Exercise 5.1

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

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

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

Exercise 5.2

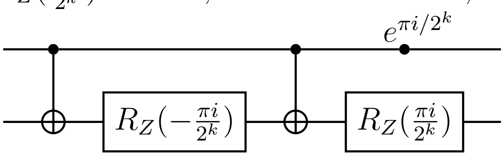
$|00\ldots0\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle = \frac{1}{2^{n/2}}\sum_{x_i\in\{0,1\}}|x_1x_2\ldots x_n\rangle$

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

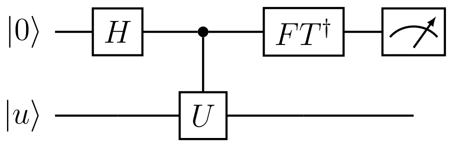
Let $|j\rangle = |j_0j_2\ldots j_{n-1}\rangle$, then the circuit implements the following,
$|j\rangle|u\rangle \to |j\rangle((U^{2^0})^{j_0}(U^{2^1})^{j_1}\ldots(U^{2^{n-1}})^{j_{n-1}})|u\rangle = |j\rangle U^{j_02^0+j_12^1+\ldots+j_{n-1}2^{n-1}}|u\rangle = |j\rangle U^j|u\rangle$

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

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{r}\sum_{s=0}^{r-1}\sum_{k=0}^{r-1} e^{-2\pi i sk/r}|x^k \bmod N\rangle = \frac{1}{r}\sum_{k=0}^{r-1}\sum_{s=0}^{r-1} e^{-2\pi i sk/r}|x^k \bmod N\rangle =$$
$$= \frac{1}{r}\sum_{k=0}^{r-1} r\delta_{k0}|x^k \bmod N\rangle = |1\rangle$$
$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}e^{2\pi i sk/r}|u_s\rangle = \frac{1}{r}\sum_{s=0}^{r-1}\sum_{k'=0}^{r-1} e^{2\pi i s(k-k')/r}|x^{k'} \bmod N\rangle = \frac{1}{r}\sum_{k'=0}^{r-1} r\delta_{k,k'}|x^{k'} \bmod N\rangle = |x^k \bmod N\rangle$$

Exercise 5.14

For V,
$$|\psi\rangle = \sum_{j=0}^{2^t-1}|j\rangle V^j|0\rangle = \sum_{j=0}^{2^t-1}|j\rangle|0 + x^j \bmod N\rangle = \sum_{j=0}^{2^t-1}|j\rangle|x^j \bmod N\rangle$$

Writing $x^j(\mod N) = (x^{j_t 2^{t-1}}(\mod N))(x^{j_{t-1}2^{t-2}}(\mod N))\dots(x^{j_1 2^0}(\mod N))$, each modular multiplication requires $O(L^2)$ gates, hence for the total product of $t-1$ modular multiplications we require $O(L^3)$ gates, and uses the circuit shown in figure 5.2. The addition of k is done after the modular multiplications and requires $O(L)$ gates, hence in total we still require $O(L^3)$ gates.

Exercise 5.15

Let $m = [x, y]$ be the lowest common multiple. Let M be any common multiple. Then we can write $M = mq + r$. x and y divide both M and m, hence they also divide r, meaning it's a common multiple, but $r < m$ and m is the lowest common multiple, therefore $r = 0$.
Now let $x = (x, y)x_1$ and $y = (x, y)y_1$ with $(x_1, y_1) = 1$. x and y divide $(x, y)x_1y_1$ hence it's a common multiple, therefore we can write $(x, y)x_1y_1 = mq_1$. Therefore, we have $x_1 = \frac{m}{y}q_1$ and $y_1 = \frac{m}{x}q_1$, hence q_1 divides both x_1 and y_1. However, $(x_1, y_1) = 1$, hence $q_1 = 1$. Hence, $[x, y] = (x, y)x_1y_1 = (x, y)x_1(x, y)y_1/(x, y) = xy/(x, y)$.
We can use Stein's gcd algorithm which requires $O(L^2)$ gates.

Exercise 5.16

$$\int_x^{x+1} \frac{1}{y^2}dy = \frac{1}{x(x+1)}$$

Consider $\frac{1}{x(x+1)} - \frac{2}{3x^2} = \frac{x-1}{3x^2(x+1)}$

For $x \geq 2$ this is always greater than 0, hence $\int_x^{x+1} \frac{1}{y^2}dy \geq \frac{2}{3x^2}$.

$$\frac{3}{4} = \frac{3}{2}\int_2^{\infty} \frac{1}{y^2}dy = \frac{3}{2}\sum_{q=2}^{\infty}\int_q^{q+1} \frac{1}{y^2}dy \geq \sum_{q=2}^{\infty}\frac{1}{q^2}$$

Therefore, $1 - \sum_q \frac{1}{q^2} \geq 1 - \frac{3}{4} = \frac{1}{4}$, hence equation 5.58 holds.

Exercise 5.17

1) $N = a^b$, taking log of both sides
$L = b \log a$
If $a = 1$, then $L = 1$ and $b = 0$.
If $a \geq 2$, then $\log a \geq 1$, hence as b is a positive integer, $b \leq L$.
2) We want to calculate 2 estimates to $x = \log N/b$, we need $O(1)$ to find y $O(L^2)$ to calculate x for a specific $b \leq L$ and $O(1)$ for calculating 2^x and finding the closest 2 integers.
3) To calculate

Exercise 5.18

N is not even so step 1 is passed, using the algorithm of the exercise 5.17

Exercise 5.19

The only non composite odd number less than 15 is 9 which is 3^2, hence as $15 = 3 * 5$ it's the smallest composite number that's odd and not a perfect power.

