FOUNDATIONS OF NUMBER-THEORY

DAVID PIERCE

Theorems about natural numbers have been known for thousands of years. Some of these theorems come down to us in Euclid's *Elements* [2], for example, or Nicomachus's *Introduction to Arithmetic* [3]. However, the *foundations* on which the proofs of these theorems are established were apparently not worked out until more recent centuries.

It turns out that all theorems about the natural numbers are logical consequences of Axiom 1 below. This axiom lists five conditions that the natural numbers meet. Richard Dedekind published these conditions in 1888 [1, II, § 71, p. 67]. In 1889, Giuseppe Peano [4, § 1, p. 94] repeated them in a more symbolic form, along with some logical conditions, making nine conditions in all, which he called axioms. Of these, the five specifically number-theoretic conditions have come to be known as the "Peano Axioms." (Note however that Dedekind and Peano treated the first natural number as 1, not 0; some writers continue to do this today.)

The foundations of number-theory are often not well understood, even today. Some books give the impression that all theorems about natural numbers follow from the so-called "Well-Ordering Principle" (Theorem 24). Others suggest that the possibility of definition by recursion (Theorem 4) can be proved by induction (Axiom 1(e)) alone. These are mistakes about the foundations of number-theory. They are perhaps not really mistakes about number-theory itself; still, they are mistakes, and it is better not to make them. This is why I have written these notes.

When proofs of lemmas and theorems here are not supplied, I have left them to the reader as exercises.

An expression like "$f\colon A \to B$" is to be read as the statement "f is a function from A to B." This means f is a certain kind of subset of the Cartesian product $A \times B$, namely a subset that, for each a in A, has exactly one element of the form (a, b); then one writes $f(a) = b$. Finally, f can also be written as $x \mapsto f(x)$.

1. **Axiom and definition.** *The set of* ***natural numbers,*** *denoted by* $\mathbb{N}$, *meets the following five conditions.*

(a) *There is a* ***first*** *natural number, called* 0 *(**zero**).*
(b) *Every* n *in* $\mathbb{N}$ *has a unique* ***successor,*** *denoted (for now) by* $\mathrm{s}(n)$.
(c) *Zero is not a successor: if* $n \in \mathbb{N}$, *then* $\mathrm{s}(n) \neq 0$.
(d) *Distinct natural numbers have distinct successors: if* $n, m \in \mathbb{N}$ *and* $n \neq m$, *then* $\mathrm{s}(n) \neq \mathrm{s}(m)$.
(e) *Proof by* ***induction*** *is possible: Suppose* $A \subseteq \mathbb{N}$, *and two conditions are met, namely*
    (i) *the* ***base*** *condition:* $0 \in A$, *and*

Date: November 9, 2007; recompiled, November 10, 2007.

(ii) *the* ***inductive*** *condition: if* $n \in A$ *(the* ***inductive hypothesis****), then* $\mathrm{s}(n) \in A$.

Then $A = \mathbb{N}$.

The natural number $\mathrm{s}(0)$ *is denoted by* 1*; the number* $\mathrm{s}(1)$*, by* 2*; &c.*

2. *Remark.* Parts (c), (d) and (e) of the axiom are conditions concerning a set with a first element and a successor-operation. For each of those conditions, there is an example of such a set that meets that condition, but not the others. In short, the three conditions are logically independent.

3. **Lemma.** *Every natural number is either* 0 *or a successor.*

Proof. Let A be the set comprising every natural number that is either 0 or a successor. In particular, $0 \in A$, and if $n \in A$, then (since it is a successor) $\mathrm{s}(n) \in A$. Therefore, by induction, $A = \mathbb{N}$. □

4. **Theorem** (Recursion)**.** *Suppose a set* A *has an element* b*, and* $f \colon A \to A$*. Then there is a* unique *function* g *from* $\mathbb{N}$ *to* A *such that*

(a) $g(0) = b$*, and*

(b) $g(\mathrm{s}(n)) = f(g(n))$ *for all* n *in* $\mathbb{N}$.

Proof. The following is only a sketch. One must prove existence and uniqueness of g. Assuming existence, one can prove uniqueness by induction. To prove existence, let $\mathcal{S}$ be the set of subsets R of $\mathbb{N} \times A$ such that

(a) if $(0, c) \in R$, then $c = b$;

(b) if $(\mathrm{s}(n), c) \in R$, then $(n, d) \in R$ for some d such that $f(d) = c$.

Then $\bigcup \mathcal{S}$ is the desired function g. □

5. *Remark.* In its statement (though not the proof), the Recursion Theorem assumes only parts (a) and (b) of Axiom 1. The other parts can be proved as consequences of the Theorem. Recursion is a method of *definition;* induction is a method of *proof.* There are sets (with first elements and successor-operations) that allow proof by induction, but not definition by recursion. In short, induction is logically weaker than recursion.

