A system of m polynomial equations in n variables:

$$\begin{aligned} f_1(x_1, x_2, \ldots, x_n) &= 0 \\ f_2(x_1, x_2, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, x_2, \ldots, x_n) &= 0 \end{aligned}$$

The f_i are polynomials with integer coefficients.

Example:

$$x^2 + ax + b = 0,$$

with a and b integers.

Another example:

$$x^2 + y^2 = 1.$$

Here we have infinitely many solutions, even in the rational numbers.

A field is a set F, given with two operations on it:

$$+\colon F \times F \to F,$$

and:

$$\cdot\colon F \times F \to F,$$

and two distinct elements in F called 0 and 1, such that:

1. for all x, y and z in F we have $(x+y)+z = x+(y+z)$,

2. for all x and y in F we have $y+x = x+y$,

3. for all x in F we have $x+0 = x$,

4. for all x in F there exists a y in F such that $x+y = 0$,

5. for all x, y and z in F we have $(xy)z = x(yz)$,

6. for all x and y in F we have $yx = xy$,

7. for all x in F we have $x \cdot 1 = x$,

8. for all non-zero x in F there exists a y in F such that $xy = 1$,

9. for all x, y and z in F we have $x(y+z) = xy+xz$,

Some examples of fields:

$\mathbf{Q}$, the rational numbers,

$\mathbf{R}$, the real numbers,

$\mathbf{C}$, the complex numbers,

the field of $\mathbf{R}$-valued rational functions on $\mathbf{R}$,

meromorphic functions,

the field $\mathbf{F}_2 = \{0, 1\}$, where $1 + 1 = 0$.

For $n \geq 1$ a positive integer,
$\mathbf{Z}/n\mathbf{Z} := \{0, 1, 2, \ldots, n-1\}$,
with the operations:

$$\begin{aligned} a + b &= a + b \bmod n, \\ a \cdot b &= ab \bmod n. \end{aligned}$$

$\mathbf{Z}/n\mathbf{Z}$ is a field if and only if n is prime.

For p a prime number, $\mathbf{F}_p$ will denote the field $\mathbf{Z}/p\mathbf{Z}$.

The classification of finite fields:

1. the number of elements of a finite field is of the form p^r, with p a prime number;

2. for each prime number p and each $r \geq 1$ there exists a field with p^r elements;

3. two finite fields with the same number of elements are isomorphic.

The field with p^r elements will de denoted $\mathbf{F}_{p^r}$.

Example:

$$\mathbf{F}_4 = \{0, 1, z, 1 + z\}$$

with

$$1 + 1 = 0, \quad z + z = 0$$

and

$$z^2 = 1 + z.$$

Another example: $\mathbf{F}_9$ is the set of $a + bi$, with a and b in $\mathbf{F}_3$, and $i^2 = -1$.

In $\mathbf{F}_{p^r}$ we have $p = 0$.

For S a system of equations as in the beginning, we define, for p prime and $r \geq 1$:

> $N_S(p, r)$ is the number of solutions of S in $\mathbf{F}_{p^r}$.

Riemann's zeta function:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

for real $s > 1$ (or complex s with $\Re(s) > 1$).

ζ extends to an analytic function on $\mathbf{C} - \{1\}$. This continuation satisfies the functional equation:

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).$$

For S a system of polynomial equations with integer coefficients, we define:

$$\zeta_S(s) = \exp\left(\sum_{p,r} \frac{N_S(p,r)}{r} p^{-rs}\right).$$

This makes sense for complex s with $\Re(s) > n+1$, where n is the number of variables in S.

Using that:

$$-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots,$$

one sees that ζ_S is Riemann's zeta function if (and, in fact, only if) $N_S(p,r) = 1$ for all p and r.

By the definition of ζ_S, we have:

$$\zeta_S(s) = \prod_p \zeta_{S,p}(s),$$

where the product runs over all prime numbers, and the $\zeta_{S,p}$ are defined by:

$$\zeta_{S,p}(s) = \exp\left(\sum_{r\geq 1} \frac{N_S(p,r)}{r} p^{-rs}\right).$$

The $\zeta_{S,p}$ have a geometrical interpretation.

The geometrical object is:

$X_{S,p}$, the set of solutions of S in $\mathbf{F}_{p^\infty}$,

together with the map:

$$f\colon X_{S,p} \to X_{S,p}$$

given by:

$$f(x_1, x_2, \ldots, x_n) = (x_1^p, x_2^p, \ldots, x_n^p).$$

$N_S(p,r)$ is the number of elements x of $X_{S,p}$ with $f^r(x) = x$.

Some explanation:

Let x and y be elements of a field in which $p = 0$; then one has $(x + y)^p = x^p + y^p$.

For an integer a, considered as an element of a field in which $p = 0$, we have:

$a^p = (1+1+\cdots+1)^p = (1^p+1^p+\cdots+1^p) = a$.

$\mathbf{F}_{p^r}$ is the set of x in $\mathbf{F}_{p^\infty}$ satisfying $x^{p^r} = x$.

$(f_i(x_1, x_2, \ldots, x_n))^p = f_i(x_1^p, x_2^p, \ldots, x_n^p)$, Lefschetz's fixed point formula:

For X a compact complex manifold and $f\colon X \to X$ differentiable, we have:

$$|\{x \in X \mid f(x) = x\}| = \sum_{i=0}^{\dim(X)} (-1)^i \mathrm{tr}(f^* | \mathrm{H}^i(X)),$$

provided the fixed points are non-degenerate.