Quantum Computing, 2016, Test 2

The key ingredient of factorization method presented on the lectures was eigenvalue estimation algorithm. Peter Shor in fact did not use the notion of eigenvalue estimation. Instead he suggested another method which also uses QFT. It consists of three steps which you are expected to explore in detail here.

Consider a, N, r, n as in setup of Order-Finding problem. First, Shor prepared the state

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |a^x \bmod N\rangle.$$

Justify that it can be rewritten as follows:

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{b=0}^{r-1} \left(\sum_{z=0}^{m_b-1} |zr+b\rangle \right) |a^b \bmod N\rangle,$$

where m_b is the largest number so that $(m_b-1)r+b \leqslant 2^n-1$. *Hint*: it is easy consequence of the properties of integer division algorithm (in fact you divide each x by r and group results by reminder b) and definition of r.

Second, Shor measured second register (to "fix" b) to get

$$|\psi_1\rangle = \frac{1}{\sqrt{m_b}} \sum_{z=0}^{m_b-1} |zr+b\rangle$$

in the first register.

Third, **show** that application of QFT to this and measurement afterwards yields equivalent information to what we had on the lecture, that is some good approximation $|\widehat{k/r}\rangle$ for randomly chosen k. To simplify argument, pretend that the $p = m_b r$ is known. In this case QFT can be taken with primitive root of unity $e^{2\pi i/p}$. Prove that in this case

$$\mathrm{QFT}\,|\psi_1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi i \frac{m_b}{r} k} |m_b k\rangle.$$

How the result of the measurement combined with p give us information equivalent to what we get on the lecture?