Density and Dirichlet theorem

4.1 Density

Let P be the set of prime numbers. We have seen in a previous presentation that, when s tends to 1 (s being real >1) one has

$$\sum_{p \in P} \frac{1}{p^s} \sim \log \frac{1}{s-1}$$

Let A be a subset of P. One says that A has for density a real number K when the ratio

$$\left(\sum_{p \in A} \frac{1}{p^s} \right) \Big/ \left(\log \frac{1}{1-s} \right)$$

tends to K when $s \to 1$. The theorem on arithmetic progressions can be refined in the following way:

*) Theorem 2. Let $m \geq 1$ and let a be such that $(a, m) = 1$. Let P_a be the set of prime numbers such that $p \equiv a \pmod m$. The set P_a has density $1/\phi(m)$.
(In other words the prime numbers are "equally distributed" between the different classes modulo m which are prime to m.)

*) Corollary. The set P_a is infinite.

4.2 Lemmas

Let χ be a character of $G(m)$. Put

$$f_\chi(s) = \sum_{p \nmid m} \chi(p)/p^s,$$

this series being convergent for $s>1$.

*) Lemma 7. If $\chi=1$, then $f_\chi \sim \log \frac{1}{s-1}$ for $s \to 1$.

Indeed, f_1 differs from the series $\sum 1/p^s$ by a finite number of terms only.

*) Lemma 8. If $\chi \neq 1$, f_χ remains bounded when $s \to 1$,

We begin by considering the function $L(s,\chi)$. As previously seen, we can express it as

$$\prod_{p \in P} 1/(1-\chi(p)p^{-s}).$$

For $Re(s)>1$ each factor is of the form $1/(1-\alpha)$ with $|\alpha|<1$. We define $\log\left(\frac{1}{1-\alpha}\right)$ as $\sum_{n=1} \alpha^n/n$ ("principal" determination of the logarith) and we define $\log(L(s,\chi))$ by the series

$$\log(L(s,\chi)) = \sum \log \frac{1}{1-\chi(p)p^{-s}} \qquad (Re(s)>1)$$

$$= \sum_{p,n} \chi(p)^n/np^{ns}.$$

We now split $\log(L(s,\chi))$ into two parts:

$$\log(L(s,\chi)) = f_\chi(s) + F_\chi(s)$$

with

$$F_\chi(s) = \sum_{p,n\geq 2} \chi(p)^n/np^{ns}.$$

Theorem 1, together with corollary 2 of proposition 10, shows that $\log L(s,\chi)$ and $F_\chi(s)$ remain bounded when $s \to 1$. Hence the same holds for $f_\chi(s)$.

4.3 Proof of theorem 2

We have to study the behavior of the function

$$g_a(s) = \sum_{p \in P_a} \frac{1}{p^s}$$

for $s \to 1$.

*) Lemma 9. One has

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi} \chi(a)^{-1} f_\chi(s),$$

the sum being extended over all characters χ of $G(m)$.

We can rewrite $\sum \chi(a)^{-1} f_\chi(s)$ by replacing $f_\chi(s)$ by its definition:

$$\sum_{p \nmid m} \left(\sum_{\chi} \chi(a^{-1}) \chi(p) \right) p^{-s}.$$

But $\chi(a^{-1})\chi(p) = \chi(a^{-1}p)$. By the corollary to proposition 4, we have:

$$\sum_{\chi} \chi(a^{-1}p) = \begin{cases} \phi(m) & \text{if } a^{-1}p \equiv 1 \pmod{m} \\ 0 & \text{otherwise.} \end{cases}$$

Hence we find the function $\phi(m)\, g_a(s)$.

Theorem 2 is now clear. Indeed, lemma 7 shows that $f_\chi(s) \sim \log \frac{1}{s-1}$ for $\chi = 1$, and lemma 8 shows that all other f_χ remain bounded. By lemma 9, we then see that $g_a(s) \sim \frac{1}{\varphi(m)} \log \frac{1}{s-1}$, and this means that the density of P_a is $\frac{1}{\varphi(m)}$.

4.4 An application

*) **Proposition 14.** Let a be an integer which is not a square. The set of prime numbers p such that $\left(\frac{a}{p}\right) = 1$ has density $1/2$.

We can assume that a is square-free. Let $m = 4|a|$, and let χ_a be the unique character modulo m such that

$$\chi_a(p) = \left(\frac{a}{p}\right) \quad \text{for all prime numbers not dividing } m.$$

Let $H \subset G(m)$ be the kernel of χ_a in $G(m)$. If p is a prime number not divisible by m, let $\bar{p}$ be its image in $G(m)$. We have $\left(\frac{a}{p}\right) = 1$ if and only if $\bar{p}$ is contained in H. By theorem 2 the set of prime numbers verifying this condition has for density the inverse of the index of H in $G(m)$, that is to say $\frac{1}{2}$.

*) **Corollary.** Let a be an integer. If the equation $X^2 - a = 0$ has a solution modulo p for almost all $p \in P$, it has a solution in $\mathbb{Z}$.

Remark: There are analogous results for other types of equations. For instance:

i) Let $f(X) = a_0 X^n + \cdots + a_n$ be a polynomial of degree n with integer coefficients, which is irreducible over $\mathbb{Q}$. Let K be the field generated by the roots of f and let $N = [K : \mathbb{Q}]$. One has $N \geq n$. Let P_f be the set of prime numbers p such that f "decomposes completely modulo p", One can prove that P_f has density $\frac{1}{N}$.
One can also give the density of the set P_f' of p such that the reduction of $f \pmod p$ has at least one root in $\mathbb{F}_p$; is is a number of the form q/N with $1 \leq q < N$.