Practice problems for Test 1

Hints

1. (a) Use the Euclidean algorithm; or write each number as a product of primes.
   (b) Use the Euclidean algorithm, and "work backwards".
2. Recall that $a\mathbb{Z}$ is the set of all multiples of a. Thus an integer $x \in a\mathbb{Z}$ if and only if $x = aq$ for some integer q.
3. (a) Recall that the congruence $ax \equiv b (\text{mod } n)$ has a solution iff $d = (a, n)$ divides b. In this case, the congruence has d distinct solutions mod n, which are congruent mod $m = \frac{n}{d}$. Now, to find one solution, you need to write b as a linear combination of a and n. E.g., use the Euclidean algorithm.
   Another way: divide a, b, and n by d.
   (b) As said above, $ax \equiv b (\text{mod } n)$ has a solution iff $d = (a, n)$ divides b.
4. Use the Chinese Remainder Theorem.
5. (a) Review pages 38 and 39.
   (b) Just use the definition.
   (c) Count the number of multiples of p, and the number of multiples of q, from 1 to pq.
6. Find $[101]_{1000}^2$, $[101]_{1000}^3$, ...
7. $f : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $f([x]_n) = [g(x)]_m$ is a well-defined function iff $[x]_n = [y]_n$ implies $[g(x)]_m = [g(y)]_m$.
8. Show that if $[x]_{mn} = [y]_{mn}$ then $[x]_m = [y]_m$ and $[x]_n = [y]_n$. Show that if $\gcd(m, n) = d > 1$ then there exists a pair $([a]_m, [b]_n)$ which is not in the image of f. For the converse, use the Chinese Remainder Theorem.
9. Review the definition of an equivalence relation.
   (a) A similar problem was done in class.
   (b) Check all the conditions for an equivalence relation.
   (c) The reflexive law says that $x^2 > 0$. Is this true?
   (d) A similar problem was done in class (the one with the sign function).
10. (a) Find the image of each element i. For $\sigma\tau$, apply τ first, and then apply σ.
    (b) We say that σ and τ commute if $\sigma\tau = \tau\sigma$
    (c) σ^{-1} is a permuation such that $\sigma^{-1}\sigma = 1_S$.
    (d) Construct the sequence $1, \sigma(1), \sigma^2(1), \ldots$. You'll get a cycle. If there are any elements left, construct another cycle...
    (e) See examples on pages 67 and 68.
    (f) See page 73.
    (g) σ is an even permutation if it can be written as a product of an even number of transpositions. It is an odd permutation if it can be written as a product of an odd number of transpositions.