Kunal Mukherjee
p 1.33(b), 1.37
1.38

1.33(b) $\dfrac{\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} \neq 1\}}{\#\mathbb{F}_p^*}$

Let $g \in \mathbb{F}_p^*$ be a primitive root. Then every $a \in \mathbb{F}_p^*$ has the form g^i for some $0 \leq i < p-1$.

The no. of a with $a^{(p-1)/q} = 1$.

Thus: $\{a \in \mathbb{F}_p^* : a^{(p-1)/q} = 1\} = \#\{0 \leq i < p-1 : (g^i)^{(p-1)/q} = 1\}$
$= \#\{0 \leq i < p-1 : g^{i(p-1)/q} = 1\}$

Since, g has order $p-1$, we have $g^k = 1$ iff $p-1 \mid k$, so.

$g^{i(p-1)/q} = 1 \rightarrow p-1 \mid i(p-1)/q \Rightarrow q \mid i$

Hence,

$$\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} = 1\} = \#\{0 \leq i < p-1 : q \mid i\} = \frac{p-1}{q}$$

It follows:

$$\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} \neq 1\} = p-1 - \#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} = 1\}$$

$$= p-1 - \frac{p-1}{q} = (p-1)\left(1 - \frac{1}{q}\right)$$

Hence,

$$\frac{\#\{a \in \mathbb{F}_p^* : a^{(p-1)/q} \neq 1\}}{\#\mathbb{F}_p^*} = 1 - \frac{1}{q}$$