T. 3.1

$n \in \mathbb{N}_{\geq 1}$.

$\ell(n)$ is the shortest length of an additron chain $a_0 = 1 < a_1 < \dots < a_{\ell(n)} = n$
i.e. $\forall k \in \mathbb{N}$ s.t. $1 \leq k \leq \ell(n)$ $\exists\ 0 \leq i, j < k$ s.t. $a_i + a_j = a_k$ with $a_i \in \mathbb{Z}\ \forall i$

a) If $2^s \leq n < 2^{s+1}$ and $s \geq 1$

$\Rightarrow s \leq \ell(n) \leq 2s$

First prove that $s \leq \ell(n)$:

We have that

$$a_0 < a_1 < a_2 < a_3 \dots \leq a_k < \dots < a_{\ell(n)} \Rightarrow n \leq 2^{\ell(n)}$$

$a_0 = 1$, $a_1 = 2$, $a_2 = 4$, $a_3 = 8$, $a_k = 2^k$, $a_{\ell(n)} = 2^{\ell(n)}$, $a_{\ell(n)} = n$

BUT $2^s \leq n \Rightarrow 2^s \leq n \leq 2^{\ell(n)} \Rightarrow 2^s \leq 2^{\ell(n)} \Rightarrow s \leq \ell(n)$ ✓

Now prove that $\ell(n) \leq 2s$:

We build an additron chain that adds up to n, where $2^s \leq n < 2^{s+1}$ for some $s \geq 1$.

The idea is to think of the binary representation of n. We must have that

$$n_{(2)} = 1 \underbrace{* * \dots *}_{s \text{ positions}}.$$

So now we look for an addition chain as described before, whose length is $L \leq 2s$.

Define an additron chain s.t.

$$a_k = 2a_{k-1} = 2^k \quad \forall k = 1, \dots, s, \quad \text{having } a_0 = 1$$

We know that such additron chain will have at least s terms, due to the first part of the exercise and $a_s = 2^s$, to which we will then add what we need to reach n.

In what follows we investigate the remaining terms of the chain (at most s).

The main idea leverages the fact that we can use the the previous s terms of the additron chain to get to the value n in the end as any positive integer can be obtained as the sum of powers of two, through its binary expansion.

I present an example to show the intent of this method:

eg: $n = 12$, $2^3 \le n < 2^4$, $s = 3$.

$n = 2^3 + 2^2$

$a_0 = 1$, $a_1 = 2$, $a_2 = 2^2$, $a_3 = 2^3$ (FIRST s steps)
$a_4 = a_3 + 2^2 = 2^3 + a_2 = 12$.

So, after adding elements up to $2^s = 8$, I want to add elements from the binary expansion of n in an increasing order.

This small example can make one realize that we want to add a_{z_j} to the previous element of the addition chain, where z_j is the exponent of the appropriate power of 2 in the expansion.
In this case $z_0 = 2$

So, if we write the binary expansion of n as

$$n = \sum_{j=0}^{\ell} 2^{z_j} \quad \text{with } \{z_j\}_{j=0}^{\ell} \text{ being a strictly increasing sequence having } z_0 \ge 0 \text{ and } z_\ell = s$$

We can define how to compute the remaining elements of the addition chain:

$$a_{s+i+1} = a_{s+i} + a_{z_i} \quad \forall\, i = 0, \dots, \ell - 1$$

This weird indexing is necessary so that we can add the right element everytime.
In the case of $n = 12 = 2^3 + 2^2$, for $i = 0$ we should be adding $a_{z_0} = a_2 = 2^2$ and NOT $a_0 = 2^0 = 1$.
($z_0 = 2$)

In this way we have $a_{s+\ell} = n$.

So, in total, the whole addition chain will be of length $s+\ell$, having s terms from the first part and ℓ terms from the second part:

1st part: $a_k = 2a_{k-1} = 2^k \quad \forall\, k = 1, \dots, s$, having $a_0 = 1$

2nd part: $a_{s+i+1} = a_{s+i} + a_{z_i} \quad \forall\, i = 0, \dots, \ell - 1$

Since $\ell \le s$, then the whole chain is of length $s + \ell \le 2s$.

So, in conclusion we have found an addition chain that sums up to $2^s \le n < 2^{s+1}$ (for $s \ge 1$) of length $L = s + \ell \le 2s$.

Therefore, the shortest length of an addition chain will be s.t.
$\ell(n) \le L \le 2s \implies \ell(n) \le 2s$ □

b) If $r \geq 1$, $s \geq 0$ are integers s.t. $2^{rs} \leq n < 2^{r(s+1)}$

$\Rightarrow \exists$ additron chain for n of length at most $(r+1)s + 2^r - 2$ and which starts with $a_i = i+1 \ \forall i \in \{0, \dots, 2^r - 2\}$.

That is: the addition chain surely starts as

$$a_0 = 1,\ a_1 = 2,\ a_2 = 3,\ \dots,\ a_{2^r-2} = 2^r - 1$$

Definition from Wikipedia "Additron chain":
"The length of an additron chain is the number of sums needed to express all its numbers, which is one less than the cardinality of the sequence"

Proceed by induction on s.

- base case: $s = 0$

  So we have $1 \leq n < 2^r$

  It's clear that we can take the additron chain

  $$a_0 = 1,\ a_1 = 2,\ a_2 = 3,\ \dots,\ a_{2^r-2} = 2^r - 1$$

  built through the rule $a_i = a_{i-1} + 1 \quad \forall i \geq 1$

  This additron chain surely contains n and is of length at most $2^r - 2$.

