# A Combinatorial Construction used in Number Theory

Wim Ruitenburg

These are notes useful for our Number Theory class.

## 1 Power Series as an Example

We precede the intended topic by first making a comparison. Recall that we can compute with power series

$$f = a_0 + a_1X + a_2X^2 + a_3X^3 + \ldots = \sum_{n\geq 0} a_nX^n$$

over the real numbers in the expected way. We add or subtract power series coefficient by coefficient. So

$$\begin{aligned}&(a_0 + a_1X + a_2X^2 + \ldots) + (b_0 + b_1X + b_2X^2 + \ldots) =\\ &= (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \ldots =\\ &= \textstyle\sum_{n\geq 0}(a_n + b_n)X^n,\end{aligned}$$

and

$$\begin{aligned}&-(a_0 + a_1X + a_2X^2 + \ldots) =\\ &= (-a_0) + (-a_1)X + (-a_2)X^2 + \ldots =\\ &= \textstyle\sum_{n\geq 0}(-a_n)X^n.\end{aligned}$$

We multiply power series by the usual 'convolution' product

$$\begin{aligned}&(a_0 + a_1X + a_2X^2 + \ldots)(b_0 + b_1X + b_2X^2 + \ldots) =\\ &= (a_0b_0) + (a_1b_0 + a_0b_1)X + (a_2b_0 + a_1b_1 + a_0b_2)X^2 + \ldots =\\ &= \textstyle\sum_{n\geq 0}(\sum_{j+k=n} a_jb_k)X^n.\end{aligned}$$

We can also divide, finding the (multiplicative) inverse of a power series. Recall that the inverse of a number $a$ is that number $b$ for which both $ab = 1$ and $ba = 1$. We often write $a^{-1}$ for this unique $b$. Recall that for real numbers $\mathbb{R}$ all nonzero numbers have a (multiplicative) inverse. For example, 0.5 is the inverse of 2, and therefore also written as $0.5 = 1/2$ or as $0.5 = \frac{1}{2}$ or as $0.5 = 2^{-1}$. However, the number 0 has no such inverse. Among power series over $\mathbb{R}$ we find that many have multiplicative inverses, though not all. For example, $1 - X$ is invertible with inverse $\sum_{n\geq 0} X^n$, since

$$(1 - X)(1 + X + X^2 + X^3 + \ldots) = 1,$$

while $X$ has no inverse. In fact, more generally, a power series $a_0+a_1X+a_2X^2+a_3X^3+\ldots$ is invertible exactly when $a_0$ is invertible (try to prove this!). Thus $(1 - X)^{-1}$ exists, while $X^{-1}$ does not exist, among the power series.

There is no relevant information lost when we write power series as infinite sequences of numbers, like

$$\begin{aligned}&f = (a_0, a_1, a_2, a_3, \ldots) = (a_n)_{n\geq 0} \quad \text{and}\\ &g = (b_0, b_1, b_2, b_3, \ldots) = (b_n)_{n\geq 0}.\end{aligned}$$

So

$$\begin{aligned}&f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots) = (a_n + b_n)_{n\geq 0} \quad \text{and}\\ &fg = (a_0b_0, a_1b_0 + a_0b_1, a_2b_0 + a_1b_1 + a_0b_2, \ldots = (\textstyle\sum_{j+k=n} a_jb_k)_{n\geq 0}.\end{aligned}$$

We have all these familiar nice[1] properties like $(fg)h = f(gh)$ and $f(g+h) = fg + fh$. For those who remember 'Foundations of Mathematics', $f$ and $g$ are in essence functions from $\mathbb{Z}^{\geq 0}$ to $\mathbb{R}$ or, in other words, elements of $\mathbb{R}^{(\mathbb{Z}^{\geq 0})}$. Sum and product are also defined by

$$(f+g)(n) = f(n) + g(n) \text{ for all } n \geq 0, \quad \text{and}$$
$$(fg)(n) = \sum_{j+k=n} f(j)g(k) \text{ for all } n \geq 0.$$

We also talk about $f$ and $g$ as sequence $f$ or sequence $g$. In such cases we usually write

$$(f+g)_n = f_n + g_n \text{ for all } n \geq 0, \quad \text{and}$$
$$(fg)_n = \sum_{j+k=n} f_j g_k \text{ for all } n \geq 0.$$

