Homework Set Three

Due Monday, May 9.

Question 1. Suppose $N = \sum_{n=0}^{j} a_n 10^n$ with $0 \leq a_j < 10$. Show that 11 divides $\sum_{n=0}^{j}(-1)^n a_n$ if and only if 11 divides N.

Question 2. Recall that a group $(G, \star)$ is a set G with binary operation $\star\colon G \times G \to G$ which satisfies

(i) (associativity) $(a \star b) \star c = a \star (b \star c)$ for any $a, b, c \in G$,

(ii) (identity) there is an element $e \in G$ such that $e \star a = a = a \star e$ for any $a \in G$, and

(iii) (inverse) there exists an element x_a for any $a \in G$ such that $x_a \star a = e = a \star x_a$.

(a) Prove that the identity element $e \in G$ is unique. (Hint: suppose $e, e' \in G$ are identity elements and consider $e \star e'$.)

(b) Prove that inverses are unique. That is, suppose $g \in G$ and $x_g, x_g' \in G$ satisfy $g \star x_g = g \star x_g' = e$. Prove that $x_g = x_g'$.

(c) Let $G = \mathbb{Q} \setminus \{1\}$. Show that the binary operation $x \odot y := x + y - xy$ makes G a group.

Question 3. Prove that 1105 is a pseudoprime, meaning 1105 is not prime, yet $2^{1104} \equiv 1 \pmod{1105}$. (Hint/Suggestion: Use the method of successive squares.)

Question 4.

(a) Use the method of successive squares to compute $7^{7386} \pmod{7387}$. Can you deduce from your answer whether or not 7387 is prime? Explain your answer.

(b) It is true that $7^{7392} \equiv 1 \pmod{7393}$. Is it possible to deduce from this that 7393 is prime or not? Explain your answer.

Question 5. (bonus) Suppose $a_1, \ldots, a_n \in \mathbb{Z}$ are such that $30 \big| \sum_{j=1}^{n} a_j$. Show that

$$30 \Bigg| \sum_{j=1}^{n} a_j^5.$$