PMATH 340 Number Theory, Solutions to Assignment 2.5

1: (a) Find $10^{50} \bmod 91$.

Solution: Note that $91 = 7 \cdot 13$. The list of powers of 10 modulo 91 repeats every $\lambda(91)$ $\big($or every $\psi(91)$ or every $\varphi(91)\big)$ terms beginning with 10^1. We have $\lambda(91) = \psi(91) = \text{lcm}(6, 12) = 12$, so the list repeats every 12 terms. Since $50 = 2 \bmod 12$, we have $10^{50} = 10^2 = 100 = 9 \bmod 91$.

(b) Find $28^{27^{26}} \bmod 25$.

Solution: Since $28 = 3 \bmod 25$ we have $28^{27^{26}} = 3^{27^{26}} \bmod 25$. Since $\lambda(25) = \lambda(5^2) = 20$, the list of powers of 3 modulo 25 repeats every 20 terms (beginning with 3^0), so we wish to find $27^{26} \bmod 20$. Since $27 = 7 \bmod 20$ we have $27^{26} = 7^{26} \bmod 20$. Since $\lambda(20) = \lambda(2^2 \cdot 5)) = \text{lcm}(2, 4) = 4$, the list of powers of 7 modulo 20 repeats every 4 terms (beginning with 7^0). Since $26 = 2 \bmod 4$ we have $7^{26} = 7^2 = 49 = 9 \bmod 20$. Thus, using the fact that $3^3 = 27 = 2 \bmod 25$, we have

$$28^{27^{26}} = 3^{27^{26}} = 3^{7^{26}} = 3^{7^2} = 3^9 = (3^3)^3 = 2^3 = 8 \bmod 25.$$

(c) Find a positive integer k such that the number 3^k ends with the digits 0001.

Solution: By the Euler-Fermat Theorem, we have $3^{\varphi(10000)} \equiv 1 \pmod{10000}$, that is $3^{\varphi(10000)} = 1 + 10000\ell$ for some integer ℓ. Thus $3^{\varphi(10000)}$ ends with the digits 0001, so we can take

$$k = \varphi(10000) = \varphi(2^4)\varphi(5^4) = 2^3(2-1) \cdot 5^3(5-1) = 8 \cdot 500 = 4000\,.$$

Alternatively, by the generalized Euler-Fermat Theorem we can take $k = \psi(10000) = \text{lcm}(8, 500) = 1000$. Better still, by the Structure Theorem for U_n, we can take $k = \lambda(10000) = \text{lcm}(4, 500) = 500$.

(d) With the help of the following table of powers of 5 mod 64, solve $11\,x^5 = 17 \bmod 64$.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
5^k	1	5	25	61	49	53	9	45	33	37	57	29	17	21	41	13	1
-5^k	63	59	39	3	15	11	55	19	31	27	7	35	47	43	23	51	63

Solution: If x is even then $11x^5$ is even so $11x^5 \neq 17 \bmod 64$. Suppose that x is odd so $x \in U_{64}$. Then we have $x = \pm 5^k$ for some $k \in \mathbb{Z}_{16}$. If $x = 5^k$ then $11x^5 = 17 \bmod 64 \iff (-5^5)(5^5k) = 5^{12} \bmod 64 \iff -5^{5k+5} = 5^{12} \bmod 64$, and this has no solution (since $-5^s \neq 5^t$ for any s, t). If $x = -5^k$ then we have $11x^5 = 17 \bmod 64 \iff (-5^5)(-5^5k) = 5^{12} \bmod 64 \iff 5^{5+5k} = 5^{12} \bmod 64 \iff 5 + 5k = 12 \bmod 16 \iff 5k = 7 \bmod 16 \iff k = 11 \bmod 16 \iff x = -5^{11} = 35 \bmod 64$.

2: (a) Find a positive integer ℓ and find primes $p_1, p_2, \cdots, p_\ell$ and positive integers $k_1, k_2, \cdots, k_\ell$ such that $U_{675} \cong \mathbb{Z}_{{p_1}^{k_1}} \times \mathbb{Z}_{{p_2}^{k_2}} \times \cdots \times \mathbb{Z}_{{p_\ell}^{k_\ell}}$.

