Number Theory Solution Set

Andy Jung and Gregory Pylypovych

September 28, 2019

1 Solutions

Easy Problem Solutions

1. You can write out the powers of 3 mod 7.
$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1 \pmod 7$. Therefore, the order is 6.

2. We note that $1025 = 2^{10} + 1 \rightarrow 2^{10} \equiv -1$ mod 1025. 2 to a power less than 10 is lower than 1025. If the order is (10+k) for some k, $2^{10} * 2^k \equiv 1$ mod $1025 \rightarrow 2^k \equiv -1$ mod 1025. Therefore, k =10 and the order is 20.

3. $a^2 \equiv -1 \bmod (a^2+1) \rightarrow a^4 \equiv 1 \bmod (a^2+1)$. By looking at the size of the powers of a, we can see that 1 or 2 are not the orders. Therefore, the order is 4.

4. $a^{c+k} \equiv a^c * a^k \equiv a^c * 1 \equiv a^c \bmod b$.

Medium Problem Solutions

1. $a^n \equiv 1 \pmod{a^n - 1}$, $a^{\phi(a^n-1)} \equiv 1 \pmod{a^n-1}$. For all $k < n$, $(a^k - 1) < (a^n - 1) \rightarrow (a^k - 1) \neq 0 \bmod (a^n - 1)$. Therefore, $ord_{a^n-1}(a) = n$ and because n is the order, $n \mid \phi(a^n - 1)$

2. $10^j - 10^i = 10^i(10^{j-i} - 1) \rightarrow 1001 \mid (10^j - 10^i) \rightarrow 1001 \mid (10^{j-i} - 1) \rightarrow 10^{j-i} \equiv 1 \pmod{1001}$. $ord_{1001}(10) = 6 \rightarrow 6 \mid (j - i)$. From this and the conditions on i and j, we can see that there are 784 possibilities.

Hard Problem Solutions

1. $p \mid 5^p - 2^p$ or $p \mid 5^q - 2^q$. Case 1: $5^p - 2^p \equiv 5*1 - 2*1 = 3 mod p$. Therefore, if p divides this term, $p = 3$ and the term becomes $117(5^q - 2^q) \rightarrow q \mid 117 \rightarrow q = 3, 13$ or $q \mid 5^q - 2^q \rightarrow q = 3$ by the same logic as for p. Using symmetry, we have the set of solutions $(p, q) = (3, 3), (3, 13), (13, 3)$.
Case 2: $p \mid 5^q - 2^q \rightarrow 5^q - 2^q \equiv 0$ (mod p). $\rightarrow 2^q((5 * 2^{-1})^q - 1) \equiv 0$ mod p $\rightarrow (5 * 2^{-1})^q - 1 \equiv 0 \bmod p$. Similarly, $(5 * 2^{-1})^p - 1 \equiv 0 \bmod q$.
Let $a = (5 * 2^{-1})$. Therefore, $ord_p(a) \mid q, ord_q(a) \mid p$ and we also know that $ord_p(a) \mid (q - 1), ord_q(a) \mid (p - 1)$. To satisfy both these conditions

$ord_p(a) = 1 \to a \equiv 1 \pmod{\text{p}} \to 5 * 2^{-1} \equiv 1 \pmod{\text{p}} \to 5 \equiv 2 \pmod{\text{p}}$, forcing p=3 as in case 1.
Therefore, the only possible solutions are $(p, q) = (3, 3), (3, 13), (13, 3)$.