Natural numbers

Marcel Schütz

October 26, 2021

Contents

Part I
Arithmetic

1 Peano Arithmetic

1.1 The Peano axioms

Signature 1. A natural number is an element.

Let k, l, m, n denote natural numbers.

Signature 2. 0 is a natural number.

Let n is nonzero stand for $n \neq 0$.

Signature 3. $\mathrm{succ}(n)$ is a natural number.

Let the direct successor of n stand for $\mathrm{succ}(n)$.

Axiom 4. (1st Peano axiom) If $\mathrm{succ}(n) = \mathrm{succ}(m)$ then $n = m$.

Axiom 5. (2nd Peano axiom) 0 is not the direct successor of any natural number.

Axiom 6. (3rd Peano axiom) Let P be a class. Assume $0 \in P$ and for all natural numbers n we have $n \in P \implies \mathrm{succ}(n) \in P$. Then every natural number is an element of P.

1.2 Immediate consequences

Proposition 7. (NN 01 01 178800) For all n we have $n = 0$ or $n = \mathrm{succ}(m)$ for some natural number m.

Proof. Define $P = \{\text{natural number } n : n = 0 \text{ or } n = \mathrm{succ}(m) \text{ for some natural number } m\}$.

$0 \in P$ and for all natural numbers n we have $n \in P \implies \mathrm{succ}(n) \in P$. Hence the thesis (by 3rd Peano axiom). □

Proposition 8. (NN 01 01 670417) For no natural number n we have $n = \mathrm{succ}(n)$.

Proof. Define $P = \{\text{natural number } n : n \neq \mathrm{succ}(n)\}$.

(BASE CASE) 0 belongs to P.

(INDUCTION STEP) For all n we have $n \in P \implies \mathrm{succ}(n) \in P$.
Proof. Let n be a natural number. Assume that $n \in P$. Then $n \neq \mathrm{succ}(n)$. If $\mathrm{succ}(n) = \mathrm{succ}(\mathrm{succ}(n))$ then $n = \mathrm{succ}(n)$. Thus it is wrong that $\mathrm{succ}(n) = \mathrm{succ}(\mathrm{succ}(n))$. Hence $\mathrm{succ}(n) \in P$. Qed.

Therefore every natural number is an element of P. Then we have the thesis. $\square$

Definition 9. Let n be nonzero. $\mathrm{pred}(n)$ is the natural number m such that $\mathrm{succ}(m) = n$.

Let the direct predecessor of n stand for $\mathrm{pred}(n)$.

1.3 Additional constants

Definition 10. $1 = \mathrm{succ}(0)$.

Definition 11. $2 = \mathrm{succ}(1)$.

Definition 12. $3 = \mathrm{succ}(2)$.

Definition 13. $4 = \mathrm{succ}(3)$.

Definition 14. $5 = \mathrm{succ}(4)$.

Definition 15. $6 = \mathrm{succ}(5)$.

Definition 16. $7 = \mathrm{succ}(6)$.

Definition 17. $8 = \mathrm{succ}(7)$.

Definition 18. $9 = \mathrm{succ}(8)$.

2 Addition

2.1 Axioms

Signature 19. $n + m$ is a natural number.

Let the sum of n and m stand for $n + m$.

Axiom 20. **(1st addition axiom)** $n + 0 = n$.

Axiom 21. **(2nd addition axiom)** $n + \mathrm{succ}(m) = \mathrm{succ}(n + m)$.

2.2 Immediate consequences

Lemma 22. $\mathrm{succ}(n) = n + 1$.

Corollary 23. **(1st Peano axiom)** If $n + 1 = m + 1$ then $n = m$.

Corollary 24. **(2nd Peano axiom)** For no n we have $n + 1 = 0$.

Corollary 25. **(3rd Peano axiom)** Let P be a class. Assume $0 \in P$ and for all n: $n \in P \implies n + 1 \in P$. Then every natural number is an element of P.

Corollary 26. **(2nd addition axiom)** $n + (m + 1) = (n + m) + 1$.

Let $n-1$ stand for $\text{pred}(n)$.

Proposition 27. $(n+1)-1=n$.

Proof. We have $\text{succ}((n+1)-1)=n+1$. Hence $((n+1)-1)+1=n+1$. Thus $(n+1)-1=n$. □

Corollary 28. Let n be nonzero. Then $(n-1)+1=n$.

