Some slides for 12th Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

14-03-2013

Quadratic residues

Let p be a prime number. If p $\nmid a$ then a is called a quadratic residue modulo p if it is congruent to a square modulo p, i.e. there exists$x \in \mathbb{Z}$ such that

$$a \equiv x^2 (\mathrm{mod}\ p).$$

Otherwise a is called a quadratic non-residue modulo p.

If $p \mid a$, then a is considered neither a quadratic residue nor a quadratic non-residue.

Legendre Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

$$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right), \text{ with } k \in \mathbb{Z}$$

Proposition 1.11.3

Let p denote and odd prime. Half of the numbers $1, 2, \ldots, p-1$ are quadratic residues; the other half are quadratic non-residues modulo p.

Theorem 1.11.4 (Euler)

Let p be an odd prime and let a be an integer not divisible by p. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Prime numbers congruent to 1 modulo 4

Lemma 3.5.18

A prime number $p \mid 3 \pmod 4$ is a prime element in $\mathbb{Z}[i]$.

Corollary 3.5.19

If p is an odd prime number dividing $x^2 + 1$ for some $x \in \mathbb{Z}$ then $p \mid 1 \pmod 4$.

Theorem 3.5.20

There are infinitely many primes congruent to 1 modulo 4.

Fermat's last theorem