Some Notes About Power Residues Modulo Prime: The Challenge To Find a Pattern of Mersenne Primes and To Discover New Primes

Kiriu, Yuki (School: Shizuoka Salesio High School)

The aim of this research is to reveal the pattern of Mersenne Primes. Therefore, I focused on revealing the pattern of power residues of 2 modulo a prime. Mersenne Primes tend to break the record of the largest known primes, but they are very difficult to find even when using computers. Previous research done related to power residues reveal the pattern for modulo composite number, but nothing about modulo prime. My project is an enormous repetition of assumptions and verification. Firstly, I made a conjecture using knowledge of literature. After that, I used Wolfram Mathamtica to check if the numbers fit the conjecture. If a counterexample were not to be found, I will try to prove and generalize it. If a counterexample were to be found, I will try to make a new one by relaxing the condition or by finding a pattern of counterexamples. As a result, I discovered several new theorems. All of these theorems revealed the unknown patterns about power residues. Especially, one of these theorems claim that there is a one-to-one correspondence between quadratic residues and residues modulo composite number, which gives a new insight about power residues. For future prospect, I strongly believe that, by further revealing the unknown pattern about power residues, it would be possible to discover the pattern of Mersenne Primes. By achieving this, the new discoveries should be possible to apply to the improvement of internet security by strengthening RSA code and Elgamal encryption.