Exercise 5.20

(Correction for the hint, $\sqrt{N/r} \to N/r$)
For $N = nr$, we have,
$$\hat{f}(\ell) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i \ell x/N} f(x) = \frac{1}{\sqrt{N}} \sum_{m=0}^{n-1} \sum_{x=0}^{r-1} e^{-2\pi i \ell (mr+x)/nr} f(x) = \frac{1}{\sqrt{N}} \sum_{x=0}^{r-1} \sum_{m=0}^{n-1} e^{-2\pi i \ell m/n} e^{-2\pi i \ell x/N} f(x) =$$
$$\frac{1}{\sqrt{N}} \sum_{x=0}^{r-1} n\delta_{\ell,zn} e^{-2\pi i \ell x/N} f(x) = \begin{cases} \sqrt{\frac{n}{r}} \sum_{x=0}^{r-1} e^{-2\pi i \ell x/N} f(x) & \text{for } \ell = zn \text{ where } z \in \mathbb{Z} \\ 0 & \text{otherwise} \end{cases}$$
Equation 5.63 is the fourier transform for a single period of $f(x)$.

Exercise 5.21

$$1) U_y |\hat{f}(\ell)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \ell x/N} |f(x+y)\rangle = e^{2\pi i \ell y/N} \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \ell (x+y)/N} |f(x+y)\rangle =$$
$$e^{2\pi i \ell y/N} \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \ell x/N} |f(x)\rangle = e^{2\pi i \ell y/N} |\hat{f}(\ell)\rangle$$
$$2) |f(x_0)\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \ell x_0/r} |\hat{f}(\ell)\rangle$$
$$\frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle U_y |f(x_0)\rangle = \frac{1}{\sqrt{2^t r}} \sum_{\ell=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i \ell x_0/r} e^{2\pi i \ell y/N} |x\rangle |\hat{f}(\ell)\rangle$$
$$\xrightarrow{FT^\dagger} \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \ell y/N} |\widetilde{\ell/r}\rangle |\hat{f}(\ell)\rangle$$
Which due to the equal superposition of the $|\hat{f}(\ell)\rangle$ gives the result from phase estimation.

Exercise 5.22

Using the fact that $|f(x_1, x_2)\rangle = |f(0, x_2 + sx_1)\rangle$ from periodicity.
$$|\hat{f}(\ell_1, \ell_2)\rangle = \frac{1}{\sqrt{r}} \sum_{x_1=0}^{r-1} e^{-2\pi i \ell_1 x_1/r} \frac{1}{\sqrt{r}} \sum_{x_2=0}^{r-1} e^{-2\pi i \ell_2 x_2/r} |f(x_1, x_2)\rangle = \frac{1}{r} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{-2\pi i (\ell_1 x_1 + \ell_2 x_2)/r} |f(x_1, x_2)\rangle =$$
$$\frac{1}{r} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{-2\pi i (\ell_1 x_1 + \ell_2 x_2)/r} |f(0, x_2 + sx_1)\rangle = \frac{1}{r} \sum_{x_1=0}^{r-1} \sum_{j=sx_1}^{r-1+sx_1} e^{-2\pi i (\ell_1 x_1 + \ell_2 (j - sx_1))/r} |f(0, j)\rangle =$$
$$\frac{1}{r} \sum_{x_1=0}^{r-1} e^{-2\pi i s x_1 (\ell_1/s - \ell_2)/r} \sum_{j=sx_1}^{r-1+sx_1} e^{-2\pi i \ell_2 j/r} |f(0, j)\rangle = \sum_{j=0}^{r-1} e^{-2\pi i \ell_2 j/r} |f(0, j)\rangle$$
when $\ell_1/s - \ell_2 \in \mathbb{Z}$.

Exercise 5.23

Should be a $+$ in the exponent.
Using $\ell_1 = \ell_2 s + nrs$
$$\frac{1}{r} \sum_{\ell_1=0}^{r-1} \sum_{\ell_2=0}^{r-1} e^{2\pi i (\ell_1 x_1 + \ell_2 x_2)/r} |\hat{f}(\ell_1, \ell_2)\rangle = \frac{1}{r} \sum_{\ell_1=0}^{r-1} \sum_{\ell_2=0}^{r-1} e^{2\pi i (\ell_1 x_1 + \ell_2 x_2)/r} \sum_{j=0}^{r-1} e^{-2\pi i \ell_2 j/r} |f(0, j)\rangle =$$

$$\frac{1}{r}\sum_{\ell_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i((\ell_2 s+nrs)x_1+\ell_2(x_2-j))/r}\,|f(0,j)\rangle = \frac{1}{r}\sum_{\ell_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i\ell_2(sx_1+x_2-j)/r}\,|f(0,j)\rangle =$$
$$\sum_{j=0}^{r-1}\delta_{x_2+sx_1,j}\,|f(0,j)\rangle = |f(0,x_2+sx_1)\rangle = |f(x_1,x_2)\rangle$$

Exercise 5.24

Let $\varphi_1 = \widetilde{sl_2/r}$ and $\varphi_2 = \widetilde{l_2/r}$. Both are t bits long, hence $\exists$ sl_2/r and l_2/r which are the convergents of the continued fractions φ_1 and φ_2 respectively, if
$$\left|\frac{sl_2}{r} - \varphi_1\right| \le \frac{1}{2r^2}$$
$$\left|\frac{l_2}{r} - \varphi_2\right| \le \frac{1}{2r^2}$$
Therefore, with the algorithm of continued fractions we can find sl_2/r and l_2/r, and hence s by dividing one by the other.