FORMALIZED MATHEMATICS
Number 1, January 1990
Université Catholique de Louvain

The Fundamental Properties of Natural Numbers

Grzegorz Bancerek[1]
Warsaw University
Białystok

Summary. Some fundamental properties of addition, multiplication, order relations, exact division, the remainder, divisibility, the least common multiple, the greatest common divisor are presented. A proof of Euclid algorithm is also given.

The article [1] provides the terminology and notation for this paper. For simplicity we adopt the following convention: x will denote an object of the type Real; k, l, m, n will denote objects of the type Nat; X will denote an object of the type **set of** Real. One can prove the following propositions:

$$x \textbf{ is } \mathrm{Nat} \textbf{ implies } x+1 \textbf{ is } \mathrm{Nat}, \tag{1}$$

$$\textbf{for } X \textbf{ st } 0 \in X \;\&\; \textbf{for } x \textbf{ st } x \in X \textbf{ holds } x+1 \in X \textbf{ for } k \textbf{ holds } k \in X, \tag{2}$$

$$k+n = n+k, \tag{3}$$

$$k+m+n = k+(m+n), \tag{4}$$

$$k+0 = k \;\&\; 0+k = k, \tag{5}$$

$$k \cdot n = n \cdot k, \tag{6}$$

$$k \cdot (m \cdot n) = (k \cdot m) \cdot n, \tag{7}$$

$$k \cdot 1 = k \;\&\; 1 \cdot k = k, \tag{8}$$

$$k \cdot (n+m) = k \cdot n + k \cdot m \;\&\; (n+m) \cdot k = n \cdot k + m \cdot k, \tag{9}$$

$$k+m = n+m \textbf{ or } k+m = m+n \textbf{ or } m+k = m+n \textbf{ implies } k = n, \tag{10}$$

[1]Supported by RPBP III.24 C1

© 1990 Fondation Philippe le Hodey
ISSN 0777-4028

(11) $$k \cdot 0 = 0 \; \& \; 0 \cdot k = 0.$$

Let us consider n, k. Let us note that it makes sense to consider the following functor on a restricted area. Then

$$n + k \qquad \text{is} \qquad \mathrm{Nat}\,.$$

The scheme *Ind* deals with a unary predicate $\mathcal{P}$ states that the following holds

$$\textbf{for}\, k \,\textbf{holds}\, \mathcal{P}[k]$$

provided the parameter satisfies the following conditions:

- $$\mathcal{P}[0],$$
- $$\textbf{for}\, k \,\textbf{st}\, \mathcal{P}[k] \,\textbf{holds}\, \mathcal{P}[k+1].$$

Let us consider n, k. Let us note that it makes sense to consider the following functor on a restricted area. Then

$$n \cdot k \qquad \text{is} \qquad \mathrm{Nat}\,.$$

One can prove the following propositions:

(12) $$k \leq n \;\&\; n \leq k \,\textbf{implies}\, k = n,$$

(13) $$k \leq n \;\&\; n \leq m \,\textbf{implies}\, k \leq m,$$

(14) $$k \leq n \,\textbf{or}\, n \leq k,$$

(15) $$k \leq k,$$

(16) $$k \leq n \,\textbf{implies}$$
$$k + m \leq n + m \;\&\; k + m \leq m + n \;\&\; m + k \leq m + n \;\&\; m + k \leq n + m,$$

(17) $$k + m \leq n + m \,\textbf{or}\, k + m \leq m + n \,\textbf{or}\, m + k \leq m + n \,\textbf{or}\, m + k \leq n + m$$
$$\textbf{implies}\, k \leq n,$$

(18) $$\textbf{for}\, k \,\textbf{holds}\, 0 \leq k,$$

(19) $$0 \neq k \,\textbf{implies}\, 0 < k,$$

(20) $$k \leq n \,\textbf{implies}\, k \cdot m \leq n \cdot m \;\&\; k \cdot m \leq m \cdot n \;\&\; m \cdot k \leq n \cdot m \;\&\; m \cdot k \leq m \cdot n,$$

