Homework 24 Solutions

Problems

1. **(a) Compute** 3^{917} (mod 140)**.**

   (b) Compute 4^{1125} (mod 105)**.**

   $\phi(140) = (1/2)(4/5)(6/7)140 = 48$. So $3^{48} = 1$ (mod 140). So $3^{917} = 3^5 = 243 = \boxed{103}$ (mod 140).

   $\phi(105) = (2/3)(4/5)(6/7)105 = 48$. So $4^{48} = 1$ (mod 105). So $4^{1}125 = 4^{21}$ (mod 105) and this can be figured out by doubling to be $\boxed{64}$ (mod 105).

2. **The method we have used for computing roots** (mod n) **can be applied to only part (c) of the following three problems. Explain why it fails for the first two problems, and solve the third.**

   (a) The 4th root of 4 (mod 77)**;**

   (b) The 7th root of 7 (mod 77)**;**

   (c) The 13th root of 13 (mod 77)**.**

   4 and $\phi(77) = 60$ are not relatively prime so we can't take 4th roots.

   7 and 77 are not relatively prime so we can't find roots of 7.

   $1/13 = 37$ (mod 60). So $13^{1/13} = 13^{37}$ (mod 77) and this can be figured out by doubling to be $\boxed{62}$ (mod 77).

3. **(a) Compute the 11th root of** 2 (mod 105)**.**

   (b) Compute the 5th root of 4 (mod 43)**.**

   First observe that $105 = 3 \times 5 \times 7$ so that $\phi(105) = 48$. This is a problem modulo 105, so this means that we work modulo 48 in the exponent. We wish to compute $2^{1/11}$ (mod 105). First we figure out (using Euclid's algorithm backwards) that $1/11 = 35$ (mod 48). So the answer will be 2^{35} (mod 105), which we can compute using doubling to be $\boxed{53}$ (mod 105).

   For the next part, observe that 43 is prime so $\phi(43) = 42$. This is a problem modulo 43, so we work modulo 42 in the exponent. We wish to compute $4^{1/5}$ (mod 43). We figure out that $1/5 = 17$ (mod 42). So the answer will be 4^{17} (mod 43), which we can compute using doubling to be $\boxed{21}$ (mod 43).