Exercises for Munemasa's lectures

1. Let p be a prime, and let a be an integer which is relatively prime to p. Regarding a as an element of $\mathbb{F}_p$, describe a^{-1} in $\mathbb{F}_p$.
2. Let K be a field, and let $K[x]$ be the univariate polynomial ring with indeterminate x. For $f(x), g(x) \in K[x] \setminus \{0\}$, show that $\deg(fg) = \deg f + \deg g$ holds.
3. With the same assumptions as in Problem 2, suppose $b \in K$ and $f(b) = 0$. Show that there exists $g(x) \in K[x]$ such that $f(x) = (x - b)g(x)$.
4. With the same assumptions as in Problem 2, show that

$$|\{b \in K \mid f(b) = 0\}| \leq \deg f.$$

5. Let p be an odd prime. For a divisor d of $p - 1$, show that the number of elements of order d in $\mathbb{F}_p$ is at most $\varphi(d)$, where φ denotes Euler's function. Deduce that $\mathbb{F}_p$ contains an element of order $p - 1$.
6. Let p be an odd prime. Show that the definitions of the quadratic residues and that of quadratic nonresidues in $\mathbb{F}_p$ given below

$$\begin{aligned} Q &= \{1, \alpha^2, \alpha^4, \ldots, \alpha^{p-3}\}, \\ N &= \{\alpha, \alpha^3, \ldots, \alpha^{p-2}\}. \end{aligned}$$

are independent of the choice of a primitive element α.
7. With the same assumptions as in Problem 6, show that $-1 \notin Q$ and $-Q = N$, provided $p \equiv -1 \pmod 4$.
8. With the same assumptions as in Problem 7, let

$$\mathcal{B} = \{Q + a \mid a \in \mathbb{F}_p\}.$$

Show that, for any distinct $x, y \in \mathbb{F}_p$,

$$|\{B \in \mathcal{B} \mid x, y \in B\}| = \frac{p-3}{4}.$$