Directed Reading Program Project: Prime-Time

Max Feldman

November 29, 2024

Inspiration / Attribution

The proof contained in this document was inspired by a youtube video by youtuber "Combo Class" and a video he made that gives a high level argument for why a peculiar function has finitely many cycles.
The link to his video is HERE

Definition of φ

$$\varphi : \mathbb{N} \to \mathbb{N}$$
$$n = p_1^{a_1} p_2^{a_2} .. p_k^{a_k} \longmapsto (p_1 + a_1)(p_2 + a_2)..(p_k + a_k)$$

It is clear that φ is multiplicative.
I.e. if $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.

Combinatorial Perspective

φ can be thought of as the sum of the squarefree kernel of the divisors of n.
That is,

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

where κ is the squarefree kernel.
That is κ takes p^a to p when $a = 1$ and takes p^a to 1 when $a \neq 1$.

Consider,

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})..\varphi(p_k^{a_k}) =$$
$$(p_1 + a_1)(p_2 + a_2)..(p_k + a_k) =$$
$$(p_1 + \sum_{i=1}^{a_1} 1)(p_2 + \sum_{i=1}^{a_2} 1)..(p_k + \sum_{i=1}^{a_k} 1)$$

When thinking about this combinatorially, in the expansion of the above any term is the product of primes that divide n and 1s.

Note that there are $\prod(a_i+1)$ terms in the expansion as well as $\prod(a_i+1)$ divisors of n.
We think of each p_i in a term as representing that it is divisible by p_i but not p_i^2.
We think of the lack of each p_i in a term as representing that it is either not divisible by p_i or is divisible by p_i^2.
With a bit of thought we see that the number of times a given term appears in the expansion is exactly the number of divisors that κ maps to the term.
And so we now see,

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

Möbius Inversion

We can use Möbius inversion to find an interesting identity

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

Behavior of φ on p^a

We ask when φ grows, shrinks, or stays the same on a prime number p to a power a.
This gives us information about what φ does to a given component of the prime factorization of n.

We first analyse the case of $p = 2$

When $a = 1$ we see $2 = 2^1 < \varphi(2^1) = 3$.
When $a = 2$ is is easy to see that $2^2 = \varphi(2^2) = 4$.
When $a = 3$, we have $8 = 2^3 > \varphi(2^3) = 5$.
It is clear that $\frac{p^{a+1}}{\varphi(p^{a+1})} > \frac{p^a}{\varphi(p^a)}$ and so for all $a > 2$ we have $2^a > \varphi(2^a)$

We now consider $p > 2$

When $a = 1$ it is clear that $p^1 = p < p + 1 = \varphi(p^1)$.
I.e. for all primes p, $p^1 < \varphi(p^1)$.
When $a > 1$ we have $\frac{p^a}{\varphi(p^a)} > \frac{2^a}{\varphi(2^a)} \geq 1$ and so $p^a > \varphi(p^a)$.

We now see,

$$p^a = \varphi(p^a)$$

if and only if $p = 2$ and $a = 2$

$$p^a < \varphi(p^a)$$

if and only if $a = 1$

$$p^a > \varphi(p^a)$$

if and only if $a > 1$ (when $p > 2$) or $a > 2$ (when $p = 2$)

Cycles of Length 1/Fixed points

We may ask about the behavior of φ as we apply it recursively on its output. We now attempt to show that there is a finite number of fixed points (integers n s.t. $\varphi(n) = n$)

We will now try to identify all integers n s.t. $\varphi(n) = n$.
It will be convenient for us to write any candidate n in the form $n = 2^t \prod p_i^{a_i} \prod q_i^{b_i}$ where $p_i^{a_i}$ are the components of n not divisible by 2 that φ shrinks ($a_i > 1$) and $q_i^{b_i}$ are the components of n not divisible by 2 that φ grows ($b_i = 1$)
Note that when $n = \varphi(n)$ we must have,

$$\frac{2^t \prod p_i^{a_i} \prod q_i^{b_i}}{(2+t)\prod(p_i + a_i)\prod(q_i + b_i)} = \frac{2^t \prod p_i^{a_i} \prod q_i}{(2+t)\prod(p_i + a_i)\prod(q_i + 1)} = 1$$

we will make use of this fact later,

We now work by cases in terms of t

Case $t = 0$:

We need to find a solution to,

$$\prod p_i^{a_i} \prod q_i = \prod(p_i + a_i)\prod(q_i + 1)$$

Notice that if $n = 1$ we have a trivial solution as the above.
If $n \neq 1$ is a solution then both $\prod p_i^{a_i}$ and $\prod q_i^{b_i}$ are not the empty product.
Notice that $2 \mid (q_1 + 1)$ yet $2 \nmid n$ and so we cannot have a non-trivial solution where $t = 0$.