Proof. Take a natural number m such that $n=m+1$. Then $(n-1)+1=((m+1)-1)+1=m+1=n$. □

2.3 Computation laws

Proposition 29. **(NN 01 02 468785)** For all n,m,k we have

$$n+(m+k)=(n+m)+k.$$

Proof. Define $P=\{\text{natural number } k : \text{for all } n,m : n+(m+k)=(n+m)+k\}$.

(BASE CASE) 0 is contained in P. Indeed $n+(m+0)=n+m=(n+m)+0$ for all natural numbers n,m.

(INDUCTION STEP) For all k we have $k\in P \implies k+1\in P$.
Proof. Let k be a natural number. Assume $k\in P$.

Let us show that $n+(m+(k+1))=(n+m)+(k+1)$ for all natural numbers n,m.
Let n,m be natural numbers. Then $n+m$ is a natural number.

$$\begin{aligned} & n+(m+(k+1)) \\ &= n+((m+k)+1) \\ &= (n+(m+k))+1 \\ &= ((n+m)+k)+1 \\ &= (n+m)+(k+1). \end{aligned}$$

Hence the thesis. End.

Therefore we have $k+1\in P$. Qed.

Thus every natural number is an element of P. □

Proposition 30. **(NN 01 02 273100)** For all n,m we have

$$n+m=m+n.$$

Proof. Define $P = \{\text{natural number } m : n + m = m + n \text{ for all natural numbers } n\}$.

(BASE CASE 1) 0 is an element of P.
Proof. Define $Q = \{\text{natural number } n : n + 0 = 0 + n\}$.

0 belongs to Q.

For all n we have $n \in Q \implies n + 1 \in Q$.
Proof. Let n be a natural number. Assume $n \in Q$.

$$(n+1)+0$$
$$= n+1$$
$$= (n+0)+1$$
$$= (0+n)+1$$
$$= 0+(n+1).$$

Qed.

Thus every natural number belongs to Q. Therefore 0 is an element of P.
Qed.

(BASE CASE 2) 1 is contained in P.
Proof. Define $Q = \{\text{natural number } n : n + 1 = 1 + n\}$.

0 is an element of Q.

For all natural numbers n we have $n \in Q \implies n + 1 \in Q$.
Proof. Let n be a natural number. Assume that n is contained in Q.

$$(n+1)+1$$
$$= (1+n)+1$$
$$= 1+(n+1).$$

Qed.

Thus every natural number belongs to Q. Therefore 1 is an element of P.
Qed.

(INDUCTION STEP) For all natural numbers n we have $n \in P \implies n + 1 \in P$.
Proof. Let n be an natural number. Assume $n \in P$.

$(n + 1) + m = m + (n + 1)$ for all natural numbers m.
Proof. Let m be a natural number.

$$(n+1)+m$$

$$= n + (1 + m)$$
$$= (1 + m) + n$$
$$= (m + 1) + n$$
$$= m + (n + 1).$$

Qed. Qed.

Hence every natural number is an element of P. □

Proposition 31. (NN 01 02 882987) For all natural numbers n, m, k we have

$$n + k = m + k \implies n = m.$$

Proof. Define $P = \{$natural number k :for all natural numbers n, m if $n + k = m + k$ then $n = m\}$.

(BASE CASE) 0 is an element of P.

(INDUCTION STEP) For all k we have $k \in P \implies k + 1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

For all natural numbers n, m we have $n+(k+1) = m+(k+1) \implies n = m$.
Proof. Let n, m be natural numbers. Assume $n + (k + 1) = m + (k + 1)$.
Then $(n + k) + 1 = (m + k) + 1$. Hence $n + k = m + k$. Thus $n = m$. Qed.

Hence the thesis. Qed.

Therefore every natural number is an element of P. □

Corollary 32. (NN 01 02 402018) For all n, m, k we have

$$k + n = k + m \implies n = m.$$

Proof. Let n, m, k be natural numbers. Assume $k + n = k + m$. We have $k + n = n + k$ and $k + m = m + k$. Hence $n + k = m + k$. Thus $n = m$. □

3 Multiplication

3.1 Axioms

Signature 33. $n \cdot m$ is a natural number.

Let the product of n and m stand for $n \cdot m$.

Axiom 34. (1st multiplication axiom) $n \cdot 0 = 0$.

Axiom 35. (2nd multiplication axiom) $n \cdot (m + 1) = (n \cdot m) + n$.

