CIS260-201/204–Spring 2008

Recitation 13 Supplementary Exercises

Friday, April 25

First Note: Please make sure that you understand the proof of Theorem 34.1, especially the uniqueness part of the proof.

1. Prove or disprove the following statements.

   (a) For all integers a, b, we have $b \mid a$ iff $a \text{ div } b = \frac{a}{b}$.

   (b) For all integers a, b, we have $b \mid a$ iff $a \bmod b = 0$.

2. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Prove that $a \equiv b \pmod{n}$ if and only if $a \bmod n = b \bmod n$.

3. Prove that the sum of any k consecutive integers is divisible by k.

4. Let a and b be positive integers. Find the sum of all the common divisors of a and b.

5. If $n \in \mathbb{Z}^+$ and $n \geq 2$, prove that

$$\sum_{i=1}^{n-1} i \equiv \begin{cases} 0 \pmod{n}, & n \text{ odd} \\ \frac{n}{2} \pmod{n}, & n \text{ even} \end{cases}.$$

6. Prove that if a and b have a greatest common divisor, it is unique, i.e., they cannot have two (distinct) greatest common divisors.

7. Suppose $a, b \in \mathbb{Z}$ are relatively prime. Recall that there exist integers x, y such that $ax + by = 1$. Prove that $\gcd(x, y) = 1$.

8. (a) Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$, prove that $a \mid c$.

   (b) Let $p, q \in \mathbb{Z}$ be prime numbers and let $a \in \mathbb{Z}$. Prove that $p \mid a$ and $q \mid a$ if and only if $pq \mid a$.

   (c) Let $m, n \in \mathbb{Z}$ and p be a prime. Prove that if $p \mid mn$, then $p \mid m$ or $p \mid n$. [**Hint**: Use Part 8(a).]

9. This problem is a continuation of Quiz 8. Let n be a positive integer and suppose $a, b \in \mathbb{Z}_n$ are both invertible. Prove or disprove the following statements.

   (a) $a \ominus b$ is invertible.

   (b) $a \oslash b$ is invertible.

10. Find the multiplicative inverse of the following elements or state that none exists.

(a) $2 \in \mathbb{Z}_{17}$	(c) $13 \in \mathbb{Z}_{1001}$	(e) $119 \in \mathbb{Z}_{1547}$	(g) $123 \in \mathbb{Z}_{4321}$
(b) $8 \in \mathbb{Z}_{17}$	(d) $101 \in \mathbb{Z}_{1001}$	(f) $121 \in \mathbb{Z}_{1547}$	(h) $447 \in \mathbb{Z}_{4321}$