Please solve the following problem.

1. Let $p$ be an odd prime. A quadratic residue modulo $p$ is a nonzero element of $\mathbb{F}_p$ that is the square of an element of $\mathbb{F}_p$.
   (a) List all the quadratic residues modulo 23.
   (b) If $n$ is a quadratic residue modulo $p$, show that $x^2 = n \pmod{p}$ has two solutions in $\mathbb{F}_p$. Deduce that there are exactly $(p - 1)/2$ quadratic residues modulo $p$.
   (c) Let $Q_p$ denote the set of all quadratic residues modulo $p$. Show that $Q_p$ is a union of binary cyclotomic cosets if and only if 2 is in $Q_p$.
   (d) Let $C_p$ be the binary cyclic code of length $p$ with zeros at all $\alpha^i$ for $i \in Q_p$. Show that $C_7$ is the Hamming code.
   (e) Factor $x^{23} - 1$ over $\mathbb{F}_2$. Find the parameters of $C_{23}$. 

Typeset by \LaTeX