Yale University Department of Mathematics
Math 350 Introduction to Abstract Algebra
Fall 2016

Problem Set # 3 (due at the beginning of class on Friday 30 September)

Notation: A subgroup $K \subset G$ is called **normal** if $gxg^{-1} \in K$ for every $x \in K$ and $g \in G$. It is common notation to denote a subgroup by $K \leqslant G$ and a normal subgroup by $K \trianglelefteq G$.

If G and H are groups, the the cartesian product $G \times H$ is a group under the operation $(g,h)\cdot(g',h') = (gg', hh')$ for all $g, g' \in G$ and $h, h' \in H$.

Reading: DF 2.2–3.2.

Problems:

1. DF 2.2 Exercises 6, 7*, 12, 14.

2. DF 2.5 Exercises 4, 10, 12*, 14*, 15.

3. DF 3.1 Exercises 5, 6, 7, 8, 9, 10, 11*, 12, 22, 25*, 26* (you actually already did part a).

4. DF 3.2 Exercises 4*, 5, 8*, 9, 13*, 14*, 16*, 19, 22* (Euler's theorem!).

5. Show that for all $n, m \geq 1$, the group S_{n+m} contains a subgroup isomorphic to $S_n \times S_m$. Conclude that $n!m!$ divides $(n+m)!$.

6. Let H be the subgroup of S_4 generated by the 3-cycles. Show that there exists a positive integer n, with n dividing the order of H, and such that H has no subgroup of order n.

7. Define the sequence $\{f_m\}_{m\geq 0}$ of **Fibonacci numbers**

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

by the recursive formula $f_{m+2} = f_m + f_{m+1}$ for all $m \geq 0$. The purpose is to prove:

Theorem. *If p is a prime number, then p divides $f_{2p(p^2-1)}$.*

(a) Prove that for each $m \geq 1$, we have

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^m = \begin{pmatrix} f_{m+1} & f_m \\ f_m & f_{m-1} \end{pmatrix}$$

(b) For any prime p, show that

$$G_p = \{M \in \mathrm{GL}_2(\mathbb{F}_p) \mid \det(M) = \pm 1\}$$

is a group under matrix multiplication and calculate its order.

(c) Consider $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ as an element in G_p. Use the order of G to bound the order of A, and then use this to conclude that $f_{2p(p^2-1)} \equiv 0 \pmod{p}$.

8. *Tricks with Euler's theorem.* You can only use pencil and paper!

(a) Find the remainder after dividing 99^{999999} by 19.

(b) Prove that every element of $(\mathbb{Z}/72\mathbb{Z})^\times$ has order dividing 12. (Hint: This is better than what a straight application of Euler's theorem will give you! Try applying Euler's theorem to a pair of relatively prime divisors of 72.)

(c) Find the last two digits of the huge number $3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}$ where there are 2016 threes appearing! (Hint: Do nested applications of Euler's theorem.)