6. **Definition** (Addition)**.** For each m in $\mathbb{N}$, the operation $x \mapsto m + x$ on $\mathbb{N}$ is the function g guaranteed by the Recursion Theorem when A is $\mathbb{N}$ and b is m and f is $x \mapsto \mathrm{s}(x)$. That is,

$$m + 0 = m,$$
$$m + \mathrm{s}(n) = \mathrm{s}(m + n).$$

7. **Lemma.** *For all* n *and* m *in* $\mathbb{N}$*,*

(a) $0 + n = n$*;*

(b) $\mathrm{s}(m) + n = \mathrm{s}(m + n)$.

8. **Theorem.** *For all* n*,* m*, and* k *in* $\mathbb{N}$*,*

(a) $\mathrm{s}(n) = n + 1$*;*

(b) $n + m = m + n$*;*

(c) $(n + m) + k = n + (m + k)$*;*

9. *Remark.* It is possible to prove by induction alone that an operation of addition with the properties described in ¶¶6–8 exists uniquely.

10. **Definition** (Multiplication)**.** For each m in $\mathbb{N}$, the operation $x \mapsto m \cdot x$ on $\mathbb{N}$ is the function g guaranteed by the Recursion Theorem when A is $\mathbb{N}$ and b is 0 and f is $x \mapsto x + m$. That is,

$$m \cdot 0 = 0,$$
$$m \cdot (n+1) = m \cdot n + m.$$

11. **Lemma.** *For all n and m in $\mathbb{N}$,*

(a) $0 \cdot n = 0$;
(b) $(m+1) \cdot n = m \cdot n + n$.

12. **Theorem.** *For all n, m, and k in $\mathbb{N}$,*

(a) $1 \cdot n = n$;
(b) $n \cdot m = m \cdot n$;
(c) $n \cdot (m+k) = n \cdot m + n \cdot k$;
(d) $(n \cdot m) \cdot k = n \cdot (m \cdot k)$;

13. *Remark.* As with addition, so with multiplication, one can prove by induction alone that it exists uniquely as described in ¶¶10–12. However, the next theorem requires also Axioms 1(c)–(d).

14. **Theorem** (Cancellation)**.** *For all n, m, and k in $\mathbb{N}$,*

(a) *if* $n + k = m + k$, *then* $n = m$;
(b) *if* $n + m = 0$, *then* $n = 0$ *and* $m = 0$;
(c) *if* $n \cdot m = 0$, *then* $n = 0$ *or* $m = 0$;
(d) *if* $n \cdot k = m \cdot k$, *then* $n = m$ *or* $k = 0$.

15. **Definition** (Exponentiation)**.** For each m in $\mathbb{N}$, the operation $x \mapsto m^x$ on $\mathbb{N}$ is the function g guaranteed by the Recursion Theorem when A is $\mathbb{N}$ and b is 1 and f is $x \mapsto x \cdot m$. That is,

$$m^0 = 1,$$
$$m^{n+1} = m^n \cdot m.$$

16. **Theorem.** *For all n, m, and k in $\mathbb{N}$,*

(a) $n^1 = n$;
(b) $0^n = 0$, *unless* $n = 0$;
(c) $n^{m+k} = n^m \cdot n^k$;
(d) $(n \cdot m)^k = n^k \cdot m^k$;
(e) $(n^m)^k = n^{m \cdot k}$.

17. *Remark.* In contrast with addition and multiplication, exponentiation requires more than induction for its existence.

18. **Definition** (Ordering)**.** If $n, m \in \mathbb{N}$, and $m + k = n$ for some k in $\mathbb{N}$, then this situation is denoted by $m \leqslant n$. That is,

$$m \leqslant n \iff \exists x\, m + x = n.$$

If also $m \neq n$, then we write $m < n$, and we say that m is a **predecessor** of n.

19. **Theorem.** *For all n, m, and k in $\mathbb{N}$,*

(a) $0 \leqslant n$;

(b) *$m \leqslant n$ if and only if $m + k \leqslant n + k$;*
(c) *$m \leqslant n$ if and only if $m \cdot (k + 1) \leqslant n \cdot (k + 1)$.*

20. **Lemma.** *For all m and n in $\mathbb{N}$,*

(a) *$m < n$ if and only if $m + 1 \leqslant n$;*
(b) *$m \leqslant n$ if and only if $m < n + 1$.*

21. **Theorem.** *The binary relation $\leqslant$ is a **total ordering:** for all n, m, and k in $\mathbb{N}$,*

(a) *$n \leqslant n$;*
(b) *if $m \leqslant n$ and $n \leqslant m$, then $n = m$;*
(c) *if $k \leqslant m$ and $m \leqslant n$, then $k \leqslant n$;*
(d) *either $m \leqslant n$ or $n \leqslant m$.*

22. **Theorem** (Strong Induction)**.** *Suppose $A \subseteq \mathbb{N}$, and one condition is met, namely*

- *if all predecessors of n belong to A (the **strong inductive hypothesis**), then $n \in A$.*

Then $A = \mathbb{N}$.

