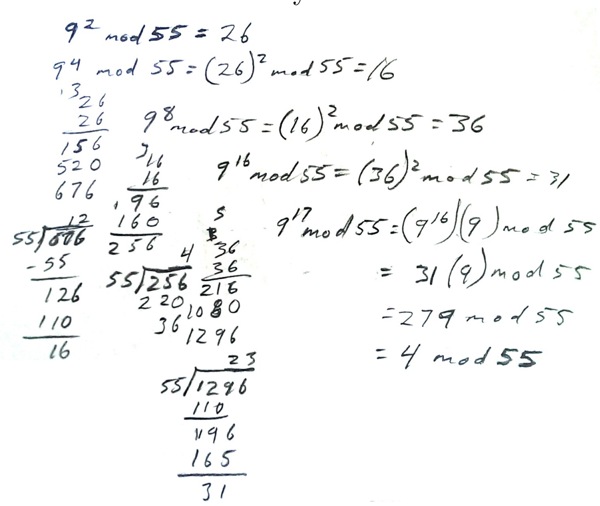
Problem 1

a) To find $b = 9^{17} \mod 55$ we calculate:

$$
\begin{aligned}
9^2 &\equiv 26 \mod 55 \\
9^4 &\equiv (26)^2 \equiv 16 \mod 55 \\
9^8 &\equiv (16)^2 \equiv 36 \mod 55 \\
9^{16} &\equiv (36)^2 \equiv 31 \mod 55 \\
9^{17} &\equiv (31)(9) \equiv 279 \equiv 4 \mod 55
\end{aligned}
$$

Here's the work done by hand:



b) We wish to find the inverse of 17 mod 40. Thus we run Euclid's Extended Algorithm while keeping track of the quotient and remainder q_i and r_i at step i and an auxiliary sequence $p_i = p_{i-2} - p_{i-1}q_{i-2} \mod 40$ where $p_0 = 0$ and $p_1 = 1$:

a	b	q_i	r_i	p_i
40	17	2	6	0
17	6	2	5	1
6	5	1	1	$-2 \mod 40$
5	1	5	0	$5 \mod 40$
				$33 \mod 40$

Thus we see that $33 \equiv -7 \mod 40$ is the inverse of 17 mod 40.

c) We wish to find an r such that $4^r \equiv 1 \mod 55$. We know $|G_N| = 10 \cdot 4$. Thus r must be one of $1, 2, 4, 5, 8, 10, 20$. Thus we calculate:

$$
\begin{aligned}
4^1 &\equiv 4 \mod 55 \\
4^2 &\equiv 16 \mod 55 \\
4^4 &\equiv (16)^2 \equiv 36 \mod 55 \\
4^5 &\equiv (36)(4) \equiv 34 \mod 55 \\
4^8 &\equiv (36)^2 \equiv 31 \mod 55 \\
4^{10} &\equiv (34)^2 \equiv 1 \mod 55
\end{aligned}
$$

Thus we observe that $r = 10$.

d) We compute:

$$17d' \equiv 1 \mod 10$$
$$7d' \equiv 1 \mod 10$$
$$d' \equiv 3 \mod 10$$

thus we use d' to confirm:

$$b^{d'} \equiv a \mod 55$$
$$4^3 \equiv 64 \mod 55$$
$$4^3 \equiv 9 \mod 55$$

and our confirmation is complete.

Problem 2

a) We wish to find the inverse of 53 mod 60. Thus we run Euclid's Extended Algorithm while keeping track of the quotient and remainder q_i and r_i at step i and an auxiliary sequence $p_i = p_{i-2} - p_{i-1}q_{i-2} \mod 40$ where $p_0 = 0$ and $p_1 = 1$:

a	b	q_i	r_i	p_i
60	53	1	7	0
53	7	7	4	1
7	4	1	3	$-1 \mod 40$
4	3	1	1	$8 \mod 40$
3	1	3	0	$-9 \mod 40$
				$17 \mod 40$

Thus we see that 17 is the inverse of 53 mod 60. We then compute Alice's message $19^{17} \equiv 2 \mod 143$ and see that $a = 2$.

b) We wish to find the inverse of 53 mod 120. Thus we run Euclid's Extended Algorithm while keeping track of the quotient and remainder q_i and r_i at step i and an auxiliary sequence $p_i = p_{i-2} - p_{i-1}q_{i-2} \mod 40$ where $p_0 = 0$ and $p_1 = 1$:

