Homework 9 Solutions

Tim Smits

1.

(a) Compute $\text{ord}_{100}(7)$.

(b) Reduce 7^{111} mod 100.

Solution:

(a) $7^4 = 2401 \equiv 1 \bmod 100$, so $\text{ord}_{100}(7) = 4$.

(b) $111 = 27 \cdot 4 + 3$, so $7^{111} \equiv 7^3 \bmod 100 \equiv 43 \bmod 100$.

2. Prove that $a^4 \equiv 1 \bmod 15$ when $(a, 15) = 1$.

Solution: Firstly, the condition $(a, 15) = 1$ is equivalent to saying that $(a, 3) = 1$ and $(a, 5) = 1$. By Fermat's little theorem, $a^2 \equiv 1 \bmod 3$ and $a^4 \equiv 1 \bmod 5$ for all a with $(a, 3) = 1$ and $(a, 5) = 1$. Squaring the first equation also says $a^4 \equiv 1 \bmod 3$. This says $3 \mid a^4 - 1$ and $5 \mid a^4 - 1$ so that $15 \mid a^4 - 1$ says $a^4 \equiv 1 \bmod 15$ for all a such that $(a, 15) = 1$.

3. Find d such that $a^d \equiv 1 \bmod 2000$ with $1 < d < 800$ for all a such that $(a, 2000) = 1$.

Solution: Write $2000 = 16 \cdot 125$. The condition $(a, 2000) = 1$ is equivalent to saying that $(a, 16) = 1$ and $(a, 125) = 1$. By Euler's theorem, $a^8 \equiv 1 \bmod 16$ and $a^{100} \equiv 1 \bmod 125$. Notice that $\text{lcm}(8, 100) = 200$, so that $a^{200} \equiv 1 \bmod 16$ and $a^{200} \equiv 1 \bmod 125$. The Chinese remainder theorem then says $a^{200} \equiv 1 \bmod 2000$.

4.

(a) Check that $a^2 \equiv 1 \bmod 8$ for all $a \in (\mathbb{Z}/8\mathbb{Z})^\times$.

(b) Prove that for any $e \in \mathbb{N}$ and $a \in \mathbb{Z}$, if $a \equiv 1 \bmod 2^e$ then $a^2 \equiv 1 \bmod 2^{e+1}$.

(c) Prove for $e \geq 3$ that $a^{2^{e-2}} \equiv 1 \bmod 2^e$.

Solution:

(a) This is clear.

(b) If $a \equiv 1 \bmod 2^e$, write $a = 1 + 2^e k$ for some $k \in \mathbb{Z}$. Squaring says $a^2 = 1 + 2^{e+1}k + 4^e k^2$, so taking this mod 2^{e+1} says $a^2 \equiv 1 \bmod 2^{e+1}$.

(c) The base case $e = 3$ is part a). Suppose that $a^{2^{e-2}} \equiv 1 \bmod 2^e$. Then write $a^{2^{e-2}} = 1 + 2^e k$ for some $k \in \mathbb{Z}$. Squaring says $a^{2^{e-1}} = 1 + 2^{e+1}k + 4^e k^2$, so taking this mod 2^{e+1} says $a^{2^{e-1}} \equiv 1 \bmod 2^{e+1}$. By induction, this proves the result for all $e \geq 3$.

5. Find $d' < d$ from problem 3 such that $a^{d'} \equiv 1 \bmod 2000$.

Solution: By problem 4, $a^4 \equiv 1 \bmod 16$. Since $100 = 16 \cdot 8 + 4$, this says $a^{100} \equiv 1 \bmod 16$. The Chinese remainder theorem then says that $a^{100} \equiv 1 \bmod 2000$, whenever $(a, 2000) = 1$.

6.

(a) Prove that $\lambda(n) \leq \varphi(n)$ for all $n \in \mathbb{N}$.

(b) Prove that for all $n \in \mathbb{N}$, that $a^{\lambda(n)} \equiv 1 \bmod n$ whenever $(a, n) = 1$.

Solution:

(a) Write $n = p_1^{e_1} \dots p_k^{e_k}$ as a product of prime powers. By definition, $\lambda(p_i^{e_i}) \leq \varphi(p_i^{e_i})$ for all i, so that $\lambda(n) = \operatorname{lcm}(\lambda(p_1^{e_1}), \dots, \lambda(p_k^{e_k})) \leq \lambda(p_1^{e_1}) \dots \lambda(p_k^{e_k}) \leq \varphi(p_1^{e_1}) \dots \varphi(p_k^{e_k}) = \varphi(n)$.

(b) Write $n = p_1^{e_1} \dots p_k^{e_k}$ as a product of prime powers. Then $(a, n) = 1$ is the same as saying $(a, p_i^{e_i}) = 1$ for all i. First, we show that $a^{\lambda(p^e)} \equiv 1 \bmod p^e$ for all prime powers. If $p = 2$, then $a^{2^{e-2}} \equiv 1 \bmod 2^e$ by problem 4, and by definition, $\lambda(2^e) = 2^{e-2}$, so that $a^{\lambda(p^e)} \equiv 1 \bmod p^e$. If p is odd, $\lambda(p^e) = \varphi(p^e)$ so by Euler's theorem, $a^{\lambda(p^e)} \equiv 1 \bmod p^e$. This proves $a^{\lambda(p^e)} \equiv 1 \bmod p^e$ for all prime powers p^e.

