Number Theory I
Spring 2018

Assignment 3.2
Due January 31

Exercise 1. Let G be a set with an associative binary operation with identity e. Our textbook states the "existence of inverses" axiom as follows: for each $a \in G$ there exists $b \in G$ so that $ab = e$. How does this differ from the axiom we stated in class? Show that the two axioms are equivalent.

Exercise 2. Let p be a prime.

- **a.** Prove that for $1 \leq k \leq p-1$, the binomial coefficient $\binom{p}{k}$ is divisible by p.
- **b.** Let $a, b \in \mathbb{Z}$. Prove that $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Exercise 3. Let G be a group.

- **a.** Prove that the identity element of G is unique. [*Suggestion:* If e_1 and e_2 are both identities, consider $e_1 e_2$.]
- **b.** Let $a \in G$. Prove that the inverse of a is unique. [*Suggestion:* If b and c are both inverses of a, consider bac.]