Math 40520 Theory of Number
Homework 3

Due Wednesday, 2015-09-23, in class

Do 5 of the following 8 problems. Please only attempt 5 because I will only grade 5.

1. Suppose $n \geq 2$ and $a \in \mathbb{Z}_n^\times$. Show that a has multiplicative order m modulo n if and only if the following two conditions are satisfied:
   (a) $a^m \equiv 1 \pmod{n}$ and
   (b) for every prime divisor p of m, $a^{m/p} \not\equiv 1 \pmod{n}$.

2. Suppose p is an odd prime and $n \geq 1$. If $d \mid \varphi(p^n)$ show that there are exactly $\varphi(d)$ numbers in $\mathbb{Z}_{p^n}^\times$ of multiplicative order d. [Hint: Use primitive roots and what you know about computing multiplicative orders.] (Remark: In the textbook this is Theorem 6.5 whose proof takes up a few pages. Don't reproduce that proof here. The textbook deduces the existence of primitive roots from this theorem whereas the point of this exercise is to go in the other direction, namely, deduce this fact from the existence of primitive roots.)

3. Suppose $n \geq 3$. Let $d = 2^r \mid 2^{n-2}$. Show that there are $2\varphi(d) = 2^r$ numbers in $\mathbb{Z}_{2^n}^\times$ of multiplicative order $d = 2^r$ unless $d = 1$ in which case there is one such number and $d = 2$ in which case there are 3 such numbers. (cf. Exercise 6.12 on page 107.) [Hint: Use primitive roots and what you know about computing multiplicative orders.]

4. Show that if $n \geq 1$ is an integer then
$$7^{2^n} \equiv 1 + 2^{n+3} \pmod{2^{n+4}}$$
and determine the multiplicative order of 7 modulo 2^m for integers $m \geq 1$.

5. (This is a slight generalization of the previous problem, but equal in difficulty.) Suppose $k \geq 2$ and $n \geq 1$ are integers. Show that
$$(2^k \pm 1)^{2^n} \equiv 1 + 2^{k+n} \pmod{2^{k+n+1}}$$
and determine the multiplicative order of $2^k \pm 1$ modulo 2^m for integers $m \geq k + 2$. (In class we did the case $k = 1$ and $3 = 2^1 + 1$, in the textbook, Lemma 6.9, they do $k = 2$ and $5 = 2^2 + 1$ and the previous exercise does $k = 3$ and $7 = 2^3 - 1$.)

6. Exercise 6.13 on page 108. [Hint: You need to show that all elements in the set are distinct. Use your knowledge of the multiplicative order of 3.] (In the textbook $U_n = \mathbb{Z}_n^\times$.)

7. A restatement of Exercise 6.10 on page 106. Show that 3 is always a primitive root modulo 7^n for all n. [Hint: Start with $3^6 \equiv 1 + 7 \cdot 6 \pmod{7^2}$ and emulate how we showed that 3 had order 2^{n-2} modulo 2^n. Use Exercise 1.] (In the textbook there is a different line of reasoning for showing this fact, based upon the textbook's different proof of the existence of primitive roots modulo p^n.)

8. (A generalization of the previous problem. You should at least read this problem.) Suppose p is a prime, $n \geq 2$ and a is an integer such that a is a primitive root modulo p^2. Show that a is then also a primitive root modulo p^n for all n. [Hint: Show that $a^{p-1} \equiv 1 + p \cdot b \pmod{p^2}$ where $b \not\equiv 0 \pmod{p}$ and look at the hint of the previous problem.]