18.435/2.111 Homework # 3 Solutions

Solution to 1:
For $N = 15$, $\frac{3}{4}$ of the possible x's with $\gcd(x, 15) = 1$ yield an r that is even and with $x^{r/2} \neq -1$. For $N = 63$, $\frac{1}{2}$ of the residues yield such an r. One way to do this is to use the Chinese remainder theorem. I will do $N = 15$ in detail so that people can see what is happening, and then give a shorter way of figuring out the answer for $N = 63$.

For $N = 15$, we will need to look at the x's modulo 3 and modulo 5. Consider the following table.

$x \pmod 3$	r_3	x (mod 5)	r_5	r	$x^{r/2} \pmod 3$	$x^{r/2} \pmod 5$
1	1	1	1	1	—	—
-1	2	1	1	2	-1	1
1	1	2	4	4	1	-1
-1	2	2	4	4	1	-1
1	1	3	4	4	1	-1
-1	2	3	4	4	1	-1
1	1	-1	2	2	1	-1
-1	2	-1	2	2	-1	-1

We found r by taking the least common multiple of r_3 and r_5. Everything else in the table should be fairly self-evident. Note that $x^{r/2} \pmod 3$ and $x^{r/2} \pmod 5$ are either 1 or -1. This has to be the case, since their squares are 1 and the only square roots of 1 modulo an odd prime p are ± 1 [this is a consequence of the muliplicative group modulo the prime being cyclic].

The procedure fails either if both the r's are odd, or if both $x^{r/2} \pmod 3$ and $x^{r/2} \pmod 5$ are -1.

Now, let's condider the case of 63. We give the relatively prime residues (mod 9) and (mod 7) and their orders r_9 and r_7 in the tables below:

r_7	residues
1	1 (mod 7)
2	-1 (mod 7)
3	2,4 (mod 7)
2	3,5 (mod 7)

r_9	residues
1	1 (mod 9)
2	-1 (mod 9)
3	4,7 (mod 9)
2	2,5 (mod 9)

In this case, the algorithm will fail if both r_7 and r_9 are odd, or if both r_7 and r_9 are even. It is easy to see that the probability that this happens is $\frac{1}{2}$.

The algorithm fails when both r_y and r_9 are odd because then r is odd. Why does it fail when they're both even? We have $r/2 = \mathrm{lcm}(r_7, r_9)/2$ is odd, and $x^{r_7/2} \equiv -1 \pmod 7$ and $x^{r_9/2} \equiv -1 \pmod 9$. Thus, $r/2 = (r_7/2)t$ for some odd integer t, and

$$x^{r/2} \equiv (x^{r_7/2})^t \equiv (-1)^t \equiv -1 \bmod 7$$

and similarly (mod 9).

Now, suppose r_7 is even and r_9 is odd. Then $r/2 = (r_7/2)t_7$ for some odd integer t, and $r/2 = r_9 t_9$ for some odd integer t_9. The argument above can be adapted to show that $x^{r_7} \equiv -1 \pmod 7$ but $x^{r_9} \equiv 1 \pmod 9$, and the factoring algorithm works.

One could also use the statement from the proof of Theorem A4.13 in Nielsen and Chuang, which says that the algorithm will fail for a number $N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ exactly when the largest powers of two dividing all the r_i are equal. Using the fact that multiplication modulo p^α forms a cyclic group for odd primes p and a little group theory, one can show that if $p \equiv 3 \pmod 4$, for exactly half the residues mod p^α, we have r_{p^α} odd and for the other half, r_{p^α} is twice an odd number, so if $N = p_1^{\alpha_1} p_2^{\alpha_2}$ with both p_1 and p_2 congruent to 3 modulo 4, the factoring algorithm chooses a bad x with probability $\frac{1}{2}$.

Problem 2: Suppose we try to apply the factoring algorithm to a number $N = p^\alpha$ which is a power of p. Will it work? If not, what goes wrong.

Solution to 2: In the statement of the problem, I accidentally forgot to say explicitly that p was prime, which is the case I meant you to consider. If p is not prime, the algorithm works fine. If p is prime, then you run into the problem that the only square roots of 1 modulo p^α are $+1$ and -1. Thus, $x^r \equiv 1 \pmod{p^\alpha}$ forces us to have $x^{r/2} \equiv -1 \pmod{p^\alpha}$. [We can't have $x^{r/2} \equiv 1 \pmod{p^\alpha}$ since r was the minimum power giving $x^r \equiv 1$]. This doesn't give us two numbers $a^2 \equiv b^2 \pmod{p^\alpha}$ with $x \not\equiv \pm y$, so we don't get a factorization.

