

# Math 322 Exam 2 Solutions

Instructor: Jay Daigle

**Problem 1.** (a) Compute  $\mu(91)$ .

(b) Compute  $\mu(9100)$ .

(c) Compute  $\sigma(36)$ .

(d) Compute  $\tau(7!)$ .

**Solution:**

(a)  $91 = 7 \cdot 13$  so  $\mu(91) = (-1)^2 = 1$ .

(b) 9100 is divisible by 4 which is a square. So  $\mu(9100) = 0$ .

(c)  $36 = 2^2 3^2$ , so  $\sigma(36) = \frac{2^3-1}{2-1} \frac{3^3-1}{3-1} = 7 \cdot 13 = 91$ .

(d)  $\tau(7!) = \tau(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2) = \tau(2^4 \cdot 3^2 \cdot 5 \cdot 7) = (5)(3)(2)(2) = 60$ .

**Problem 2.** (a) Compute  $5^{1234} \pmod{18}$ . (Hint: use Euler's Theorem)

(b) Show that  $30240 = 2^5 \cdot 3^3 \cdot 5 \cdot 7$  is 4-perfect.

**Solution:**

(a) We know that  $\phi(18) = 3(3-1)(2-1) = 6$ . Thus  $5^6 \equiv 1 \pmod{18}$ . Then

$$5^{1234} = (5^6)^{205} \cdot 5^4 \equiv 5^4 \equiv (25)^2 \equiv 7^2 \equiv 49 \equiv 13 \pmod{18}.$$

(b) We compute that

$$\sigma(30240) = \frac{2^6-1}{2-1} \frac{3^4-1}{3-1} \frac{5^2-1}{5-1} \frac{7^2-1}{7-1} = (63)(40)(6)(8) = 2^7 \cdot 3^3 \cdot 5 \cdot 7 = 120960 = 4 \cdot 30240.$$

**Problem 3.** Show that  $6601 = 7 \cdot 23 \cdot 41$  is a Carmichael number.

**Solution:** Suppose  $(b, 6601) = 1$ . Then

$$b^6 \equiv 1 \pmod{7}$$

$$b^{22} \equiv 1 \pmod{23}$$

$$b^{40} \equiv 1 \pmod{41}$$

$$(b^6)^{1100} \equiv 1 \pmod{7}$$

$$(b^{22})^{300} \equiv 1 \pmod{23}$$

$$(b^{40})^{165} \equiv 1 \pmod{41}$$

Thus by the Chinese Remainder Theorem,  $b^{6600} \equiv 1 \pmod{7 \cdot 23 \cdot 41 = 6601}$ . Thus 6601 is pseudoprime to any base it is relatively prime to, and thus by definition is a Carmichael number.

**Problem 4.** (a) Find (with proof) every number  $n$  with  $\phi(n) = 6$ .

(b) Find (with proof) every number  $n$  with  $\phi(n) = 9$ .

**Solution:**

1. Suppose  $p$  is a prime factor of  $n$ . Then  $\phi(p)|6$  so  $\phi(p) = 1, 2, 3, 6$ . Thus  $p = 2, 3, 4, 7$ , and 4 isn't prime, so we can only have  $p = 2, 3, 7$ . Thus we take  $n = 2^a 3^b 7^c$ .

Then we have  $\phi(n) = 2^{a-1} \cdot 2 \cdot 3^{b-1} \cdot 6 \cdot 7^{c-1}$ , and we immediately see that  $c \leq 1$ .

If  $c = 0$  then we have  $n = 2^a 3^b$ . Assume  $a, b > 0$ . Then  $6 = \phi(n) = 2^{a-1} \cdot 2 \cdot 3^{b-1}$  so we must have  $b = 2$ , which gives  $a = 1$ . So  $\phi(18) = 6$ .

If  $c = 0, a = 0$  then we have  $n = 3^b$  and  $\phi(n) = 2 \cdot 3^{b-1}$ , which again gives  $b = 2$ . Thus  $\phi(9) = 6$ .

If  $c = 0, b = 0$ , then  $n = 2^a$  and  $6 = \phi(n) = 2^{a-1}$  which isn't possible.

Now if  $c > 0$ , we have  $6 = \phi(n) = \phi(2^a 3^b) \phi(7^c) = \phi(2^a 3^b) \cdot 6 \cdot 7^{c-1}$ . Thus  $c = 1$  and we have  $\phi(2^a 3^b) = 1$ . This implies that either  $2^a 3^b = 1$  or  $2^a 3^b = 2$ , so we have  $\phi(7) = 6$  and  $\phi(14) = 6$ .

Thus the final set of solutions is  $n \in \{7, 9, 14, 18\}$ .

2. We know that  $\phi(n)$  is even unless  $n = 1$  or  $n = 2$ , in which case  $\phi(n) = 1$ . So there are no  $n$  with  $\phi(n) = 9$ .

**Problem 5.** If  $n$  is square-free, show that

$$\sum_{d|n} (\mu(d))^2 \phi(d) = n.$$

**Solution:**

Suppose  $n$  is square-free. Then  $d$  is square-free for any  $d|n$ , so  $\mu(d) = \pm 1$  and  $(\mu(d))^2 = 1$ . Thus

$$n = \sum_{d|n} \phi(d) = \sum_{d|n} (\mu(d))^2 \phi(n/d)$$

Note:  $\sum_{d|n} \mu(d)^2 \phi(d) \neq \left(\sum_{d|n} \mu(d)^2\right) \left(\sum_{d|n} \phi(d)\right)$ . This is easy to see if you write it out with actual numbers:

$$\begin{aligned} \sum_{d|6} \mu(d)^2 \phi(d) &= \mu(1)^2 \phi(1) + \mu(2)^2 \phi(2) + \mu(3)^2 \phi(3) + \mu(6)^2 \phi(6) \\ \left(\sum_{d|6} \mu(d)^2\right) \left(\sum_{d|6} \phi(d)\right) &= (\mu(1)^2 + \mu(2)^2 + \mu(3)^2 + \mu(6)^2)(\phi(1) + \phi(2) + \phi(3) + \phi(6)) \\ &= \mu(1)^2 \phi(1) + \mu(2)^2 \phi(1) + \mu(3)^2 \phi(1) + \mu(6)^2 \phi(1) \\ &\quad + \mu(2)^2 \phi(1) + \mu(2)^2 \phi(2) + \mu(3)^2 \phi(2) + \mu(6)^2 \phi(2) \\ &\quad + \mu(3)^2 \phi(1) + \mu(2)^2 \phi(3) + \mu(3)^2 \phi(3) + \mu(6)^2 \phi(3) \\ &\quad + \mu(6)^2 \phi(1) + \mu(2)^2 \phi(6) + \mu(3)^2 \phi(6) + \mu(6)^2 \phi(6) \end{aligned}$$