Solution: Since $675 = 3^3 \cdot 5^2$ and $\varphi(3^3) = 3^3 - 3^2 = 18$ and $\varphi(5^2) = 5^2 - 5^2 = 20$, we have

$$U_{675} \cong U_{3^3} \times U_{5^3} \cong \mathbb{Z}_{18} \times \mathbb{Z}_{20} \cong \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_5$$

so we can take $\ell = 4$ and ${p_1}^{k_1} = 2^1$, ${p_2}^{k_2} = 2^2$, ${p_3}^{k_3} = 3^2$ and ${p_4}^{k_4} = 5^1$.

(b) Find the number squares, the number of cubes, and the number of fourth powers in U_{125}.

Solution: Recall that for an element a with $\text{ord}(a) = n$ in a finite group G, we have $\langle a^k \rangle = \langle a^d \rangle$ where $d = \gcd(k, n)$ and $\text{ord}(a^k) = n/d$. We know that U_{125} is cyclic. Let $a \in U_{125}$ be a generator, so we have $\text{ord}(a) = |U_{125}| = \varphi(125) = 100$. The set of squares in U_{125} is the set $\langle a^2 \rangle = \{1, a^2, a^4, \cdots\}$ so the number of squares in U_{125} is equal to $\text{ord}(a^2) = \frac{100}{\gcd(2,100)} = \frac{100}{2} = 50$. The set of cubes in U_{125} is the set $\langle a^3 \rangle = \{1, a^3, a^6, a^9, \cdots\}$ so the number of cubes is equal to $\text{ord}(a^3) = \frac{100}{\gcd(3,100)} = \frac{100}{1} = 100$. The set of fourth powers is $\langle a^4 \rangle$ and the number of fourth powers is $\frac{100}{\gcd(4,100)} = \frac{100}{4} = 25$. More generally, if $n = p^k$ where p is an odd prime, then the number of m^{th} powers in U_n is equal to $\frac{\varphi(n)}{\gcd(m,\varphi(n))}$.

(c) For $n = 18900$, find the universal exponent $\lambda(n)$ and find the number of elements in U_n of order $\lambda(n)$.

Solution: Note that $18900 = 4 \cdot 27 \cdot 25 \cdot 7$ so we have

$$U_n \cong U_4 \times U_{27} \times U_{25} \times U_7 \cong \mathbb{Z}_2 \times \mathbb{Z}_{18} \times \mathbb{Z}_{20} \times \mathbb{Z}_6$$
$$\lambda(n) = \text{lcm}\big(\lambda(4), \lambda(27), \lambda(20), \lambda(7)\big) = \text{lcm}(2, 18, 20, 6) = 180\,.$$

The number of elements in U_n of order 180 is equal to the number of elements in $\mathbb{Z}_2 \times \mathbb{Z}_{18} \times \mathbb{Z}_{20} \times \mathbb{Z}_6$ of order 180. For $a = (a_1, a_2, a_3, a_4) \in \mathbb{Z}_2 \times \mathbb{Z}_{18} \times \mathbb{Z}_{20} \times \mathbb{Z}_6$ we have $\text{ord}(a_1)\big|2$, $\text{ord}(a_2)\big|18$, $\text{ord}(a_3)\big|20$, $\text{ord}(a_4)\big|6$ and $\text{ord}(a) = \text{lcm}\big(\text{ord}(a_1), \cdots, \text{ord}(a_n)\big)$. To have $\text{ord}(a) = 180 = 4 \cdot 9 \cdot 5$, note that $\text{ord}(a_2)$ must be a multiple of 9 (since none of the orders of a_1, a_3, a_4 is a multiple of 9) and $\text{ord}(a_3)$ must be both a multiple of 4 and a multiple of 5 (since none of the orders of a_1, a_2, a_4 are multiples of 4 or 5). Thus $\text{ord}(a) = 180$ when $\text{ord}(a_2) \in \{9, 18\}$ and $\text{ord}(a_3) = 20$ (the elements a_1, a_4 are arbitrary). There are $\varphi(9) + \varphi(18) = 12$ choices for a_2, $\varphi(20) = 8$ choices for a_3, 2 choices for a_1 and 6 choices for a_4 giving a total of $12 \cdot 8 \cdot 2 \cdot 6 = 1152$ elements of order 180.