3.2 Computation laws

Proposition 36. (NN 01 03 539933) For all n, m, k we have

$$n \cdot (m + k) = (n \cdot m) + (n \cdot k).$$

Proof. Define $P = \{\text{natural number } k : n \cdot (m + k) = (n \cdot m) + (n \cdot k) \text{ for all natural numbers } n, m\}$.

(BASE CASE) 0 is an element of P. Indeed for all natural numbers n, m we have $n \cdot (m + 0) = n \cdot m = (n \cdot m) + 0 = (n \cdot m) + (n \cdot 0)$.

(INDUCTION STEP) For all natural numbers k we have $k \in P \implies k + 1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

For all natural numbers n, m we have $n \cdot (m + (k + 1)) = (n \cdot m) + (n \cdot (k + 1))$.
Proof. Let n, m be natural numbers.

$$\begin{aligned} & n \cdot (m + (k + 1)) \\ &= n \cdot ((m + k) + 1) \\ &= (n \cdot (m + k)) + n \\ &= ((n \cdot m) + (n \cdot k)) + n \\ &= (n \cdot m) + ((n \cdot k) + n) \\ &= (n \cdot m) + (n \cdot (k + 1)). \end{aligned}$$

Hence the thesis. Qed. Qed.

Therefore every natural number is contained in P. □

Proposition 37. (NN 01 03 322712) For all n, m, k we have

$$(n + m) \cdot k = (n \cdot k) + (m \cdot k).$$

Proof. Define $P = \{\text{natural number } k : (n + m) \cdot k = (n \cdot k) + (m \cdot k) \text{ for all natural numbers } n, m\}$.

(BASE CASE) 0 belongs to P. Indeed $(n+m) \cdot 0 = 0 = 0+0 = (n \cdot 0)+(m \cdot 0)$ for all natural numbers n, m.

(INDUCTION STEP) For all natural numbers k we have $k \in P \implies k + 1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

$(n+m) \cdot (k+1) = (n \cdot (k+1)) + (m \cdot (k+1))$ for all natural numbers n, m.
Proof. Let n, m be natural numbers. We have $((n \cdot k) + ((m \cdot k) + n)) + m = (((n \cdot k) + n) + (m \cdot k)) + m$. Hence

$$(n + m) \cdot (k + 1)$$

$$= ((n + m) \cdot k) + (n + m)$$
$$= ((n \cdot k) + (m \cdot k)) + (n + m)$$
$$= (((n \cdot k) + (m \cdot k)) + n) + m$$
$$= ((n \cdot k) + ((m \cdot k) + n)) + m$$
$$= (((n \cdot k) + n) + (m \cdot k)) + m$$
$$= ((n \cdot k) + n) + ((m \cdot k) + m)$$
$$= (n \cdot (k + 1)) + (m \cdot (k + 1)).$$

Qed. Qed.

Thus every natural number is an element of P. □

Proposition 38. (NN 01 03 866630) $n \cdot 1 = n$.

Proof. $n \cdot 1 = n \cdot (0 + 1) = (n \cdot 0) + n = 0 + n = n$. □

Corollary 39. (NN 01 03 302621) $n \cdot 2 = n + n$.

Proof. $n \cdot 2 = n \cdot (1 + 1) = (n \cdot 1) + n = n + n$. □

Proposition 40. (NN 01 03 299637) For all n, m, k we have

$$n \cdot (m \cdot k) = (n \cdot m) \cdot k.$$

Proof. Define $P = \{\text{natural number } k : n \cdot (m \cdot k) = (n \cdot m) \cdot k \text{ for all natural numbers } n, m\}$.

(BASE CASE) 0 is contained in P. Indeed for all natural numbers n, m we have $n \cdot (m \cdot 0) = n \cdot 0 = 0 = (n \cdot m) \cdot 0$.

(INDUCTION STEP) For all natural numbers k we have $k \in P \implies k + 1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

For all natural numbers n, m we have $n \cdot (m \cdot (k + 1)) = (n \cdot m) \cdot (k + 1)$.
Proof. Let n, m be natural numbers.

$$n \cdot (m \cdot (k + 1))$$
$$= n \cdot ((m \cdot k) + m)$$
$$= (n \cdot (m \cdot k)) + (n \cdot m)$$
$$= ((n \cdot m) \cdot k) + (n \cdot m)$$
$$= ((n \cdot m) \cdot k) + ((n \cdot m) \cdot 1)$$
$$= (n \cdot m) \cdot (k + 1).$$

Qed. Qed.

