
Hand in to Frank Tuesday 17 September:

15. 20 points

Let m be a positive integer. Show that $\mathbb{Z}_m^* := \mathbb{Z}_m \setminus \{0\}$ is a group under multiplication if and only if m is a prime number. Let p be a prime number. Using that \mathbb{Z}_p is a field and in a field a polynomial of degree n has at most n roots, or any other valid facts, prove that \mathbb{Z}_p^* is a cyclic group of order $p-1$. Use this to prove Wilson's Theorem that $(p-1)!$ is congruent to -1 modulo p .

Hand in for the grader Tuesday 17 September:

16. Prove that every finitely generated subgroup of the rational numbers \mathbb{Q} is cyclic. Give an example (with proof) of a subgroup of \mathbb{Q} that is not finitely generated.
17. Let H, K be subgroups of a group G . Show that any right coset of $H \cap K$ is the intersection of a right coset of H with a right coset of K . Use this to prove Poincaré's Theorem that if H and K have finite index, then so does $H \cap K$.
18. Show that the symmetric group S_n may be generated by two elements.
19. List all of the elements of S_4 in cycle notation. Use this to prove that D_{24} , the dihedral group of order 24, is not isomorphic to S_4 .
20. Let $SL_2(\mathbb{Z}_3)$ be the group of 2×2 matrices of determinant 1 with entries in the field \mathbb{Z}_3 with three elements. Show that $SL_2(\mathbb{Z}_3)$ has order 24, and that it is not isomorphic to S_4 . Is it isomorphic to D_{24} ?