Solutions to 18.781 Problem Set 4 - Fall 2008

Due Tuesday, Oct. 7 at 1:00

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

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

To show the relation, we only have to show this equality of sets:

$$\{d \in \mathbb{N} \mid d|n\} = \{\frac{n}{d} \in \mathbb{N} \mid d|n\}.$$

So we have the following string of equivalences.

$$\begin{aligned} x \in \{d \in \mathbb{N} \mid d|n\} &\Leftrightarrow \exists y \in \mathbb{N} \text{ s.t. } xy = n \\ &\Leftrightarrow \exists y \in \mathbb{N} \text{ s.t. } y|n \text{ and } \frac{n}{y} = x \\ &\Leftrightarrow x \in \{\frac{n}{d} \in \mathbb{N} \mid d|n\}. \end{aligned}$$

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

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

Here we can manipulate the index in the summation to show that the two sums are equal. Note that this method can also be used above.

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

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.

For this problem I will ignore some of the tricky convergence issues to give a more intuitive explanation. We start by rewriting the index of the sum using the fundamental theorem of arithmetic!

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \sum_{n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}} \frac{1}{(p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k})^s} = \sum_{\substack{r_i \in \mathbb{N} \cup \{0\} \\ r_i \longrightarrow 0}} \prod_i \frac{1}{(p_i^{r_i})^s}.$$

Note that the requirement that a sequence of nonnegative integers converge to zero is the same as assuming that only finitely many are nonzero. This shows that the last sum is in fact the same as the middle one. So now we do a massive "distribution" of this sum of products.

$$\sum_{\substack{r_i \in \mathbb{N}\cup\{0\} \\ r_i \longrightarrow 0}} \prod_i \frac{1}{(p_i^{r_i})^s} = \prod_{i\geq 1} \sum_{r\geq 0} \frac{1}{(p_i^r)^s} = \prod_{i\geq 1} \sum_{r\geq 0} \frac{1}{(p_i^s)^r}.$$

and now we recognize the geometric series and compute it;

$$= \prod_{i\geq 1} \frac{1}{1-(p_i^{-s})} = \prod_{p \text{ prime}} \frac{1}{1-\frac{1}{p^s}}.$$

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

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

We compute the product of $\zeta(s)$ with this summation.

$$\zeta(s) \cdot \sum_{n\geq 1} \frac{\mu(n)}{n^s} = \left(\sum_{n\geq 1} \frac{1}{n^s}\right)\left(\sum_{n\geq 1} \frac{\mu(n)}{n^s}\right) = \sum_{m\geq 1}\sum_{n\geq 1}\left(\frac{1}{m^s}\cdot\frac{\mu(n)}{n^s}\right)$$
$$= \sum_{r\geq 1}\sum_{mn=r}\left(\frac{1}{m^s}\cdot\frac{\mu(n)}{n^s}\right) = \sum_{r\geq 1}\frac{1}{r^s}\left(\sum_{mn=r}\mu(n)\right).$$

Now we notice that the interior sum is just the sum of $\mu(n)$ over the divisors of r. This is shown in the book to equal zero unless $r = 1$, in which case it is one. So we have that

$$\zeta(s) \cdot \sum_{n\geq 1} \frac{\mu(n)}{n^s} = \frac{1}{1^s}\cdot 1 + \frac{1}{2^s}\cdot 0 + \frac{1}{3^s}\cdot 0 + \cdots = 1.$$

So we have shown that the product of the sum with $\zeta(s)$ is identically one, which means that the sum must be $\frac{1}{\zeta(s)}$.

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

Note that we have that $70! \equiv -1 \pmod{71}$ from Wilson's Theorem. Relating this information to the problem at hand,

$$63!(64)(65)(66)(67)(68)(69)(70) = 70! \equiv -1 \pmod{71}.$$

We calculate this product mod 71:

$$(64)(65)(66)(67)(68)(69)(70) \equiv (-7)(-6)(-5)(-4)(-3)(-2)(-1) \equiv -5040 \equiv 1.$$

This immediately gives that $63! \equiv 70! \equiv -1 \pmod{71}$. Now, the same trick can be used to finish the problem. From the work above, we know

$$-1 \equiv 61!(62)(63) \equiv 61!(-9)(-8) \equiv 61!(72) \equiv 61! \pmod{71}.$$

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.

