\ &\quad - ((l_1 + l_2 + l_3)^4 + (l_1 + l_2 + l_4)^4 + (l_1 + l_2 + l_5)^4 + (l_1 + l_3 + l_4)^4 + \\ &\quad (l_1 + l_3 + l_5)^4 + (l_1 + l_4 + l_5)^4 + (l_2 + l_3 + l_4)^4 + (l_2 + l_3 + l_5)^4 + \\ &\quad (l_2 + l_4 + l_5)^4 + (l_3 + l_4 + l_5)^4) \\ &\quad + ((l_1 + l_2 + l_3 + l_4)^4 + (l_1 + l_2 + l_3 + l_5)^4 + (l_1 + l_2 + l_4 + l_5)^4 + \\ &\quad (l_1 + l_3 + l_4 + l_5)^4 + (l_2 + l_3 + l_4 + l_5)^4) + \\ &\quad - ((l_1 + l_2 + l_3 + l_4 + l_5)^4) \end{aligned}$$

Now we gather coefficients of same powers, say we collect all l_1^4 ,

$$(5|1) \rightarrow (-1)l_1^4$$

$$(5|2) \rightarrow (+4)l_1^4$$

$$(5|3) \rightarrow (-6)l_1^4$$

$$(5|4) \rightarrow (+4)l_1^4$$

$$(5|5) \rightarrow (-1)l_1^4$$

so it's basically the Pascal triangle coefficients, why is this? Well, for example, for $(5|1)$, first we fix **one** l and then choose a partner for it from the remaining **four**, however in this case we only need one l and we already fixed it, so we will just need **zero** partner, *i.e.* $\binom{4}{0} = 1$.

For $(5|2)$ we first pick an l and then choose a partner (again because $(5|2)$ means we need **2** l 's in total) for it from 4 available choices, which is $\binom{4}{1}$, *i.e.* this l will appear $\binom{4}{1} = 4$ times, for $(5|3)$ it's the same thing we first pick an l and then choose *two* partners for it, *i.e.* this l will then appear $\binom{4}{2} = 6$ times, and for $(5|3)$, it's pick an l and choose $\binom{4}{3} = 4$ partners and so on and therefore the coefficients of l_1 is just those of Pascal triangle's but with the signs alternating between plus and minus. And this is true for other l 's not just l_1 .

We now need to tackle the cross terms say $l_1^3 l_2$, first thing to note that this cross product is always preceded by a constant (which again is from Pascal triangle), for $(l_1 + l_2)^4$ it is $4l_1^3 l_2$, note that this coefficient is the same no matter how many terms are being exponentiated, *i.e.* even for $(l_1 + l_2 + l_3 + \dots + l_w)^4$, the coefficient for $l_1^3 l_2$ is still 4 because it is still $\binom{4}{3}$ no matter what, this is because

$$(l_1 + l_2 + \dots)^4 = \underbrace{(l_1 + l_2 + \dots)}_{\text{bin \#1}} \underbrace{(l_1 + l_2 + \dots)}_{\text{bin \#2}} \underbrace{(l_1 + l_2 + \dots)}_{\text{bin \#3}} \underbrace{(l_1 + l_2 + \dots)}_{\text{bin \#4}}$$

To get $l_1^3 l_2$ we need to gather **three** l_1 's and we have **four** bins to choose for as shown above that's why we have 4 choose 3, $\binom{4}{3} = 4$ possibilities. And as the number of bins are the same no matter how many l 's we have the number of possibilities is still the same.

We also have other cross terms like $l_1^2 l_3 l_4$, in this case, we need to gather **two** l_1 's from **four** bins so it's $\binom{4}{2} = 6$, next we need to choose **one** l_3 from the remaining **two** bins

which is $\binom{2}{1} = 2$ and once we've chosen the bin for l_2 , the other bin will definitely contain l_3 , so in total there are

$$\binom{4}{2} \times \binom{2}{1} = 6 \times 2 = 12$$

and since the number of bins is constant no matter what this coefficient remains the same no matter how many l 's we have.

