1. Recursive functions.

For each $n \in \mathbb{N}$ we let
$$\mathbb{N}^n$$
be $\{\emptyset\}$ if $n = 0$ and we let it be the set of n-tuples $(x_1, \ldots, x_n)$ where $x_i \in \mathbb{N}$ for $i \in \{1, \ldots, n\}$. For $m, n \in \mathbb{N}$ we let
$$\mathbb{N}^n_m$$
be the set of f such that $f : \mathbb{N}^n \to \mathbb{N}^m$.

Note that
$$\mathbb{N}^0_m \ni f \mapsto f(\emptyset) \in \mathbb{N}^m$$
is univalent with range $\mathbb{N}^m$; in what follows we shall identify $\mathbb{N}^0_m$ with $\mathbb{N}^m$ via this mapping.

Definition 1.1. Suppose $A \subset \mathbb{N}^n$. We define
$$1_A \in \mathbb{N}^n$$
by setting
$$1_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A; \end{cases}$$
we call 1_A the **indicator function of** A.

Suppose $R \in \mathbb{N}^n_1$. We say R is **logical** if $R(x) \in \{0, 1\}$ whenever $x \in \mathbb{N}^n$. Evidently,
$$R = 1_{\{x \in \mathbb{N}^n : R(x) = 1\}}$$
if R is logical. We let
$$\mathbb{L}^n$$
be the set of $R \in \mathbb{N}^n$ such that R is logical. Evidently, the members of $\mathbb{L}^n$ are the indicator functions of subsets of $\mathbb{N}^n$.

If $R, S \in \mathbb{L}^n$ we define
$$\sim R, \quad R \vee S, \quad R \wedge S, \quad R \to S, \quad R \leftrightarrow S$$
in the natural way; we note that all these functions belong to $\mathbb{L}^n$.

We define
$$\mathrm{Z} \in \mathbb{N}^1_1 \quad \text{and} \quad \mathrm{N} \in \mathbb{N}^1_1$$
requiring that
$$\mathrm{Z}(x) = 0 \quad \text{and} \quad \mathrm{N}(x) = x + 1 \quad \text{for } x \in \mathbb{N}.$$
Whenever $n, i \in \mathbb{N}^+$ and $1 \le i \le n$ we define
$$\mathrm{U}^n_i \in \mathbb{N}^n_1$$
by requiring that
$$\mathrm{U}^n_i(x) = x_i \quad \text{for } x = (x_1, \ldots, x_n) \in \mathbb{N}^n.$$

Suppose $n, m \in \mathbb{N}$, $l_1, \ldots, l_m \in \mathbb{N}$ and $f_i \in \mathbb{N}^n_{l_i}$, $i = 1, \ldots, m$. We define
$$(f_1, \ldots, f_m) \in \mathbb{N}^n_{\sum_{i=1}^m l_i},$$
the **concatenation of** $f_1, \ldots, f_m$, by letting
$$(f_1, \ldots, f_m)(x) = (f_1(x), \ldots, f_m(x)) \quad \text{for } x \in \mathbb{N}^n.$$

Suppose $m \in \mathbb{N}$, $n_1, \ldots, n_m \in \mathbb{N}$, $N_1, \ldots, N_m \in \mathbb{N}$ $f_i \in \mathbb{N}^{n_i}_{l_i}$, $i = 1, \ldots, m$. We define

$$f_1 \times \cdots \times f_m \in \mathbb{N}^N_M \quad N = \sum_{i=1}^m n_i,\ M = \sum_{i=1}^m N_i,$$

the **product** $f_1, \ldots, f_m$, by letting

$$(f_1 \times \cdots \times f_m)(x_1, \ldots, x_m) = (f_1(x), \ldots, f_m(x)) \quad \text{for } x \in \mathbb{N}^{\sum_{i=1}^m n_i}.$$

