

## Math 4150 Homework 6 Solutions

**Problem 2.** Let  $r = e_n(a^s)$ . Then  $a^{sr} = (a^s)^r \equiv 1 \pmod{n}$ , so  $e_n(a)|sr$ , that is,  $st|sr$  so  $t|r$ . Moreover, we have  $(a^s)^t = a^{st} \equiv 1 \pmod{n}$ , so  $e_n(a^s)|t$ , that is,  $r|t$ . Therefore  $r = t$ , so  $e_n(a^s) = t$ .

**Problem 4.** Let  $r = e_m(a)$ . Since  $a^n = m + 1$ , we clearly have  $a^n \equiv 1 \pmod{m}$ , so  $r|n$ . We have, by definition of  $r$ ,  $m|a^r - 1$ , so  $a^n - 1|a^r - 1$ . In particular  $n \leq r$ , and since  $r|n$ , we must have  $r = n$ .

**Problem 5.** Let  $g$  be a primitive root modulo  $p$ . The numbers  $1, 2, \dots, p-1$  are congruent to  $g, g^2, \dots, g^{p-1}$  in some order. Therefore we have

$$1^k + 2^k + \dots + (p-1)^k \equiv g^k + (g^2)^k + \dots + (g^{p-1})^k = g^k + (g^k)^2 + \dots + (g^k)^{p-1}.$$

If  $p-1|k$  then  $g^k = 1$ , so the above sum becomes  $1 + 1 + \dots + 1 = p-1$ , which is  $-1$  modulo  $p$ . If  $p-1 \nmid k$ , then  $g^k \neq 1$  and so the above sum is

$$= \frac{g^{kp} - 1}{g^k - 1} - 1 = \frac{g^p - 1}{g^k - 1} - 1 \equiv 0 \pmod{p}.$$

**Problem 7.** Suppose first that 2 is a primitive root modulo  $q$ . By Fermat's theorem,  $2^{2p} = 2^{q-1} \equiv 1 \pmod{q}$ , so  $(2^p - 1)(2^p + 1) \equiv 0 \pmod{q}$ . Since  $q$  is prime, we have either  $2^p \equiv 1 \pmod{q}$  or  $2^p \equiv -1 \pmod{q}$ . However, if it were the case that  $2^p \equiv 1 \pmod{q}$ , then  $e_q(2)|p$ , and in particular  $e_q(2) < q-1$ , so 2 is not a primitive root modulo  $q$ , which is a contradiction. Thus we must have  $2^p \equiv -1 \pmod{q}$ .

Now suppose that  $2^p \equiv -1 \pmod{q}$  and let  $r = e_q(2)$ . Since  $2^{2p} \equiv 1 \pmod{q}$ , we know  $r|2p$ . If  $r < 2p$ , then  $r$  must be either  $1, 2$ , or  $p$ . However, in these cases we would have  $2^r \equiv 2, 4, -1 \pmod{q}$ , respectively, contradicting the definition of  $r$ . Therefore  $r = 2p = q-1$ , so 2 is a primitive root modulo  $q$ .

**Problem 8.** Suppose first that  $e_q(2)|(p-1)$  and  $e_p(2)|(q-1)$ . Then  $2^{p-1} \equiv 1 \pmod{q}$ , so  $2^{(p-1)q} \equiv 1 \pmod{q}$ . Thus  $2^{pq-1} = 2^{(p-1)q+(q-1)} \equiv 1 \cdot 2^{q-1} \equiv$

$1 \pmod{q}$  by Fermat's theorem. A similar argument shows that  $2^{pq-1} \equiv 1 \pmod{p}$ , so by the Chinese remainder theorem,  $2^{pq-1} \equiv 1 \pmod{pq}$ ; hence  $pq$  is a pseudoprime to the base 2.

Now suppose that  $pq$  is a pseudoprime to the base 2, that is,  $2^{pq-1} \equiv 1 \pmod{pq}$ . Then  $2^{pq-1} \equiv 1 \pmod{p}$ , so  $e_p(2)|(pq-1)$ . By Fermat's theorem,  $e_p(2)|(p-1)$ . Therefore  $e_p(2)|[(pq-1)-(p-1)] = (q-1)p$ . Since  $e_p(2) < p$ , then  $e_p(2)$  is coprime to  $p$ , and so  $e_p(2)|(q-1)$ . A similar argument shows that  $e_q(2)|(p-1)$ .