So now for $4l_1^3l_2$ we have

$$\begin{aligned} (5|1) &\rightarrow (0) \\ (5|2) &\rightarrow (+1)4l_1^3l_2 \\ (5|3) &\rightarrow (-3)4l_1^3l_2 \\ (5|4) &\rightarrow (+3)4l_1^3l_2 \\ (5|5) &\rightarrow (-1)4l_1^3l_2 \end{aligned}$$

again Pascal triangle, why is this? This time we fix **two** l 's (instead of just one for l^4 above), and then calculate how many partners this couple might have, for $(5|2)$, we only need **two** in total so because we already fixed two of them we just need **zero** partner from the three remaining ones, *i.e.* $\binom{3}{0} = 1$. For $(5|3)$, again we fix **two** l 's and choose one more partner (because in total we need 3) from the remaining three, *i.e.* $\binom{3}{1} = 3$ and so on. This is also true for any two-term cross terms.

And this pattern continues for higher cross terms like $l_1^2l_2l_3$, *e.g.* for $(5|4)$ we fix **three** l 's and then choose one partner from the remaining **two**, which means $\binom{2}{1} = 2$.

The pattern continues for any k , say we now have $k = 6$ while m stays the same, $m = 4$, in this case we have $(6|1), (6|2), (6|3), (6|4), (6|5), (6|6)$, and the number of say l_1^4 is given by the recipe above, fix an l and then choose a partner for it depending on which combination $(6|j)$ you're on, therefore the general formula is

In Exercises 10, 11, and 12, $d(n)$ denotes the number of positive divisors of n .

Problem 2.10. Prove that $\prod_{t|n} t = n^{d(n)/2}$.

Again, let's decompose n into its primal constituents $n = \prod_i^N p_i^{\alpha_i}$ then $d(n)$ is given by

$$d(n) = d\left(\prod_i^N p_i^{\alpha_i}\right) = \prod_i^N (\alpha_i + 1)$$

To see why this is we just need to recall that the number of combinations an N -digit (base-10) number has is

$$\# \text{ of combo} = \underbrace{10 \times 10 \times 10 \times \dots \times 10}_{N \text{ of them}}$$

because each digit can take 10 possible different values. For our case, each prime factor plays the role of a digit, however, each has different possible values, which is $(\alpha_i + 1)$ because we can have $p_i^0, p_i^1, p_i^2, \dots, p_i^{\alpha_N}$ so the total number of combinations for $\prod_i^N p_i^{\alpha_i}$ is

$$\# \text{ of combo} = \underbrace{(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \dots (\alpha_N + 1)}_{N \text{ prime factors}}$$

Next, we can decompose $\prod_{t|n} t$ in terms of its primal constituents as well, say we focus on p_1 of $\prod_i^N p_i^{\alpha_i}$, the divisors of $p_1^{\alpha_1}$ are $p_1^0, p_1^1, \dots, p_1^{\alpha_1}$, so if we multiply all of them we have $p_1^{1+2+3+\dots+\alpha_1} = p_1^{\frac{\alpha_1(\alpha_1+1)}{2}} = (p_1^{\alpha_1})^{\frac{\alpha_1+1}{2}}$.

But here $p_1^{\alpha_1}$ is not alone, each divisor of $p_1^{\alpha_1}$, *i.e.* p_1^j , $0 \leq j \leq \alpha_1$, occurs $(\alpha_2 + 1)(\alpha_3 + 1) \dots (\alpha_N + 1)$ times, so the final exponent for p_1 in $\prod_{t|n} t$ is

$$(p_1^{\alpha_1})^{\frac{(\alpha_1+1)}{2}(\alpha_2+1)(\alpha_3+1)\dots(\alpha_N+1)} = (p_1^{\alpha_1})^{d(n)/2}$$

