Number Theory I
Spring 2018

Assignment 12.3
Due April 18

**Exercise 1.** Let $a, b, c \in \mathbb{Z}$. Given a commutative ring $R$, recall that

$$\mathcal{S}(R) = \{r \in R \,|\, ar^2 + br + c = 0\}.$$

**a.** If $R$, $R'$ are commutative rings and $\sigma : R \to R'$ is an isomorphism, prove that $\sigma$ yields a bijection $\mathcal{S}(R) \to \mathcal{S}(R')$.

**b.** If $R_1, R_2, \ldots, R_n$ are commutative rings, prove that

$$\mathcal{S}(R_1 \times R_2 \times \cdots \times R_n) = \mathcal{S}(R_1) \times \mathcal{S}(R_2) \times \cdots \times \mathcal{S}(R_n).$$

**Exercise 2.** Determine if $a$ is a square modulo $p^m$.

**a.** $a = 3$, $p = 7$, $m = 13$.

**b.** $a = 1162076$, $p = 127$, $m = 3$

**c.** $a = 581869302$, $p = 5463458093$, $m = 1$

**Exercise 3.** Let $m \geq 3$ and $a \in \mathbb{Z}$ be odd. Show that $a \equiv b^2 \pmod{2^m}$ for some $b$ if and only if $a^{2^{m-3}} \equiv 1 \pmod{2^m}$ and $a \equiv 1 \pmod{4}$. This is the $\pmod{2^m}$ version of Euler's Criterion. [*Suggestion:* Recall that every element of $\mathbb{Z}/2^m\mathbb{Z}$ can be written in the form $\pm 5^k + 2^m\mathbb{Z}$, and that 5 has multiplicative order $2^{m-2} \pmod{2^m}$.]