A.A. If U is an n-qbit gate, then controlled-U or cU is an $(n+1)$-qbit gate defined by

$$\alpha\,|0\rangle\,|\psi\rangle + \beta\,|1\rangle\,|\phi\rangle \mapsto \alpha\,|0\rangle\,|\psi\rangle + \beta\,|1\rangle\,U\,|\phi\rangle\,.$$

A.B. The subroutine in Shor's algorithm outputs an integer y such that, with probability about 0.4, y is within rounding error of an integer multiple of $2^n/r$.

A.C. $\mathcal{O}(n^2)$ primitive gates are required to implement the n-qbit Fourier transform.

A.D. In this course (not necessarily other quantum theory courses), an *observable* is a matrix A such that $A^* = A$ (i.e., A is Hermitian) and $AA^* = I$ (i.e., A is unitary). [An equally good answer is: $A^* = A$ and $A^2 = I$.]

A.E. A code for correcting single-qbit X, Y, or Z errors must have at least 5 qbits.

A.F. In our 7-qbit code, if the error Y_2 happens, then the syndrome is $1, 1, -1, 1, 1, -1$.

A.G. If the error X_5 happens, then the syndrome is $1, 1, 1, -1, -1, 1$.

A.H. If the error Z_1 happens, then the syndrome is $1, -1, 1, 1, 1, 1$.

B. [We did this in class.] Well,

$$\begin{aligned}(UU^*)_{kj} &= \sum_\ell U_{k\ell}U^*_{\ell j} \\ &= \sum_\ell \frac{1}{2^{n/2}} e^{i\pi(2/2^n)k\ell} \frac{1}{2^{n/2}} e^{-i\pi(2/2^n)\ell j} \\ &= \frac{1}{2^n}\sum_z e^{i\pi(2/2^n)(k-j)\ell}.\end{aligned}$$

If $k = j$, then we get $\frac{1}{2^n}\sum 1 = 2^n/2^n = 1$. If $k \neq j$, then the terms in the sum are 2^n complex numbers evenly spaced around the unit circle. So they add to 0. Consequently, $UU^* = I$ and so U is unitary.

C.A. [I'll omit the drawing. It is part of Mermin's Fig. 5.9. It has seven codeword wires and one ancillary wire. The ancillary wire has Hadamards. The rest of the diagram is the second column of controlled Zs in Mermin's figure.]

C.B. First, $\bar{Z} = Z^{\otimes 7} = Z_0Z_1Z_2Z_3Z_4Z_5Z_6$. Second, because Z anti-commutes with X but $\bar{Z}$ interacts with each M_k on exactly two wires, $\bar{Z}$ commutes with each M_k. Thus

$$\begin{aligned}\bar{Z}\,|\bar{0}\rangle &= \bar{Z}2^{-3/2}(I+M_0)(I+M_1)(I+M_2)\,|0000000\rangle \\ &= 2^{-3/2}(I+M_0)(I+M_1)(I+M_2)Z^{\otimes 7}\,|0000000\rangle\,.\end{aligned}$$

But on each wire $Z|0\rangle = |0\rangle$. Thus $\bar{Z}|\bar{0}\rangle = |\bar{0}\rangle$, as one would hope. Similarly,

$$\begin{aligned}\bar{Z}|\bar{1}\rangle &= \bar{Z}2^{-3/2}(I+M_0)(I+M_1)(I+M_2)X^{\otimes 7}|0000000\rangle \\ &= 2^{-3/2}(I+M_0)(I+M_1)(I+M_2)Z^{\otimes 7}|1111111\rangle\,.\end{aligned}$$

But now on each wire $Z|1\rangle = -|1\rangle$, so $\bar{Z}|\bar{1}\rangle = (-1)^7|\bar{1}\rangle = -|\bar{1}\rangle$, as desired.

D.A. [I'll omit the drawing. It's in Mermin's book and your class notes.]

D.B. We know that $b^r - 1$ is divisible by N. If we get lucky in that r is even, then $r/2$ is an integer, and

$$b^r - 1 = (b^{r/2} - 1)(b^{r/2} + 1).$$

The integer $b^{r/2} - 1$ can't be divisible by N, or else the period would be $r/2 < r$. If we get lucky, then $b^{r/2} + 1$ is also not divisible by N. Then the factors of N are distributed in a nontrivial way between $b^{r/2} - 1$ and $b^{r/2} + 1$. Computing the GCD of N with either of these numbers gives a nontrivial factor of N.