18.781 Problem Set 4 - Fall 2008

Due Tuesday, Oct. 7 at 1:00

1. (a) Prove that for any arithmetic functions f,

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right).$$

(b) Prove that if g is another arithmetic function, then

$$\sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{d}\right)\, g(d).$$

2. The *Riemann Zeta function* is one of the most important functions in number theory (and the subject of a million dollar research prize!). It is defined for complex arguments s as

$$\zeta(s) := \sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-\frac{1}{p^s}},$$

although the above formulas only converge for $\Re(s) > 1$.

(a) Prove that the sum and product formulas for $\zeta(s)$ are actually equal.

(b) Prove that the inverse of the zeta function can be written as

$$\frac{1}{\zeta(s)} = \sum_{n\geq 1} \frac{\mu(n)}{n^s}.$$

3. (Niven 2.1.17) Show that $61! \equiv 63! \equiv -1 \pmod{71}$.

4. (Niven 2.1.51) Prove that

$$(p-1)! \equiv p-1 \pmod{P},$$

where $P = 1 + 2 + \cdots + p - 1$.
Hint: Use the Chinese Remainder Theorem and Wilson's Theorem.

5. The *harmonic sums* are defined as

$$H_n := \sum_{\substack{m\leq n \\ (m,n)=1}} \frac{1}{m},$$

and we write $H_n = \frac{A_n}{B_n}$ as fractions. For example, $H_p = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$ for any prime p, and $H_{12} = 1 + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} = \frac{552}{385}$. It is a fact that if $n > 1$, H_n is never an integer, and thus $B_n \neq 1$.

(a) Prove that $p \mid A_p$ for any prime p.
Hint: Pair the terms $\frac{1}{i}$ and $\frac{1}{p-i}$.

(b) Prove that $n \mid A_n$ for all n.

(Bonus) Prove that $p^2 \mid A_p$ for any prime $p \geq 5$.

(Bonus) Find and prove a formula for $A_n \bmod n^2$ for all n.

6. (Niven 2.4.4) Show that the Carmichael number 561 is composite by showing that it is not a strong probable prime for base 2.

7. Recall that a composite integer n is a Carmichael number if it is a probable prime for all bases, so $a^n \equiv a \pmod{n}$ for all a.

   (a) Suppose that n is squarefree. Prove that n is a Carmichael number if and only if $(p-1) \mid (n-1)$ for every prime divisor $p \mid n$.
   Hint: Use the Chinese Remainder Theorem on the congruence $a^n \equiv a \pmod{n}$.

   (b) Prove that every Carmichael number is squarefree.
   Hint: If n has a square factor, you just need to find one a such that $a^n \not\equiv a \pmod{n}$.

8. (Niven 2.4.5) Show that 2047 is a strong probable prime for 2.

9. (Niven 2.4.10 & 2.4.11)

   (a) Suppose that n is a pseudoprime for the base a, but is not a strong pseudoprime. Show that there is then some k such that $a^k \equiv m \not\equiv \pm 1 \pmod{n}$ but $a^{2k} \equiv 1 \pmod{n}$. Prove that at least one of $(n, m+1)$ and $(n, m-1)$ is a nontrivial divisor of n.

   (b) Show that 341 is a pseudoprime for the base 2, but is not a strong pseudoprime. In particular, $2^{85} \equiv m \not\equiv \pm 1 \pmod{341}$, but $2^{170} \equiv 1 \pmod{341}$. Find a nontrivial divisor of 341.

10. (Niven 2.4.14abd) Use the Pollard rho method to find a proper divisor of

    (a) 8131,

    (b) 7913,

    (c) 16019.

11. (Niven 2.5.1) Suppose that $b \equiv a^{67} \pmod{91}$, with $(a, 91) = 1$. Find $\overline{k}$ such that $b^{\overline{k}} \equiv a \pmod{91}$. If $b = 53$, what is $a \bmod 91$?

(Bonus) Define the *composite factorials* as (this is nonstandard notation)

$$n¡ := \prod_{\substack{m \leq n \\ (m,n)=1}} m.$$

So $p¡ = (p-1)!$, and for example, $15¡ = 1 \cdot 2 \cdot 4 \cdot 7 \cdot 8 \cdot 11 \cdot 13 \cdot 15 \equiv 1 \pmod{15}$.

(a) Prove that if $n = pq$ with p, q prime, then $n¡ \equiv 1 \pmod{n}$.

(b) Determine a general formula for $n¡ \bmod n$.