Question 1

(a) We notice that if we increase our n bits to $n+1$ bits, then we will have to apply every prior c-R_k gate to this $n^{\text{th}}+1$ register for $k \in \{2,\dots,n\}$ in addition to the new c-R_{n+1} gate. So, if we have n registers, and we let $k \in \{2,\dots,n\}$, we see that there will be $n-k+1$ c-R_k gates in C_n. We see that we have exactly n Hadamard gates, so

$$\text{Total} = n + \sum_{k=2}^{n}(n-k+1) = n + n\sum_{k=2}^{n} - \sum_{k=2}^{n} k + \sum_{k=2}^{n} = n + n(n-1) - \left(\frac{n(n+1)}{2} - 1\right) + (n-1)$$

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

(b) We know that for some ket $|\mu\rangle$, and c-$R_k = |0\rangle\langle 0| + e^{i2\pi/2^k}|1\rangle\langle 1|$,

$$E(\text{c}-R_k, I) = \max_{|\mu\rangle} \|(\text{c}-R_k - I)|\mu\rangle\| = \max_{|\mu\rangle} \left\| \left(e^{i2\pi/2^k} - 1\right)|1\rangle\langle 1|\mu\rangle \right\|$$

but since $|\mu\rangle$ is a proper ket, it has norm 1, and thus the maximal such ket in this computation better be when $\langle 0|\mu\rangle = 1$, so

$$E(\text{c}-R_k, I) = \left(\left(e^{i2\pi/2^k} - 1\right)\left(e^{-i2\pi/2^k} - 1\right)\right)^{\frac{1}{2}} = \sqrt{1 - e^{i2\pi/2^k} - e^{-i2\pi/2^k} + 1} = \sqrt{2 - 2\cos\frac{2\pi}{2^k}}$$

where we recoginize the trigonometric identity to give us

$$E(\text{c}-R_k, I) = 2\sqrt{\frac{1-\cos\frac{2\pi}{2^k}}{2}} = 2\sin\frac{\pi}{2^k} \leq 2\frac{\pi}{2^k} = \frac{2\pi}{2^k}$$

as required.

(c) First, we notice that from theorem we know $E^*(F_{n,k+1}, F_{n,k}) = E(F_{n,k+1}, F_{n,k})$. Next, we know that the difference between $F_{n,k+1}$ and $F_{n,k}$ are the c-R_k gates that are missing in the first $n-k$ registers for $F_{n,k}$, but everything else is the same. So, that is to say

$$E^*(F_{n,k+1}, F_{n,k}) = E(F_{n,k+1}, F_{n,k})$$

$$= E(H\otimes\cdots\otimes H\prod_{m=2}^{k-1}\text{c-}R_m \underbrace{H\prod_{m=2}^{k}\text{c-}R_m \otimes H\prod_{m=2}^{k}\text{c-}R_m \otimes\cdots\otimes H\prod_{m=2}^{k}\text{c-}R_m}_{n-k+1\text{ times}}$$

$$, H\otimes\cdots\otimes H\prod_{m=2}^{k-2}\text{c-}R_m \otimes \underbrace{H\prod_{m=2}^{k-1}\text{c-}R_m \otimes H\prod_{m=2}^{k-1}\text{c-}R_m \otimes\cdots\otimes H\prod_{m=2}^{k-1}\text{c-}R_m}_{n-k+2\text{ times}})$$

where the $n-k+1$ comes from **(a)**, as in there are $n-k+1$ c-R_k gates in $F_{n,k+1}$. So, applying our subadditive property, we will notice that the only differences that remain in each component will be the $n-k+1$ c-R_k gates, that is

$$E(F_{n,k+1}, F_{n,k}) \leq \sum_{m=1}^{n-k+1} E(\text{c-}R_k, I) \leq (n-k+1)\frac{2\pi}{2^k}$$

where we use the result from **(b)** to get the final inequality.

(d) Using the given inequality, we want to apply our above result

$$\begin{aligned} E^*(F_n, F_{n,r}) &\leq E^*(F_n, F_{n,n}) + E^*(F_{n,n}, F_{n,n-1}) + \cdots + E^*(F_{n,r+1}, F_{n,r}) \\ &\leq \frac{2\pi}{2^n} + 2\frac{2\pi}{2^{n-1}} + \cdots + (n-r+1)\frac{2\pi}{2^r} = 2\pi \sum_{k=r}^{n} \frac{n-k+1}{2^k}\,. \end{aligned}$$

We recognize that there is a geometric series in there, but more importantly we have to apply the assumption that n is very large, since that is the entire point after all. Then, we can use an upper bound by pushing the series to infinity, where we know

$$\sum_{k=0}^{\infty} \frac{k}{2^k} = 2 \quad \& \quad \sum_{k=0}^{\infty} \frac{1}{2^k} = \frac{1}{1-\frac{1}{2}} = 2\,.$$

So, we get that

$$\begin{aligned} E^*(F_n, F_{n,r}) &\leq 2\pi \sum_{k=r}^{n} \frac{n-k+1}{2^k} = \frac{2\pi}{2^r}\left((n-r+1)\sum_{k=0}^{n-r}\frac{1}{2^k} - \sum_{j=0}^{n-r}\frac{j}{2^j}\right) \\ &< \frac{2\pi}{2^r}\left((n-1)\sum_{k=0}^{\infty}\frac{1}{2^k} - \sum_{j=0}^{\infty}\frac{j}{2^j}\right) = \frac{2\pi}{2^r}\left((n-1)\cdot 2 - 2\right) = \frac{2\pi}{2^r}(2n) = \frac{4n\pi}{2^r} \end{aligned}$$

as required.