We know the proof of the summation formula for P:

$$P = 1 + 2 + \cdots + p - 1 = \frac{(p-1)p}{2} = \frac{p-1}{2} \cdot p.$$

We can assume p is odd by computing the case for $p = 2$, which holds because $1! = 1$. Next we compute $(p-1)!$ modulo the two factors. Since $\frac{p-1}{2} \mid (p-1)!$, it is clear that $(p-1)! \equiv 0 \pmod{\frac{p-1}{2}}$. We also have $(p-1)! \equiv -1 \pmod{p}$ by Wilson's Theorem. Now, note

$$\begin{aligned} p - 1 &\equiv 0 \pmod{\frac{p-1}{2}}, \\ p - 1 &\equiv -1 \pmod{p}. \end{aligned}$$

Since p prime implies $(\frac{p-1}{2}, p) = 1$, we may apply Chinese Remainder Theorem to claim that because $(p-1)!$ and $p-1$ are equivalent modulo the two relatively prime factors of P, they are congruent mod P.

5. The *harmonic sums* are defined as

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

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 $\frac{1}{p-i}$.
We want to show that $p | A_p$ for prime p. Since we are assuming the fraction representation is in lowest terms, this means that $p | A_p$ and $p \nmid B_p$. So first we note that if we collect all of the terms together by taking the common denominator of $(p-1)!$, we have that $p \nmid (p-1)!$. Now we see what the hint gives us. For any $1 \le i \le p-1$,

$$\begin{aligned} \frac{1}{i} + \frac{1}{p-i} &= \frac{(p-i)+i}{i(p-i)} = \frac{p}{i(p-i)} \\ &= \frac{1 \cdot 2 \cdot \cdots \cdot (i-1)(i+1)(\ldots)(p-i-1)(p-i+1)(\ldots)(p-1)p}{(p-1)!}. \end{aligned}$$

That last fraction is just to show that when we combine all of these pairs together over the common denominator $(p-1)!$, each term has a factor of p in the numerator. So the entire sum will have a factor of p in the numerator, and since there is no such factor in the denominator, it will not get canceled when reducing the fraction.

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

Here we can use the exact same trick as above. The key difference is our common denominator should be chosen to be

$$C_n = \prod_{\substack{m \le n \\ (m,n)=1}} m.$$

Then this denominator has the necessary quality that it is coprime to n, so just as above, we know that the factor of n we get in the numerator will not be canceled when reducing the fraction.

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

(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.

For the strong probable prime test, we write $561 - 1$ as the product $2^4 \cdot 35$. So we need to calculate $2^{35} \pmod{561}$. We can calculate this by successive squaring and reduction:

n	$2^{2^n} \pmod{561}$
0	2
1	4
2	16
3	256
4	460
5	103

So $2^{35} = 2^{32} \cdot 2^3 \equiv 103 \cdot 8 \equiv 263 \pmod{561}$. Now, if we successively square and reduce this number, we get

$$\begin{aligned} 2^{70} &\equiv 166 \\ 2^{140} &\equiv 67 \\ 2^{280} &\equiv 1 \end{aligned}$$

So we have found that $2^{280} \equiv 1 \pmod{561}$. Now, that alone not enough to show that 561 is Carmichael, but we not that in the line before we got the 1, we found that $2^{140} \equiv 67$. So this shows that we have found a square root of $1 \pmod{561}$ that is not 1 or -1. Thus 561 cannot be prime.

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 $a^n \equiv a \pmod{n}$.

We are given that n is squarefree, so we can write its prime factorization: $n = p_1 p_2 \dots p_l$. Then n is a Carmichael number if and only if

$$\forall a \in \mathbb{Z},\ a^n \equiv a \pmod{n}.$$

Using CRT, we have that this is true if and only if, for each $1 \leq i \leq l$,

$$\forall a \in \mathbb{Z},\ a^n \equiv a \pmod{p_i}.$$

Since this equation is trivial for $a \equiv 0$, we can assume we can divide by a, and so it is equivalent to

$$\forall a \in \mathbb{Z} \text{ such that } p \not| a,\ a^{n-1} \equiv 1 \pmod{p_i}.$$

But we know that every unit mod p has order dividing $p-1$, and in fact, there is some element with order $p-1$. So choosing a as this number implies that $(p_i - 1)|(n-1)$ for each i. So we have shown the equivalence.

