Math 40520 Theory of Number
Homework 3

Due Wednesday, 2015-09-23, in class

Do 5 of the following 7 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, $a^{m/p} \not\equiv 1 \pmod{n}$.

   Proof. The only if part follows from the minimality of the multiplicative order. Now suppose that m is as in the problem and r is the order of a. From class $r \mid m$ and if $r \neq m$ then there must exist a prime $p \mid m$ such that $r \mid m/p$. Indeed, take p to be any prime dividing m/r. Then $a^{m/p} = (a^r)^{m/(pr)} \equiv 1 \pmod{n}$ getting a contradiction. Thus $m = r$ is the order. □

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.)

   Proof. Let a be a primitive root. Every element of $\mathbb{Z}_{p^n}$ is of the form a^k for some k such that $0 \leq k < \varphi(p^n)$. This element has order $d = \varphi(p^n)/(\varphi(p^n), k)$ which is then a divisor of $\varphi(p^n)$. Fixing d we seek to count k between 0 and $\varphi(p^n)$ such that $d = \varphi(p^n)/(\varphi(p^n), k)$ or, equivalently, $(\varphi(p^n), k) = m = \varphi(p^n)/d$. Then we may write $k = lm$ such that l is coprime to $\varphi(p^n)/m = d$ and so we now seek to count l between 0 and $d = \varphi(p^n)/m$ coprime to d and there are $\varphi(d)$ such l and therefore that many elements of order d. □

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.]

   Proof. Recall that $\mathbb{Z}_{2^n}^\times = \{\pm 3^k\}$ so we seek to count elements of the form 3^k or -3^k of order $d = 2^r$. From class the order of 3^k is $2^{n-2}/(2^{n-2}, k)$ and this equals 2^r if and only if $(2^{n-2}, k) = 2^{n-2-r}$, i.e., iff $2^{n-2-r} \mid k$ and $k/2^{n-2-r}$ is odd. This is the same count as the number of odd $k/2^{n-2-r}$ between 0 and $2^r - 1$, which equals 2^{r-1}. This count is true for all $r \geq 1$, whereas when $d = 1 = 2^0$ then there is exactly one element of order 1, namely 1.

   We now count those -3^k of order 2^r. First, note that if $\mathrm{ord}_{2^n}(3^k) > 2$ then $\mathrm{ord}_{2^n}(-3^k) = \mathrm{ord}_{2^n}(3^k)$. Indeed, let 2^r be this order. Then clearly $(-3^k)^{2^r} = 3^{k \cdot 2^r} \equiv 1 \pmod{2^n}$. Since $2^r > 2$ it follows that

2^{r-1} is even so again $(-3^k)^{2^{r-1}} \equiv (3^k)^{2^{r-1}} \not\equiv 1 \pmod{2^n}$. Thus for order 2^r with $r \geq 2$ again the number of such elements of order 2^r is 2^{r-1}. The total number of elements of order $d = 2^r$ with $r \geq 1$ is thus $2 \cdot 2^{r-1} = 2^r$ as desired.

It remains to treat the case $d = 1$ in which case we already saw there is exactly one element of order 1 and the case $d = 2$. We counted 1 element of order 2 of the form 3^k, namely $3^{2^{n-3}}$. If an element of the form -3^k has order 2 then necessarily 3^k has order 1 or 2 or otherwise 3^k would have the same order as -3^k. Thus 3^k is either 1 (order 1) or $3^{2^{n-3}}$ (order 2). Clearly -1 has order 2 and $-3^{2^{n-3}}$ also has square 1 but is clearly not 1. Thus the 3 elements of order 2 are -1 and $\pm 3^{2^{n-3}}$. □

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 $m \geq 1$.

Proof. The congruence follows from the following problem using $7 = 2^3 - 1$. For the multiplicative order part, we can use the following problem when $m \geq 4$ to deduce that 7 has multiplicative order 2^{m-3}.

For $m = 1$ note that $7 \equiv 1$ so has order 1. For $m = 2, 3$, $7 \equiv -1 \pmod{2^m}$, which has order 2. □

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 $7 = 2^3 - 1$.)

Proof. We do this by induction on n. The case $n = 1$ is the base case. Then $(2^k \pm 1)^2 \equiv 1 \pm 2^{k+1} \pmod{2^{k+2}}$ and now clearly $2^{k+1} \equiv -2^{k+1} \pmod{2^{k+2}}$ so the relation follows.

