The Perforation of p-adics: Closing a Gap in Hensel's Lemma Through the Convergence Inequality

Uzun, Imaad (School: New Rochelle High School)

Hensel’s Lemma is the foundation of p-adic number theory and, as discovered in this study, a possible way to revolutionize the math behind elliptic curve cryptography. It works by lifting a root f(a) of a polynomial f to a root mod p, which can be more effective at finding integer solutions where none may exist otherwise. A common method of proving Hensel’s Lemma involves the following inequality which bounds the distance between a p-adic solution and its nth approximation: |{alpha} − a_n|_p ≤ (|f'(a)|_p) * (|f(a)/f'(a)^2|_p)^2^(n-1). Showing the values of n for which this ‘convergence inequality’ becomes an equality is vital for the practical use of p-adic approximate roots. However, such equality has never been proven for any values of n > 10, making our current understanding of its behavior incomplete. The goal of this study was to show that the inequality holds as an equality for greater values of n (and then all n), which I constructed a computer program in Python to demonstrate numerically. Then, I was successfully able to show equality for all values of n by induction, supported by the program’s outcomes. Thus, I amended our understanding of the inequality’s behavior, which I showed to be directly applicable to approximating rational points on elliptic curves, a tactic that could save hundreds of millions of dollars per year on cybersecurity in the US if harnessed. No such proof has been documented before, making this a novel discovery.