## 2 The Dirichlet Product

Given the *example* of power series in Section 1, we now consider a different but similar such nice structure. Let us consider functions from $\mathbb{N} = \mathbb{Z}^{>0}$ to $\mathbb{R}$ or, in other words, elements of $\mathbb{R}^{\mathbb{N}}$. Its elements are written as

$$s = (s_1, s_2, s_3, s_4, \ldots) = (s_n)_{n>0} \quad \text{or}$$
$$t = (t_1, t_2, t_3, t_4, \ldots) = (t_n)_{n>0}.$$

Note that we do not have an $s_0$ or a $t_0$. We define addition and subtraction as we did before in the power series case. So for example

$$s + t = (s_1 + t_1, s_2 + t_2, s_3 + t_3, \ldots) = (s_n + t_n)_{n>0}.$$

We define a *new* product, called Dirichlet product or Dirichlet convolution, by

$$s * t = (\textstyle\sum_{de=n} s_d t_e)_{n>0},$$

also written

$$s * t = (\sum_{d|n} s_d t_{\frac{n}{d}})_{n>0}.$$

This product has nice properties like

$$s * t = t * s,$$
$$s * (t+u) = s * t + s * u, \quad \text{and}$$
$$s * (t * u) = (s * t) * u.$$

For this last equation, observe that both sides are equal to

$$s * (t * u) = (\textstyle\sum_{def=n} s_d t_e u_f)_{n>0}.$$

Consider the following sequences

$$O = (0, 0, 0, 0, 0, \ldots),$$
$$I = (1, 0, 0, 0, 0, \ldots), \quad \text{and}$$
$$E = (1, 1, 1, 1, 1, \ldots).$$

We easily verify that for all $s$ we have

$$s * O = O,$$
$$s * I = s, \quad \text{and}$$
$$s * E = (\textstyle\sum_{de=n} s_d)_{n>0} = (\sum_{d|n} s_d)_{n>0}.$$

[1] Commutative ring properties and more, from abstract algebra.

So $O$ plays a role like the zero number 0 among $\mathbb{R}$ or $\mathbb{Z}$, and $I$ plays a role like the unity number 1 among $\mathbb{R}$ or $\mathbb{Z}$. Multiplication by $E$ is of special interest in number theory.

When does a sequence $s$ have a multiplicative inverse, that is, have an element $x = (x_1, x_2, x_3, x_4, \ldots)$ such that $s * x = I$? Such $x$ may be called $x = s^{-1}$. Given $s$, to compute $x$ we have to find values $x_1, x_2, x_3, \ldots$ satisfying the system of equations

$$\begin{aligned}
&s_1x_1 = 1,\\
&s_2x_1 + s_1x_2 = 0,\\
&s_3x_1 + s_1x_3 = 0,\\
&s_4x_1 + s_2x_2 + s_1x_4 = 0,\\
&s_5x_1 + s_1x_5 = 0,\\
&s_6x_1 + s_3x_2 + s_2x_3 + s_1x_6 = 0,\\
&\ldots,\\
&\textstyle\sum_{de=n} s_d x_e = 0,\\
&\ldots.
\end{aligned}$$

So $x_1$ exists exactly when $s_1$ is invertible. Observe that if $x_1, x_2, \ldots, x_{n-1}$ can be found for some $n > 1$ (so $s_1$ is invertible), then $x_n$ can also be computed by moving all but the last term to the right of the equation, and divide by $s_1$. So if $n > 1$, then

$$x_n = -s_1^{-1} \textstyle\sum_{de=n, e<n} s_d x_e = -s_1^{-1} \sum_{de=n, 1<d} s_d x_e.$$

Thus sequence $s$ is invertible exactly when its term $s_1$ is invertible.

Some examples about multiplicative inverses.

First example. Let $s = (s_1, 0, 0, 0, 0, \ldots)$ with $s_1$ invertible. Since $0 = s_2 = s_3 = s_4 = \ldots$, we easily compute that $s^{-1} = (s_1^{-1}, 0, 0, 0, 0, \ldots)$.

Second example. Let $s = (0, 1, 0, 0, 0, \ldots)$. Since the first term of the series equals 0, this $s$ is not invertible.

Third example. Let $S_2 = (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, \ldots)$ be such that $s_n = 1$ when $n$ is of the form $2^k$, and $s_n = 0$ otherwise. We leave it as a non-trivial exercise to show that $S_2^{-1} = (1, -1, 0, 0, 0, 0, \ldots)$, that is, $x_1 = 1$ and $x_2 = -1$ and all other $x_i = 0$.

Fourth example. Let $p$ be prime. Let sequence $S_p$ be such that $s_n = 1$ when $n$ is of the form $p^k$, and $s_n = 0$ otherwise. We leave it as exercise to show that $S_p^{-1}$ is such that $x_1 = 1$ and $x_p = -1$ and all other $x_i = 0$.

