Universitá degli Studi Roma Tre - Corso di Laurea in Matematica

Esercizio supplementare CR510

Dario Giannini

24 Marzo 2014

1. Dato un primo dispari p e un elemento a in $\mathbb{F}_p$. Dimostrare che:

   (a) Per ogni x in $\mathbb{F}_p$ esistono u e v in $\mathbb{F}_p$ tali che $x = u^2 - av^2$.

   (b) Sia α in $\mathbb{F}_{p^2}$ radice quadrata di a, allora $\phi : \mathbb{F}_p[\alpha]^* \longrightarrow \mathbb{F}_p^*$, $u+\alpha v \longmapsto u^2 - (\alpha v)^2$ é un omomorfismo di gruppi moltiplicativi.

SOLUZIONE:

(a) Si considerino i due insiemi:
$A := \{u \in \mathbb{F}_p : \exists k \in \mathbb{F}_p \text{ per cui } k^2 \equiv u(modp)\}$
$B := \{x + av^2 : v \in \mathbb{F}_p\}$
A di fatto é l'insieme dei redidui quadratici modulo p quindi avrá cardinalitá uguale a $\frac{p+1}{2}$. Stessa cosa si puó dire del secondo insieme in quanto a e x sono fissati e i suoi elementi sono ottenuti al variare di v nell'insieme dei residui quadratici modulo p.
Riassumendo il tutto si ha che:

$$|A| + |B| = p + 1 > p = |\mathbb{F}_p|$$

Quindi per il principio delle gabbie e dei piccioni si deve avere che $A \cap B \neq \emptyset$, ossia devono esistere u e v in $\mathbb{F}_p$ tali che $x = u^2 - av^2$.

(b) Si vuole dimostrare che ϕ é un omomorfismo di gruppi moltiplicativi:
$\phi(u_1 + \alpha v_1) * \phi(u_2 + \alpha v_2) = \phi[(u_1 + \alpha v_1) * (u_2 + \alpha v_2)]$.
$\phi(u_1 + \alpha v_1) * \phi(u_2 + \alpha v_2) = (u_1^2 - av_1^2) * (u_2^2 - av_2^2) =$
$u_1^2 u_2^2 - av_2^2 u_1^2 - av_1^2 u_2^2 + a^2 v_1^2 v_2^2$.
$\phi[(u_1 + \alpha v_1) * (u_2 + \alpha v_2)] = \phi[(u_1 u_2 + av_1 v_2) + \alpha(v_1 u_2 + u_2 v_1)] =$
$u_1^2 u_2^2 - av_2^2 u_1^2 - av_1^2 u_2^2 + a^2 v_1^2 v_2^2$.