

1056-BB-607      **Alice Silverberg\***, Mathematics Department, UC Irvine, Irvine, CA 92697-3875. *Counting points on elliptic curves, from Gauss to the present.*

In his *Disquisitiones Arithmeticae*, Gauss published a simple formula for the number of solutions mod  $p$  to  $x^3 - y^3 = 1$ . In his last diary entry, Gauss gave a similar result for the number of solutions mod  $p$  to  $x^2 + y^2 + x^2y^2 = 1$ . In modern language, these results can be viewed as part of an extensive history of counting points on elliptic curves over finite fields, which now has applications to cryptography. This talk will discuss some of this history. (Received September 14, 2009)