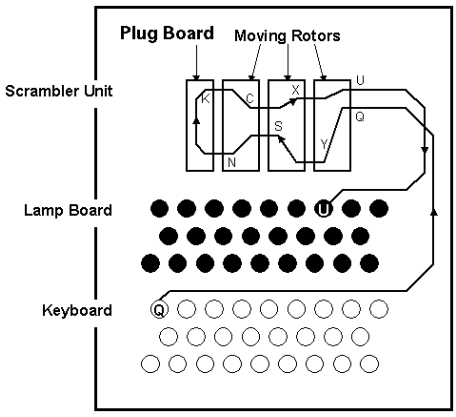
62) Let G be a group and $a \in G$ with $|a| = n$. For an integer $1 \leq k \leq n$ we set $b := a^k$.
a) Show that $b^n = (a^k)^n = e$.
b) Let $d = |b|$ and write $n = qd + r$ with $r < d$. Show that $b^r = e$.
c) Conclude from the definition of order that $r = 0$ and that therefore $d = \left|a^k\right|$ must be a divisor of n.
d) Show that $\left|a^k\right| = \dfrac{n}{\gcd(n,k)}$.

63) a) Show that for every natural number n there is a group with n elements.
b) Give an example of a natural number n such that there are two *different* groups with n elements.

64) Let G be a (not necessarily abelian!) group and $a, b \in G$. Prove that $|ab| = |ba|$.

65)* The German "Enigma" encryption machine, used in the second world war, produced (by a set of moving rotors) in each step a permutation $\sigma \in S_{26}$ (Interpreting the numbers 1-26 as letters in the alphabet.)
a) Show that it is not always possible to use the *same* setting (i.e. the same permutation σ) to encrypt and decrypt. (This causes problems for dumb operators – they would need to change settings between encryption or decryption.)
b) To ease handling for the operators (who understood little math), the German military had the "clever" idea to add a "plug-board" (on the picture in front of the machine) that swapped pairs of letters (this creates a permutation π that has a cycle type as $(1,2)(3,4)(5,6)\cdots(25,26)$) and to feed the encryption through the old mechanism (σ), then through the plug-board, and in reverse back through the mechanism. So the encryption performed now was of the form $\mu = \sigma^{-1}\pi\sigma$.
Show that this encryption is self-reverting, i.e. that $\mu^2 = 1$. (Thus the same setting could be used for encryption and decryption.)
c) Show that μ must be the product of thirteen 2-cycles.
d) How many possibile σ exist. How many possible μ exists? Explain, based on this count, why consequentially the "clever" idea was really stupid (and indeed was one of the reasons the code could be broken).



Problems marked with a * are bonus problems for extra credit.