NAP 2019, MODULE II, CLASS #7, MAY 31, 2019

Michel Waldschmidt

• Answer to questions. If f is a polynomial of degree d, then f is irreducible if and only if the polynomial $x^d f(1/x)$ is irreducible.

• Exercise: the polynomials in $\mathbb{Z}[x]$ which are irreducible modulo p for all p are the polynomials $\pm x + a$ with $a \in \mathbb{Z}$.

• Construction of angle bisector with ruler and compass is easy. Trisecting an angle is sometimes possible, sometimes impossible. Example: impossible to construct a nonagon with ruler and compass.

• Construction of a regular polygon with n sides using only ruler and compass. Examples.

If it is possible with n, it is possible with $2n$. Further, if d divides n, it is also possible with d.

• For p an odd prime, if a regular polygon with p sides can be constructed with ruler and compass, then p is a Fermat prime. Irreducibility of the cyclotomic polynomial $(x^p-1)/(x-1)$.

• $F_5 = 2^{2^5}+1$ is divisible by 641 (Euler).

If p is a prime number which divide F_5, then $2^{32} \equiv -1 \pmod p$, hence 2 is of order 64 modulo p and therefore p is congruent to 1 modulo 64.

We have $641 = 5^4 + 2^4 = 2^7 \cdot 5 + 1$, hence $2^7 \cdot 5 \equiv -1 \pmod{641}$ and $5^4 \equiv -2^4 \pmod{641}$. Therefore

$$1 \equiv (2^7 \cdot 5)^4 \equiv 2^{28} \cdot 5^4 \equiv -2^{28} \cdot 2^4 \equiv -2^{32} \pmod{641}.$$

In fact $F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$.

• Result: a regular polygon with n sides ($n \geq 3$) can be constructed with ruler and compass if and only if $n = 2^a p_1 \cdots p_r$, where $a \geq 0$, $r \geq 0$ and $p_1, \dots, p_r$ are distinct Fermat primes.

Part of this result is proved, what is missing for a full proof (will be done in other modules) is :

– irreducibility of the cyclotomic polynomial $(x^{p^2}-1)/(x^p-1)$ of degree $p(p-1)$

and

– if p is a Fermat prime, a regular polygon with p sides can be constructed with ruler and compass.