Elementary Number Theory Homework #8

Replace this text with your name

Due: Replace this text with a due date

Exercise (8.1.5)**.** Given that a has order 3 modulo p, where p is an odd prime, show that $a+1$ must have order 6 modulo p.
[*Hint:* From $a^2+a+1 \equiv 0 \pmod{p}$, it follows that $(a+1)^2 \equiv a \pmod{p}$ and $(a+1)^3 \equiv -1 \pmod{p}$.]

Solution: Replace this text with your solution. □

Exercise (8.1.13)**.** (a) Find two primitive roots of 10.

(b) Use the information that 3 is a primitive root of 17 to obtain the eight primitive roots of 17.

Solution: Replace this text with your solution. □

Exercise (8.2.5)**.** Find all positive integers less than 61 having order 4 modulo 61.

Solution: Replace this text with your solution. □

Exercise (8.2.6)**.** Assuming that r is a primitive root of the odd prime p, establish the following facts:

(a) The congruence $r^{(p-1)/2} \equiv -1 \pmod{p}$ holds.

(b) If r' is any other primitive root of p, then rr' is not a primitive root of p.
[*Hint:* By part (a), $(rr')^{(p-1)/2} \equiv 1 \pmod{p}$.]

(c) If the integer r' is such that $rr' \equiv 1 \pmod{p}$, then r' is a primitive root of p.

Solution: Replace this text with your solution. □

Exercise (8.3.5)**.** Obtain all the primitive roots of 41 and 82.

Solution: Replace this text with your solution. □

Exercise (8.3.9)**.** If $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, define the *universal exponent* $\lambda(n)$ of n by

$$\lambda(n) = \operatorname{lcm}(\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$$

where $\lambda(2) = 1$, $\lambda(2^2) = 2$, and $\lambda(2^k) = 2^{k-2}$ for $k \geq 3$. Verify that, for $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, $\lambda(5040) = 12$ and $\phi(5040) = 1152$.

Solution: Replace this text with your solution. □

Exercise (8.4.5)**.** If r and r' are both primitive roots of the odd prime p, show that for $\gcd(a, p) = 1$

$$\operatorname{ind}_{r'} a \equiv (\operatorname{ind}_r a)(\operatorname{ind}_{r'} r) \pmod{p-1}.$$

Solution: Replace this text with your solution. □

Exercise (8.4.7)**.** If r is a primitive root of the odd prime p, verify that

$$\operatorname{ind}_r(-1) \equiv \operatorname{ind}_r(p-1) = \frac{1}{2}(p-1).$$

Solution: Replace this text with your solution. □