Hence every natural number is contained in P. □

Proposition 41. (NN 01 03 850937) For all n, m we have

$$n \cdot m = m \cdot n.$$

Proof. Define $P = \{$natural number $m : n \cdot m = m \cdot n$ for all natural numbers $n\}$.

(BASE CASE 1) 0 is contained in P.
Proof.

For all natural numbers n we have $n \cdot 0 = 0 \cdot n$.
Proof. Define $Q = \{$natural number $n : n \cdot 0 = 0 \cdot n\}$.

0 is contained in Q.

For all natural numbers n we have $n \in Q \implies n+1 \in Q$.
Proof. Let n be a natural number. Assume $n \in Q$. Then

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

Qed. Qed. Qed.

(BASE CASE 2) 1 belongs to P.
Proof. Let us show that for all natural numbers n we have $n \cdot 1 = 1 \cdot n$. Define $Q = \{$natural number $n : n \cdot 1 = 1 \cdot n\}$.

0 is contained in Q.

For all natural numbers n we have $n \in Q \implies n+1 \in Q$.
Proof. Let n be a natural number. Assume $n \in Q$. Then

$$(n+1) \cdot 1$$

$$= (n \cdot 1) + 1$$

$$= (1 \cdot n) + 1$$

$$= 1 \cdot (n+1).$$

Qed.

Thus every natural number is contained in Q. Hence the thesis. End. Qed.

(INDUCTION STEP) For all natural numbers m we have $m \in P \implies m+1 \in P$.
Proof. Let m be a natural number. Assume $m \in P$.

For all natural numbers n we have $n \cdot (m+1) = (m+1) \cdot n$.
Proof. Let n be a natural number. Then

$$n \cdot (m+1)$$

$$= (n \cdot m) + (n \cdot 1)$$

$$= (m \cdot n) + (1 \cdot n)$$

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

Qed. Qed.

Hence every natural number is contained in P. □

Proposition 42. (NN 01 03 692941) For all n, m we have

$$n \cdot m = 0 \implies (n = 0 \text{ or } m = 0).$$

Proof. Let n, m be natural numbers. Assume $n \cdot m = 0$.

If n and m are not equal to 0 then we have a contradiction.
Proof. Assume $n, m \neq 0$. Take natural numbers n', m' such that $n = (n' + 1)$ and $m = (m' + 1)$. Then

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

Hence $0 = k + 1$ for some natural number k. Contradiction. Qed.

Thus $n = 0$ or $m = 0$. □

Proposition 43. (NN 01 03 799692) Assume $k \neq 0$. Then for all n, m we have

$$n \cdot k = m \cdot k \implies n = m.$$

Proof. Define $P = \{$natural number n :for all natural numbers m if $n \cdot k = m \cdot k$ and $k \neq 0$ then $n = m\}$.

(BASE CASE) 0 is contained in P.
Proof. Let us show that for all natural numbers m if $0 \cdot k = m \cdot k$ and $k \neq 0$ then $0 = m$. Let m, k be natural numbers. Assume that $0 \cdot k = m \cdot k$ and $k \neq 0$. Then $m \cdot k = 0$. Hence $m = 0$ or $k = 0$. Thus $m = 0$. End. Qed.

(INDUCTION STEP) For all natural numbers n we have $n \in P \implies n + 1 \in P$.
Proof. Let n be a natural number. Assume $n \in P$.

For all natural numbers m if $(n+1) \cdot k = m \cdot k$ and $k \neq 0$ then $n+1 = m$.
Proof. Let m be natural numbers. Assume $(n + 1) \cdot k = m \cdot k$ and $k \neq 0$.

Case $m = 0$. Then $(n + 1) \cdot k = 0$. Hence $n + 1 = 0$. Contradiction. End.

Case $m \neq 0$. Take a natural number m' such that $m = m' + 1$. Then $(n+1) \cdot k = (m'+1) \cdot k$. Hence $(n \cdot k) + k = (m' \cdot k) + k$. Thus $n \cdot k = m' \cdot k$ (by NN 01 02 882987). Then we have $n = m'$. Therefore $n + 1 = m' + 1 = m$. End. Qed. Qed.

Thus every natural number is contained in P. □

Corollary 44. (NN 01 03 169506) Assume $k \neq 0$. Then for all n, m we have

$$k \cdot n = k \cdot m \implies n = m.$$

Proof. Let n, m be natural numbers. Assume $k \cdot n = k \cdot m$. We have $k \cdot n = n \cdot k$ and $k \cdot m = m \cdot k$. Hence $n \cdot k = m \cdot k$. Thus $n = m$. □

4 Exponentiation

4.1 Axioms

Signature 45. n^m is a natural number.