(e) We use the upper bound we just computed to find an $\tilde{r}$ given we have an $\epsilon > 0$ and n, we see (using the natural log)

$$\epsilon = \frac{4n\pi}{2^{\tilde{r}}} \implies 2^{\tilde{r}} = \frac{4n\pi}{\epsilon} \implies \tilde{r} = \frac{\log(4n\pi) - \log(\epsilon)}{\log(2)}\,.$$

(f) Assuming $n \gg 0$, we see that the total number of gates in $\tilde{C}_n$ will be the n hadamard gates plus the c-R_k gates that were not removed, so

$$\text{total} = n + \sum_{k=0}^{\tilde{r}-1}(n-k+1) \approx n + \sum_{k=0}^{\tilde{r}-1} n = n + n(\tilde{r}-1) = n\tilde{r}\,.$$

Now, we again apply our approximation for large n to $\tilde{r}$ to get

$$\tilde{r} = \frac{\log(4n\pi) - \log(\epsilon)}{\log(2)} \approx \frac{\log(n) - \log(\epsilon)}{\log(2)} \approx \log\left(\frac{n}{\epsilon}\right)$$

and so the total number of gates is $\approx n\tilde{r} = n\log\left(\frac{n}{\epsilon}\right)$, as expected.

Question 2

(a) By the period finding algorithm, we know that if we want our approximations to hold for the case where n may or may not divide d, we need $d = 2^n > N^2 = 15^2 = 225$, and the smallest such n is exactly $n = 8$, and hence $d = 256$.

(b) We need to use the continued fraction expansion to find the value for r. The period finding algorthim tells us that we are guarenteed (by theorem) that each given x has a possbile value for j/r withen $1/2d \approx 0.001953125$. First, we notice that our first value for x is $\frac{64}{256} = 1/4$, and so a continued fraction expansion will not give us an appropriate measure for a possible r value.

For the second term, we have the continued fraction expansion of $\frac{107}{256}$ which is $[0; 2, 2, 1, 1, 4, 1, 3]$, which is a compact form for writing the a_i values in increasing order ($[a_0; a_1, a_2, \ldots, a_n]$). We look at the expansions to see

$$\frac{1}{2} = 0.5 \quad \frac{2}{5} = 0.4 \quad \frac{3}{7} \approx 0.42857142857142855 \quad \frac{5}{12} \approx 0.4166666666666667 \quad \frac{23}{55} \approx 0.41818181818181815$$

and notice that $|\frac{5}{12} - \frac{107}{256}| = 0.001302 < \frac{1}{2d}$, but $55 > 15$, so we don't use any terms after that fraction. So, we guess that $r = 12$ from this value. Unfortunately, we could have gotten unlucky with our guess, so we continue and check the other values.

For the third term, we see that the continued fraction expansion of $\frac{108}{256}$ which is $[0; 2, 2, 1, 2, 3]$ and we see the first few terms to be

$$\frac{1}{2} = 0.5 \quad \frac{2}{5} = 0.4 \quad \frac{3}{7} \approx 0.42857142857142855 \quad \frac{8}{19} \approx 0.42105263157894735\,.$$

The last term has a denominator too large, so we guess the appropriate term to be $\frac{3}{7}$, but $|\frac{3}{7} - \frac{108}{256}| \approx 0.006696 > \frac{1}{2d}$, and so we can't use this as a guess for our r value.

The final term $\frac{235}{256}$ has $[0; 1, 11, 5, 4]$ as it's continued fraction coeffecients, and further

$$\frac{1}{1} = 1 \quad \frac{11}{12} \approx 0.9166666666666666 \quad \frac{56}{61} \approx 0.9180327868852459\,.$$

Notice the last term has a denominator > 15, so we disregard it. Then, notice $|\frac{11}{12} - \frac{235}{256}| = 0.001302 < \frac{1}{2d}$ and hence we can guess $r = 12$ as a period again!

We see that the two terms for which the period finding algorithm works, it gives us $r = 12$, and hence we can propose with some certainty that r is indeed 12.

Question 3

(a) Notice that gcd(315,14) = 7, and therefore we will not have well defined solutions for the order, since there is no such r such that $14^r = 1 \bmod 315$.

(b) From a simple C++ script, we can find that the order of 46 mod 315 is 3. So, our order is odd, and according to our algorithm, this will be no good as finding a possible root. The reason for this being that since r is odd, we won't be able to find any non-trivial factor of 315, since we can't reduce our term any further.

(c) If we let $a = 104$, we see that we get the order $r = 6$, which is even. So,

$$(104^3 - 1)(104^3 + 1) \equiv 0 (\mathrm{mod}\, 315)$$

and next we check what $(104^3 + 1)$ is modulo 315. We compute this to get

$$104^3 + 1 \equiv 0 (\mathrm{mod}\, 315)$$

which tells us that this $a = 104$ is no good, since we won't be able to find a non-trivial root anymore from this pair. The reason for this is that since we have this congruency with 315, the gcd again will be just one of the values, which is still a trivial factor of 315.

(d) Finally choosing $a = 34$, we can find that the order will be $r = 6$, which is still even. Then, we see that

$$34^3 + 1 \equiv 245 (\mathrm{mod}\, 315)$$

and so we see that

$$\gcd(34^3 + 1, 315) = 35 \quad \& \quad \gcd(34^3 - 1, 315) = 9\,.$$

So, we know that each prime factor of 315 either divides 9 or 35, and hence our non-trivial factors tell us that $315 = 35 \cdot 3^2$.