Problem 3: Suppose we try to apply the factoring algorithm, but we forget to check whether $\gcd(x, N) = 1$ and accidentally choose an x with $1 < x < N$ and $\gcd(x, N) > 1$. Will the algorithm still work? If not, what goes wrong?

Solution to 3: In the algorithm, we need to construct the unitary transformation U acting on $|\,a\rangle$ for $0 \le a < N$ as $U\,|\,a\rangle = |\,ax \bmod N\rangle$. This transformation is not unitary if $\gcd(x, N) > 1$. To see this, note that there are two unequal residues a_1 and $a_2 < N$ such that $a_1 x \bmod N = a_2 x \bmod N$. To see this explicitly, consider a prime p dividing both x and N. The transformation U has to take both $|\,a_1\rangle = |\,0\rangle$ and $|\,a_2\rangle = |\,N/p\rangle$ to $|\,0\rangle$.

Solution to 4:
We have

$$\tilde{f} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i \ell x/N} f(x).$$

Now, let's write $x = ry + z$ where $0 \le z < r$. We can rewrite the sum above

$$\tilde{f} = \frac{1}{\sqrt{N}} \sum_{z=0}^{r-1} \sum_{y=0}^{N/r-1} e^{-2\pi i \ell (ry+z)/N} f(ry+z).$$

Breaking the exponential in two parts and using the fact that $f(ry+z) = f(z)$, we get

$$\tilde{f} = \frac{1}{\sqrt{N}} \sum_{z=0}^{r-1} e^{-2\pi i \ell z/N} f(z) \sum_{y=0}^{N/r-1} e^{-2\pi i \ell r y/N}$$

The second piece is just 0 unless ℓ is an integer multiple of N/r, in which case it is N/r [the book has a typo]. This gives

$$\tilde{f} = \frac{\sqrt{N}}{r} \sum_{z=0}^{r} e^{-2\pi i \ell(z)/N} f(z).$$

if ℓ is an integer multiple of N/r and 0 otherwise.

The part about relating the result to 5.63 was fairly vague, and several students had questions about it. What I assume Nielsen and Chuang wanted you to do was use it to prove the approximation in Step 3 of the period-finding algorithm. You can do this by breaking the sum on x from 0 to $2^t - 1$ into two parts, where the first part runs from 0 to $N - 1$ where N is an integer multiple of r and the second part contains the remaining terms.

Solution to 5. The period-finding algorithm doesn't work well for the function

$$\begin{aligned} f(x) &= 1 \qquad \text{if } r \text{ divides } x \\ f(x) &= 0 \qquad \text{if } x \text{ is not a multiple of } r. \end{aligned}$$

Let's analyze it. We have the superposition

$$\frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |\, x\rangle \,|\, f(x)\rangle$$

and we take the inverse Fourier transform of it. This is

$$\frac{1}{2^t} \sum_{x=0}^{2^t-1} \sum_{y=0}^{2^t-1} e^{-2\pi i x y/2^t} \,|\, y\rangle \,|\, f(x)\rangle$$

This sum splits into two parts, the case where $f(x) = 0$ and the case where $f(x) = 1$. Let's do the case where $f(x) = 0$ first. We get that the amplitude on the state $|\, y\rangle \,|\, 0\rangle$ is:

$$\frac{1}{2^t} \sum_{\substack{x=0 \\ r \text{ does not divide } x}}^{2^t-1} e^{-2\pi i x y/2^t}$$

Suppose $y = 0$. Then, all the terms in this sum are 1, and there are roughly $(r-1)/r$ terms in the sum, since we get one term for all the x that are not integer multiples of r. Thus, the amplitude of the sum is around $(r-1)/r$, and the probability of seeing $|\, 0\rangle \,|\, 0\rangle$ is the square of the amplitude, or approximately $(r-1)^2/r^2 \approx 1 - 2/r$. This outcome doesn't tell us anything about r, since it says that $0/2^t$ is a fraction close to $0/r$, which is true for any r. Now, suppose $y \neq 0$. We again have the amplitude

$$\frac{1}{2^t} \sum_{\substack{x=0 \\ r \text{ does not divide } x}}^{2^t-1} e^{-2\pi i x y/2^t}.$$

