Note Title 4/2010

1. Suppose $a \in \mathbf{Z}_n$. Prove $a \in U(n)$ if and only if a is relatively prime to n. What is $|U(n)|$ if n is prime? Explain. What is the multiplicative inverse of 5 in $\mathbf{Z}_{18}$?

If $a \in U(n)$, there exists s with $as \equiv 1 \bmod n$, so $as - 1 = nq$ for some q, so $1 = as - nq$, so if d divides both a and n, then d divides 1, so $d = 1$ ☺

Conversely if a and n are relatively prime, $1 = as + nt$ for some s and t, so $1 \equiv as \bmod n$ ☺

If n is prime, all nonzero elements of $\mathbb{Z}_n$ are relatively prime to n

so $|U(n)| = n - 1$

In $\mathbb{Z}_{18}$ $5^2 = 25 = 7$, $5^3 = 35 = -1$, so $5^6 = 1 = 5 \cdot 5^5 = 5 \cdot (-25) = 5 \cdot 11$

2. Prove or disprove $U(8) \cong U(12)$.

$U(8) = \{1, 3, 5, 7\}$

In $\mathbb{Z}_8$: $3^2 = 9 = 1$, $5^2 = 25 = 1$, $7^2 = 49 = 1$

so $U(8)$ has no elements of order 4, so $U(8)$ is not cyclic

Since $3 \cdot 5 = 15 = 7$, $U(8) = \langle 3, 5 \rangle$

$U(12) = \{1, 5, 7, 11\}$

In $\mathbb{Z}_{12}$: $5^2 = 25 = 1$, $7^2 = 49 = 1$, $11^2 = 121 = 1$

so $U(12)$ is not cyclic either.

Since $5 \cdot 7 = 35 = 11$, $U(12) = \langle 5, 7 \rangle$

Define $f: U(8) \to U(12)$ by

x	$f(x)$
1	1
3	5
5	7
7	11

By inspection f is an automorphism ☺

3. Let $H = \{(), (12)(34), (13)(24), (14)(23)\}$. Prove that H is a subgroup of A_4 (you may use the word *similarly* as appropriate). List all the cosets of H in A_4. Is H isomorphic to $\mathbf{Z}_4$? Explain.

Each permutation in H is even, so $H \subset A_4$

$() \in H$ ✓ · If $\sigma \in H$, $\sigma^2 = ()$ (so $\sigma^{-1} = \sigma$)

$(12)(34) \cdot (13)(24) = (14)(23) \in H$ and other products work out similarly, so H is closed $\therefore H < A_4$

Lagrange: $|A_4| = |H|\,[A_4 : H]$, $12 = 4\,[A_4 : H]$ So there are 3 cosets: H and

$(123)H = \{(123), (134), (243), (142)\}$

$(132)H = \{(132), (234), (124), (143)\}$

H has no elements of order 4, so $H \ncong \mathbb{Z}_4$

4. Suppose G is a group with $|G| = 11$. Prove or disprove that G must be cyclic.

Suppose $a \in G$, $a \neq e$. By Lagrange's theorem $|\langle a \rangle|$ divides 11, so $|\langle a \rangle| = 11$, so $\langle a \rangle = G$ ☺

5. Suppose G is a group with $|G|$ a positive integer power of a prime p. Prove that G has an element of order p.

Suppose $|G| = p^n$, $n > 0$ and let $a \in G$, $a \neq e$

By Lagrange's theorem $|\langle a \rangle|$ divides p^n, so $|a| = p^k$, $k > 0$

Then $e = a^{p^k} = \left(a^{p^{k-1}}\right)^p$ so $a^{p^{k-1}}$ has order p ☺

$\uparrow \neq e$