LECTURE OUTLINE: A SPECIAL CUBIC MODULO PRIMES

GERGELY HARCOS

Theorem. *Let $p \neq 3$ be a prime. If $p \equiv \pm 1 \pmod 9$ then $x^3 - 3x - 1$ has three distinct roots modulo p. Otherwise $x^3 - 3x - 1$ has no root modulo p.*

The main steps of proof are the following.

1. Let $\mathbb{F}_p$ be the field of residues modulo p. For any positive integer n, the polynomial $x^n - 1$ splits into linear factors in some field F containing $\mathbb{F}_p$.

2. We assume $p \nmid n$. Then the linear factors of $x^n - 1$ in F are distinct for which we use the familiar notion of derivation on polynomials.

3. By induction on $m \mid n$, there are $\varphi(m)$ primitive m-th roots of unity in F. In particular, F contains some primitive n-th root of unity ξ and then $x^n - 1 = \prod_{i=0}^{n-1}(x - \xi^i)$ in F.

4. Let $n = 9$, $p \neq 3$, F and ξ as before. Then

$$x^3 - 3x - 1 = (x + \xi + \xi^{-1})(x + \xi^2 + \xi^{-2})(x + \xi^4 + \xi^{-4}),$$

and the factors on the right hand side are distinct.

5. The elements of $\mathbb{F}_p$ are precisely the fixed points of the map $x \mapsto x^p$ in F. So the real question is: how many of the elements $\xi + \xi^{-1}$, $\xi^2 + \xi^{-2}$, $\xi^4 + \xi^{-4}$ are fixed by this map? The answer is 3 when $p \equiv \pm 1 \pmod 9$ and 0 when $p \equiv \pm 2, \pm 4 \pmod 9$.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, POB 127, BUDAPEST H-1364, HUNGARY

E-mail address: gharcos@renyi.hu