Whenever $n \in \mathbb{N}^n_1$, $h \in \mathbb{N}(n+1, 1)$ and $f \in \mathbb{N}^{n+1}_1$ we say f **is obtained from** g **and** h **by recursion** if

$$f(x, 0) = g(x) \quad \text{for } x \in \mathbb{N}^n$$

and

$$f(x, y+1) = h(x, y, f(x, y)) \quad \text{for } y \in \mathbb{N} \text{ and } x \in \mathbb{N}^n.$$

Suppose $g \in \mathbb{N}^{n+1}_1$. We say g is **ample** if

$$\{y \in \mathbb{N} : g(x, y) = 0\} \neq \emptyset \quad \text{for } x \in \mathbb{N}^n$$

in which case we define

$$\mu(g) \in \mathbb{N}^n_1$$

by requiring that

$$\mu(g)(x) = \min\{y : g(x, y) = 0\}.$$

One calls $\mu(g)$ the **minimalization of** g. We will often write

$$f(x) = \mu_y g(x, y) \quad \text{for } x \in \mathbb{N}^n$$

if $f = \mu(g)$.

Definition 1.2. (See page 120 in Mendelson.) Suppose $m, n \in \mathbb{N}^n_m$. We say f is **primitive recursive** if one of the following holds:

(i) $m = 1 = n$ and either $f = \mathrm{Z}$ or $f = N$;
(ii) $m = 1$ and $f = \mathrm{U}^n_i$ for some $i \in \{1, \ldots, n\}$;
(iii) there are $l \in \mathbb{N}$, $g \in \mathbb{N}^n_l$ and $h \in \mathbb{N}^l_m$ such that g and h are primitive recursive and $f = g \circ h$;
(iv) there are $n, m \in \mathbb{N}$, $l_1, \ldots, l_m \in \mathbb{N}$ and, for each $i = 1, \ldots, m$, $g_i \in \mathbb{N}^n m_i$ such that g_i is primitive recursive and $f = (g_1, \ldots, g_m)$.
(v) g and h are primitive recursive and f is obtained from g and h by recursion.

We say f is **recursive** if one of (i)-(iv) above hold with "primitive recursive" replaced by "recursive" or if $m = 1$ and there is $g \in \mathbb{N}^{n+1}_1$ such that g is recursive, g is ample and $f = \mu(g)$.

Note the obvious circularity in these definitions. The "right" way to do it is to set up a language with appropriate production, parse trees, etc. We leave that to the interested reader.

If $A \subset \mathbb{N}^n$ we say A is **(primitive)recursive** if 1_A is (primitive)recursive.

1.1. **Let's make lots of recursive functions.** Suppose $n \in \mathbb{N}^+$ and $c \in \mathbb{N}^m$. We let

$$\mathrm{C}^n_c(x) = c \quad \text{for } x \in \mathbb{N}^n.$$

Suppose $m \in \mathbb{N}^+$. If $m = 1$ then $\mathrm{C}^n_0 = \mathrm{Z} \circ \mathrm{U}^n_1$. Since

$$\mathrm{C}^n_{c+1} = \mathrm{N} \circ \mathrm{C}^n_c$$

we see by induction on c that C^n_c is primitive recursive. If $m > 1$ then

$$\mathrm{C}^n_c = (\mathrm{C}^n_{c_1}, \ldots, \mathrm{C}^n_{c_m}).$$

For $x, y \in \mathbb{N}$ we let

$$\mathrm{A}(x, y) = x + y, \quad \mathrm{M}(x, y) = xy, \quad \mathrm{P}(x, y) = x^y;$$

we leave to the reader the simple exercise of using induction to show that each of these functions is primitive recursive. By induction one also sees that the $n \mapsto n!$ is primitive recursive.

I claim that

$$1_0 \in \mathbb{N}^1_1 \text{ is primitive recursive;}$$

indeed,

$$1_0(y + 1) = \mathrm{Z}(y, 1_0(y))$$

so our assertion follows by induction.

