

# 14 $\lambda D$ 中的数字与算术

## Numbers and arithmetic in $\lambda D$

读书笔记

许博

### 1 用于自然数的皮亚诺公理

皮亚诺假设存在一个集合  $\mathbb{N}$ ，一个特定的成员  $0$ ，以及一个由  $\mathbb{N}$  到  $\mathbb{N}$  的后继函数  $s$ 。所以在  $\mathbb{N}$  中，我们有成员  $0, s(0), s(s(0))$  等，表示  $0, 1, 2$  等。

之后，皮亚诺通过添加公理，使得这些形式化的数字行为符合预期。为了保证函数  $s$  一定产生新的数字，皮亚诺添加了两条公理：

$$ax-nat_1 : \forall x \in \mathbb{N} (s(x) \neq 0)$$

$$ax-nat_2 : \forall x, y \in \mathbb{N} (s(x) = s(y) \Rightarrow x = y)$$

公理  $ax-nat_2$  表示  $s$  是一个单射的函数，而  $ax-nat_1$  隐含了  $s$  不是满射的。这两条公理决定了不同层数  $s$  的自然数不相同。

除此之外，皮亚诺还添加了另一条公理，以通过数学归纳法确定所有自然数的性质：

$$ax-nat_3 : (P0 \wedge \forall x : \mathbb{N}. (Px \Rightarrow P(sx))) \Rightarrow \forall x : \mathbb{N}. Px$$

**引理 1.1** 对于所有  $n \in \mathbb{N} : n = 0 \vee \exists m \in \mathbb{N} (n = s(m))$

### 2 以公理方式引入整数

整数的公理化假设存在一个  $\mathbb{Z}$ ，一个特定的成员  $0$ ，以及一个由  $\mathbb{Z}$  到  $\mathbb{Z}$  的后继函数  $s$ 。包含如下公理：

- (1)  $\mathbb{Z} := \perp : *_s$
  - (2)  $0 := \perp : \mathbb{Z}$
  - (3)  $s := \perp : \mathbb{Z} \rightarrow \mathbb{Z}$
  - (4)  $ax-int_1 := \perp : bijective(\mathbb{Z}, \mathbb{Z}, s)$
  - (5)  $inj-suc := \dots \text{ use } \wedge-el_1 \dots : injective(\mathbb{Z}, \mathbb{Z}, s)$
  - (6)  $surj-suc := \dots \text{ use } \wedge-el_2 \dots : surjective(\mathbb{Z}, \mathbb{Z}, s)$
- |                  |  |
|------------------|--|
| $y : \mathbb{Z}$ | <ol style="list-style-type: none"> <li>(7) <math>a_7(y) := surj-suc\ y : \exists^{\geq 1} x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)</math></li> <li style="border: 1px solid black; padding: 2px; margin: 2px 0;"> <math>x_1, x_2 : \mathbb{Z} \mid u : sx_1 =_{\mathbb{Z}} y \mid v : sx_2 =_{\mathbb{Z}} y</math> </li> <li>(8) <math>a_8(\dots) := eq-sym(\mathbb{Z}, sx_2, y, v) : y =_{\mathbb{Z}} sx_2</math></li> <li>(9) <math>a_9(\dots) := eq-trans(\mathbb{Z}, sx_1, y, sx_2, u, a_8(\dots)) : sx_1 =_{\mathbb{Z}} sx_2</math></li> <li>(10) <math>a_{10}(\dots) := inj-suc\ x_1\ x_2\ a_9(\dots) : x_1 =_{\mathbb{Z}} x_2</math></li> <li>(11) <math>a_{11}(y) := \dots \text{ use } \Rightarrow-in \text{ and } \forall-in \dots : \exists^{\leq 1} x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)</math></li> <li>(12) <math>a_{12}(y) := \dots \text{ use } \wedge-in \text{ on } a_7(y) \text{ and } a_{11}(y) \dots :</math><br/> <math>\exists^1 x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)</math></li> <li>(13) <math>a_{13} := \dots \text{ use } \forall-in \dots : \forall y : \mathbb{Z}. \exists^1 x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)</math></li> <li>(14) <math>p := \lambda y : \mathbb{Z}. \iota(\mathbb{Z}, \lambda x : \mathbb{Z}. (sx =_{\mathbb{Z}} y), a_{12}(y)) : \mathbb{Z} \rightarrow \mathbb{Z}</math></li> </ol> |
|------------------|--|
- |                  |   |
|------------------|---|
| $y : \mathbb{Z}$ | <ol style="list-style-type: none"> <li>(15) <math>s-p-ann(y) := \iota-prop(\mathbb{Z}, \lambda x : \mathbb{Z}. (sx =_{\mathbb{Z}} y), a_{12}(y)) : s(py) =_{\mathbb{Z}} y</math></li> <li>(16) <math>a_{16}(y) := s-p-ann(sy) : s(p(sy)) =_{\mathbb{Z}} sy</math></li> <li>(17) <math>p-s-ann(y) := inj-suc\ (p(sy))\ y\ a_{16}(y) : p(sy) =_{\mathbb{Z}} y</math></li> </ol> |
|------------------|---|

