

Computational Number Theory

HW 3

Due Date: 01/11/2022

1. The following is a partially-filled Cayley table of a group G whose elements are $\{a, b, c, d\}$. Fill the rest of the table. Which 4-element group is it isomorphic to?

*	a	b	c	d
a	b			
b		b		
c				a
d				

2. Let $(G, *)$ be a group with identity element e and $d \in \mathbb{N}$. Show that the set $S = \{x \in G : x^d = e\}$ forms a subgroup of G .
3. Let π_1 be the permutation of $1, 2, \dots, n$ that swaps 1 and 2 and fixes every other element; let π_2 be the permutation of $1, 2, \dots, n$ that sends i to $i+1$ (with $\pi_2(n) = 1$). Show that the group generated by $\{\pi_1, \pi_2\}$ is equal to S_n .
4. Let M be a two by two non-singular matrix with entries from \mathbb{Z}_p , where p is prime.
 - (a) Show that M^k is the identity matrix for some k .
 - (b) Find a natural number r such that M^r is the identity matrix for every non-singular two by two matrix M .
5. Let p, q be primes with $p > q$. Find an exact expression for the number of irreducible polynomials of degree q in $\mathbb{F}_q[x]$.
6. In $\mathbb{Z}_5[x]$, find x^{2022} modulo $(x^2 + x + 2)$ using pen and paper.
7. Let \mathbb{F}_q be a finite field. Show the following:
 - (a) $\sum_{a \in \mathbb{F}_q} a = 0$;
 - (b) $\prod_{a \in \mathbb{F}_q^*} a = -1$;
 - (c) If $q > 3$, then $\sum_{a \in \mathbb{F}_q} \sum_{b \in \mathbb{F}_q, b \neq a} ab = 0$.