For $x, y \in \mathbb{N}$ we let

$$x \sim y = \begin{cases} x - y & \text{if } x \geq y, \\ 0 & \text{if } x < y. \end{cases}$$

Proposition 1.1. $(x, y) \mapsto x \sim y$ is primitive recursive.

Proof. We have $(x + 1) \sim 1 = \mathrm{U}^2_1(x, x \sim 1)$ so $x \mapsto x \sim 1$ is primitive recursive by induction. Since $x \sim (y + 1) = (x \sim y) \sim 1$ our assertion follows by induction. $\square$

If $R, S \in \mathbb{L}^n$ we have

$$\begin{aligned} \sim R &= 1 \sim R, \\ R \vee S &= (R + S) \sim (RS), \\ R \wedge S &= RS, \\ R \to S &= \sim R \vee S, \\ R \leftrightarrow S &= (R \to S) \wedge (S \to R). \end{aligned}$$

It follows that these five functions are primitive recursive if R and S are. This implies that if $A, B \subset \mathbb{N}^n$ are (primitive)recursive then so are $A \cup B$, $A \cap B$ and $A \sim B$.

We have

$$\begin{aligned} (y \leq x) &= 1_{\{0\}}(y \sim x), \\ (y \geq x) &= (x \leq y), \\ (x = y) &= ((x \leq y) \wedge (y \leq x)) \\ (x < y) &= ((x \leq y) \wedge (\sim (x = y))) \\ (x > y) &= (y < x) \end{aligned}$$

so all these logical functions of two variables are primitive recursive.

If $a \in \mathbb{N}$ then

$$1_{\{a\}}(x) = (x = a)$$

so $1_{\{a\}}$ is primitive recursive. If $a \in \mathbb{N}^n$ the

$$1_{\{a\}} = \Pi_{i=1}^{n} 1_{\{a_i\}}$$

so $1_{\{a\}}$ is primitive recursive.

If F is a finite subset of $\mathbb{N}^n$ then

$$1_F = \sum_{a \in F} 1_{\{a\}}$$

is primitive recursive.

We have

$$\max\{x, y\} = y + (x \sim y) \quad \text{and} \quad \min\{x, y\} = x + y - \max\{x, y\}$$

so these functions are primitive recursive.

Since

$$|x - y| = (x \sim y) + (y \sim x)$$

this function is primitive recursive.

We let

$$x \operatorname{mod} y \quad \text{and} \quad y/x$$

be, respectively, the remainder after division of y by x and the quotient of division of y by x. Since

$$x \operatorname{mod} (y + 1) = N(x \operatorname{mod} y) + 1_{\mathbb{N}^+}(|x - N(x \operatorname{mod} y)|)$$

and

$$(y + 1)/x = (y/x) + 1_{\{0\}}(|x - N(x \operatorname{mod} y)|)$$

we find that these functions are primitive recursive.

We will write

$$x \equiv y \mod z$$

if $x \operatorname{mod} z = y \operatorname{mod} z$.

We let

$$y|x = ((x \operatorname{mod} y) = 0)$$

and note that $y|x = 1$ if and only if y divides x.

Suppose $f \in \mathbb{N}_1^2$ is (primitive)recursive. Since

$$\sum_{y \leq z+1} f(x, y) = \sum_{y \leq z} + f(x, z) \quad \text{for } x, z \in \mathbb{N}$$

we find that

$$(x, z) \mapsto \sum_{y \leq z} f(x, y) \quad \text{if (primitive)recursive.}$$

It follows that

$$\mathrm{D}(y) = \sum_{x \leq y} 1_{\{0\}}(x \operatorname{mod} y),$$

which is the number of divisors of y, is primitive recursive. This in turn implies that the logical function

$$\Pr(x) = (\mathrm{D}(x) = 2) \wedge (x \neq 0) \wedge (x \neq 1)$$

is primitive recursive; note that $\Pr(x) = 1$ if and only if x is a prime.

