TSINGHUA MATHCAMP 2021 COURSE: NUMBER THEORY

EMMANUEL LECOUTURIER, LECTURER

A well-known result, first conjectured by Girard in 1625, claimed without proof by Fermat in 1640 and finally proved by Euler in 1749, is that an odd prime number p is a sum of two squares of integers if and only if 4 divides $p-1$, *eg.* $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$ etc. While one easily sees that $p = x^2 + y^2$ implies $p \equiv 1$ (modulo 4), the converse is not *a priori* obvious. We may consider other similar questions, *eg.* when does the equation $p = x^2 + 14y^2$ have solutions in $x, y \in \mathbf{Z}$? The answer turns out to lie much deeper than before.

Theorem. *A prime number p is of the form x^2+14y^2 if and only if the following two conditions hold:*

(i) $p \equiv 1, 9, 15, 23, 25$ *or* 39 *(modulo* 56*).*
(ii) *The equation $X^4 + 2X^2 - 7 \equiv 0$ (modulo p) has a solution.*

The necessity of condition (i) (which is the analogue of $p \equiv 1$ (modulo 4) in the result of Euler), is easy to show. However, condition (ii) will lead us to what is called *class field theory*, one of the major mathematical achievements of the 20st century. We hope to make the proof of this theorem accessible to Mathcampers, without assuming much background (namely, some basic knowledge in algebra such as prime numbers, congruences, polynomials and complex numbers). Many fascinating related subjects such as quadratic forms, Galois theory, algebraic number theory etc. will be explored.

Regular homework will be assigned, and one or more accessible research projects will be proposed to the students during the first week of Mathcamp.