Math 417 – Seventeenth Day – Class

Bruce Reznick
University of Illinois at Urbana-Champaign

October 2, 2020

Before I repeat the frames with the overview, I'd like to answer a few questions I've gotten overnight.

1. An extremely alert student noted that on frames from Sept. 9 (Day 7), I multiplied permutations in the wrong order. This was corrected on Sept. 11 (Day 8), so keep that in mind when studying.

2. A student writes to ask whether "generators" will be on the test. What I said was:

Yes, they might be on the test. I might give you a cyclic group and one generator and ask you to find another generator, but it won't involve large numbers: for example, I wouldn't ask you to decide if $[2]_{37}$ is a generator of $((\mathbb{Z}/37\mathbb{Z})^*, \odot)$.

3. Another student asked about the nature of the first exam, so I think it's worthwhile to put this all in one place.

a. I will email you the exams on Thursday night (10/8). They will be due back to me by 11:59PM on Saturday night (10/10). I will try to acknowledge receipt with reasonable speed, depending on the time of day.

b. My intention is that this test would be the same length as a typical hour exam, with a median time to finish around 45 minutes.

c. There will be no class on Friday 10/9.

d. There will be multiple equivalent variations on the problems of the exam, sent to different people.

e. I will ask you to block out a **consecutive** period of time to work on the test. If you take more than two hours, please indicate that on your paper.

f. It is very important to show your work and explain your steps.

g. As always, read the problems carefully.

h. The exam is open book, open notes and open to the class notes I've been providing. You may use a calculator, but it shouldn't be necessary.

i. **This is a non-collaborative exam. Please do not talk to anyone else about the test unless you know that everyone in the conversation has taken it.**

j. Despite the relaxed nature of these rules, I am attaching a link to §1-402 of the Student Code regarding Academic Integrity. I've read it, and I hope you have too.

https://studentcode.illinois.edu/article1/part4/1-402/

Here are the frames again. Please let me know if you have questions or if I missed something.

Number theory topics: $\mathbb{Z}, \mathbb{Q}$, divisibility, $m \mid n$, congruence mod n, $a \equiv b \mod n$, $[a]_n$, prime numbers, gcd, $gcd(m,n)$, relatively prime integers, the existence of prime factorization, Euclidean Algorithm. Know what the Euler phi function $\phi(n)$ means, but you won't have to calculate it. Know that $gcd(m,n) = g$ implies that there exist integers r, s so that $g = mr + ns$ (findable through the EA) and if $gcd(m,n) = 1$ and $n \mid mr$, then $n \mid r$.

Group Theory Vocabulary: commutative, associative, binary operations, the definition of a group, and an identity and inverses in a group, abelian groups, cyclic groups ($C_n = \langle a \rangle, a^n = e$ or $(\mathbb{Z}/n\mathbb{Z}, \oplus)$), the symmetric group S_n in general, and in more detail S_3, the Klein group V and the dihedral group D_4.

More Group Theory: subgroups, $H \leq G$, the order of a group $|G|$, the order of an element in a group, isomorphisms, homomorphisms (plus kernel $Ker(\phi)$ and image $Im(\phi)$), left and right cosets of a subgroup, normal subgroup $H \trianglelefteq G$ and what that means, direct product of two groups $G \times H$, factor groups as a result of a normal subgroup, G/H consisting of the cosets of H. If $\phi : G \to H$ is a homomorphism, then $K = Ker(\phi) \trianglelefteq G$ and G/K is isomorphic to $Im(\phi)$.

More things to be able to do: Read a group multiplication table. If you know G and H, you should be able to work with $G \times H$ and if $gcd(m, n) = 1$, you should know that $C_m \times C_n \approx C_{mn}$. How to decide if a subset H of G is a subgroup, how to find the subgroups of cyclic groups and the connection with gcd, Lagrange's Theorem. How to compute the orders of elements in cyclic groups and in direct products.

With permutations, know cycles and transpositions. Write permutations in multiple ways, for example if $\pi : \{1,2,3,4\} \to \{1,2,3,4\}$ and $\pi(1) = 2, \pi(2) = 4, \pi(3) = 3, \pi(4) = 1$, then we might write this as:

$$\pi : 1 \mapsto 2 \mapsto 4 \mapsto 1, 3 \mapsto 3,$$

$$\pi = (124)(3), \quad \pi = (124), \qquad \pi = \binom{1234}{2431}$$

Know how to multiply permutations in the right order.

Not on this test $\phi(n)$ (except incidentally as $|((\mathbb{Z}/n\mathbb{Z})^*, \odot)|$), repeating decimals as such, Cayley's Theorem, odd/even permutations, the book's theorem on the classification of finite abelian groups. What we've done this week on $Aut(G)$, i_g, etc.

Send me an email if there's something I missed.