(b) Prove that every Carmichael number is squarefree.
Hint: If n has a square factor, you just need to find one a such that $a^n \not\equiv a \pmod{n}$.
So now consider some prime divisor of n with $p^2|n$. Then for $a = \frac{n}{p} \in \mathbb{Z}$,

$$a^2 = \frac{n^2}{p^2} = n \cdot \frac{n}{p^2} \equiv 0 \not\equiv a \pmod{n}.$$

So n is not a Carmichael number.

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

We use the same method in problem 6: $2046 = 2 \cdot 1023$, so now we calculate 2^{1023} by successive squaring. Since 1024 is the tenth power of two, I'll just find 2^{1024} and divide by 2.

n	$2^{2^n} \pmod{2047}$
0	2
1	4
2	16
3	256
4	32
5	1024
6	512
7	128
8	8
9	64
10	2

So $2^{1023} = 2^{2^{10}} \cdot 2^{-1} \equiv \frac{2}{2} \equiv 1 \pmod{2047}$, so 2047 is a strong probable prime for the base 2. However, it should be noted that if we didn't take this absolutely algorithmic approach, we could've seen that $2047 = 2^{11} - 1$, so $2^{11} \equiv 1$. Thus every power of 2 caluclated above could've been reduced mod 11, to make the calculations easier.

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 $a^{2k} \equiv 1$

(mod n). Prove that at least one of $(n, m+1)$ and $(n, m-1)$ is a nontrivial divisor of n.

When the strong pseudoprime test fails and the pseudoprime test succeeds, we know we are exactly in the case where

$$a^{\frac{n-1}{2^i}} \equiv 1 \pmod{n}, \text{ but } a^{\frac{n-1}{2^{i+1}}} \not\equiv \pm 1 \pmod{n}.$$

This means that, letting $k = \frac{n-1}{2^{i+1}}$, $a^k \equiv m \not\equiv \pm 1 \pmod{n}$, but $a^2 k \equiv 1$. Therefore $m^2 \equiv 1$ for some $m \not\equiv \pm 1 \pmod{n}$.

Then we have $n|(m^2-1) \Longleftarrow n|(m+1)(m-1)$, but $n \not| (m+1)$ and $n \not| (m-1)$. If $(n, m+1) = 1$, then $n|(m+1)(m-1) \Longleftarrow n|(m-1)$, which is a contradiction. If $(n, m+1) = n$, then $n|(m+1)$, also a contradiction. Therefore $(n, m+1)$ 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.

So we have that $340 = 2^2 \cdot 85$, so we find $2^{85} \pmod{341}$.

n	$2^{2^n} \pmod{341}$
0	2
1	4
2	16
3	256
4	64
5	4
6	16

Now, $2^{85} = 2^{64} \cdot 2^{16} \cdot 2^4 \cdot 2 \equiv 16 \cdot 64 \cdot 16 \cdot 2 \equiv 32 \pmod{341}$. But $2^{170} \equiv 32^2 = 1024 \equiv 1 \pmod{341}$. So we have $m = 32$. This gives us the possible prime divisors $31, 3, 11$, and a quick division shows $341 = 11 \cdot 31$.

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

(a) 8131,

Starting with 3, and using the polynomial $f(x) = x^2 + 1$, we get the series: 3, 10, 101, 2071, 4005, 5694,...

Now, checking the gcd's of the differences of terms s and $2s$, we have:

(8131,10-3)=1, (8131,2071-10)=1, but (8131,5694-101)=47. So we get $8131 = 47 \cdot 173$.

(b) 7913,

Here let's start with 2 using the polynomial $f(x) = x^2 - 1$, just to change things up. We get: 2, 3, 8, 63, 3968, 6066, 905, 3985, 6746, 852,...

Now checking gcd's:

(7913,3-2)=1, (7913,63-3)=1, (7913,6066-8)=1, (7913,3985-63)=1, but (7913,852-3968)=41. Thus $7913 = 41 \cdot 193$.

(c) 16019.

This one is done exactly as the previous; using $f(x) = x^2 + 1$ and beginning with 1, we find that $(x_{20} - x_{10}, 16019) = 83$.

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 $a \bmod 91$?

First, calculate $\phi(91) = 72$. Next, use the Euclidean algorithm to find that $27 \cdot 72 - 29 \cdot 67 = 1$. Reducing mod 72 implies that $-29 \cdot 67 equiv 43 \cdot 67 \equiv 1 \pmod{72}$, so $\overline{k} = 43$. Using successive squaring then gives $a \equiv 53^{43} \equiv 53 \pmod{91}$.

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

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

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 $n¡ \mod n$.