公理  $ax-int_1$  表示  $s$  是一个双射函数：单射以及满射。由满射性可得，对于所有  $y \in \mathbb{Z}$ ，存在一个  $x \in \mathbb{Z}$ ，使得  $s(x) = y$ 。由单射性可得， $y$  确定时，满足  $s(x) = y$  的  $x$  是唯一的。

行 (14) 中定义的  $p$ ， $p(y)$  表示  $y$  的前驱，也即  $s(x) = y$  中的  $x$ ，可以发现， $p$  是  $s$  的逆函数。

除了上图中出现的公理  $ax-int_1$ ，还有公理  $ax-int_2$ ，也即用于整数的归纳法，与自然数的版本相比较，在增加了前驱方向的归纳：

$P : \mathbb{Z} \rightarrow *_p$	$ax-int_2(P) := \perp :$ $[P\ 0 \wedge \forall x : \mathbb{Z}. (Px \Rightarrow (P(sx) \wedge P(px)))] \Rightarrow \forall x : \mathbb{Z}. Px$
----------------------------------	--

Figure 14.4 The induction axiom for integer numbers

此时我们可以将从 0 “向上” 的整数，也即自然数，作为  $\mathbb{Z}$  的一个子集

$\mathbb{N}$ :

- |     |  |
|-----|--|
|     | $P : \mathbb{Z} \rightarrow *_p$   |
| (1) | $\text{nat-cond}(P) := P\,0 \wedge \forall x : \mathbb{Z}. (Px \Rightarrow P(sx)) : *_p$   |
| (2) | $\mathbb{N} := \lambda x : \mathbb{Z}. \Pi P : \mathbb{Z} \rightarrow *_p. (\text{nat-cond}(P) \Rightarrow Px) : \mathbb{Z} \rightarrow *_p$                   |
| (3) | $\text{zero-prop} := \dots [\text{Exerc. 14.2(a)}] \dots : 0 \in \mathbb{N}$   |
| (4) | $\text{clos-prop} := \dots [\text{Exerc. 14.2(b)}] \dots : \forall x : \mathbb{Z}. (x \in \mathbb{N} \Rightarrow sx \in \mathbb{N})$                           |
| (5) | $a_5 := \dots \text{use } \wedge\text{-in } \dots : \text{nat-cond}(\mathbb{N})$   |
| (6) | $\text{nat-smallest} := \dots [\text{Exerc. 14.3}] \dots :$<br>$\Pi Q : \mathbb{Z} \rightarrow *_p. (\text{nat-cond}(Q) \Rightarrow (\mathbb{N} \subseteq Q))$ |

Figure 14.5 The natural numbers as a subset of  $\mathbb{Z}$

其中  $\text{nat-cond}(P)$  表示  $P$  满足自然数的归纳法的谓词，也即覆盖了所有的自然数，可以看到，如果一个整数  $x$  对于任意满足  $\text{nat-cond}$  的谓词  $P$ ，都有  $Px$  成立，则  $x$  是一个自然数。而满足  $\text{nat-cond}$  的谓词并不一定只作用于自然数，所以  $\text{nat-smallest}$  表示了  $\mathbb{N}$  是这些子集中的最小子集。