(21) $$0 \neq k + 1,$$

(22) $$k = 0 \,\textbf{or}\, \textbf{ex}\, n \,\textbf{st}\, k = n + 1,$$

(23) $$k + n = 0 \,\textbf{implies}\, k = 0 \;\&\; n = 0,$$

(24) $$k \neq 0 \;\&\; (n \cdot k = m \cdot k \,\textbf{or}\, n \cdot k = k \cdot m \,\textbf{or}\, k \cdot n = k \cdot m) \,\textbf{implies}\, n = m,$$

(25) $$k \cdot n = 0 \textbf{ implies } k = 0 \textbf{ or } n = 0.$$

The scheme *Def_by_Ind* concerns a constant $\mathcal{A}$ that has the type Nat, a binary functor $\mathcal{F}$ yielding values of the type Nat and a binary predicate $\mathcal{P}$ and states that the following holds

$$(\textbf{for } k \textbf{ ex } n \textbf{ st } \mathcal{P}[k,n]) \ \& \ \textbf{for } k,n,m \textbf{ st } \mathcal{P}[k,n] \ \& \ \mathcal{P}[k,m] \textbf{ holds } n = m$$

provided the parameters satisfy the following condition:

- $$\textbf{for } k,n \textbf{ holds}$$ $$\mathcal{P}[k,n] \textbf{ iff } k = 0 \ \& \ n = \mathcal{A} \textbf{ or ex } m,l \textbf{ st } k = m+1 \ \& \ \mathcal{P}[m,l] \ \& \ n = \mathcal{F}(k,l).$$

Next we state several propositions:

(26) $$\textbf{for } k,n \textbf{ st } k \leq n+1 \textbf{ holds } k \leq n \textbf{ or } k = n+1,$$

(27) $$\textbf{for } n,k \textbf{ st } n \leq k \ \& \ k \leq n+1 \textbf{ holds } n = k \textbf{ or } k = n+1,$$

(28) $$\textbf{for } k,n \textbf{ st } k \leq n \textbf{ ex } m \textbf{ st } n = k+m,$$

(29) $$k \leq k+m,$$

(30) $$k < n \textbf{ iff } k \leq n \ \& \ k \neq n,$$

(31) $$\textbf{not } k < 0.$$

Now we present three schemes. The scheme *Comp_Ind* deals with a unary predicate $\mathcal{P}$ states that the following holds

$$\textbf{for } k \textbf{ holds } \mathcal{P}[k]$$

provided the parameter satisfies the following condition:

- $$\textbf{for } k \textbf{ st for } n \textbf{ st } n < k \textbf{ holds } \mathcal{P}[n] \textbf{ holds } \mathcal{P}[k].$$

The scheme *Min* concerns a unary predicate $\mathcal{P}$ states that the following holds

$$\textbf{ex } k \textbf{ st } \mathcal{P}[k] \ \& \ \textbf{for } n \textbf{ st } \mathcal{P}[n] \textbf{ holds } k \leq n$$

provided the parameter satisfies the following condition:

- $$\textbf{ex } k \textbf{ st } \mathcal{P}[k].$$

The scheme *Max* concerns a unary predicate $\mathcal{P}$ and a constant $\mathcal{A}$ that has the type Nat, and states that the following holds

$$\textbf{ex } k \textbf{ st } \mathcal{P}[k] \ \& \ \textbf{for } n \textbf{ st } \mathcal{P}[n] \textbf{ holds } n \leq k$$

provided the parameters satisfy the following conditions:

- $$\textbf{for } k \textbf{ st } \mathcal{P}[k] \textbf{ holds } k \leq \mathcal{A},$$

- $$\mathbf{ex}\, k\ \mathbf{st}\ \mathcal{P}[k].$$

We now state a number of propositions:

(32) $$\mathbf{not}\,(k < n \ \&\ n < k),$$

(33) $$k < n \ \&\ n < m \ \mathbf{implies}\ k < m,$$

(34) $$k < n \ \mathbf{or}\ k = n \ \mathbf{or}\ n < k,$$

(35) $$\mathbf{not}\, k < k,$$

(36) $$k < n \ \mathbf{implies}$$
$$k + m < n + m \ \&\ k + m < m + n \ \&\ m + k < m + n \ \&\ m + k < n + m,$$

