18.310A Problem Set 4

Rishad Rahman

1. We can do this easily using a chart.

a	b	b'
107	73	$34 = 107 - 73$
73	34	$5 = 73 - 2(34) = 3(73) - 2(107)$
34	5	$4 = 34 - 6(5) = 13(107) - 19(73)$
5	4	$1 = 5 - 4 = 22(73) - 15(107)$

   so $k = -15$ and $l = 22$.

2. We have $w = 73m + 29 \equiv 18 \bmod 107 \Rightarrow m \equiv -11 \cdot 73^{-1} \equiv -11 \cdot 22 \equiv -242 \equiv 79 \bmod 107$. So $w \equiv 73(79) + 29 \equiv 5796 \bmod (73 \cdot 107)$.

3. $p^{q-1} + q^{p-1} \equiv q^{p-1} \equiv 1 \bmod p$ and similarly $p^{q-1} + q^{p-1} \equiv 1 \bmod q$ by FLT and so the result follows by CRT.

4. Obviously 1 satisfies $x^3 \equiv 1 \bmod p$. Also notice $m^{3a} \equiv 1 \bmod p$ by FLT so m^a also satisfies it for any m not divisible by p. Suppose $m^a \neq 1 \bmod p$. Then $m^{2a} \neq 1 \bmod p$ but $m^{6a} \equiv 1 \bmod p$ so 1, $m^a \bmod p$, and $m^{2a} \bmod p$ are three distinct solutions since $m^a \neq 1 \bmod p$. Why does such m^a exist? Well by the Fundamental Theorem of Algebra there can't be more than a values of m such that $m^a \equiv 1 \bmod p$ so there must exist an m^a which this doesn't hold and the aforementioned follows. We showed there are are at least three solutions but again the FTA forces it to be equal to 3.

5. Note the cube roots of 1 mod a prime p can be written as 1, x, x^2. This also implies that the cube roots of n^3 can be written as n, nx, nx^2. Note a residues must exist in order for n, nx, nx^2 to span all $3a = p - 1$ residues of $p - 1$. If it wasn't spanned then we can cube the non-spanned value to get a new cubic residue. Therefore we have $a + 1$ possible cubic residues where the extra 1 comes from the 0 case. Similarly there are $b + 1$ possible cubic residues for q. By CRT $n^3 \bmod pq \Leftrightarrow (n^3 \bmod p, n^3 \bmod q)$. We just got to show the reverse direction to complete the bijection which would then show there are $\boxed{(a+1)(b+1)}$ cubic resudues modulo pq. We know by CRT (j, k) modulo $(p, q) \Leftrightarrow l$ modulo pq. Suppose $x \equiv l \bmod pq$, then $x^3 \equiv l^3 \bmod pq \Rightarrow x^3 \equiv l^3 \equiv j^3 \bmod p$ and $x^3 \equiv l^3 \equiv k^3 \bmod q$ so we have (j^3, k^3) modulo $(p, q) \Leftrightarrow l^3$ modulo pq which completes the bijection.