Math 8245 **Homework 1, due Monday 29 September** **PJW**

GAP questions:

1. Let $p_1, p_2, p_3, \ldots = 2, 3, 5, \ldots$ be the sequence of primes, and define

$$E_n = p_1 \cdot p_2 \cdots p_n + 1.$$

These are the numbers which appear in Euclid's proof that there are infinitely many primes, and have the property that E_n is not divisible by any of $p_1, \ldots, p_n$. Write a program in GAP which prints out which of the numbers E_n are prime, where $1 \leq n \leq 80$.
[This exercise tests use of loops and the GAP functions for integers. Instead of typing in your program live within a GAP session, you could try creating the program in a separate file in the directory from which you started GAP, and read in the file to GAP using Read("filename"); That way you do not need to type everything again when you make corrections.]

2. Consider the groups:

$$\begin{aligned}
g1 &= \langle (1,2,3,4,5,6,7,8), (2,4)(3,7)(6,8) \rangle \\
g2 &= \langle (1,2,3,4,5,6,7,8), (2,8)(3,7)(4,6) \rangle \\
g3 &= \langle (1,2,3,4,5,6,7,8), (2,6)(4,8) \rangle \\
g4 &= \langle (1,4,6,8,10,12,14,15)(2,3,5,7,9,11,13,16), \\
&\qquad (1,2)(3,15)(4,16)(5,14)(6,13)(7,12)(8,11)(9,10) \rangle \\
g5 &= \langle (1,2,3,4,5,6,7,8), (9,10) \rangle.
\end{aligned}$$

(a) For each group compute
(i) a list of the elements of the group,
(ii) a list of the orders of the elements of the group.
(b) Determine whether any of these groups are isomorphic to one another.
[Computer algorithms which establish an isomorphism between two groups are very poor — they basically run through all possible bijections and see if any of them are group homomorphisms. Instead, to show that certain groups are isomorphic here you should identify the groups in question as groups you already know something about, and use some theory to establish isomorphism.]
(c) In the case of the group $g1$, compute the lattice of subgroups. Show that $g1$ has a subgroup which is cyclic of order 8, another subgroup which is dihedral of order 8, and a third subgroup which is quaternion of order 8. In each case provide generators for the subgroup in question. Draw a picture of the lattice of subgroups, where one subgroup is shown immediately below another if one is a maximal subgroup of the other — in other words, draw the Hasse diagram.

[There are commands `ConjugacyClassesSubgroups` and `LatticeSubgroups` which I am sure some of you would be tempted to explore in tackling this problem. I suggest that it would be at least as easy for you to construct the lattice of subgroups by intelligent direct use of the functions I have already shown you in GAP. If you do insist on finding out about the subgroup functions I have just mentioned, be warned that I ask for a lattice of subgroups, not of conjugacy classes of subgroups, so I want all subgroups in the picture. Also, I ask for a picture, not the kind of output which these built-in functions produce.]

Theory questions: These are taken from the end of section 1, and have the same numbering as the questions there.

2. (The modular law.) Let A be a ring and $U = V \oplus W$ an A-module which is the direct sum of A-modules V and W. Show by example that if X is any submodule of U then it need not be the case that $X = (V \cap X) \oplus (W \cap X)$. Show that if we make the assumption that $V \subseteq X$ then it is true that $X = (V \cap X) \oplus (W \cap X)$.

5. Let
$$\rho_1 : G \to GL(V)$$
$$\rho_2 : G \to GL(V)$$
be two representations of G on the same vector space V which are injective as homomorphisms. (One says that such a representation is *faithful*.) Consider the three statements
(a) the RG-modules given by ρ_1 and ρ_2 are isomorphic,
(b) the subgroups $\rho_1(G)$ and $\rho_2(G)$ are conjugate in $GL(V)$,
(c) for some automorphism $\alpha \in \mathrm{Aut}(G)$ the representations ρ_1 and $\rho_2\alpha$ are isomorphic.
Show that (a) $\Rightarrow$ (b) and that (b) $\Rightarrow$ (c).

6. One form of the Jordan-Zassenhaus theorem states that for each n, $GL(n, \mathbb{Z})$ (that is, $\mathrm{Aut}(\mathbb{Z}^n)$) has only finitely many conjugacy classes of subgroups of finite order. Assuming this, show that for each finite group G and each integer n there are only finitely many isomorphism classes of representations of G on $\mathbb{Z}^n$.

10. Let $G = \langle x, y \mid x^2 = y^2 = 1 = [x, y] \rangle$ be the Klein four-group, $R = \mathbb{F}_2$, and consider the two representations ρ_1 and ρ_2 specified on the generators of G by
$$\rho_1(x) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_1(y) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
and
$$\rho_2(x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_2(y) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Calculate the socles of these two representations.

Extra questions: Do **not** hand in.

3. Write a function `AllOnes(n)` which given the non-negative integer n returns the integer 11...111 with n 1s. The syntax for functions is
```
allones:=function(n)
    local ;
    ...
    return(output);
end;
```

4. Suppose you are given a function `Conway` which when applied to a list of integers such as `[1,3,3,2]` returns `[1,1,2,3,1,2]`, for example. Write a routine in GAP which prints out the first 10 iterates of Conway applied to a list, e.g. applied to `[1,3,3,2]` it will return the 10 lists
```
[1,3,3,2]
Conway([1,3,3,2])
Conway(Conway([1,3,3,2]))
...
```
Bear in mind that within `Print` the string `"\n"` forces a line break before the next output is printed.

11. Let $G = C_p = \langle x \rangle$ and $R = \mathbb{F}_p$ for some prime p. Consider the two representations ρ_1 and ρ_2 specified by

$$\rho_1(x) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho_2(x) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Calculate the socles of these two representations. Show that the second representation is the direct sum of two non-zero subrepresentations.