Chapter 6

Developments and Open Problems

“Une pierre
deux maisons
trois ruines
quatre fossoyeurs
un jardin
des fleurs
un raton laveur”
Jacques Prévert

The tone and the level of the prerequisites of this final chapter differ from the previous chapters. Here we will present a panorama—necessarily partial and one-sided—of some important research areas in number theory. In particular, every section contains at least one open problem. This last chapter also includes many statements whose proofs surpass the level of this book but which also provide an opportunity to combine and expand on the mathematics introduced in the preceding chapters. The chosen themes—the number of solutions of equations over a finite field, algebraic geometry, $p$-adic numbers, Diophantine approximation, the $a,b,c$ conjecture and generalizations of zeta and $L$-series—have all been introduced, either implicitly or explicitly, in the previous chapters. We will freely use themes from algebraic geometry and Galois theory, described respectively in Appendices B and C.
1. The Number of Solutions of Equations over Finite Fields

In order to deepen your understanding of this section, you could first consult Weil’s original article [78] and Appendix C of [35].

The successes brought about by the introduction of the Riemann $\zeta$ function, then the Dedekind $\zeta_K$ function, naturally lead to the study of following generalization. We consider a finitely generated ring $A$ over $\mathbb{Z}$ or $\mathbb{F}_p$, in other words $A := \mathbb{Z}[t_1, \ldots, t_n] = \mathbb{Z}[X_1, \ldots, X_n]/I$ or $A := \mathbb{F}_p[t_1, \ldots, t_n] = \mathbb{F}_p[X_1, \ldots, X_n]/I$. It is easy to see that if $p$ is a maximal ideal in $A$, then $A/p$ is a finite field. We denote by $N_p = \text{card}(A/p)$. Letting $M_A$ be the set of maximal ideals in $A$, we can therefore set

$$\zeta_A(s) := \prod_{p \in M_A} \left(1 - N_p^{-s}\right)^{-1}.$$ 

If $A = \mathbb{Z}$, we recover the Riemann $\zeta$ function, and if $A = \mathcal{O}_K$ (for a number field $K$), we recover the Dedekind $\zeta_K$ function. Furthermore, in the case where $\mathbb{Z} \subset A$, every maximal ideal $p$ contains exactly one prime number since $p \cap \mathbb{Z}$ is a non-zero prime ideal. If we denote by $M_{A,p}$ the maximal ideals which contain $p$ (this set is in bijection with the maximal ideals of $A/pA$), then $M_A = \bigcup_{p \in M_{A,p}} M_{A,p}$, and we can write:

$$\zeta_A(s) = \prod_p \prod_{p \in M_{A,p}} \left(1 - N_p^{-s}\right)^{-1} = \prod_p \zeta_{A/pA}(s).$$

We can therefore, at least momentarily, concentrate on the case $A = \mathbb{F}_p[t_1, \ldots, t_n] = \mathbb{F}_p[X_1, \ldots, X_n]/I$ (we will come back to the case of varieties defined over $\mathbb{Q}$ or $\mathbb{Z}$ in the last section of this chapter). Let $V$ denote the affine variety defined by the ideal $I$ in $A^n$. The maximal ideals of $\overline{\mathbb{F}}_p[t_1, \ldots, t_n]$ correspond to points of $V(\overline{\mathbb{F}}_p)$, and the maximal ideals of $A = \mathbb{F}_p[X_1, \ldots, X_n]/I$ correspond to conjugacy classes under $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ in $V(\overline{\mathbb{F}}_p)$. We denote by $|V|$ the set of these classes\footnote{In the language of Grothendieck schemes, we are talking about closed points of the scheme $V = \text{spec}(A)$.}. If $x \in V(\overline{\mathbb{F}}_p)$ and if $p$ is the corresponding maximal ideal in $A$, then $N_p = p^{\deg(x)}$ where $\deg(x) := [\mathbb{F}_p(x) : \mathbb{F}_p]$. Since a point in $V(\mathbb{F}_{p^m})$ has a field of definition equal to $\mathbb{F}_{p^d}$ where $d$ divides $m$, we see that

$$\text{card } V(\mathbb{F}_{p^m}) = \sum_{x \in |V|, \deg(x) \mid m} \deg(x).$$

We thus obtain a second expression for $\zeta_A(s)$: