Group structure of Rational Points on the Elliptic Curve

B.S.Satpute
HOD Mathematics, Vaidyanath College Parli-V, Dist. Beed, Pin-431515

Received: July 02, 2018 Accepted: August 25, 2018

ABSTRACT *Fermat's last theorem is proved by using a long chain of arguments, based on many mathematicians deep work, culminated in Wile's last decisive step. Wiles proof is based on theory of elliptic curves. A big part of this theory is devoted to understanding the "Rational points" on these curves.*
In this paper we discuss the group structure of rational points on the elliptic curve by chord method.

Keywords: *Rational points, Elliptic curves.*

1) Introduction:-

Weierstrass form: -

The equation $y^2 = P(x)$ Where P is a cubic polynomial with rational coefficients
As far as rationality is concerned, restricting ourselves to Weierstrass forms results in no loss of generality.

Elliptic curve: -

Although the formal definition of an elliptic curve is fairly technical and requires some background in algebraic geometry, it is possible to describe some features of elliptic curves over the rational numbers using only high school algebra and geometry.

A cubic rational curve in Weierstrass form $y^2 = P(x)$, where the polynomial P has no double or triple roots, is called as Elliptic. Any elliptic curve can be written as a plane algebraic curve defined by an equation of the form:

$$y^2 = P(x) = x^3 + ax + b$$

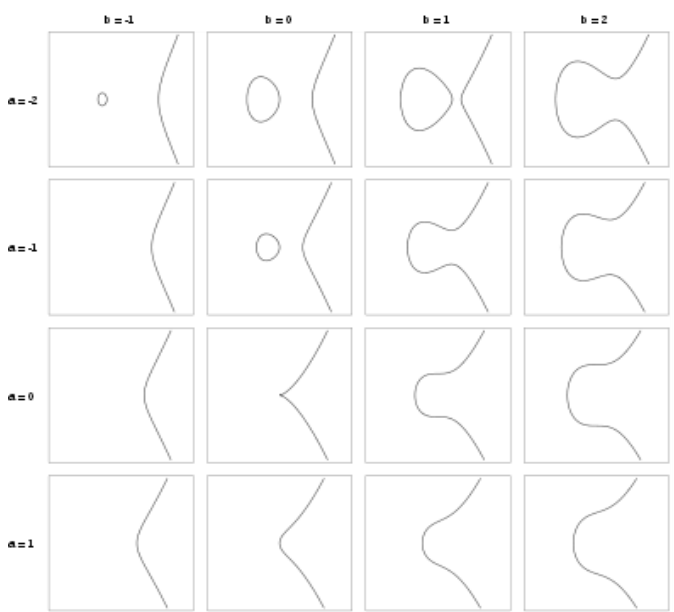


Figure 1

The theory of elliptic curves displays one of the most beautiful interplays between number theory, algebra, and geometry.

2) Group Structure of Rational Points on the Elliptic Curve by Chord Method.

Operation *:-Given an Elliptic curve, we consider the line l through two of its rational points**,** say A and B. Since the elliptic curve is cubic, there must be a third intersection point with l. We denote it by A*B**.** This point is rational. If a cubic polynomial has rational coefficients and two rational roots, the third root is also rational. Indeed, the sum $r_1 + r_2 + r_3 = -c_2/c_3 \in Q^2$(Binary).The operation (A, B) → A*B on the set of

rational points of elliptic curve does not define a group structure. Since there is no point playing role of identity element.

Identity: - We begin with identity A+O=A. We fix a rational point O (assuming it exist at infinity).Here we are manipulating what we want.

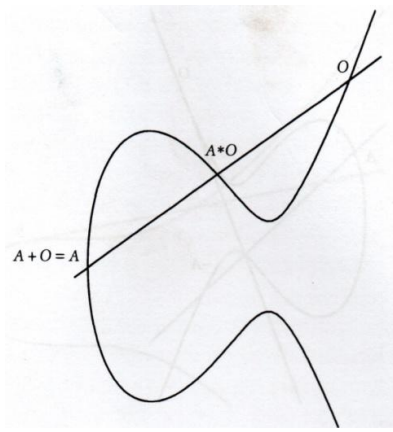


Figure 2

Operation +: Define A+B as the third intersection of the line through O and A*B. Our aim is to show that the operation (A, B) → A+B defines a group structure on the set of rational points on the elliptic curve. Although the definition of the sum of two rational points on an elliptic curve appears in the works of Cauchy (c.1835), the fact that this operation defines group structure was only recognized by Poincare around 1901.

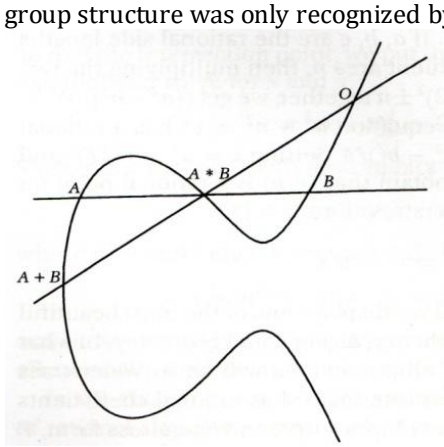
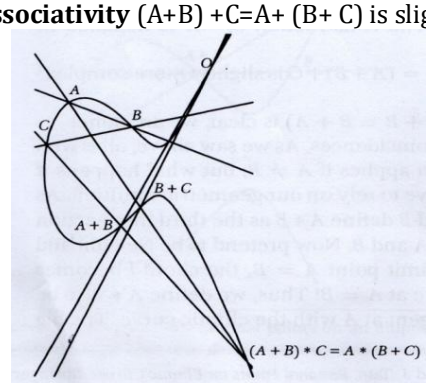


Figure 3

Associativity: - Associativity (A+B) +C=A+ (B+ C) is slightly more complex



Figure

Existence of inverse:- the negative of a point, the identity A+(-A)=O requires that the line through A*(-A) and O should have no further intersection with the elliptic curve . This follows that this line must be tangent to the curve at O (A nonvertical line tangent to the elliptic curve meets the curve at exactly one other point). (-A) depicted in figure5

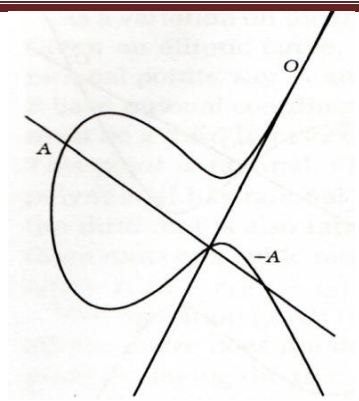


Figure 4

Abelian: - The commutativity A+B = B+A is clear

As we saw above all is well and the chord construction applies if A is not equal to B

But what happens if A=B. at this point we have to rely on out geometric intuition. As usual, let the distinct and B define A*B as third intersection point of the line l through A and B. Now pretend to be Newton and let B approaches A. at the limit point A=B, the chord l becomes tangent to the elliptic curve at A = B. Thus we define A*A to be the intersection of the tangent at A with the elliptic curve.

Thus the set of rational points on elliptic curve with manipulated identity O at infinity forms an abelian group structure.

References:-

1) Gobar Toth, Glimbses of algebra and geometry, Springer, 2002.
2) N.Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer, 1993.
3) Wikipedia, the free encyclopedia.