We can analyze this by breaking it into two sums as follows

$$\frac{1}{2^t}\left(\sum_{x=0}^{2^t-1} e^{-2\pi i x y/2^t} - \sum_{\substack{x=0 \\ r \text{ divides } x}}^{2^t-1} e^{-2\pi i x y/2^t}\right).$$

If $y \neq 0$, the first sum is 0, so we need only to analyze the second sum. Changing the index of summation, this is

$$-\frac{1}{2^t}\sum_{x'=0}^{(2^t-1)/r} e^{-2\pi i r x' y/2^t},$$

which is the same sum we saw in the phase estimation algorithm. By the same analysis, we find that if $y/2^t$ is close to a fraction d/r, the sum has a value close to $2^t/r$, and if $y/2^t$ is far from a fraction d/r, the sum has a negligible value. Thus, for each of the $r-1$ fractions d/r, $d \neq 0$, we obtain a y with $y/2^t \approx d/r$ with probability $1/r^2$. From most of these fractions we will be able to recover r, so this case usually succeeds, but this case only occurs with probability around $1/r$.

If $f(x) = 1$, then x must be a multiple of r, and the amplitude is

$$\frac{1}{2^t}\sum_{\substack{x=0 \\ r \text{ divides } x}}^{2^t-1} e^{-2\pi i x y/2^t}.$$

This sum is the same as for the case where $y \neq 0$ and $f(x) = 0$, so this case again occurs with probability approximately $1/r$, and if we are in this case we succeed most of the time.

The period-finding algorithm thus succeeds for this f with probability approximately $2/r$. The large failure probability is due to this function essentially having period 1, or more precisely, its being very close to a function with period 1. The Fourier tranform picks out this period with high probability, and the period of r with only fairly low probability.

Solution to 6: Recall the geometric description of Grover's algorithm, where we have a basis in which ψ rotates by an angle of θ with each iteration. We start with an angle of $\theta/2$, and we a target set with probability 1 when $\theta = \pi/2$. Thus, we want $3\theta/2 = \pi/2$, or $\theta/2 = \pi/6$. But recall

$$\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}.$$

This gives $M/N = 1/4$.

Solution to 7: Let the target set be T. Define

$$\begin{aligned} |\,\beta\rangle &= \frac{1}{\sqrt{M}}\sum_{x\in T}|\,x\rangle \\ |\,\alpha\rangle &= \frac{1}{\sqrt{N-M}}\sum_{x\notin T}|\,x\rangle \\ |\,\psi\rangle &= \frac{1}{\sqrt{N}}\sum_{x}|\,x\rangle \end{aligned}$$

Then we have that the starting state

$$|\,\psi\rangle = \frac{\sqrt{M}}{\sqrt{N}}|\,\beta\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|\,\alpha\rangle$$

and after the first step

$$O\,|\,\psi\rangle = e^{i\phi}\frac{\sqrt{M}}{\sqrt{N}}|\,\beta\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|\,\alpha\rangle\,.$$

Now, note the inner products

$$\begin{aligned} \langle\beta|\psi\rangle &= \frac{\sqrt{M}}{\sqrt{N}} \\ \langle\alpha|\psi\rangle &= \frac{\sqrt{N-M}}{\sqrt{N}} \end{aligned}$$

Also, note that

$$H^{\otimes n}[(1-e^{i\phi})\,|\,0\rangle\langle 0\,| - I]H^{\otimes n} = (1-e^{i\phi})\,|\,\psi\rangle\langle\psi\,| - I$$

Thus, we get that

$$\tilde{G}\,|\,\psi\rangle \;=\; (1-e^{i\phi})(\frac{M}{N}e^{i\phi} + \frac{N-M}{M})(\frac{\sqrt{N-M}}{N}|\,\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}|\,\beta\rangle) - e^{i\phi}|\,\beta\rangle - |\,\alpha\rangle$$

We can now pull off the coefficients on $|\,\alpha\rangle$ and $|\,\beta\rangle$. We find that we get

$$e^{i\phi}(-\frac{M}{N}2\cos\phi - \frac{N-2M}{N})\sqrt{\frac{N-M}{N}}\,|\,\alpha\rangle$$

which can be made 0 for the appropriate choice of ϕ, provided M is between $N/4$ and N.

A generalization of this technique shows that if you known M, and choose the appropriate number of Grover iterations followed by one of these iterations, you can put all the amplitude on the target states.