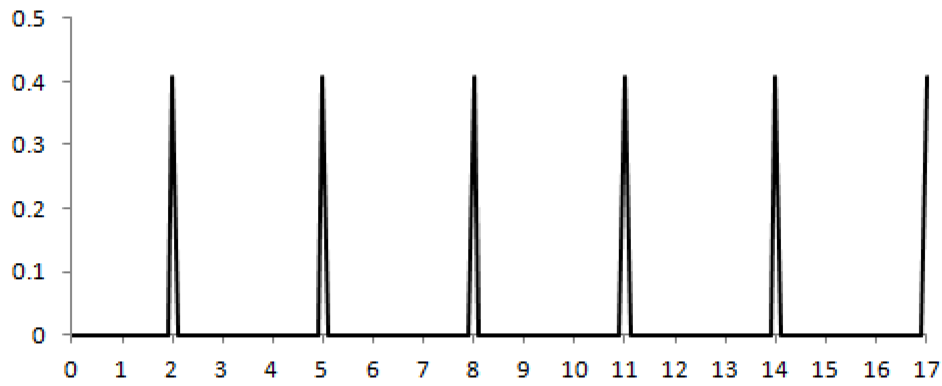
a	b	q_i	r_i	p_i
120	53	2	14	0
53	14	3	11	1
14	11	1	3	-2
11	3	3	2	7
3	2	2	1	-9
2	1	1	0	34
				-43

Thus we see that -43 is the inverse of 53 mod 120. We then decrypt $19^{-43} \equiv 2 \mod 143$ and we see that Eve got it right.

Problem 3

a) (i) We have 6 values of x in the range 0-17 that map to 16, which leaves the "input" in the state:

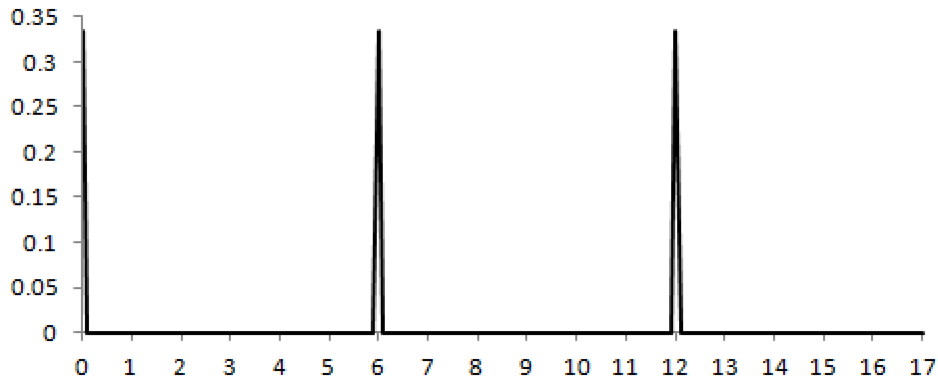
$$|\Psi\rangle = \frac{1}{\sqrt{6}}(|2\rangle + |5\rangle + |8\rangle + |11\rangle + |14\rangle + |17\rangle)$$



(ii) To accomplish this I wrote the following python script which computes eq 3.20 for $0 \leq y < 18$:

```
import cmath
for y in range(18):
    sum = 0
    for x in range(18):
        expValue = cmath.exp((2*cmath.pi*1j*x*y)/18)
        if ((4**x)%21)==16:
            sum = sum + (expValue*(1/cmath.sqrt(6)))
    sum = sum * (1/cmath.sqrt(18))
    print str(y) + " yields " + str(sum)
```

The following graph shows the 3 non zero values of the modulus-squared $|\tilde{\gamma}(y)|^2$:



(iii) The various non-zero measurements of y would be measured with probability $\frac{1}{3}$.

(iv) *Not sure about this one.* We can use $\frac{y}{18}$ to extract $\frac{j}{r}$ from continued fractions as described by appendix K.

b) (i) We have 10 values of x in the range 0-64 that map to 16, which leaves the "input" in the state:

$$|\Psi\rangle = \frac{1}{\sqrt{10}}(|4\rangle + |10\rangle + |16\rangle + |22\rangle + |28\rangle + |34\rangle + |40\rangle + |46\rangle + |52\rangle + |58\rangle)$$

(ii) *Not sure about this one.*

(iii) *Not sure about this one.* We can use $\frac{y}{64}$ to extract $\frac{j}{r}$ from continued fractions as described by appendix K.

