Exercise 5.1

$U|j\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle$

$\langle j'| U^\dagger U|j\rangle = \frac{1}{N}\sum_{k'=0}^{N-1}\sum_{k=0}^{N-1} e^{-2\pi ij'k'/N}e^{2\pi ijk/N}\delta_{k,k'} = \dfrac{1}{N}\sum_{k=0}^{N-1} e^{2\pi i(j-j')k/N} = \dfrac{1}{N}N\delta_{j,j'} = \delta_{j,j'}$

Therefore, $U^\dagger U = I$, hence U is unitary.

Exercise 5.2

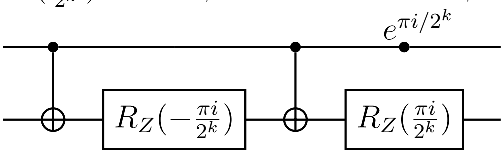
$|00\dots 0\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle = \dfrac{1}{2^{n/2}}\sum_{x_i\in\{0,1\}}|x_1x_2\dots x_n\rangle$

Exercise 5.3

For each y_k we perform 2^n additions and there are 2^n y_k to calculate, hence in total we require $\Theta(2^{2n})$ operations.
(Cooley-Turkey Algorithm) For each x_k we can separate the sum into odd and even indices, then we require 2^n operations assuming the two separate sums are known. This can be done recursively, splitting each sum into 2 pieces. This leads to the number of operations to be $\Theta(2^n\log 2^n) = \Theta(n2^n)$.

Exercise 5.4

Let $R_k = e^{i\alpha}AXBXC$ with $ABC = I$. Taking $\alpha = \frac{\pi i}{2^k}$, $A = I$ $B = R_Z(-\frac{\pi i}{2^k})$ and $C = R_Z(\frac{\pi i}{2^k})$ we see that $ABC = I$ and $AXBXC = XR_Z(-\frac{\pi i}{2^k})XR_Z(\frac{\pi i}{2^k}) = XXR_Z(\frac{\pi i}{2^k})R_Z(\frac{\pi i}{2^k}) = R_Z(\frac{2\pi i}{2^k})$. Hence, the circuit will be,



Exercise 5.5

$FT^{-1} = FT^\dagger$

Exercise 5.6

In the circuit we have $m = \frac{n(n+1)}{2} = \Theta(n^2)$ R_k gates. Using the result of Box 4.1,
$E(U,V) \le m\frac{1}{p(n)} = \Theta(\frac{n^2}{p(n)})$

Exercise 5.7

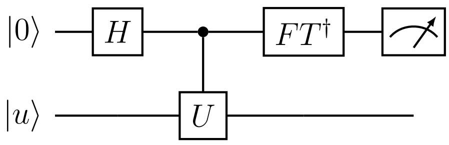
Let $|j\rangle = |j_0j_2\dots j_{n-1}\rangle$, then the circuit implements the following,
$|j\rangle|u\rangle \to |j\rangle((U^{2^0})^{j_0}(U^{2^1})^{j_1}\dots(U^{2^{n-1}})^{j_{n-1}})|u\rangle = |j\rangle U^{j_02^0+j_12^1+\dots+j_{n-1}2^{n-1}}|u\rangle = |j\rangle U^j|u\rangle$

Exercise 5.8

With probability $|c_u|^2$ we will be measuring φ_u for the state $|u\rangle$. If t is of the form of 5.35 each $\tilde{\varphi}_u$ is accurate to n bits of φ_u with probability $1-\epsilon$. Hence, the total probability of measuring φ_u accurate to n bits is $|c_u|^2(1-\epsilon)$.

Exercise 5.9

For this U $\varphi_0 = 0$ and $\varphi_1 = \frac{1}{2}$, hence the circuit is,



The state before the measurement is $|0\rangle|u_0\rangle - |1\rangle|u_1\rangle$, hence after the measurement it will collapse into the $+1$ or -1 eigenbasis. For a first register with a single qubit $FT^\dagger = H$, hence this is the same circuit as that in Exercise 4.34.

Exercise 5.10

$5 = 5 \bmod 21$, $5^2 = 4 \bmod 21$,$5^3 = 20 \bmod 21$, $5^4 = 16 \bmod 21$, $5^5 = 17 \bmod 21$ and $5^6 = 1 \bmod 21$. Hence, the order is 6.

Exercise 5.11

As $gcd(x, N) = 1$, from Euler's formula $x^{\varphi(N)} = 1 \bmod N$. $\varphi(N)$ is the number of y such that $gcd(y, N) = 1$ and $y < N$, hence $\varphi(N) < N$. Therefore, there always exists a number $r \leq N$, such that $x^r = 1(\mathrm{mod} N)$.

Exercise 5.12

$\langle y'| U^\dagger U |y\rangle = \langle xy'|xy\rangle = \langle y'|y\rangle \bmod N$
$0 \leq y \leq N-1$, hence $\langle y'|y\rangle \bmod N = \langle y'|y\rangle = \delta_{y,y'}$. Therefore, $\langle y'| U^\dagger U |y\rangle = \delta_{y,y'}$. Hence, U is unitary.

Exercise 5.13

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{r}\sum_{s=0}^{r-1}\sum_{k=0}^{r-1} e^{-2\pi i s k/r}|x^k \bmod N\rangle = \frac{1}{r}\sum_{k=0}^{r-1}\sum_{s=0}^{r-1} e^{-2\pi i s k/r}|x^k \bmod N\rangle =$$

$$= \frac{1}{r}\sum_{k=0}^{r-1} r\delta_{k0}|x^k \bmod N\rangle = |1\rangle$$

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} e^{2\pi i s k/r}|u_s\rangle = \frac{1}{r}\sum_{s=0}^{r-1}\sum_{k'=0}^{r-1} e^{2\pi i s(k-k')/r}|x^{k'} \bmod N\rangle = \frac{1}{r}\sum_{k'=0}^{r-1} r\delta_{k,k'}|x^{k'} \bmod N\rangle = |x^k \bmod N\rangle$$

Exercise 5.14

Exercise 5.15

Exercise 5.16

Exercise 5.17

Exercise 5.18

Exercise 5.19

Exercise 5.20