HOMEWORK ASSIGNMENT #7 SOLUTIONS

Notice that this assignment is due on Monday instead of Friday, because of the second midterm. You can use a calculator to calculate products mod n.

(1) Consider the group $(\mathbb{Z}/n\mathbb{Z}, +)$.

(a) Show that the order of $a \mod n$ in this group is equal to $n/\gcd(a,n)$.
(b) Let d be a positive integer which divides n. Find the number of elements of $(\mathbb{Z}/n\mathbb{Z}, +)$ with order d.

Solution.

(a) The order of $a \mod n$ is the smallest positive integer d such that $n \mid ad$. Another way of saying this is that ad is the least common multiple of a, n, or that $\operatorname{lcm}(a,n) = ad$. Since $\operatorname{lcm}(a,n) = an/\gcd(a,n)$, this implies that $d = n/\gcd(a,n)$, as desired.
(b) An element $a \mod n$ of $\mathbb{Z}/n\mathbb{Z}$ has order d if and only if $\gcd(a,n) = n/d$. Therefore the answer is equal to the number of integers a, with $1 \leq a \leq n$, satisfying $\gcd(a,n) = n/d$. Any a which satisfies this can be written in the form $a = (n/d)a'$, where $1 \leq a' \leq d$. We also know that $\gcd(a,n) = \gcd((n/d)a', n) = \gcd(a', d) = 1$, and the number of $1 \leq a' \leq d$ with $\gcd(a', d) = 1$ is $\phi(d)$. So there are $\phi(d)$ elements of $\mathbb{Z}/n\mathbb{Z}$ with order d. (For the second to last inequality, we use the fact that if $d \mid a, b$, then $\gcd(a,b)/d = \gcd(a/d, b/d)$.

(2) Suppose m, n are positive integers which are not coprime. Show that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/nm\mathbb{Z}$. (In particular this shows that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is not cyclic.)

Solution. Let $d > 1$ be a common divisor of m, n. First, notice that $\mathbb{Z}/nm\mathbb{Z}$ has an element of order nm. To show that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/nm\mathbb{Z}$ are not isomorphic, we show that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has no elements of order nm. Indeed, given any $(a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, consider $nm/d \cdot (a,b)$. This is equal to $((nm/d)a, (nm/d)b)) = ((m/d)(na), (n/d)(mb)) = ((m/d)0, (n/d)0) = (0,0)$, because $na = 0, mb = 0$ regardless of the values of a, b. Therefore every element in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has order less than or equal to mn/d, and in particular no elements have order nm.

(3) Suppose m, n are positive integers which are coprime. Show that $U_n \times U_m$ is isomorphic to U_{mn}.

Solution. The map which sends an element $(a \mod n, b \mod m)$ to $c \mod mn$, where $c \equiv a \mod n, c \equiv b \mod m$, given by the Chinese Remainder Theorem, is the isomorphism in question. First, notice that this preserves the multiplication operation, because if $c' \equiv a \mod n, c' \equiv b \mod m$, then $cc' \equiv aa' \mod n, cc' \equiv bb' \mod m$. We now check that this map really is a bijection.

First we should check that this map actually sends elements of $U_n \times U_m$ to U_{nm}. Indeed, if $\gcd(a,n) = 1, \gcd(b,m) = 1$, then $\gcd(c,n) = \gcd(a,n) = 1, \gcd(c,m) = \gcd(b,m) = 1$, and because n, m are relatively prime, this implies that $\gcd(c, mn) =$

1. So $c \mod mn$ really is an element of U_{mn}. The map is a bijection because it has inverse $c \mod mn \mapsto (c \mod n, c \mod m)$.

(4) (a) Show that 5 is a primitive root mod 18.
(b) Which powers of $5 \mod 18$ are also primitive roots mod 18?

Solution.