Therefore, $a^{\lambda(p_i^{e_i})} \equiv 1 \bmod p_i^{e_i}$ for all i. Since $\lambda(p_i^{e_i}) \mid \operatorname{lcm}(\lambda(p_1^{e_1}), \dots, \lambda(p_k^{e_k})) = \lambda(n)$ for all i, this says $a^{\lambda(n)} \equiv 1 \bmod p_i^{e_i}$ for all i. By the Chinese remainder theorem, we then find $a^{\lambda(n)} \equiv 1 \bmod n$ as desired.

7. Find all n such that $\lambda(n) = \varphi(n)$.

Solution: Write $n = p_1^{e_1} \dots p_k^{e_k}$, so that $\lambda(n) = \operatorname{lcm}(\lambda(p_1^{e_1}), \dots, \lambda(p_k^{e_k}))$ and $\varphi(n) = \varphi(p_i^{e_1}) \dots \varphi(p_k^{e_k})$. Recall that $\operatorname{lcm}(a_1, \dots, a_n) = a_1 \dots a_n$ if and only if all a_i are relatively prime. If $\lambda(p_i^{e_i})$ are not all relatively prime, then clearly $\operatorname{lcm}(\lambda(p_1^{e_1}), \dots, \lambda(p_k^{e_k})) < \lambda(p_1^{e_1}) \dots \lambda(p_k^{e_k})$, which will say that $\lambda(n) < \varphi(n)$. Therefore, we require that all $\lambda(p_i^{e_i})$ are relatively prime. If p is odd, then $\lambda(p^e) = \varphi(p^e)$ is even. So there can be at most one odd prime in the factorization of n. If $p = 2$, then $\lambda(2^e)$ is even unless $e = 0, 1$. Therefore any n of the form $n = p^k$ or $n = 2p^k$ for p odd will work. Since $\lambda(4) = \varphi(4) = 2$, and $\lambda(2) = \varphi(2) = 1$ and $\lambda(1) = \varphi(1) = 1$, we also see that $n = 1, 2, 4$ will work. Since $\lambda(2^e) < \varphi(2^e)$ for $e \geq 3$, these are the only possible cases where n is a power of 2 that will work.

We then see that the only possibles choices for n are $n = 1, 2, 4, p^k, 2p^k$ for p odd, and it's clear that all such choices work by definition of $\lambda(n)$.

8.

(a) Prove that if $f(x) \equiv g(x) \bmod n$, that $f'(x) \equiv g'(x) \bmod n$.

(b) Prove that $[f(x)+g(x)]' = [f(x)]'+[g(x)]'$, $[cf(x)]' = [c][f(x)]'$ and $[f(x)g(x)]' = [f(x)]'[g(x)]+[f(x)][g(x)]'$.

Solution:

(a) Write $f(x) = a_m x^m + \ldots + a_0$ and $g(x) = b_m x^m + \ldots + b_0$ for $a_i, b_i \in \mathbb{Z}$ where the coefficients are allowed to be 0. If $f(x) \equiv g(x) \bmod n$, this says $n \mid f(x) - g(x) = (a_m - b_m)x^m + \ldots + (a_0 - b_0)$, so that $a_i \equiv b_i \bmod n$ for all $0 \leq i \leq m$. Since $f'(x) = ma_m x^{m-1} + \ldots + a_1$ and $g'(x) = mb_m x^{m-1} + \ldots + b_1$, we then immediately see that $n \mid i(a_i - b_i)$ for $1 \leq i \leq m$, so that $f'(x) \equiv g'(x) \bmod n$.

(b) Pick representatives $f(x), g(x) \in \mathbb{Z}[x]$ for the classes $[f(x)]$ and $[g(x)] \in (\mathbb{Z}/n\mathbb{Z})[x]$. By the usual properties of the derivative, we have $(f(x)+g(x))' = f'(x)+g'(x)$, $(cf(x))' = cf'(x)$ and $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$. As $[f(x)]' = [f'(x)]$ by part a), reducing mod n then immediately says $[f(x) + g(x)]' = [f(x)]' + [g(x)]'$, $[cf(x)]' = [c][f(x)]'$ and $[f(x)g(x)]' = [f(x)]'[g(x)] + [f(x)][g(x)]'$.

9. Prove that a is a repeated root of $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ if and only if $f(a) = f'(a) = 0$.

Solution: Suppose that a is a repeated root of $f(x)$, so that $f(x) = (x - a)^2 g(x)$ for some $g(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$. Then $f'(x) = 2(x - a)g(x) + (x - a)^2 g'(x)$, which says $f'(a) = 0$. On the other hand, suppose that $f(a) = f'(a) = 0$. By the factor theorem, write $f(x) = (x - a)h(x)$ for some $h(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$. Then $f'(x) = h(x) + (x - a)h'(x)$ says $f'(a) = h(a) = 0$. We may then write $h(x) = (x - a)g(x)$ for some $g(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$, so that $f(x) = (x - a)^2 g(x)$ says a is a repeated root of $f(x)$.

10. Find a non-constant polynomial $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ such that $f'(x) = 0$.

Solution: Take $f(x) = x^n$, so that $f'(x) = nx^{n-1} \equiv 0 \bmod n$.