Universidad Autónoma de Yucatán
Facultad de Matemáticas

SEMISTABLE ELLIPTIC CURVES OVER $\mathbb{Q}$ AND SERRE'S CONSTANT.

Thesis presented by
L.M. Alejandro Argáez García

Waiting for title of
Maestro en Ciencias Matemáticas

Mérida, Yucatán, México
18 August 2010

Acknowledgments

I would like to thank my parents, for all their support through the years, for being unconditionally on my side in good or bad. My Father, Carlos Argáez Carrillo, who is the smartest person which I've ever known and my inspiration to be a mathematician. My Mother, Nelly Josefina García Díaz, who always encourage me to pursuit greater things in life and who also did not allow me to drop off school when I tried to. To my sisters and brother; Nelly, Josefina and Carlos, thank you for caring of me when we were young and for all the time we spend together playing and doing funny things.

Thanks to my advisor Javier Diaz, for convincing me to go to work with Kirti Joshi, my second advisor, at the University of Arizona, to both for all their support through my master's study. Also, I want to thank my friends, Israel García Lara who helped me on the understanding of Phyton and all his advice and opinions related to my programming; to my friend Alejandro Lara, a helpful hand on my journey in North America, to my friend Eduardo Hernandez Mezquita, who has been there through most ups and downs during my college years. And last but not least, to Marisol Aguilar de Salazar for all her patience, advice and English expertise.

Thank you to CONACYT to support me economically on my master's studies.

Abstract

It was on 1972, that Jean-Pierre Serre with his article "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques" proved that for an elliptic curve without complex multiplication, there is only a finite number of prime numbers such that the Galois representation associated to an elliptic curve module a prime is not surjective; if we consider working with a semistable elliptic curve, there are certain conditions to figure if the representation of this curve is not surjective, therefore, it simplifies its analysis from a computational point of view. The multiplication of the prime numbers that don't have a surjective representation is named as "Serre's Constant". Serre's proposition had an issue: there are an infinite amount of prime numbers and so, an infinite number of cases that could be studied on a computational matter. Six years later on 1978, Barry Mazur proved through the association of Galois representation to a semistable elliptic curve module a prime, that for every prime equal or higher than eleven, this representation is surjective; this leaves only four possible prime numbers that could have none surjective representations. It wasn't until 1994 that Andrew Wiles proved the last Fermat theorem using semistable elliptic curves with Galois representations associated to this elliptic curves; particularly speaking, he used the representations for the primes three and five.

Considering the previous explanation, we wonder: is it possible to get a result that shows when the Galois representation associated to a semistable elliptic curve module a prime is not surjective? The answer of this interrogative is the work contained in this thesis.

This thesis contains a series of studies of Galois representations associated with semistable elliptic curves and rational numbers. This followed two paths: practical and theorical. Working with the results that were given by Serre, a program was generated, using free software "Software for Algebra and Geometry Experimentation (Sage)"©, from where four conjectures were generated, three of them were successfully proved and are showed here as theorems. The first one of this theorems gives us Serre's constant independence on isogenous semistable elliptic curves; the second one gives us the only possible values of Serre's constant and finally, the third theorem explains how to reach this values.

At the end, this thesis closes the study of Galois representation associated to semistable elliptic curves module a prime.

Contents