1.3 Primes in arithmetic progression

Our first partial result towards Dirichlet's theorem introduces analytic approach. We prove that not only the two kinds of odd primes $p = 1 + 4n$ and $p = 3 + 4n$ are infinite in number, but that they are in a sense equidistributed: for both $a = 1$ and $a = 3$ we have, for $x > 1$,

$$\sum_{p=a+4n\le x} \frac{\log p}{p} = \frac{1}{2}\sum_{p\le x}\frac{\log p}{p} + O(1) = \frac{\log x}{2} + O(1)\ .$$

An important tool in the proof is *Abel's inequality*, Proposition B.1.7: if $a_i \in \mathbb{C}, b_i \in \mathbb{R}$, $i = 1, 2, \ldots, n$, and $b_1 \ge b_2 \ge \cdots \ge b_n \ge 0$, then

$$\left|\sum_{i=1}^{n} a_i b_i\right| \le Ab_1,\ \ A = \max_{1\le m\le n} |a_1 + a_2 + \cdots + a_m|\ .$$

We apply it four times or so. Important is also the function $\chi :\ \mathbb{Z} \to \{-1, 0, 1\}$,

$$\chi(n) = \begin{cases} (-1)^{(n-1)/2} & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even}\ . \end{cases}$$

So $\chi(4n+1) = 1$, $\chi(4n+3) = -1$ and $\chi(2n) = 0$. Two crucial properties, both immediate from the definition, are

$$\left|\sum_{n\in I}\chi(n)\right| \le 1 \ \text{ and }\ \chi(ab) = \chi(a)\chi(b)\ ,$$

where $I \subset \mathbb{Z}$ is any finite interval and $a, b \in \mathbb{Z}$. The proof only uses finite sums, with the exception of

$$L(1,\chi) := \sum_{n=1}^{\infty}\frac{\chi(n)}{n}\ .$$

This infinite series conditionally converges by Abel's inequality ($a_i = \chi(i), b_i = 1/i$), which further gives

$$L(1,\chi) = 1 + \sum_{n=3}^{\infty}\frac{\chi(n)}{n} \ge 1 - \frac{1}{3} = \frac{2}{3}\ .$$

In particular, $L(1,\chi) \ne 0$.

Proposition 1.3.1 *For $x > 1$, let*

$$S = S(x) := \sum_{2<p\le x}\frac{\log p}{p} = \log x + O(1)$$

(by Theorem 1.2.8). Then for $x > 1$ we have

$$\sum_{p=1+4n\le x}\frac{\log p}{p} = \frac{S}{2} + O(1) \quad \textit{and} \quad \sum_{p=3+4n\le x}\frac{\log p}{p} = \frac{S}{2} + O(1)\ .$$

Proof. We denote the first sum by $A = A(x)$ and the second by $B = B(x)$. Then

$$S = A + B \quad \text{and} \quad C = C(x) := A - B = \sum_{p \le x} \frac{\chi(p) \log p}{p} \; .$$

As $A = (S + C)/2$ and $B = (S - C)/2$, it suffices to show that $C = O(1)$ for $x > 1$.

We have, for $x > 1$,

$$O(1) = \sum_{n \le x} \frac{\chi(n) \log n}{n} = \sum_{n \le x} \frac{\chi(n)}{n} \sum_{d \,|\, n} \Lambda(d) = \sum_{d \le x} \frac{\chi(d)\Lambda(d)}{d} \sum_{e \le x/d} \frac{\chi(e)}{e} \; .$$

The first equality follows by Abel's inequality ($a_i = \chi(i), b_i = i^{-1} \log i$), the second by Proposition 1.2.7 and the third by changing summation order and using complete multiplicativity of χ. By Abel's inequality ($a_i = \chi(i), b_i = 1/i$), the last sum equals $L(1, \chi) - \sum_{e > x/d} \chi(e)/e = L(1, \chi) + O(d/x)$. Thus, by Proposition 1.2.7,

$$O(1) = L(1, \chi) \sum_{d \le x} \frac{\chi(d)\Lambda(d)}{d} + O(1/x) \sum_{d \le x} \Lambda(d) = L(1, \chi) \sum_{d \le x} \frac{\chi(d)\Lambda(d)}{d} + O(1) \; .$$

Since $L(1, \chi) \neq 0$, we may divide by it and get

$$\sum_{d \le x} \frac{\chi(d)\Lambda(d)}{d} = O(1) \; .$$

We split the sum in two, over $d = p \le x$ and $d = p^k \le x$ with $k \ge 2$, as in the proof of Proposition 1.2.7. The second sum is bounded by a convergent series, and we have the desired conclusion

$$C = \sum_{p \le x} \frac{\chi(p) \log p}{p} = O(1) \; .$$

□

The same argument works for primes of the forms $p = 1 + 3n$ and $p = 2 + 3n$; we replace χ with the mapping χ' given by $\chi'(3n) = 0$, $\chi'(3n + 1) = 1$ and $\chi'(3n + 2) = -1$. In Chapter 2 we extend it to general primes $p = a + mn$.

The second partial result towards Dirichlet's theorem demonstrates power of algebraic methods. We show that any arithmetic progression

$$1 + mn, \; n = 1, 2, \ldots ,$$

contains infinitely many primes. We start with the case when m itself is a prime number, and demonstrate by a simple argument existence of one prime of the form $1 + mn$. Let p be a prime dividing $2^m - 1 \ge 3$. Thus $2^m \equiv 1$ modulo p, and as $2^1 \not\equiv 1$ modulo p, 2 has multiplicative order m modulo p. By Fermat's little theorem, $2^{p-1} \equiv 1$ modulo p ($p \neq 2$). Hence m divides $p - 1$, which we wanted to show. We have obtained the next result.