(a) There are a variety of ways to show 5 is primitive mod 18; we will use the condition which asks us to check $5^{\phi(18)/q} \not\equiv 1 \mod 18$ for all prime divisors q of $\phi(18)$. Since $\phi(18) = 6$, we want to calculate $5^{6/2}, 5^{6/3} \mod 18$. These are equal to $17, 7 \mod 18$, respectively, neither of which are $\equiv 1 \mod 18$, so 5 is primitive mod 18.
(b) Because U_{18} has order $\phi(18) = 6$, the primitive elements of U_{18} are those of order 6. Furthermore, U_{18} is cyclic, so by the first problem in this assignment, the elements of order 6 are those powers of 5 whose exponents are relatively prime to 6; ie, $5^1, 5^5 \mod 18$. One checks that $5^5 \equiv 11 \mod 18$.

(5) $p = 229$ is a prime. How many elements of U_{229} are

(a) squares in U_{229}?
(b) cubes in U_{229}?
(c) eighth powers in U_{229}?

Solution. Let g be primitive mod 229.

(a) We want to count the number of g^i such that $g^i = g^{2k}$ for some integer k. In other words, we want to determine the total number of $i \mod 228$ such that $i \equiv 2k \mod 228$. Since $2 \mid 228$, there are exactly $228/2 = 114$ such i, so there are 114 squares in U_{229}.
(b) This time we want to find the number of i satisfying $i \equiv 3k \mod 228$. Since $3 \mid 228$, there are exactly $228/3 = 76$ cubes in U_{229}.
(c) This time we want to find the number of i satisfying $i \equiv 8k \mod 228$. Since $\gcd(8, 228) = 4$, this has a solution exactly when $4 \mid i$; therefore there are $228/4 = 57$ eighth powers in U_{229}.

(6) Show that 112 is a primitive root mod 11, but not a primitive root mod 121. Find a primitive root mod 121.

Solution. $112 \equiv 2 \mod 11$, so we will check that 2 is primitive mod 11. Since $\phi(11) = 10$, we want to check that $2^{10/2}, 2^{10/5} \not\equiv 1 \mod 11$. Indeed, $2^5 \equiv -1 \mod 11, 2^2 \equiv 4 \mod 11$, so 2, and hence 112, is primitive mod 11.

To check that 112 is not primitive mod 121, we check that $112^{10} \equiv 1 \mod 121$, so that 112 has order 10, not $\phi(121) = 110$, in U_{121}. Using whatever favorite method you have to calculate $112^{10} \mod 121$, one checks that $112^{10} \equiv 1 \mod 121$.

By the proof of the fact that U_{p^2} is cyclic, we know that if g is not primitive mod p^2, then $g + p$ is. In our case, $g = 112, p = 11$, so $g + p = 123 \equiv 2 \mod 121$ is cyclic mod 121. So 2 is primitive mod 121. (As a matter of fact, any number g with $g \equiv 2 \mod 11, g \not\equiv 112 \mod 121$, would work.)

(7) (a) True or false: suppose p, q are odd primes. If g is a primitive root mod p and mod q, then g is a primitive root mod pq.
(b) True or false: suppose p is an odd prime, $e \geq 1$. If g is a primitive root mod 2 and mod p^e, then g is a primitive root mod $2p^e$.

Solution.

(a) False. In general U_{pq} is not even cyclic, so there is no possible way for g to be primitive in U_{pq}, regardless of the value of g.
(b) True. First, notice that because $\gcd(g, 2) = \gcd(g, p) = 1$, we also have $\gcd(g, 2p^e) = 1$. We also know that the smallest d such that $g^d \equiv 1 \mod p^e$ is $d = \phi(p^e)$, because g is primitive mod p^e. On the other hand, $\phi(2p^e) = \phi(p^e)$. Therefore if $g^d \equiv 1 \mod 2p^e$, then $g^d \equiv 1 \mod p^e$, so $\phi(p^e) \mid d$. So the smallest positive d such that $g^d \equiv 1 \mod 2p^e$ is $d = \phi(p^e)$, which means that g is primitive mod $2p^e$ as well. (Notice that $g^{\phi(p^e)} \equiv 1 \mod 2p^e$ is true because of Fermat-Euler.)