Math 113H

Professor Ken Ribet

Answers to First Midterm Exam February 18, 1991

1. *Let G be a cyclic group of order 6^{100}. How many subgroups does G have? (Don't just write down a number; give some explanation.)*

A cyclic group G of order N has precisely one subgroup of order d if d divides N and no subgroup of order d if d doesn't divide N. Hence the number of subgroups of G is the number of positive divisors of N. The number of divisors of 6^{100} is 101^2.

2. *Let G be a group of order 11^2 which is not cyclic. How many elements of order 11 are there in G? How many subgroups does G have?*

Since G is not cyclic, the order of an element of G can be only 1 or 11. The identity element of G is the unique element of order 1. Hence there are $11^2 - 1 = 120$ elements of order 11. Among the subgroups of G there is (e) and G itself. All other subgroups of G have order 11. A given subgroup of G which has order 11 consists of the identity element and 10 elements of order 11. The number of subgroups of G with order 11 is then $120/10 = 12$. The total number of subgroups is 14.

3. *Find an integer x such that $x \equiv 23$ mod 69 and $x \equiv 34$ mod 397. (Don't bother simplifying your answer if it is complicated.) The identity $4 \cdot 397 = 23 \cdot 69 + 1$ will probably be useful.*

Use the method which was discussed in class. This gives $23 \cdot 4 \cdot 397 - 23 \cdot 34 \cdot 69 = -17434$ as an answer. If we prefer a positive answer, we can add $69 \cdot 397$, thereby getting 9959 as another answer. Of course, "$23 \cdot 4 \cdot 397 - 23 \cdot 34 \cdot 69$" is a perfectly acceptable answer as it stands; there was no need to come up with its numerical value.

4. *Here are two relations on the set of rational numbers. Which are equivalence relations? (Explain your answers.)*
a. Two rational numbers are related if their sum may be written $\frac{p}{q}$ with p and q integers such that p is even and q is odd.
b. Two rational numbers are related if their difference may be written $\frac{p}{q}$ where p and q are integers such that q is not divisible by 4.

The first one isn't even transitive. For example, $1/2 + 1/2 = 1$ cannot be written p/q in the indicated way, so $1/2$ is not related to itself. The second appears to be an equivalence relation: one simply checks the axioms. For example, the transitivity would follow if we knew that the sum of two p/q's of the indicated type is again of the indicated type. This is okay because the denominator of the sum of two p/q's is the least common multiple of the two q's. If neither q is divisible by 4, then the least common multiple isn't divisible by 4 either.

5. *Let g be an element of a finite group G. Define a map $\phi\colon \mathbf{Z} \to G$ by $\phi(n) = g^n$ for $n \in \mathbf{Z}$. Show that ϕ is a homomorphism of groups. Prove that the kernel of ϕ consists precisely of the multiples of the order of g.*

Showing that ϕ is a homomorphism is completely straightforward. The main point is to know that $g^n = e$ if and only if n is a multiple of $\mathrm{o}(g)$. For this, we let $t = \mathrm{o}(g)$ and write $n = qt + r$ where $0 \leq r < t$. We have $g^n = g^r$, and g^r is the identity element if and only if $r = 0$, in view of the definition of t.