(37) $$k \leq n \ \mathbf{implies}\ k \leq n + m,$$

(38) $$k < n + 1 \ \mathbf{iff}\ k \leq n,$$

(39) $$k \leq n \ \&\ n < m \ \mathbf{or}\ k < n \ \&\ n \leq m \ \mathbf{or}\ k < n \ \&\ n < m \ \mathbf{implies}\ k < m,$$

(40) $$k \cdot n = 1 \ \mathbf{implies}\ k = 1 \ \&\ n = 1,$$

(41) $$k + 1 \leq n \ \mathbf{iff}\ k < n.$$

The scheme *Regr* concerns a unary predicate $\mathcal{P}$ states that the following holds

$$\mathcal{P}[0]$$

provided the parameter satisfies the following conditions:

- $$\mathbf{ex}\, k\ \mathbf{st}\ \mathcal{P}[k],$$
- $$\mathbf{for}\, k\ \mathbf{st}\ k \neq 0 \ \&\ \mathcal{P}[k]\ \mathbf{ex}\, n\ \mathbf{st}\ n < k \ \&\ \mathcal{P}[n].$$

In the sequel $k1$, t, $t1$ will denote objects of the type Nat. The following propositions are true:

(42) $$\mathbf{for}\, m\ \mathbf{st}\ 0 < m\ \mathbf{for}\, n\ \mathbf{ex}\, k,t\ \mathbf{st}\ n = (m \cdot k) + t \ \&\ t < m,$$

(43) $$\mathbf{for}\, n,m,k,k1,t,t1$$
$$\mathbf{st}\ n = m \cdot k + t \ \&\ t < m \ \&\ n = m \cdot k1 + t1 \ \&\ t1 < m \ \mathbf{holds}\ k = k1 \ \&\ t = t1.$$

We now define two new functors. Let k, l have the type Nat. The functor

$$k \div l,$$

yields the type Nat and is defined by

$$(\mathbf{ex}\, t\ \mathbf{st}\ k = l \cdot \mathbf{it} + t \ \&\ t < l)\ \mathbf{or}\ \mathbf{it} = 0 \ \&\ l = 0.$$

The functor

$$k \bmod l,$$

yields the type Nat and is defined by

$$(\mathbf{ex}\, t\ \mathbf{st}\ k = l \cdot t + \mathbf{it}\ \&\ \mathbf{it} < l)\ \mathbf{or}\ \mathbf{it} = 0\ \&\ l = 0.$$

Next we state four propositions:

$$\text{(44)} \quad \mathbf{for}\, k,l,n\ \mathbf{being}\ \mathrm{Nat}\ \mathbf{holds}\ n = k \div l\ \mathbf{iff}\ (\mathbf{ex}\, t\ \mathbf{st}\ k = l \cdot n + t\ \&\ t < l)\ \mathbf{or}\ n = 0\ \&\ l = 0,$$

$$\text{(45)} \quad \mathbf{for}\, k,l,n\ \mathbf{being}\ \mathrm{Nat}\ \mathbf{holds}\ n = k \bmod l\ \mathbf{iff}\ (\mathbf{ex}\, t\ \mathbf{st}\ k = l \cdot t + n\ \&\ n < l)\ \mathbf{or}\ n = 0\ \&\ l = 0,$$

$$\text{(46)} \quad \mathbf{for}\, m,n\ \mathbf{st}\ 0 < m\ \mathbf{holds}\ n \bmod m < m,$$

$$\text{(47)} \quad \mathbf{for}\, n,m\ \mathbf{st}\ 0 < m\ \mathbf{holds}\ n = m \cdot (n \div m) + (n \bmod m).$$

Let k, l have the type Nat. The predicate

$$k \mid l \qquad \text{is defined by} \qquad \mathbf{ex}\, t\ \mathbf{st}\ l = k \cdot t.$$

