# 18.781 Problem Set 3 - Fall 2008

Due Tuesday, Sep. 30 at 1:00

1. (Niven 2.3.3) Solve the congruences $x \equiv 1 \pmod 4, x \equiv 0 \pmod 3, x \equiv 5 \pmod 7$.

2. (Niven 2.3.8) Find the smallest positive integer whose remainder is $1, 2, 3, 4$, and $5$ when divided by $3, 5, 7, 9$, and $11$, respectively. What is the second smallest such integer?

3. (Niven 2.3.18) For any $k \geq 1$, prove that there exist $k$ consecutive positive integers that are each divisible by a square number. For example, the sequence $\{48, 49, 50\}$ works for $k = 3$.

4. This problem presents an iterative approach to solving the simultaneous congruences $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \ldots x \equiv a_k \pmod{m_k}$, where all of the $m_i$ are coprime (thereby proving CRT). This technique is especially useful when the $a_i$ are all relatively close in value. The algorithm follows:

   (i) Given $a_1, m_1, a_2, m_2, \ldots, a_k, m_k$, re-number indices so that $a_1 \leq a_2 \cdots \leq a_k$.
   (ii) Use the Euclidean algorithm to find $y$ such that $ym_1 \equiv 1 \pmod{m_2}$.
   (iii) Set $a' := a_1 + (a_2 - a_1)ym_1 \pmod{m'}$, where $m' = m_1 m_2$.
   (iv) If $k \geq 3$, return to step (ii) with $a', m', a_3, m_3, \ldots, a_k, m_k$.

   (a) Prove that the algorithm works by showing that the final output $a'$ is the unique solution $x$ modulo $m_1 m_2 \cdots m_k$ (the main details to verify are in (iii)).
   (b) Solve the congruences $x \equiv 4 \pmod 5, x \equiv 5 \pmod 7, x \equiv 6 \pmod{11}$.

5. (Niven 2.3.20) Prove that there is a simultaneous solution of $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$ iff $a_1 \equiv a_2 \pmod{(m_1, m_2)}$. Prove that the solution is unique modulo $[m_1, m_2]$.

6. (Niven 2.3.25) Prove that the number of integers $1 \leq n \leq mk$ that satisfy $(n, m) = 1$ is $k\phi(m)$.

7. (Niven 2.3.26) Prove that $\phi(nm) = n\phi(m)$ if every prime divisor of $n$ also divides $m$.

8. (Niven 4.2.4) Find the smallest $m$ for which there exists another $n \neq m$ with $\sigma(m) = \sigma(n)$.

9. (Niven 4.2.5) Prove that
$$\prod_{d|n} d = n^{d(n)/2}.$$

10. (Niven 4.2.9) Suppose that $f(n)$ and $g(n)$ are multiplicative.

    (a) Prove that $F(n) := f(n)g(n)$ is also multiplicative.
    (b) If $g(n) \neq 0$ for all $n$, prove that $G(n) := f(n)/g(n)$ is multiplicative.

11. (Niven 4.2.12) Prove that $\omega(n) = \#\{d \mid n\}$ is odd iff $n$ is a square.

12. (Niven 4.2.16 and 4.2.19) A positive integer $n$ is a perfect number if $\sigma(n) = 2n$ (i.e., $n$ is the sum of its proper divisors; for example, $6 = 1 + 2 + 3$ is perfect). Prove that if $2^m - 1 = p$ is prime, then $2^{m-1}p$ is perfect.

(Bonus) Prove that every even perfect number has this form.

*Remark: It is widely believed that there are no odd perfect numbers, although this is still an open conjecture!*

13. (Niven 4.2.1) Find $n$ such that $\mu(n) + \mu(n+1) + \mu(n+2) = 3$.

14. (Niven 4.2.2) Prove that $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$ for all $n$.

(Bonus) (a) Prove that if $f$ and $g$ are multiplicative, then

$$F(n) := \sum_{d|n} f(d)g(n/d)$$

is multiplicative.

(b) Prove that if

$$F(n) = \sum d \mid nf(d),$$

then $f(n)$ is also multiplicative.

(c) Define

$$F(n) := \begin{cases} 1 & \text{if } n \text{ is square,} \\ 0 & \text{otherwise.} \end{cases}$$

Use Möbius inversion to find $f(n)$ such that

$$F(n) = \sum_{d|n} f(d).$$

Prove that $f$ is multiplicative and find an explicit formula for $f(n)$.