LPDJLQH D VHFUHW

A FILM OF ART AND MATHEMATICS ON ELLIPTIC CURVES AND CRYPTOGRAPHY

by José Francisco Rodrigues

Pythagorean triples such as (3, 4, 5) or (4961, 6480, 8161) were well known by ancient Babylonians around 1600 B.C. They were also aware of their correspondence to right triangles with integer sides and to the problem of splitting a given square number into two squares. Although such triples have been studied in detail since the time of Euclid, around 300 B.C., it was only in the middle of the XVII century that Pierre de Fermat stated the famous observation: "No cube can be split into two cubes, nor any biquadrate into two biquadrates, nor generally any power beyond the second into two of the same kind".

This became the famous "Fermat's Last Theorem", stating that the equation $A^N + B^N = C^N$ has no nonzero integer solutions when N is greater than 2. It was completely proven in 1994, about three and a half centuries later, using the XX century theory of elliptic curves!

Elliptic curves have deep and beautiful properties. They are plane curves of the type

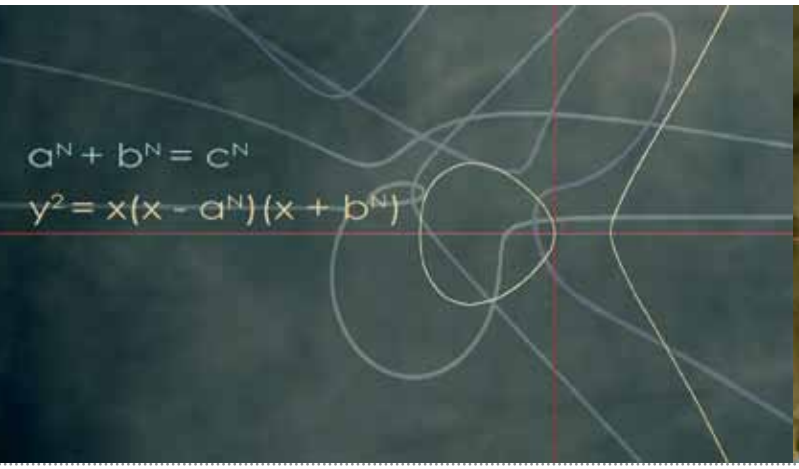
$$y^2 = x^3 + ax + b$$

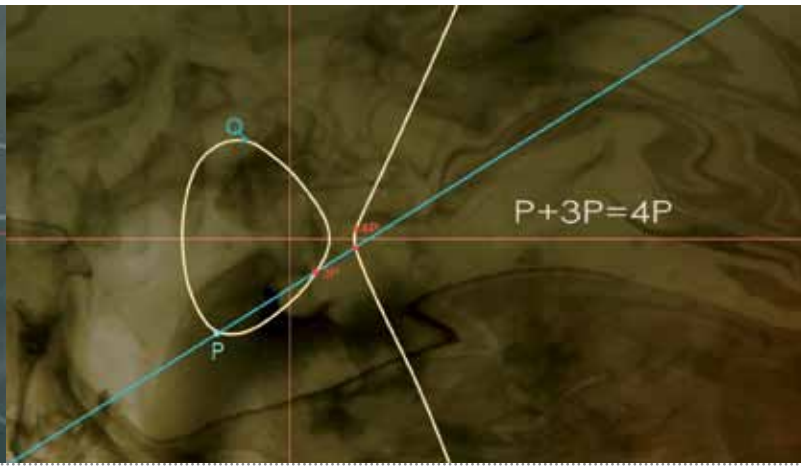
that have been studied since the XIX century. That equation in the affine plane corresponds to the homogeneous equation

$$y^2z = x^3 + axz^2 + bz^3,$$

which describes in space a family of algebraic surfaces with two parameters a and b. The computational variation of these equations generates beautiful animations that stimulate our imagination and evoke our mathematical creativity.

Cryptography refers to secure methods to transmit and safeguard secret and valuable information. Since 1977 the RSA public key system has been widely used. It is based on prime number theory and on the difficulty of factoring very large integers. With





The first public presentation of the movie LPDJLQH D VHFUHW was done the 26 September 2010 in Óbidos during the opening of the Workshop "Raising the Public Awareness in Mathematics". The movie exists in four languages, English, German, Portuguese and Spanish, and can be freely downloaded from http://www.cim.pt/LPD-UHW

the impact of the elliptic curve method for integer factorization, Elliptic Curve Cryptography (ECC) was invented by mathematicians in 1985, and since then the mathematical sophistication of cryptography has been raised to a whole new level.

The security of the ECC algorithms is based on the discrete logarithm problem of elliptic curves, which seems to be a much harder problem in finite field arithmetic. Recent mathematical advances imply that a certain desired security level can be attained with significantly smaller keys, for instance, a 160-bit ECC key provides the same level of security as a 1024-bit RSA key.

The theory of elliptic curves illustrates the beauty of the links between number theory, algebra and geometry and provides a powerful mathematical tool to strengthen security of e-commerce and secure communications. The old and unreliable method of the Caesar cipher of using only the simple arithmetic operation to encipher a message in the usual Latin alphabet by means of the formula $d = c - 3 \pmod{26}$ is outdated. But, it gives us the key to decipher the title of this film:

_____ – _____

Credits

Movie: LPDJLQH D VHFUHW

Initiative: Centro Internacional de Matemática; Casa da Animação; Mathematisches Forschungsinstitut Oberwolfach

Original Idea: José Francisco Rodrigues

Conception: Victor Fernandes; Stephan Klaus; Armindo Moreira; José Francisco Rodrigues

Realization and Production: Victor Fernandes; Armindo Moreira

Surfer Movies: Andreas Matt; Bianca Violet

Original Music: Victor Fernandes; Armindo Moreira

Acknowledgements: CMAF/Universidade de Lisboa; Fundação Calouste Gulbenkian; IMAGINARY exhibition; Vila de Óbidos

Sponsor: Ciência Viva