HOMEWORK #1

DUE 9/25/13 AT START OF CLASS

Problem 1 (D&F 0.3.3). Recall that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9. In fact, the remainder of any positive integer after division by 9 is the same as the sum of the digits modulo 9. Prove this.
[Hint: let $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$ be any positive integer.]

Problem 2 (D&F 0.3.11,12,13). Consider the set

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \exists [c] \in \mathbb{Z}/n\mathbb{Z} \text{ with } [a][c] = [1]\}.$$

(a) Prove that if $[a], [b] \in (\mathbb{Z}/n\mathbb{Z})^\times$, then so is $[a] * [b]$.
(b) Let $n \in \mathbb{Z}$, $n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if a and n are not relatively prime, there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 (\operatorname{mod} n)$ and deduce that there cannot be an integer c such that $ac \equiv 1 (\operatorname{mod} n)$.
(c) Let $n \in \mathbb{Z}$, $n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if a and n are relatively prime then there is an integer c such that $ac \equiv 1 (\operatorname{mod} n)$.
[Hint: use the fact that the g.c.d of two integers is a $\mathbb{Z}$-linear combination of the integers: read Section 0.2.]
(d) Conclude Proposition 0.3.4 and that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group under multiplication of congruence classes.

Problem 3 (D&F 0.1.5). Determine whether the following functions f are well-defined:

(a) $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(\frac{a}{b}) = a$.
(b) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(\frac{a}{b}) = \frac{a^2}{b^2}$

Problem 4 (D&F 0.1.7). Let A and B be sets and let f be a map from A to B.

(a) Prove that the relation

$$a \sim b \text{ if and only if } f(a) = f(b)$$

is an equivalence relation.
(b) Now suppose f is a surjective map. Prove that the equivalence classes of the relation in (a) are the fibers of f.

Problem 5 (D&F 1.1.24). Let G be a group. If a and b are commuting elements of G prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.
[Hint: do this first for positive n.]

Problem 6 (D&F 1.1.25). Let G be a group. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

Problem 7 (D&F 1.1.17). Let G be a group. Let x be an element of G. Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

Problem 8 (D&F 1.1.32). Let G be a group. If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Challenge Problem. Use Problems 7 and 8 to prove the following: If G is a group of order 4, then either G has an element of order 4 or every nonidentity element of G has order 2.