Suppose $R \in \mathbb{L}^{n+1}$; consider

$$\begin{aligned}&\forall_{y<z}\, y\, R(x,z),\\ &\exists_{y<z}\, y\, R(x,z),\\ &\mu_{y<z}\, R(x,y);\end{aligned}$$

the definition of the first two as logical functions should be clear; the third is the function whose value at (x,z) is the least $y<z$ such that $R(x,y)=1$ if there is such a value and is z if no such value exists. They equal

$$\begin{aligned}&\Pi_{y<z} R(x,z),\\ &0<\sum_{y<z} R(x,z),\\ &\sum_{y<z} \Pi_{u\le y} R(x,z),\end{aligned}$$

respectively; it follows that they are (primitive)recursive if R is.

Theorem 1.1. Let

$$\mathrm{Pth} : \mathbb{N} \to \{p \in \mathbb{N} : \mathrm{Pr}(p) = 1\}.$$

be such that $\mathrm{Pth}(0) = 2$ and

$$\mathrm{Pth}(n+1) = \mu_{y \le \mathrm{Pth}(n)!+1}(\mathrm{Pth}(n) < y) \wedge \mathrm{Pr}(y).$$

Then Pth is primitive recursive and

$$\mathrm{Pth}(n+1) = \min\{p : \mathrm{Pr}(p) = 1 \text{ and } \mathrm{Pr}(n) < p\}.$$

Proof. The point here is that if p is a prime and q is the first prime after p then $q \le p! + 1$. □

For each $n \in \mathbb{N}$ we define

$$\alpha : \mathbb{N}^2 \to \mathbb{N}$$

by letting $\alpha(n,j) = 0$ if $n = 0$ and, if $n > 0$ letting

$$\alpha(n,j) = \mu_{m<n}(\mathrm{Pth}(j)^m | n) \wedge \sim (\mathrm{Pth}(j)^{m+1} | n)$$

and we define

$$\lambda : \mathbb{N} \to \mathbb{N}$$

be letting $\lambda(n) = 0$ if $n = 0$ and, if $n > 0$, letting

$$\lambda(n) = \sum_{m \le n} \mathrm{Pr}(m) \wedge (m|n) \wedge (n \ne 0).$$

By virtue of the foregoing, these functions are primitive recursive and, if $n > 0$,

$$n = \Pi_{i=0}^{\lambda(n)} \mathrm{Pth}(i)^{\alpha(n,i)}.$$

1.1.1. *The function* Γ. We let

$$\mathbb{N}^* = \bigcup_{n=0}^{\infty} \mathbb{N}^n.$$

We define

$$\Gamma : \mathbb{N}^* \to \mathbb{N}$$

by letting $\Gamma(\emptyset) = 0$ and letting

$$\Gamma(x) = 2^{n-1}\Pi_{i=1}^n \mathrm{Pth}(i)^{x_i} \quad \text{for } x \in \mathbb{N}^n.$$

Thus Γ is univalent with range equal $\mathbb{N}$. We say the $c \in \mathbb{N}$ is the **code of** $x \in \mathbb{N}^n$ if $\Gamma(x) = c$.

Definition 1.3. We let

$$\mathrm{Len}(x) = \lambda(x) = \alpha(x, 0) \quad \text{for } x \in \mathbb{N}.$$

We let

$$\mathrm{Cmp}(x, i) = \alpha(x, i) \quad \text{for } x \in \mathbb{N}.$$

We let

$$\mathrm{Sum}(x, i) = \sum_{1 \le j < i} \alpha(x, j) \quad \text{for } (x, i) \in \mathbb{N}^2.$$

Note that these functions are primitive recursive.

