# 1

$G$ is a finite group and $A, B \subseteq G$. Prove that if $|A| + |B| > |G|$, then $AB = G$.
**Proof:**
Trivially $AB \subseteq GG \subseteq G$, because $G$ is a group and is closed under multiplication.
$X = \{a^{-1} : a \in A\}$. From the cancelativity of $G$: $|X| = |A|$ and also for the right "coset" $Xg : |Xg| = |A|$. Then $\exists x \in Xg \cap B$, because there is more elements in $Xg$ and $B$ together than in $G$. This means, that $\exists b \in B, a' \in A : b = a'^{-1}g$. Then $a' \cdot (a'^{-1} \cdot g) = g \in AB \Rightarrow G \subseteq AB$.

# 2

Prove, that every element of a finite field $F$ is a sum of two squares $(x^2 + y^2)$.
**Proof:**
Consider a field of characteristics $p$. If $p = 2$, then obviously $0 = 0^2 + 0^2, e = e^2 + 0^2$.
For $p > 2$: $X = \{x^2 | x \in F \backslash \{0\}\}$ and has $\frac{p-1}{2}$ elements (because both $a, (-a)$ map to $a^2$). The total size of $X' = \{x^2 | x \in F\}$ is $\frac{p+1}{2}$.
$\forall f \in F :\ Y_f = \{f - x^2 | x \in F\}$. $Y_f$ must also have the same number of elements ($\frac{p+1}{2}$) from the same principle $(k - x^2 = k - (-x)^2)$.
Since $X', Y_f \subseteq F$ and $|X'| + |Y_f| = p + 1 > p = |F|$, then $\forall f \in F : \exists a \in X' \cap Y_f : x^2 = a = f - y^2 \to f = x^2 + y^2$.