Solutions where $t = 0$: $n = 1$.

Case $t = 1$:

We must have,

$$2\prod p_i^{a_i} \prod q_i = 3\prod(p_i + a_i)\prod(q_i + 1)$$

Note that if there is more than one q_i then we have that the right hand side is divisible by 2^2 yet the left hand side is not.
And so we have at most one q_i

We first consider the case where $\prod q_i$ is the empty product.
Then,

$$\prod \frac{p_i^{a_i}}{p_i + a_i} = \frac{3}{2}$$

and so we see that 3 must divide the numerator, we let $y > 1$ denote the maximum power of 3 that divides n
We now get,

$$\frac{3^y}{3+y} \prod \frac{p_i^{a_i}}{p_i + a_i} = \frac{3}{2}$$

and so,

$$\prod \frac{p_i^{a_i}}{p_i + a_i} = \frac{3+y}{3^{y-1}2}$$

yet for all $y > 1$ we have,

$$1 \leq \prod \frac{p_i^{a_i}}{p_i + a_i} = \frac{3+y}{3^{y-1}2} < 1$$

a contradiction.
And so we cannot have a solution where we have no q_i.
And so we must have one and only one q_i which we will denote q,
We then have,

$$2q \prod p_i^{a_i} \; = 3(q+1) \prod (p_i + a_i)$$

And so 3 divides the left hand side.
In the case where $3 \mid p$ we have $2 \cdot 3 \prod p_i^{a_i} \; = 3 \cdot 4 \prod (p_i + a_i)$ so we must have that 4 divides the left hand side which it clearly does not as we selected $t = 1$.
This means that we must have $3 \mid \prod p_i^{a_i}$.
We let $s > 1$ denote the maximum power of 3 that divides n.
We now have,

$$2q3^s \prod p_i^{a_i} \; = 3(q+1)(3+s) \prod (p_i + a_i)$$

and so

$$\frac{2q3^{s-1}}{(q+1)(3+s)} = \prod \frac{p_i + a_i}{p_i^{a_i}}$$

Notice that for $s > 2$ we get,

$$1 < \frac{2q3^{s-1}}{(q+1)(3+s)} = \prod \frac{p_i + a_i}{p_i^{a_i}} \leq 1$$

a contradiction so we must have $s = 2$,

$$6q \prod p_i^{a_i} \; = (q+1)5 \prod (p_i + a_i)$$

And so 5 divides the left hand side. Namely 5 divides either q or $\prod p_i^{a_i}$.
Case 5 divides q:

Thus we must have $q = 5$

$$6 \cdot 5 \prod p_i^{a_i} = 6 \cdot 5 \prod (p_i + a_i)$$
$$\prod p_i^{a_i} = \prod (p_i + a_i)$$

That is the remaining components of n must be the empty product.
We then have $n = 2^1 3^2 5^1 = 90$ and we verify $\varphi(90) = 90$.

Case 5 divides $\prod p_i^{a_i}$
We let $r > 1$ denote the highest power of 5 that divides n.
We must have,

$$1 < \frac{5^{r-1} 6q}{(q+1)(5+r)} = \prod \frac{p_i + a_i}{p_i^{a_i}} \leq 1$$

a contradiction and so we have no solutions where $5 \mid \prod p_i^{a_i}$.

We have now exhaused all cases for $t = 1$ and have found

Solutions where $t = 1$: $n = 90$.

Case $t = 2$:

Say that $n = 2^2 \prod p_i^{a_i} \prod q_i^{b_i}$ is a solution, then,

$$2^2 \prod p_i^{a_i} \prod q_i = (2+2) \prod (p_i + a_i) \prod (q_i + 1)$$
$$\prod p_i^{a_i} \prod q_i = \prod (p_i + a_i) \prod (q_i + 1)$$

i.e. any solution with $t = 2$ can be divided by 4 to yield a solution to the $t = 0$ case.
Since there is only the trivial solution to the $t = 0$ then $n = 4(1)$ is the only potential candidate with $t = 2$.
Clearly $\varphi(4) = 4$.
We now see this is the only solution.

Solutions where $t = 2$: $n = 4$.

