Oral Exam Questions
Shanshan Ding, April 15th 2010

Major: Probability; Minor: Algebraic Number Theory
Committee: Robin Pemantle (chair), Jonathan Block, David Harbater

DH: (Started with something super easy, perhaps because I must have appeared to be on the verge of fainting) What is the unit group of $\mathbb{Z}/13\mathbb{Z}$? $\mathbb{Z}/83\mathbb{Z}$? $\mathbb{Z}/15\mathbb{Z}$? You said that $(\mathbb{Z}/15\mathbb{Z})^\times$ is of order 8, so which group is it?

Is 13 a square mod 83? Is 83 a square mod 13? How many elements of $(\mathbb{Z}/83\mathbb{Z})^\times$ are squares? In general, if you have a cyclic group of even order, how many are squares? What about a cyclic group of odd order?

What is the ring of integers in $\mathbb{Q}(\sqrt{83})$? Which primes ramify, which primes split, and which primes are inert in this ring? What are the decomposition and inertial groups in each case? If you know the behavior of the first 200 primes, can you predict the rest?

What can you say about the cardinality of primes that split in $\mathbb{Q}(\sqrt{83})$? Which theorem tells you that? Can you give an example of a field where 1/82 of the primes split?

RP: State the weak law of large numbers, including careful definitions of all terms that appear – random variable, IID, convergence in probability. Can mutual independence be weakened to pairwise independence?

Say you have a sequence of random variables X_n, where X_0 is uniform between 0 and 1, and X_n is uniform between 0 and X_{n-1}. What is the likely order of the magnitude of X_n? What is the expectation of X_n?

JB: Tell me about large deviations.

RP: Let X_n be $\pm 1/n$ with probability 1/2 each. What can you say about the sequence S_n? Since you invoked martingale theory, perhaps you should define martingales.

(Most difficult question of the exam; luckily they decided to take a break after giving me this question, so I had some time to think) Consider an infinite binary tree. Suppose I delete some edges, and that each edge is kept with probability p. What is the probability that, starting from the top node, I am able to travel down an infinite path?

DH: Revisit the field $\mathbb{Q}(\sqrt{83})$. You were able to determine how a prime behaves there by simply considering its remainder mod some integer. What other fields have this property?

What can you say about primes in arithmetic progressions? You quoted Chebotarev density theorem in claiming that 1/2 of primes split in $\mathbb{Q}(\sqrt{83})$. Give another argument using Dirichlet density theorem.

Consider the field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Is it Galois over $\mathbb{Q}$? What is the Galois group? Classify the behavior of primes in this extension. What is the unit group in its ring of integers?

Say something about class numbers.

RP / JB: Tell us about the Erdös-Kac theorem, including the main ideas of its proof.

RP: Define a stopping time τ. True or false: for a martingale X_n, we always have $\mathbb{E}X_\tau = \mathbb{E}X_0$. OK, it is false in general, but when is it true? Define uniform integrability.

JB: In a sequence of fair coin flips, what is the expected number of flips before you attain the string HT? (RP: Your argument is very cute...where did you see it before? Me: yeah, thanks for pointing out that I could not have thought of it on my own. He's right though, I had seen it before and in no way could have come up with it spontaneously.)

JB / RP: How do you know that in this case $\mathbb{E}X_\tau = \mathbb{E}X_0$? Give an elementary argument for the finiteness of $\mathbb{E}\tau$.

*The examination lasted about two hours.