MATH 601 (DUE 11/13)

HIDENORI SHINOHARA

Contents

1. Factoring Polynomials with Coefficients in Finite Fields

Exercise. (Problem 14) For $a \in \mathbb{F}_q$, what are the possible values for $a^{(q-1)/2}$? How many different a take each value?

Proof. Let $\langle \alpha \rangle = (\mathbb{F}_q)^*$. Let $k \in \mathbb{Z}$. If k is even, then $(\alpha^k)^{(q-1)/2} = (\alpha^{k/2})^{q-1} = 1$. If $k = 2l+1$ for some l, then $(\alpha^k)^{(q-1)/2} = \alpha^{l(q-1)} \cdot \alpha^{(q-1)/2} = \alpha^{(q-1)/2}$. Therefore,

$$a^{(q-1)/2} = \begin{cases} 0 & (a = 0) \\ 1 & (\exists l \in \mathbb{Z}, a = \alpha^{2l}) \\ \alpha^{(q-1)/2} & (\exists l \in \mathbb{Z}, a = \alpha^{2l+1}). \end{cases}$$

This is well defined because every nonzero element in $\mathbb{Z}_q$ is in $\langle \alpha \rangle$ and $2 \mid |\langle \alpha \rangle| = q-1$, so the parity of the exponent is well defined. Hence, 1 value gives 0, $(q-1)/2$ values give 1, and $(q-1)/2$ values give $\alpha^{(q-1)/2}$. $\square$