Exercise 1

	Squares	Non-squares
(1) in $\mathbb{F}_3$:	0, 1	2
$\mathbb{F}_5$:	0, 1, 4	2, 3
$\mathbb{F}_7$:	0, 1, 2, 4	3, 5, 6
$\mathbb{F}_{11}$:	0, 1, 3, 4, 5, 9	2, 6, 7, 8, 10
$\mathbb{F}_{13}$:	0, 1, 3, 4, 9, 10, 12	2, 5, 6, 7, 8, 11
$\mathbb{F}_{17}$:	0, 1, 2, 4, 8, 9, 13, 15, 16	3, 5, 6, 7, 10, 11, 12, 14
$\mathbb{F}_{19}$:	0, 1, 4, 5, 6, 7, 9, 11, 16, 17	2, 3, 8, 10, 12, 13, 14, 15, 16
$\mathbb{F}_{23}$:	0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18	5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22
$\mathbb{F}_{29}$:	0, 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28	2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27
$\mathbb{F}_{31}$:	0, 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28	3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30

(2) $\boxed{\frac{p-1}{2}}$. There are $p-1$ non-zero numbers in $\mathbb{F}_p$, and they come in pairs, because $n^2 = -n^2$.

Also, since p is prime, we know that $n^2 \neq m^2$ if $n \neq m$, because $\gcd(n, m) = 1$ in $\mathbb{F}_p$. (if $n \neq 0$ & $m \neq 0$)

Exercise 3

$127 \equiv 3 \bmod 4$
$127 \equiv 7 \bmod 8$

(1) $\left(\frac{66}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{3}{127}\right)\left(\frac{11}{127}\right)$

$= 1 \times -\left(\frac{127}{3}\right) \times -\left(\frac{127}{11}\right)$

$= 1 \times -\left(\frac{1}{3}\right) \times -\left(\frac{6}{11}\right)$

$= 1 \times -(1) \times -(-1) = -1 \Rightarrow$ **no**

(2) $\left(\frac{80}{127}\right) = \left(\frac{2}{127}\right)^4 \left(\frac{5}{127}\right) = 1^4 \times \left(\frac{127}{5}\right) = 1 \times \left(\frac{2}{5}\right) = -1 \Rightarrow$ **no**

(3) $\left(\frac{122}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{61}{127}\right) = 1 \times \left(\frac{127}{61}\right) = \left(\frac{5}{61}\right) = \left(\frac{61}{5}\right) = \left(\frac{1}{5}\right) =$ **1**

(4) $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ since $5 \equiv 1 \bmod 4$

squares in $\mathbb{F}_5$

$\Rightarrow \left(\frac{p}{5}\right) = 1$ if $p \equiv k \bmod 5$ for k in $\{1, 4\}$

(5) $\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) \text{ if } p \equiv 1 \bmod 4 \Rightarrow p \equiv 1 \bmod 3 \\ -\left(\frac{p}{3}\right) \text{ otherwise} \Rightarrow p \equiv 2 \bmod 3 \end{cases}$

$\Rightarrow p \equiv \pm 1 \bmod 12$