Topic Proposal
MATH 194-02
Winter 2021

Kevin Guillen
1747199

January 5, 2022

1 P-adic Numbers

Just like real numbers are an extension of the rational numbers, so are p-adic numbers, but in a different way. This is done by using a different interpretation of closeness which allows p-adic numbers to encode congruence information in useful ways.

I'd approach this by going over the history of p-adic numbers, their construction, covering important theorems, and their application to solving certain problems in number theory, algebra, and/or analysis. Give examples of some very non-intuitive results in gives that can't be obtained with reals.

2 Elliptic Curves

An elliptic curve is an algebraic curve which has a specified point O, and is defined over the a field K and describes points over the Cartesian product of the field K.

Go over history of elliptic curves. Build up the idea using basic algebra and geometry with the real numbers and then go more into it through the lens of algebraic geometry. Talk about applications such as elliptic curve cryptography, and applications in solving other pure math problems.

3 RSA Cryptosystem

RSA is a public-key cryptosystem that is still widely used today. A user publishes a key based on two large prime numbers which are kept secret, and anyone can encrypt messages based on that published key, but only be decoded by the user who knows the prime numbers used.

Talk about the history of RSA, giving examples of how the algorithm works, why it is secure. Describe how it is used alongside weaker, but faster cryptosystems. Talk about the future of it with the concern of quantum computers.