Problem 4

a) We observe the following:

- (3.54)
- $\delta_j = 0$ if y_j is an integer multiple of $2^n/r$
- there are $r-1$ different values of j
- r is a large number

Using these observations, we then conclude:

$$\sum_{j=1}^{r-1} p(y_j) = \sum_{j=1}^{r-1} \frac{1}{r} \approx 1$$

b) We observe:

$$y = 7 \cdot 2^{19}$$
$$2^{19} = \frac{7 \cdot 2^{25}}{r}$$
$$r = \frac{7 \cdot 2^{25}}{2^{19}} = 448$$

We then confirm that $255^{448} \equiv 1 \mod 16843009$.

c)

$$t = a^{r/2} \mod N = 65536 = 2^{16}$$
$$gcd(N, t-1) = p = 257$$
$$gcd(N, t+1) = q = 2^{16} + 1 = 65537$$

Thus we have our prime factors of N, namely 257 and 65537.

Problem 5

a) Following the steps of appendix K we observe:

$$x = \frac{7080}{2^{14}}$$
$$x = \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{4 + \dots}}}}}$$

I happened to get lucky here because the first partial sum I computed was the one ending in $a_3 = 2$ which is equal to $\frac{35}{81}$. I checked the partial sum of $a_4 = 4$ and found that to be $\frac{73}{169}$ which had a denominator too large. Thus, since 81 is the only multiple of 81 less than 100 we conclude that $r = 81$ and confirm that

$$\frac{35}{81} \cdot 2^{14} = 7079.506173\dots$$

is within half of 7078.

b) Following the steps of appendix K we observe:

$$x = \frac{2979}{2^{14}} = \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{1489 + \dots}}}$$

$$z = \frac{14564}{2^{14}} = \cfrac{1}{1 + \cfrac{1}{8 + \cfrac{1}{455 + \dots}}}$$

Now, for both of these, it's clear that the partial sum of a_2 will be much too large. We first compute the partial sum of a_1 of x to be $\frac{2}{11}$. We verify that $\frac{2}{11} \cdot 2^{14} = 2978.909090\dots$ which is indeed within half of 2979. Thus we know that r is a multiple of 11 less than 100. We next compute the partial sum of a_1 of z to be $\frac{8}{9}$. We verify that $\frac{8}{9} \cdot 2^{14} = 14563.5555\dots$ which is indeed within half of 14564. Thus we know that r is a multiple of 9 less than 100. Hence, we can conclude that $r = 99$ as this is the least common multiple of both 9 and 11 that is less than 100.

Problem 6

a) For $n = 4$, 4 H and 6 V are required, making 10 in total. For $n = 5$, 5 H and 10 V are required, making 15 in total. For arbitrary n, we need n H gates and we need $\frac{(n-1)n}{2}$ V gates making $n + \frac{n(n-1)}{2}$ gates in total.

b) l would still be 22 here as we might use around $n = 4000$ for factoring a 617 digit number which still satisfies the inequality $1/2^l < 1/(500n\pi)$ from the text.

c) We solve the following system of equations:

$$Ce^{\beta 232^{1/3}} = 2$$
$$Ce^{\beta 309^{1/3}} = 2000$$

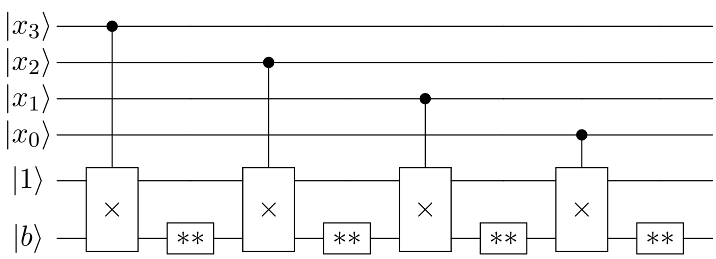
to find $C = 2.37 \times 10^{-30}$ and $\beta = 11.21\dots$. We then compute:

$$Ce^{\beta 309^{1/3}} = 6.87 \times 10^{11}$$

or about 700 billion years which is many times the currently accepted age of the universe.

Problem 7

(i)



Note that the $**$ gate squares b mod N. Also note that we omitted 4 input bits for ease in construction of the circuit.

(ii) *Help Me Al! You're my only hope.*