但目前仍存在一个问题，整数集合  $\mathbb{Z}$  不能保证其的左右是无限的，比如对于集合  $\{a, b, c, d\}$ ，令  $a = 0$ ，有  $s(a) = b, s(b) = c, s(c) = d, s(d) = a$ ， $s$  同样是双射的，并且适用于归纳法。解决方式是添加一个公理，以确保 0 的前驱不是自然数：

$$ax\text{-int}_3 := \perp\!\!\!\perp : \neg(p0 \in \mathbb{N})$$

至此我们拥有了整数，自然数，以及负数。

### 3 ‘新’ $\mathbb{N}$ 的基本性质

在‘新’的  $\mathbb{N}$  中，之前的皮亚诺公理依然成立。对于自然数的数学归纳法，需要重新表述为： $(P0 \wedge \forall x : \mathbb{Z}. (x \in \mathbb{N} \Rightarrow (Px \Rightarrow P(sx)))) \Rightarrow \forall x : \mathbb{Z}. (x \in \mathbb{N} \Rightarrow Px)$ 。

**引理 3.1**  $\forall x : \mathbb{Z}. (x \in \mathbb{N} \Rightarrow (x =_{\mathbb{Z}} 0 \vee px \in \mathbb{N}))$

- (1)  $\text{nat-split} := \dots : \forall x : \mathbb{Z}. (x \in \mathbb{N} \Rightarrow (x =_{\mathbb{Z}} 0 \vee \exists px \in \mathbb{N}))$
- (2)  $\text{nat-split-alt} := \dots : \forall x : \mathbb{Z}. (\neg(x \in \mathbb{N}) \vee x =_{\mathbb{Z}} 0 \vee \exists px \in \mathbb{N})$
- (3)  $\boxed{x : \mathbb{Z}} \quad \text{pos}(x) := \exists px \in \mathbb{N}$
- (4)  $\boxed{x : \mathbb{Z}} \quad \text{neg}(x) := \neg(x \in \mathbb{N})$
- (5)  $\text{trip} := \text{nat-split-alt} : \forall x : \mathbb{Z}. (\text{neg}(x) \vee x =_{\mathbb{Z}} 0 \vee \text{pos}(x))$

Figure 14.9 Positive and negative numbers, and the tripartition property

**Lemma 14.3.2** (a)  $\forall x : \mathbb{Z}. (\text{pos}(sx) \Leftrightarrow x \in \mathbb{N}),$   
 (b)  $\forall x : \mathbb{Z}. (\text{pos}(sx) \Leftrightarrow (x =_{\mathbb{Z}} 0 \vee \text{pos}(x))),$   
 (c)  $\forall x : \mathbb{Z}. (\text{neg}(px) \Leftrightarrow (x =_{\mathbb{Z}} 0 \vee \text{neg}(x))).$

**Lemma 14.3.3** (a)  $\forall x : \mathbb{Z}. (\text{pos}(x) \Leftrightarrow x \neq_{\mathbb{Z}} 0 \wedge \neg \text{neg}(x)),$   
 (b)  $\forall x : \mathbb{Z}. (\text{neg}(x) \Leftrightarrow x \neq_{\mathbb{Z}} 0 \wedge \neg \text{pos}(x)),$   
 (c)  $\forall x : \mathbb{Z}. (x =_{\mathbb{Z}} 0 \Leftrightarrow \neg \text{pos}(x) \wedge \neg \text{neg}(x)).$

## 4 整数加法

为了计算形式化的数字，形式化算术运算。首先是加法，通过如下形式的递归定义：

- (i)  $m + 0 = m,$
- (ii)  $m + s(n) = s(m + n).$

可以发现  $m$  没有变动，递归基于第二个操作数，因此可以重新表述为：

- (i)  $+_m(0) = m,$
- (ii)  $+_m(s(n)) = s(+_m(n)).$

而对于操作数是负数的情况，可以由 (ii) 推导得到，因此，对于整数而言，这两个定义足够。

用于整数的良构递归定义：

**Theorem 14.4.3** (*Recursion Theorem for  $\mathbb{Z}$* )

Let  $A$  be a type,  $a : A$  and let  $f_1, f_2 : A \rightarrow A$ .