It follows that if $n \in \mathbb{N}^+$ and $x = (x_1, \ldots, x_n) \in \mathbb{N}^n$ then

$$\mathrm{Len}(x) = n;$$

$$x_i = \mathrm{Cmp}(x, i), \quad 1 \le i \le n;$$

and

$$\mathrm{Sum}(x, i) = \sum_{1 \le j < i} x_j, \quad 1 \le i \le n.$$

Remark 1.1. The introduction of Len and Cmp is purely cosmetic.

Definition 1.4. We define the function

$$\mathrm{GetSubStr} : \mathbb{N}^3 \to \mathbb{N}$$

as follows. Suppose $(x, i, l) \in \mathbb{N}^3$; if $1 \le i \le \mathrm{Len}(x)$, $0 < l$ and $i + l - 1 \le \mathrm{Len}(x)$ then

$$\mathrm{GetSubStr}(x, i, l) = \Gamma(x_i, \ldots, x_{i+l-1});$$

otherwise $\mathrm{GetSubStr}(x, i, l) = 0$.

We define the logical function

$$\mathrm{IsSubStr} : \mathbb{N}^4 \to \{0, 1\}$$

by requiring that $\mathrm{IsSubStr}(x, y, i, l) = 1$ for $(x, y, i, l) \in \mathbb{N}^4$ if and only if

$$\mathrm{GetSubStr}(x, i, l) = y.$$

Proposition 1.2. GetSubStr and IsSubStr are recursive.

Exercise 1.1. Prove this.

1.1.2. *"Course of values" recursion.* See pp. 129 and 130 in Mendelson.

For $f \in \mathbb{N}^{n+1}$ we define
$$\Lambda(f) \in \mathbb{N}^{n+1}$$
by letting $\Lambda(f)(x,0) = 0$ and letting
$$\Lambda(f)(x,y) = \Gamma(f(x,0),\ldots,f(x,y-1)) \quad \text{for } y > 0.$$
Note that
$$\Lambda(f)(x,y) = \Lambda(f)(x,y-1)\mathrm{Pth}(y)^{f(y)}.$$

Proposition 1.3. Suppose $n \in \mathbb{N}$, $h(x,y,z)$, $(x,y,z) \in \mathbb{N}^n \times \mathbb{N} \times \mathbb{N}$, is (primitive)recursive and $f(x,y)$, $(x,y) \in \mathbb{N}^n \times \mathbb{N}$ is such that
$$f(x,y) = h(x,y,\Lambda(f)(x,y)) \quad \text{for } (x,y) \in \mathbb{N}^n \times \mathbb{N}.$$
Then $\Lambda(f)$ and, consequently, f are (primitive)recursive.

Proof. We have
$$\Lambda(f)(x,0) = \Gamma(\emptyset) = 0$$
and
$$\Lambda(f)(x,y+1) = \Lambda(f)(x,y)\mathrm{Pth}(y)^{f(x,y)} = \Lambda(f)(x,y)\mathrm{Pth}(y)^{h(x,y,\Lambda(f)(y))}.$$
$\square$

For each $x, y \in \mathbb{N}$ we define
$$x * y \in \mathbb{N}$$
to be the code of the concatenation of the tuple with code x with the tuple with code y. One easily checks (see pp. 126 and 127 in Mendelson) that $(x,y) \mapsto x * y$ is primitive recursive and that
$$(x * y) * z = x * (y * z) \quad \text{for } x,y,z \in \mathbb{N}.$$

Example 1.1. (The Fibonacci sequence. Let $f(0) = 0, f(1) = 1, f(2) = 1$ and, for $y \geq 3$, let
$$f(y) = f(y-1) + f(y-2) = \mathrm{Cmp}(\Lambda(f)(y), y-1) + \mathrm{Cmp}(\Lambda(f)(y), y-2).$$
Let
$$h(y,z) = (y = 1) + (y = 2) + \mathrm{Cmp}(y, z \sim 1) + \mathrm{Cmp}(y, z \sim 2) \quad \text{for } y, z \in \mathbb{N}.$$
Then
$$f(y) = h(y, \Lambda(f)(y)) \quad \text{for } y \in \mathbb{N}.$$
It follows that f is primitive recursive.