For the inductive step, write $(2^k \pm 1)^{2^n} = 1 + 2^{k+n} + 2^{k+n+1}a$. Then

$$\begin{aligned}(2^k \pm 1)^{2^{n+1}} &= (1 + 2^{k+n} + 2^{k+n+1}a)^2 \\ &= 1 + 2^{2(k+n)} + 2^{2(k+n+1)}a^2 + 2^{k+n+1} + 2^{k+n+2}a + 2^{2k+2n+1}a \\ &\equiv 1 + 2^{k+n+1} \pmod{2^{k+n+2}}\end{aligned}$$

as $2(k+n) \geq k+n+2$. □

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 $U_n = \mathbb{Z}_n^\times$.)

Proof. From class we need to show that the 2^{n-1} elements $\{\pm 3^k | 0 \leq k < n-2\}$ are distinct in $\mathbb{Z}_{2^n}^\times$. Since this set has 2^{n-1} elements and we exhibited 2^{n-1} distinct elements in the former set it follows that the two sets are equal. Suppose that $3^i = 3^j$ or $-3^i = -3^j$ for $i > j$ in $\{0, 1, \ldots, n-3\}$. Then $3^{i-j} = 1$ where $i - j$ is nonzero but smaller than $n - 3$ which contradicts the fact we proved in class that $\operatorname{ord}_{2^n}(3) = 2^{n-2}$. Now suppose that $3^i = -3^j$ for $i \neq j$. Then $3^{i-j} = -1$ which has order 2. The order of 3^{i-j} is $2^{n-2}/(2^{n-2}, i-j)$ so we'd need that $(2^{n-2}, i-j) = 2^{n-3}$. As $i - j$ can be taken positive but less than 2^{n-2} the only possibility is $i - j = 2^{n-3}$. But $3^{2^{n-3}} \equiv 1 + 2^{n-1} \not\equiv -1 \pmod{2^n}$ so we get a contradiction. □

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.]

   Proof. By induction, as in class, we get that $3^{6\cdot 7^n} \equiv 1 + 7^{n+1}\cdot 6 \pmod{7^{n+2}}$. To check that the order of 3 modulo 7^n is indeed $6\cdot 7^{n-1} = \varphi(7^n)$ we use the first exercise. First, clearly $3^{6\cdot 7^{n-1}} \equiv 1 \pmod{7^n}$. Next we have to check that $3^{6\cdot 7^{n-2}} \not\equiv 1$ which is clear as it is $\equiv 1+7^{n-1}\cdot 6 \pmod{7^n}$. We also have to check that $3^{2\cdot 7^{n-1}}$ and $3^{3\cdot 7^{n-1}}$ are $\not\equiv 1 \pmod{7^n}$. But then these congruences would also yield congruences modulo 7 as well so we'd have $3^{2\cdot 7^{n-1}}$ or $3^{3\cdot 7^{n-1}}$ is $\equiv 1 \pmod 7$. But 3 has order 6 modulo 7 so we'd have $6 \mid 2\cdot 7^{n-1}$ or $6 \mod 3\cdot 7^{n-1}$ which is clearly impossible. □

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.]

   Proof. As $a^{p-1} \equiv 1 \pmod p$ it follows that $a^{p-1} \equiv 1 + p\cdot b \pmod{p^2}$ for some b and since a has order $p(p-1)$ modulo p^2 it follows that $p \nmid b$. By induction we again get that

$$a^{(p-1)p^n} \equiv 1 + p^{n+1}\cdot b \pmod{p^{n+2}}$$

   and so $a^{(p-1)p^{n-2}} \not\equiv 1 \pmod{p^n}$. To show that a has order $p^{n-1}(p-1)$ we use Exercise 1. We need to check that $a^{(p-1)p^{n-2}} \not\equiv 1 \pmod{p^n}$, which we already did, and for each prime $q \mid (p-1)$ that $a^{p^{n-1}(p-1)/q} \not\equiv 1 \pmod{p^n}$. Suppose $a^{p^{n-1}(p-1)/q} \equiv 1 \pmod{p^n}$ for some q. Then reduce modulo p^2. As a is primitive modulo p^2, it has order $p(p-1)$ and so $p(p-1) \mid p^{n-1}(p-1)/q$ which is impossible as p and $p-1$ are coprime and $p-1 \nmid (p-1)/q$. □