  That means that $1 \leq n \leq 2^r - 1$ can indeed be represented by an additron chain of length at most $2^r - 2$ ✓

- inductive step: HP: let $s \geq 1$, assume the statement true for $s-1$,

  i.e. $\forall r, \tilde{n} \geq 1$ s.t. $2^{r(s-1)} \leq \tilde{n} < 2^{rs}$

  $\Rightarrow \exists$ additron chain for $\tilde{n}$ of length at most $(r+1)(s-1) + 2^r - 2$ and which starts with $a_i = i+1 \ \forall i \in \{0, \dots, 2^r - 2\}$.

  Consider integers $r \geq 1$, $s \geq 0$ s.t. $2^{rs} \leq n < 2^{r(s+1)}$. (1)

  We perform the euclidean division

  $$n = n' 2^r + b, \text{ where we have } 0 \leq b < 2^r \quad (2)$$

  But then we have $n' = (n - b) \cdot 2^{-r}$ and therefore:

  $$2^{r(s-1)} - 1 \overset{(2)}{\leq} 2^{rs-r} - b \cdot 2^{-r} = (2^{rs} - b) 2^{-r} \overset{(1)}{\leq} n' \overset{(1)}{<} (2^{r(s+1)} - b) 2^{-r} = 2^{rs+r-r} - b \cdot 2^{-r} \overset{(2)}{\leq} 2^{rs}$$

  ($b < 2^r$; $b \geq 0$)

  Hence, $2^{r(s-1)} - 1 < n' < 2^{rs}$

  Therefore, $2^{r(s-1)} \leq n' < 2^{rs}$ (because n' is an integer)

  $\Rightarrow$ we can apply the inductive hypothesis on n'

So we know that there is an addition chain for n' of length at most $(r+1)(s-1)+2^r-2$ and which starts with $a_i = i+1 \ \forall i \in \{0, \dots, 2^r-2\}$.

Now we have to ADD a chain of length $r+1$ to the one just obtained for n', in order to obtain a chain of length $(r+1)s+2^r-2$.

Let $L \leq (r+1)(s-1)+2^r-2$ (3)
be the length of the addition chain for n'.

We will use the fact that $n = n'2^r+b$.

So, first of all, we add the terms

$$a_{L+1} = a_L + a_L = 2a_L = 2n'$$
$$a_{L+2} = 2a_{L+1} = 2^2 n'$$
$$\vdots$$
$$a_{L+r} = 2^r n'$$

to the addition chain.

Therefore, we just added r terms to get to
$a_{L+r} = 2^r n' = n - b$

The last element of the addition chain will be

$$a_{L+r+1} = a_L + b$$

This is possible to do because we have that $0 \leq b < 2^r$ (2).

This means that b is one of the first 2^r-1 elements of the chain.
In other words, b is one of the $a_i = i+1$ for $i \in \{0, \dots, 2^r-2\}$ with which the chain starts, by inductive hypothesis.

Therefore, $a_{L+r+1} = n$ and this chain to obtain n is of length

$$L+r+1 \overset{(3)}{\leq} (r+1)(s-1)+2^r-2+r+1 = (r+1)s + 2^r-2 \quad \square$$

T. 3.5

Th: $\sum_{d \mid n} \varphi(d) = n$

Let us define the function $F(n) := \sum_{d \mid n} \varphi(d)$

We note that

$$F(p^k) = \sum_{i=0}^{k} \varphi(p^i) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^{k-1}) + \varphi(p^k)$$

$\varphi(p^i) = p^{i-1}(p-1)$

$$= 1 + p - 1 + p(p-1) + \ldots + p^{k-2}(p-1) + p^{k-1}(p-1)$$

$$= 1 + p - 1 + p^2 - p + \ldots + p^{k-1} - p^{k-2} + p^k - p^{k-1}$$

$$= p^k.$$

Therefore, $F(p^k) = p^k$ for $k \in \mathbb{N}_{\geq 1}$ and p prime.

Now, let $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ with $p_1, \ldots, p_r$ are distinct primes.

By using the multiplicative property of F, we have

$$F(n) = F(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})$$

$$\overset{(*)}{=} F(p_1^{k_1}) \cdot \ldots \cdot F(p_r^{k_r})$$

$$= p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$$

$$= n.$$

To conclude the proof, we just have to show the validity of $(*)$, that is the multiplicative property of F.

Th: φ is a multiplicative function if the elements of the product are coprime $\Rightarrow F$ is also multiplicative

proof Assume $a, b \in \mathbb{N}$ s.t. $\gcd(a,b) = 1$.

We want to prove that $F(ab) = F(a)\,F(b)$.

We have that $F(ab) = \sum_{d \mid ab} \varphi(d)$.

It's possible to write any divisor of ab as a product of a divisor d_1 of a and a divisor d_2 of b and have $\gcd(d_1, d_2) = 1$.

Therefore

$$F(ab) = \sum_{d \mid ab} \varphi(d) = \sum_{d_1 \mid a,\, d_2 \mid b} \varphi(d_1 d_2) \overset{\varphi \text{ is multiplicative } (\gcd(d_1,d_2)=1)}{=} \sum_{d_1 \mid a,\, d_2 \mid b} \varphi(d_1)\,\varphi(d_2)$$

$$= \sum_{d_1 \mid a} \sum_{d_2 \mid b} \varphi(d_1)\,\varphi(d_2) = \sum_{d_1 \mid a} \left(\varphi(d_1) \sum_{d_2 \mid b} \varphi(d_2) \right)$$

$$= \left(\sum_{d_1 \mid a} \varphi(d_1) \right) \left(\sum_{d_2 \mid b} \varphi(d_2) \right)$$

$$= F(a) \cdot F(b).$$

This concludes the proof $\square$