

ARITHMETIC FUNCTIONS (MA2316, TENTH WEEK)

VLADIMIR DOTSENKO

This week, we shall start discussing arithmetic functions. It is a somewhat vague term, referring to functions defined for all positive integers and having something to do with arithmetic properties of their argument.

Let us discuss some examples of arithmetic functions.

Example 1. *The Euler's totient function ϕ which we already encountered before: its value at an integer n is equal to the number of integers k between 1 and n that are coprime to n .*

Example 2. *The Möbius function μ : its value at an integer n is equal to 0 if n is not square-free, and is equal to $(-1)^k$ if n is square-free with exactly k different prime divisors.*

The Möbius function is probably best known to mathematicians outside number theory, for it appears in the the statement of the following celebrated result.

Theorem 1 (Möbius inversion formula). *Suppose that for two functions $f, g: \mathbb{N} \rightarrow \mathbb{C}$ we have*

$$f(n) = \sum_{d|n} g(d).$$

Then we can recover values of g as

$$g(n) = \sum_{d|n} \mu(d) f(n/d).$$

Proof. Let us note that for each $n > 1$ we have

$$\sum_{d|n} \mu(d) = 0.$$

Indeed, if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then the divisors d of n for which $\mu(d) \neq 0$ are precisely $p_{i_1} p_{i_2} \cdots p_{i_s}$; for such a divisor we have $\mu(d) = (-1)^s$, and there are $\binom{k}{s}$ divisors like that. Overall,

$$\sum_{d|n} \mu(d) = \sum_{1 \leq s \leq k} \binom{k}{s} (-1)^s = (1 - 1)^k = 0,$$

since $n > 1$ implies $k > 0$. Therefore,

$$\sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(d) \sum_{r|n/d} g(r) = \sum_{r|n} g(r) \sum_{d|n/r} \mu(d) = g(n),$$

since by the above computation we have $\sum_{d|n/r} \mu(d) = 0$ unless $n/r = 1$, that is $r = n$. □

Corollary. *If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, we have*

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Proof. Indeed, we know from previous lectures that

$$\sum_{d|n} \phi(d) = n.$$

Therefore by Möbius inversion, we have

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \mu(d) \frac{1}{d} = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

□

Example 3. The number-of-divisors function τ : its value at an integer n is equal to the number of positive integer divisors of n .

Example 4. The sum-of-divisors function σ : its value at an integer n is equal to the sum of all positive integer divisors of n .

Example 5. The von Mangoldt function Λ : its value at an integer n is equal to 0 if n is not a prime power, and is equal to $\ln p$ if $n = p^k$ for some prime p and some integer $k > 0$.

Example 6. The prime number counting function π : its value at an integer n is equal to the number of primes not exceeding n .

Many arithmetic functions behave irregularly, e.g. do not exhibit any monotonic or “continuous” behaviour (as far as “continuous” goes for functions defined on a discrete set!), so it is often beneficial to consider their “mean values”, which for a function α produces another slightly more regular function M_α defined by the formula

$$M_\alpha(n) = \frac{1}{n} \sum_{k=1}^n \alpha(k).$$

There are two important arithmetic functions that have a mean value flavour, the Chebyshev θ function defined as

$$\theta(n) = \sum_{p \leq n, p \text{ prime}} \ln p,$$

and the Chebyshev ψ function, which is the sum function of von Mangoldt function:

$$\psi(n) = \sum_{k \leq n} \Lambda(k) = n M_\Lambda(n).$$

These functions are the additive versions of two functions that we considered in the beginning of the course; indeed,

$$e^{\theta(n)} = \prod_{p \leq n, p \text{ prime}} p,$$

and

$$e^{\psi(n)} = \text{lcm}(1, 2, \dots, n).$$

Let me formulate several statements about arithmetic functions, and indicate proofs or meaning or relevance (or all of the above) of these statements. Everywhere below

- $f(n) \sim g(n)$ means that $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1$,
- $f(n) = O(g(n))$ means that for some n_0 and some C we have $|f(n)| \leq C|g(n)|$ for all $n > n_0$,
- $f(n) = o(g(n))$ means that for each $\epsilon > 0$, there exists n_0 such that we have $|f(n)| \leq \epsilon|g(n)|$ whenever $n > n_0$.

In general, O -estimates are more precise than o -estimates, and easier to work with, e.g. can under some assumptions pulled out of integrals and sums. For instance, $f(n) = o(1)$ just means that $f(n)$ tends to zero, while $f(n) = O(\frac{1}{n})$ gives some idea about the rate of convergence.

Next week we are going to prove the following classical results.

Theorem 2. *We have*

$$M_\tau(n) = \ln n + O(1).$$

Theorem 3. *We have*

$$M_\phi(n) = \frac{3n}{\pi^2} + O(\ln n).$$

Theorem 4. *We have*

$$\theta(n) = \psi(n) + O(\sqrt{n})$$

and

$$\pi(n) = \frac{\psi(n)}{\ln n} + O\left(\frac{n}{(\ln n)^2}\right).$$