MAT 4233 Final Sp. 2015

1. Suppose k is a common divisor of a and b.
Then $\exists\ a', b'$ $\quad a = a'k$, $b = b'k$. Bézout $\Rightarrow$
$\exists\ s, t$ $\quad \gcd(a,b) = sa + tb = sa'k + tb'k = (sa' + tb')k$ ☺

2. S_3

$\langle (1,2,3) \rangle$ $\quad$ $\langle (1,2) \rangle$ $\quad$ $\langle (1,3) \rangle$ $\quad$ $\langle (2,3) \rangle$

$\langle () \rangle$

$\langle (1,2) \rangle = \{(), (1,2)\}$ etc.
$\langle (1,2,3) \rangle = \{(), (1,2,3), (1,3,2)\}$

3. Let $\ell = \operatorname{lcm}(m,n)$. If $x \in \langle \ell \rangle$, $\ell \mid x$, but $m \mid \ell$, so $m \mid x$, so $x \in \langle m \rangle$. Similarly $x \in \langle n \rangle$.

Conversely, suppose $x \in \langle m \rangle \cap \langle n \rangle$. Then $m \mid x$ & $n \mid x$.
By division algorithm $\exists\ q, r$ $\quad x = q\ell + r$, $\quad 0 \le r < \ell$
Then $r = x - q\ell$ is a common multiple of m & n.
Since $r < \ell$, $r = 0$. $\therefore \ell \mid x$, so $x \in \langle \ell \rangle$ ☺

4. $\tau = (1,2,4)(3,5)$. Since $2015 \equiv -1 \bmod 3$ and $2015 \equiv 1 \bmod 2$, and disjoint cycles commute,

$$\tau^{2015} = (1,2,4)^{2015}(3,5)^{2015} = (1,2,4)^{-1}(3,5) = (1,4,2)(3,5).$$

5. If $\phi \in \operatorname{Aut}(\mathbb{Z}_m)$, it is onto, so $\exists k$ $\phi(k) = k\phi(1) = 1$
Thus $\phi(1)$ is a unit, so define $\theta : \operatorname{Aut}(\mathbb{Z}_m) \to U(m)$ by $\theta(\phi) = \phi(1)$. Hom?

$$\theta(\phi \circ \psi) = (\phi \circ \psi)(1) = \phi(\psi(1)) = \psi(1)\phi(1) = \theta(\psi)\theta(\phi) = \theta(\phi)\theta(\psi)$$ ☺

If $\phi \in \ker\theta$, $\theta(\phi) = \phi(1) = 1$, so $\forall k \quad \phi(k) = k\phi(1) = k$,
so $\phi = Id$. $\therefore \theta$ is injective.

Given $k \in U(m)$, define $\phi : \mathbb{Z}_m \to \mathbb{Z}_m$ by $\phi(x) = kx$.

Is $\phi \in Aut(\mathbb{Z}_m)$?

$\phi(x+y) = k(x+y) = kx + ky = \phi(x) + \phi(y)$, so ϕ is a hom.

Since k is a unit, the equation $kx = 0$ has the unique sol. $x = 0$,
so ϕ is injective, so as a self map on a finite set, bijective. ☺

$\theta(\phi) = \phi(1) = k$, so θ is surjective. ☺

6. Given $\phi \in Aut(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$, then ϕ is a bijection.

Since $\phi([0,0]) = [0,0]$, the restriction of ϕ to
$X = (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \setminus \{[0,0]\} = \{[1,0],[0,1],[1,1]\}$ is a permutation
on 3 elements. That's our $\theta(\phi) \in S_3$ for a map
$\theta : Aut(\mathbb{Z}_2 \oplus \mathbb{Z}_2) \to S_3$. Since both automorphisms
and permutations are composed, θ is an injective hom.

Since every element of X is the sum of the other two,
and is its own additive inverse, every permutation on X
defines an automorphism of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$,
so θ is surjective. ☺

7. Take powers of 11 mod 45:

$\langle 11\rangle = \{11, 31, 26, 16, 41, 1\}$

Note: $|11| = 6$, $|U(45)| = \phi(5\cdot 3^2) = 4\cdot 6 = 24$

$\therefore$ By Lagrange's theorem the index is $\frac{24}{6} = 4$

Cosets: $\langle 11\rangle$, $2\langle 11\rangle = \{22, 17, 7, 32, 37, 2\}$,

$4\langle 11\rangle = \{44, 34, 14, 19, 29, 4\}$,

$8\langle 11\rangle = \{43, 23, 28, 38, 13, 8\}$.

Powers of 2: 4, 8, 16 $\therefore |2\langle 11\rangle| = 4$, so $\frac{U(45)}{\langle 11\rangle}$ is cyclic.

8. $\phi(xy) = (xy)^n = x^n y^n = \phi(x)\phi(y)$, so ϕ is a hom.
(since G is commutative.)

Since n is coprime to m, Bézout $\Rightarrow \exists\, s,t \quad 1 = sn + tm$

If $x^n = e$, $x = x^{sn+tm} = (x^n)^s (x^m)^t = e^s e^t = e$.

Alt: Lagrange $\Rightarrow |x| \mid m$. If $x^n = e$, $|x| \mid n$,
so $|x| \mid \gcd(m,n) = 1$, so $x = e$.

$\therefore \phi$ is injective, so as a self-map on a finite set, bijective. ☺

9. $\phi(1) = \phi(5\cdot 20) = 20\cdot\phi(5) = 20\cdot[2,9] = [40, 180] = [1,4]$

Check: $\phi(5) = 5\,\phi(1) = 5[1,4] = [5,20] = [2,9]$ ☺

Since 4 is coprime to 11, $|4| = 11$, so $|[1,4]| = \mathrm{lcm}(3,11) = 33$.

$\therefore [1,4]$ generates $\mathbb{Z}_3 \oplus \mathbb{Z}_{11}$, so ϕ is an isomorphism.

10.

σ	τ	$\phi(\sigma)$	$\phi(\tau)$	$\phi(\sigma)+\phi(\tau)$	$\sigma\cdot\tau$	$\phi(\sigma\cdot\tau)$
even	even	0	0	0	even	0
even	odd	0	1	1	odd	1
odd	even	1	0	1	odd	1
odd	odd	1	1	0	even	0

$\therefore \phi$ is a hom.

If $G = S_n$, $\ker\phi = A_n$, so $A_n \trianglelefteq S_n$. ☺