Then there exists exactly one function  $g : \mathbb{Z} \rightarrow A$  such that

- $g 0 =_A a,$
- $g(sx) =_A f_1(gx)$  if  $x : \mathbb{Z}$  and  $\text{pos}(sx),$
- $g(px) =_A f_2(gx)$  if  $x : \mathbb{Z}$  and  $\text{neg}(px).$

对于一个能够终止的作用于整数集合的递归定义，存在一个唯一的函数  $g$  满足。形式化为：

$A : *_s \mid a : A \mid f_1, f_2 : A \rightarrow A$
$spec-rec-th(A, a, f_1, f_2) := \dots :$ $\exists^1 g : \mathbb{Z} \rightarrow A. [g\ 0 =_A a \wedge$ $\forall x : \mathbb{Z}. [(pos(s\ x) \Rightarrow (g(s\ x) =_A f_1(g\ x))) \wedge$ $(neg(p\ x) \Rightarrow (g(p\ x) =_A f_2(g\ x)))] ]$

Figure 14.10 The Recursion Theorem for  $\mathbb{Z}$  in  $\lambda D$

而如果给定的函数  $f$  是一个双射函数，则可以定义良构递归为：

**Theorem 14.4.5** (*Recursion Theorem for  $\mathbb{Z}$ , with bijection*)

Let  $A$  be a type,  $a : A$  and  $f : A \rightarrow A$ , a bijection.

Then there exists exactly one function  $g : \mathbb{Z} \rightarrow A$  such that

- $g\ 0 =_A a$ ,
- $g(s\ x) =_A f(g\ x)$  for all  $x : \mathbb{Z}$ .

在  $\lambda D$  中形式化  $+_m$  以及  $+$ :

- (1)  $a_1 := ax-int_1 : bijective(\mathbb{Z}, \mathbb{Z}, s)$
- (2)  $\boxed{m : \mathbb{Z}}$   
 $rec-add-prop(m) := \lambda g : \mathbb{Z} \rightarrow \mathbb{Z}. (g\ 0 =_{\mathbb{Z}} m \wedge \forall x : \mathbb{Z}. (g(s\ x) =_{\mathbb{Z}} s(g\ x))) :$   
 $(\mathbb{Z} \rightarrow \mathbb{Z}) \rightarrow *_p$
- (3)  $rec-add-lem(m) := \dots \text{ use Theorem 14.4.5 } \dots :$   
 $\exists^1 g : \mathbb{Z} \rightarrow \mathbb{Z}. (rec-add-prop(m)\ g)$
- (4)  $plus(m) := \iota(\mathbb{Z} \rightarrow \mathbb{Z}, rec-add-prop(m), rec-add-lem(m)) : \mathbb{Z} \rightarrow \mathbb{Z}$   
**Notation:**  $+_m$  for  $plus(m)$

Figure 14.11 Addition  $+_m : \mathbb{Z} \rightarrow \mathbb{Z}$  in  $\lambda D$

- (1)  $plus := \lambda x : \mathbb{Z}. \lambda y : \mathbb{Z}. (+_x\ y) : \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}$   
**Notation:**  $x + y$  for  $plus\ x\ y$
- (2)  $\boxed{x : \mathbb{Z}}$   
 $plus-i(x) := \dots : x + 0 =_{\mathbb{Z}} x$
- (3)  $\boxed{y : \mathbb{Z}}$   
 $plus-ii(x, y) := \dots : x + s\ y =_{\mathbb{Z}} s(x + y)$
- (4)  $plus-iii(x, y) := \dots : x + p\ y =_{\mathbb{Z}} p(x + y)$

Figure 14.12 Properties of addition in  $\mathbb{Z}$ , formalised in  $\lambda D$

## 5 $\lambda D$ 中基础计算的一个例子

证明  $1 + 2 = 3$ :

- (i)  $1 := s\ 0 : \mathbb{Z}$
- (ii)  $2 := s\ 1 : \mathbb{Z}$
- (iii)  $3 := s\ 2 : \mathbb{Z}$
- (1)  $a_1 := eq-refl(\mathbb{Z}, 1 + 2) : 1 + 2 = 1 + s\ 1$
- (2)  $a_2 := plus-ii(1, 1) : 1 + s\ 1 = s(1 + 1)$
- (3)  $a_3 := eq-refl(\mathbb{Z}, s(1 + 1)) : s(1 + 1) = s(1 + s\ 0)$
- (4)  $a_4 := eq-cong_1(\mathbb{Z}, \mathbb{Z}, s, 1 + s\ 0, s(1 + 0), plus-ii(1, 0)) :$   
 $s(1 + s\ 0) = s(s(1 + 0))$
- (5)  $a_5 := eq-cong_1(\mathbb{Z}, \mathbb{Z}, \lambda n : \mathbb{Z}. s(s(n)), 1 + 0, 1, plus-i(1)) :$   
 $s(s(1 + 0)) = s(s\ 1)$
- (6)  $a_6 := eq-refl(\mathbb{Z}, s(s\ 1)) : s(s(1)) = 3$
- (7)  $a_7 := eq-trans(\mathbb{Z}, 1 + 2, 1 + s\ 1, s(1 + 1), a_1, a_2) : 1 + 2 = s(1 + 1)$
- (8)  $a_8 := eq-trans(\mathbb{Z}, 1 + 2, s(1 + 1), s(1 + s\ 0), a_7, a_3) : 1 + 2 = s(1 + s\ 0)$
- (9)  $a_9 := eq-trans(\mathbb{Z}, 1 + 2, s(1 + s\ 0), s(s(1 + 0)), a_8, a_4) : 1 + 2 = s(s(1 + 0))$
- (10)  $a_{10} := eq-trans(\mathbb{Z}, 1 + 2, s(s(1 + 0)), s(s\ 1), a_9, a_5) : 1 + 2 = s(s\ 1)$
- (11)  $a_{11} := eq-trans(\mathbb{Z}, 1 + 2, s(s\ 1), 3, a_{10}, a_6) : 1 + 2 = 3$