the same case goes for any other p_i , thus $\prod_{t|n} t = n^{d(n)/2}$. As a concrete example, take $n = p_1^2 p_2^3$, the divisors of n are

$$\begin{array}{cccc} p_1^0 & p_2^0 & p_1^0 & p_2^1 & p_1^0 & p_2^2 & p_1^0 & p_2^3 \\ p_1^1 & p_2^0 & p_1^1 & p_2^1 & p_1^1 & p_2^2 & p_1^1 & p_2^3 \\ p_1^2 & p_2^0 & p_1^2 & p_2^1 & p_1^2 & p_2^2 & p_1^2 & p_2^3 \end{array}$$

so you can see that $(p_1^0 p_1^1 p_1^2)$ occurs $4 = (\alpha_2 + 1)$ times $\rightarrow (p_1^0 p_1^1 p_1^2)^{\alpha_2+1}$.

Problem 2.11. Prove that $d(n)$ is odd if, and only if, n is square.

As shown above for $n = \prod_i^N p_i^{\alpha_i}$, $d(n) = \prod_i^N (\alpha_i + 1)$, so to get $d(n)$ to be odd we need *all* of α_i to be even so that $(\alpha_i + 1)$ is odd, therefore n must be even

Problem 2.12. Prove that $\sum_{t|n} d(t)^3 = \left(\sum_{t|n} d(t) \right)^2$.

The above relationship is evidently not true in general, we therefore need to utilize the properties of $d(t)$ to derive it. One thing to note is that $g(n) = \sum_{t|n} d(t)^3$ is multiplicative as $d(t)$ is. Therefore we just need to consider $g(p^\alpha) = \sum_{t|p^\alpha} d(t)^3$.

My strategy would be to utilize induction. Assume that $\sum_{t|p^\alpha} d(t)^3 = \left(\sum_{t|p^\alpha} d(t)\right)^2$ is true up to some p^α , we now want to know what happens with $p^{\alpha+1}$

$$\sum_{t|p^{\alpha+1}} d(t)^3 = d(p^{\alpha+1})^3 + \sum_{t|p^\alpha} d(t)^3$$

and $d(p^{\alpha+1}) = \alpha + 2$ thus

$$\begin{aligned} d(p^{\alpha+1})^3 + \sum_{t|p^\alpha} d(t)^3 &= (\alpha + 2)^3 + \left(\sum_{t|p^\alpha} d(t)\right)^2 \\ &= (\alpha + 2)^2(\alpha + 2) + \left(\sum_{t|p^\alpha} d(t)\right)^2 \\ &= (\alpha + 2)^2 + (\alpha + 2)^2(\alpha + 1) + \left(\sum_{t|p^\alpha} d(t)\right)^2 \\ &= d(p^{\alpha+1})^2 + (\alpha + 2) \cdot 2 \frac{(\alpha + 2)(\alpha + 1)}{2} + \left(\sum_{t|p^\alpha} d(t)\right)^2 \\ &= d(p^{\alpha+1})^2 + 2d(p^{\alpha+1}) \left(\sum_{t|p^\alpha} d(t)\right) + \left(\sum_{t|p^\alpha} d(t)\right)^2 \\ &= \left(d(p^{\alpha+1}) + \sum_{t|p^\alpha} d(t)\right)^2 \\ \sum_{t|p^{\alpha+1}} d(t)^3 &= \left(\sum_{t|p^{\alpha+1}} d(t)\right)^2 \end{aligned}$$

Going to line 5 we have used the fact that $\sum_{t|p^\alpha} d(t) = \sum_{i=1}^{\alpha+1} i = \frac{(\alpha+1)(\alpha+2)}{2}$ since $d(p^j) = j + 1$. We can of course dispel induction for a bruter force approach by expanding $\sum_{t|p^{\alpha+1}} d(t)^3 = \sum_{i=1}^{\alpha+1} i^3$ but this requires us to know the formula for a sum of consecutive cubes $\sum_{i=1}^n i^3 = \left(\frac{n(n+1)}{2}\right)^2$