Case $t = 3$:

We must have,

$$2^3 \prod p_i^{a_i} \prod q_i = 5 \prod (p_i + a_i) \prod (q_i + 1)$$

And since $t = 3$ we must have that there are at most 3 q_i terms in n
And so we must have $5 \mid \prod p_i^{a_i} \prod q_i$,

Case $5 \mid \prod p_i^{a_i}$,
Let $s > 1$ be the maximum power of 5 that divides n, we get,

$$8 \cdot 5^{s-1} \prod p_i^{a_i} \prod q_i = (5+s) \prod (p_i + a_i) \prod (q_i + 1)$$

and then for any integer $s > 1$,

$$\frac{8 \cdot 5^{s-1}}{5+s} = \frac{\prod(p_i + a_i) \prod(q_i + 1)}{\prod p_i^{a_i} \prod q_i} \leq \frac{\prod(q_i + 1)}{\prod q_i} \leq \frac{(q_1+1)(q_2+1)(q_3+1)}{q_1 q_2 q_3} < \frac{8 \cdot 5^{s-1}}{5+s}$$

a contradiction and so we must have $5 \mid \prod q_i$.
Then we have,

$$5 \cdot 8 \prod p_i^{a_i} \prod q_i = 5(6) \prod (p_i + a_i) \prod (q_i + 1)$$

$$4 \prod p_i^{a_i} \prod q_i = 3 \prod (p_i + a_i) \prod (q_i + 1)$$

And so $3 \mid \prod p_i^{a_i} \prod q_i$
Case $3 \mid \prod p_i^{a_i}$, let $k > 1$ be the maximum power of 3 that divides n,

$$4 \cdot 3^{k-1} \prod p_i^{a_i} \prod q_i = (3+k) \prod (p_i + a_i) \prod (q_i + 1)$$

and there are at most two remaining q_i terms that we have not accounted for,

$$3 = \frac{12}{4} \leq \frac{4 \cdot 3^{k-1}}{3+k} = \prod \frac{p_i^{a_i}}{(p_i + a_i)} \prod \frac{q_i + 1}{q_i} \leq \frac{q_i + 1}{q_i} \leq \left(\frac{8}{7}\right)\left(\frac{12}{11}\right) < 3$$

a contradiction,
and so we must have $3 \mid \prod q_i$,
That is there is some $q_i = 3$,
Putting all the terms together we find,

$$120 \prod p_i^{a_i} \prod q_i = 120 \prod (p_i + a_i) \prod (q_i + 1)$$

and so any solution with $t = 3$ must be divisible by 120 and divide by 120 to a solution with $t = 0$.
Since 1 is the only solution with $t = 0$ we have that 120 is the only possible solution with $t = 3$.
Clearly $120 = 2^3 \cdot 3 \cdot 5 = (2+3)(3+1)(5+1)$.
Thus we see 120 is the only solution with $t = 3$.

Solution where $t = 3$: $n = 120$.

Case $t > 3$:
We take $L_t := \frac{2^t}{2+t}$
Notice for $t > 3$ we have,

$$\frac{8}{3} \leq L_t$$

We let ρ_i denote the i^{th} odd prime
Next we take $S_t := \prod_{i=1}^{t} \frac{\rho_i+1}{\rho_i}$ we get
Notice for $t = 4$,

$$S_t = \frac{4 \cdot 6 \cdot 8 \cdot 12}{3 \cdot 5 \cdot 7 \cdot 11} < L_t = \frac{8}{3}$$

We now say that for $t = k$ we have $S_t < L_t$
We take $l_t := \frac{2(2+t)}{3+t}$ and
take $s_t := \frac{12}{11}$
Notice,

$$L_{t+1} = L_t l_t$$

and,

$$S_{t+1} \leq S_t r_t$$

Notice,

$$\frac{12}{11} = r_t < \frac{12}{7} \leq l_t$$

for all $t > 3$ since $S_t < L_t$ and $s_t < l_t$
And so we have,

$$S_{t+1} \leq S_t s_t < L_t l_t = L_{t+1}$$

We now have shown induction,
Since we have a base case with $t = 4$ we now see that $S_t < L_t$ for all $t > 3$

We assume that there is a solution where $t > 3$
We let n_t be such a solution with specific $t > 3$
We write n_t in the form we have seen earlier,

$$n_t = 2^t \prod p_i^{a_i} \prod q_i$$

and take $R_t := \prod \frac{q_i+1}{q_i}$
Notice we have,

$$2^t \prod p_i^{a_i} \prod q_i = (2+t) \prod (p_i + a_i) \prod (q_i + 1)$$

and so,

$$L_t = \frac{\prod (p_i + a_i) \prod (q_i + 1)}{\prod p_i^{a_i} \prod q_i} \leq \prod \frac{q_i + 1}{q_i} \leq S_t < L_t$$

this is a contradiction,
And so we see that there cannot be a solution where $t > 3$

Soltuions where $t > 3$: N/A

Complete list of Fixed points

In the previous section we discovered 4 fixed points and showed that there can be no others.
The four fixed points we found are:

$$1, 4, 90, 120$$