## CS3222 Exercises 5 (Quantum Algorithms II)

1. Find the inverse of $8(\bmod 21)$.
2. Show that if $a$ and $b$ are both inverses of $x(\bmod n)$, then $a=b(\bmod n)$.
3. Show that the order $r$ of $x$ modulo $n$ satisfies $r \leq n$.
4. Show that if $0<x<N, \operatorname{gcd}(x, N)=1$, and $L=\lceil\log (N)\rceil$, then the operation $U$ on $\boldsymbol{Q}^{\otimes L}$ given by:

$$
\begin{array}{ll}
U|y\rangle=|x y(\bmod N)\rangle & \text { for } 0<y<N-1 \\
U|y\rangle=|y\rangle & \text { for } N<y<2^{L}-1
\end{array}
$$ is a permutation of the standard basis of the state space and is therefore unitary.

5. Find the regular continued fraction expansion of $37 / 17$.
6. Regarding the continued fraction expansion, show by induction that all the rational convergents $p_{j} / q_{j}$ satisfy $p_{j-1} q_{j}-q_{j-1} p_{j}=(-1)^{j}$ and deduce that $\operatorname{gcd}\left(p_{j}, q_{j}\right)=1$.
7. Find $\operatorname{gcd}(231,315)$.
8. Consider Shor's algorithm on p. 123 of the notes, for factoring $N=15$, with the assumption that in step (i) we choose $x=13$. Find the order of 13 modulo 15 for step (iii) and verify that step (v) leads to the factorisation. Repeat for factoring $N=91$ with $x=4$, and for $N=18$ with $x=5$.