1.2. **Gödel's β-function.** Let
$$\beta(x,y,z) = x \bmod (1 + (z+1)y) \quad \text{for } x,y,z \in \mathbb{N}.$$
Note that β is primitive recursive.

Theorem 1.2. For any positive integer n and any $k \in \mathbb{N}^n$ there exist $b, c \in \mathbb{N}$ such that
$$\beta(b,c,i) = k_i \quad \text{for } i \in \{1,\ldots,n\}.$$

We need two lemmas.

Proof.

Lemma 1.1. Suppose $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$,

$$I = \left\{ \sum_{i=1}^{n} m_i a_i : m \in \mathbb{Z}^n \right\}$$

and

$$d = \min\{m : m \in I \text{ and } m > 0\}.$$

Then

$$I = \{nd : n \in \mathbb{Z}\}.$$

In particular,

$$d \text{ is the greatest common divisor of } a_1, \dots, a_n$$

and there is $m = (m_1, \dots, m_n) \in \mathbb{Z}^n$ such that

$$d = \sum_{i=1}^{n} m_i a_i.$$

Proof. I is an *ideal* in the ring $\mathbb{Z}$; that is, if $x, y \in I$ the $x + y \in I$ and if $x \in \mathbb{Z}$ and $y \in I$ then $xy \in I$. Let $J = \{nd : n \in \mathbb{Z}\}$. Evidently, $J \subset I$. Suppose $b \in I$ and $b > 0$. By the Euclidean algorithm there are $q, r \in \mathbb{N}$ such that $b = qd + r$ and $0 \le r < d$. Were it the case that $r > 0$ we would have $r = b - qd \in I$ which contradicts the minimality of d. If $b \in I$ and $b < 0$ we find that $-b = qd$ for some $q \in \mathbb{N}$ so $b = (-q)d$. So $J = I$, as desired. $\square$

Lemma 1.2. **(Chinese remainder theorem.)** Suppose $x \in \mathbb{N}^n$ and

$$(x_i, x_j) = 1 \quad \text{whenever } 1 \le i < j \le n.$$

Then for any $y \in \mathbb{N}^n$ there is $z \in \mathbb{N}$ such that

$$z \equiv y_i \mod x_i, \; i = 1, \dots, n.$$

Moreover, any two such zs differ by a multiple of $X = x_1 \cdots x_n$.

Proof. Let $w \in \mathbb{N}^n$ be such that $X = w_i x_i$, $i = 1, \dots, n$. Then $(w_i, x_i) = 1$, $i = 1, \dots, n$ so, by the preceding Lemma, there is an integer z_i such that $w_i z_i \equiv 1 \mod x_i$. Let $z = \sum_{i=1}^{n} w_i z_i y_i$. For any $1 \le i \le n$ we have

$$z \equiv w_i z_i \equiv 1 \mod y_i,$$

as desired.

If z' is another such integer, the difference $z - z'$ is divisible by each x_i and, therefore, divisible by X. $\square$

Proof of the Theorem. Let j be the largest of n and $k_1, \dots, k_n$ and let $c = j!$. For each $i = 1, \dots, n$ let $u_i = 1 + (i + 1)c$.

Suppose $1 \le l < m \le n$. Suppose p were a prime dividing both u_l and u_m. Then p would divide $(m - l)c$. Since $1 \le m - l < n \le j$ this would imply that p would divide $j! = c$. But that would imply p divides 1. Thus u_l and u_m are relatively prime.

By the Chinese Remainder Theorem there is a natural number $b < u_1 \cdots u_n$ such that $b \equiv k_i \mod u_i$, $i = 1, \dots, n$, proving the Theorem. $\square$