Figure 14.13 A proof in  $\lambda D$  that  $1 + 2 = 3$

## 6 用于加法的算术公理

- |     |  |  |
|-----|--|--|
| (1) | <div style="border: 1px solid black; display: inline-block; padding: 2px 5px;"><math>x : \mathbb{Z}</math></div> | $plus-i-alt(x) := \dots : 0 + x = x$                                 |
| (2) | <div style="border: 1px solid black; display: inline-block; padding: 2px 5px;"><math>y : \mathbb{Z}</math></div> | $plus-ii-alt(x, y) := \dots : s\ x + y = s(x + y)$                   |
| (3) |  | $plus-iii-alt(x, y) := \dots : p\ x + y = p(x + y)$                  |
| (4) |  | $comm-add(x, y) := \dots : x + y = y + x$                            |
| (5) | <div style="border: 1px solid black; display: inline-block; padding: 2px 5px;"><math>z : \mathbb{Z}</math></div> | $assoc-add(x, y, z) := \dots : x + (y + z) = (x + y) + z$            |
| (6) |  | $right-canc-add(x, y, z) := \dots : x + z = y + z \Rightarrow x = y$ |
| (7) |  | $left-canc-add(x, y, z) := \dots : x + y = x + z \Rightarrow y = z$  |

Figure 14.14 More properties of addition in  $\mathbb{Z}$

## 7 用于自然数和负数的加法下的闭包

**Lemma 14.7.1** (*Closure of  $\mathbb{N}$  under addition*)

$$\forall x, y : \mathbb{Z}. ((x \in \mathbb{N} \wedge y \in \mathbb{N}) \Rightarrow x + y \in \mathbb{N}).$$

**Lemma 14.7.2** (*Characterisation of negative numbers*)

$$\forall x : \mathbb{Z}. (neg(x) \Leftrightarrow \exists y : \mathbb{Z}. (pos(y) \wedge x + y = 0)).$$

**Lemma 14.7.3** (*Closure for negative integers*)

$$\forall x, y : \mathbb{Z}. (neg(x) \wedge neg(y) \Rightarrow neg(x + y)).$$

## 8 整数减法

定义减法:  $x - y := \iota_{z:\mathbb{Z}}(z + y = x)$ 。性质不再赘述。

## 9 整数的相反数

定义相反数:  $-x := 0 - x$ 。

## 10 整数上的非相等关系

定义  $\leq_{\mathbb{Z}} := \lambda x : \mathbb{Z}. \lambda y : \mathbb{Z}. (y - x \in \mathbb{N}) : \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow *_{\mathcal{P}}$ 。

定义  $<_{\mathbb{Z}} := \lambda x : \mathbb{Z}. \lambda y : \mathbb{Z}. (x \leq_{\mathbb{Z}} y \wedge x \neq y) : \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow *_{\mathcal{P}}$ 。

## 11 整数乘法

定义乘法为:

$$(i) \ m \cdot 0 = 0,$$

$$(ii) \ m \cdot s(n) = (m \cdot n) + m.$$

## 12 可除性

定义可除性为:  $m$  可以整除  $n$ , 如果存在  $q : \mathbb{Z}$  使得  $m \cdot q = n$ 。

需要注意的是, 可除性在自然数上是一个偏序关系。