Next we state a number of propositions:

$$\text{(48)} \quad \mathbf{for}\, k,l\ \mathbf{being}\ \mathrm{Nat}\ \mathbf{holds}\ k \mid l\ \mathbf{iff}\ \mathbf{ex}\, t\ \mathbf{st}\ l = k \cdot t,$$

$$\text{(49)} \quad \mathbf{for}\, n,m\ \mathbf{holds}\ m \mid n\ \mathbf{iff}\ n = m \cdot (n \div m),$$

$$\text{(50)} \quad \mathbf{for}\, n\ \mathbf{holds}\ n \mid n,$$

$$\text{(51)} \quad \mathbf{for}\, n,m,l\ \mathbf{st}\ n \mid m\ \&\ m \mid l\ \mathbf{holds}\ n \mid l,$$

$$\text{(52)} \quad \mathbf{for}\, n,m\ \mathbf{st}\ n \mid m\ \&\ m \mid n\ \mathbf{holds}\ n = m,$$

$$\text{(53)} \quad k \mid 0\ \&\ 1 \mid k,$$

$$\text{(54)} \quad \mathbf{for}\, n,m\ \mathbf{st}\ 0 < m\ \&\ n \mid m\ \mathbf{holds}\ n \leq m,$$

$$\text{(55)} \quad \mathbf{for}\, n,m,l\ \mathbf{st}\ n \mid m\ \&\ n \mid l\ \mathbf{holds}\ n \mid m + l,$$

$$\text{(56)} \quad n \mid k\ \mathbf{implies}\ n \mid k \cdot m,$$

$$\text{(57)} \quad \mathbf{for}\, n,m,l\ \mathbf{st}\ n \mid m\ \&\ n \mid m + l\ \mathbf{holds}\ n \mid l,$$

$$\text{(58)} \quad n \mid m\ \&\ n \mid k\ \mathbf{implies}\ n \mid m \bmod k.$$

Let us consider k, n. The functor

$$k\ \mathrm{lcm}\ n,$$

with values of the type Nat, is defined by

$$k \mid \textbf{it} \ \& \ n \mid \textbf{it} \ \& \ \textbf{for}\, m \ \textbf{st}\ k \mid m \ \& \ n \mid m \ \textbf{holds it} \mid m.$$

Next we state a proposition

(59) $$\textbf{for}\, M \ \textbf{being}\ \mathrm{Nat}$$
$$\textbf{holds}\ M = k \operatorname{lcm} n \ \textbf{iff}\ k \mid M \ \& \ n \mid M \ \& \ \textbf{for}\, m \ \textbf{st}\ k \mid m \ \& \ n \mid m \ \textbf{holds}\ M \mid m.$$

Let us consider k, n. The functor

$$k \operatorname{gcd} n,$$

yields the type Nat and is defined by

$$\textbf{it} \mid k \ \& \ \textbf{it} \mid n \ \& \ \textbf{for}\, m \ \textbf{st}\ m \mid k \ \& \ m \mid n \ \textbf{holds}\ m \mid \textbf{it}\,.$$

We now state a proposition

(60) $$\textbf{for}\, M \ \textbf{being}\ \mathrm{Nat}$$
$$\textbf{holds}\ M = k \operatorname{gcd} n \ \textbf{iff}\ M \mid k \ \& \ M \mid n \ \& \ \textbf{for}\, m \ \textbf{st}\ m \mid k \ \& \ m \mid n \ \textbf{holds}\ m \mid M.$$

The scheme *Euklides* deals with a unary functor $\mathcal{F}$ yielding values of the type Nat, a constant $\mathcal{A}$ that has the type Nat and a constant $\mathcal{B}$ that has the type Nat, and states that the following holds

$$\textbf{ex}\, n \ \textbf{st}\ \mathcal{F}(n) = \mathcal{A} \operatorname{gcd} \mathcal{B} \ \& \ \mathcal{F}(n+1) = 0$$

provided the parameters satisfy the following conditions:

- $$0 < \mathcal{B} \ \& \ \mathcal{B} < \mathcal{A},$$
- $$\mathcal{F}(0) = \mathcal{A} \ \& \ \mathcal{F}(1) = \mathcal{B},$$
- $$\textbf{for}\, n \ \textbf{holds}\ \mathcal{F}(n+2) = \mathcal{F}(n) \bmod \mathcal{F}(n+1).$$

References

[1] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1, 1990.

Received January 11, 1989