We encounter more examples of inverses farther below.

Some further examples of sequences are:

1. $\tau$ with $\tau(n)$ equal to the number of divisors of $n$, So $\tau = (1, 2, 2, 3, 2, 4, 2, \ldots)$ where, for example, $\tau(4) = 3$ since $n = 4$ has the 3 divisors 1, 2, and 4.

2. $\sigma$ with $\sigma(n)$ equal to the sum of the divisor of $n$. So $\sigma = (1, 3, 4, 7, 6, 12, 8, \ldots)$ where, for example, $\sigma(6) = 12$ since $n = 6$ has the sum of divisors $1+2+3+6 = 12$.

3. $\mu$, the Möbius inversion function, is defined by

   - $\mu(1) = 1$,
   - $\mu(n) = 0$ if $p^2|n$ for some prime $p$, and
   - $\mu(n) = (-1)^k$ if $n$ is a product of $k > 0$ different prime numbers $n = p_1p_2p_3 \ldots p_k$.

4. $\varphi$, Euler's totient function, is defined by

   - $\varphi(1) = 1$, and

- $\varphi(n) = n(1-1/p_1)(1-1/p_2)(1-1/p_3)\dots(1-1/p_k)$, where $n$ has standard prime decomposition $n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\dots p_k^{a_k}$. Note that $\varphi(n) = (p^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1})(p_3^{a_3} - p_3^{a_3-1})\dots(p_k^{a_k} - p_k^{a_k-1})$. It is shown elsewhere that $\varphi(n)$ equals the number of elements of $\{0, 1, 2, 3, \dots, n-1\}$ that are relatively prime to $n$.

5. For each $s \in \mathbb{R}$ a sequence $N_s$ with $N_s(n) = n^s$ (we may even choose $s \in \mathbb{C}$). We may write $N$ as short for $N_1$. We have $N_0 = E$.

6. For each subset $C \subseteq \mathbb{N}$ a sequence $E_C$ with

   - $E_C(n) = 1$ if $n \in C$, and
   - $E_C(n) = 0$ if $n \notin C$.

   If $C = \emptyset$ we have $E_C = O$, if $C = \mathbb{N}$ we have $E_C = E$, and if $C = \{1\}$ we have $E_C = I$. If $C = \{p^k \mid k \geq 0\}$ for a prime $p$, then $E_C = S_p$

A sequence $s$ is called *multiplicative* if $s(mn) = s(m)s(n)$ for all relatively prime pairs $m$ and $n$. We easily see that $O$, $I$, $E$, all $S_p$, $\tau$, $\sigma$, $\mu$, $\varphi$, and all $N_s$ are multiplicative. Some of these are *completely multiplicative* in that $s(mn) = s(m)s(n)$ for all $m$ and $n$. So $O$,$I$, $E$, all $S_p$, and all $N_s$ are completely multiplicative.

If $s$ is multiplicative and $n$ has prime number decomposition $n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\dots p_k^{a_k}$, then

$$s(n) = s(p_1^{a_1})s(p_2^{a_2})s(p_3^{a_3})\dots s(p_k^{a_k}).$$

So if $s$ and $t$ are multiplicative and $s(p^a) = t(p^a)$ for all primes $p$ and $a \geq 0$, then $s = t$.

We leave it as an exercise to show that if $s$ and $t$ are multiplicative, then so is $s * t$. As another a bit more difficult exercise, if $s$ is multiplicative and invertible, then $s^{-1}$ is also multiplicative.

Some easy applications. Since $(E * \mu)(1) = 1$, and $(E * \mu)(p^a) = 0$ for all prime powers $p^a > 1$, we have $E * \mu = I$. Clearly $\tau = E * E$. So $\tau * \mu = E * E * \mu = E * I = E$, and therefore

$$\textstyle\sum_{de=n} \tau(d)\mu(e) = 1, \text{ for all } n.$$

Similarly, $\sigma = N * E$. So $\sigma * \mu = N$, and therefore

$$\textstyle\sum_{de=n} \sigma(d)\mu(e) = n, \text{ for all } n.$$

We easily compute that $\varphi(1) = (N * \mu)(1) = 1$ and $(\varphi)(p^a) = (N * \mu)(p^a) = p^a - p^{a-1}$ for all prime powers $p^a > 1$. So $\varphi = N * \mu$, so also $\varphi * E = N$, and therefore

$$\textstyle\sum_{de=n} \varphi(d) = n, \text{ for all } n.$$