Proof. Let B comprise the natural numbers whose predecessors belong to A. As 0 has no predecessors, they belong to A, so $0 \in B$. Suppose $n \in B$. Then all predecessors of n belong to A, so by assumption, $n \in A$. Thus, by Lemma 20(b), all of the predecessors of $n + 1$ belong to A, so $n + 1 \in B$. By induction, $B = \mathbb{N}$. In particular, if $n \in \mathbb{N}$, then $n + 1 \in B$, so n (being a predecessor of $n + 1$) belongs to A. Thus $A = \mathbb{N}$. □

23. *Remark.* In general, strong induction is a proof-technique that can be used with some *ordered* sets. By contrast, "ordinary" induction involves sets with first elements and successor-operations, but possibly without orderings. Strong induction does not follow from ordinary induction alone; neither does ordinary induction follow from strong induction.

24. **Theorem.** *The set of natural numbers is **well-ordered** by $\leqslant$: that is, every non-empty subset of $\mathbb{N}$ has a least element with respect to $\leqslant$.*

Proof. Use strong induction. Suppose A is a subset of $\mathbb{N}$ with no least element. We shall show A is empty, that is, $\mathbb{N} \smallsetminus A = \mathbb{N}$. Let $n \in \mathbb{N}$. Then n is not a least element of A. This means one of two things: either $n \notin A$, or else $n \in A$, but also $m \in A$ for some predecessor of n. Equivalently, if no predecessor of n is in A, then $n \notin A$. In other words, if every predecessor of n is in $\mathbb{N} \smallsetminus A$, then $n \in \mathbb{N} \smallsetminus A$. By strong induction, we are done. □

25. *Remark.* We have now shown, in effect, that if a total order $(A, \leqslant)$ admits proof by strong recursion, then it is well-ordered. The converse is also true.

26. **Theorem** (Recursion with Parameter)**.** *Suppose A is a set with an element b, and $F \colon \mathbb{N} \times A \to A$. Then there is a* unique *function G from $\mathbb{N}$ to A such that*

(a) *$G(0) = b$, and*
(b) *$G(n + 1) = F(n, G(n))$ for all n in $\mathbb{N}$.*

Proof. Let $f\colon \mathbb{N}\times A \to \mathbb{N}\times A$, where $f(n,x) = (n+1, F(n,x))$. By recursion, there is a unique function g from $\mathbb{N}$ to $\mathbb{N}\times A$ such that $g(0) = (0,b)$ and $g(n+1) = f(g(n))$. By induction, the first entry in $g(n)$ is always n. The desired function G is given by $g(n) = (n, G(n))$. Indeed, we now have $G(0) = b$; also, $g(n+1) = f(n, G(n)) = (n+1, F(n, G(n)))$, so $G(n+1) = F(n, G(n))$. By induction, G is unique. □

27. *Remark.* Recursion with Parameter allows us to define the set of predecessors of n as $\operatorname{pred}(n)$, where $x \mapsto \operatorname{pred}(x)$ is the function G guaranteed by the Theorem when A is the set of subsets of $\mathbb{N}$, and b is the empty set, and F is $(x,Y) \mapsto \{x\}\cup Y$. Then we can write $m < n$ if $m \in \operatorname{pred}(n)$ and prove the foregoing theorems about the ordering.

28. **Definition** (Factorial)**.** The operation $x \mapsto x!$ on $\mathbb{N}$ is the function G guaranteed by the Theorem of Recursion with Parameter when A is $\mathbb{N}$ and b is 1 and F is $(x,y) \mapsto (x+1)\cdot y$. That is,

$$0! = 1,$$
$$(n+1)! = (n+1)\cdot n!$$

References

[1] Richard Dedekind. *Essays on the theory of numbers. I:Continuity and irrational numbers. II:The nature and meaning of numbers.* Authorized translation by Wooster Woodruff Beman. Dover Publications Inc., New York, 1963.

[2] Euclid. *Euclid's Elements.* Green Lion Press, Santa Fe, NM, 2002. All thirteen books complete in one volume, the Thomas L. Heath translation, edited by Dana Densmore.

[3] Nicomachus of Gerasa. *Introduction to Arithmetic*, volume XVI of *University of Michigan Studies, Humanistic Series.* University of Michigan Press, Ann Arbor, 1938. First printing, 1926.

[4] Guiseppe Peano. The principles of arithmetic, presented by a new method. In Jean van Heijenoort, editor, *From Frege to Gödel.*

[5] Jean van Heijenoort. *From Frege to Gödel. A source book in mathematical logic, 1879–1931.* Harvard University Press, Cambridge, Mass., 1967.

Mathematics Dept, Middle East Technical Univ., Ankara 06531, Turkey
E-mail address: `dpierce@metu.edu.tr`
URL: `http://www.math.metu.edu.tr/~dpierce`