Let the square of n stand for n^2. Let the cube of n stand for n^3.

Axiom 46. (1st exponentiation axiom) $n^0 = 1$.

Axiom 47. (2nd exponentiation axiom) $n^{m+1} = n^m \cdot n$.

4.2 Computation laws

Proposition 48. (NN 01 04 876526) Assume that $n \neq 0$. Then

$$0^n = 0.$$

Proof. Take a natural number m such that $n = m + 1$. Then

$0^n = 0^{m+1} = 0^m \cdot 0 = 0$. □

Proposition 49. (NN 01 04 577060) For all natural numbers n we have

$$1^n = 1.$$

Proof. Define $P = \{\text{natural number } n | 1^n = 1\}$.

(BASE CASE) P contains 0.

(INDUCTION STEP) For all natural numbers n we have $n \in P \implies n + 1 \in P$.
Proof. Let n be a natural number. Assume $n \in P$. Then

$1^{n+1} = 1^n \cdot 1 = 1 \cdot 1 = 1$. Qed.

Hence every natural number is contained in P . □

Proposition 50. **(NN 01 04 848167)** $n^1 = n$.

Proof. $n^1 = n^{0+1} = n^0 \cdot n = 1 \cdot n = n$. $\square$

Proposition 51. **(NN 01 04 846549)** $n^2 = n \cdot n$.

Proof. $n^2 = n^{1+1} = n^1 \cdot n = n \cdot n$. $\square$

Proposition 52. **(NN 01 04 461164)** For all n, m, k we have

$$k^{n+m} = k^n \cdot k^m.$$

Proof. Define $P = \{$natural number $k : n^{m+k} = n^m \cdot n^k$ for all natural numbers $n, m\}$.

(BASE CASE) P contains 0.
Proof. Let us show that for all natural numbers n, m we have $n^{m+0} = n^m \cdot n^0$. Let n, m be natural numbers. Then

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

(INDUCTION STEP) For all natural numbers k we have $k \in P \implies k + 1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

Let us show that for all natural numbers n, m we have $n^{m+(k+1)} = n^m \cdot n^{k+1}$. Let n, m be natural numbers. Then

$$\begin{aligned}
&n^{m+(k+1)} \\
&= n^{(m+k)+1} \\
&= n^{m+k} \cdot n \\
&= (n^m \cdot n^k) \cdot n \\
&= n^m \cdot (n^k \cdot n) \\
&= n^m \cdot n^{k+1}.
\end{aligned}$$

End. Qed.

Hence every natural number is contained in P. $\square$

Proposition 53. **(NN 01 04 531499)** For all n, m, k we have

$$k^{n \cdot m} = (k^n)^m.$$

Proof. Define $P = \{$natural number $k : n^{m \cdot k} = (n^m)^k$ for all natural numbers $n, m\}$.

(BASE CASE) P contains 0. Indeed $(n^m)^0 = 1 = n^0 = n^{m \cdot 0}$ for all natural numbers n, m.

(INDUCTION STEP) For all natural numbers k we have $k \in P \implies k+1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

For all natural numbers n, m we have $(n^m)^{k+1} = n^{m\cdot(k+1)}$.
Proof. Let n, m be natural numbers. Then

$$\begin{aligned}
&(n^m)^{k+1} \\
&= (n^m)^k \cdot n^m \\
&= n^{m\cdot k} \cdot n^m \\
&= n^{(m\cdot k)+m} \\
&= n^{m\cdot(k+1)}.
\end{aligned}$$

Qed. Qed.

Therefore every natural number is contained in P. □

Proposition 54. (NN 01 04 644237) For all natural numbers n, m, k we have

$$((n \cdot m)^k) = n^k \cdot m^k.$$

Proof. Define $P = \{\text{natural number } k : (n \cdot m)^k = n^k \cdot m^k \text{ for all natural numbers } n, m\}$.

(BASE CASE) P contains 0. Indeed $((n \cdot m)^0) = 1 = 1 \cdot 1 = n^0 \cdot m^0$ for all natural numbers n, m.

(INDUCTION STEP) For all natural numbers k we have $k \in P \implies k+1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

$((n \cdot m)^{k+1}) = n^{k+1} \cdot m^{k+1}$ for all natural numbers n, m.
Proof. Let n, m be natural numbers.

(Claim) We have

$$\begin{aligned}
&(n^k \cdot m^k) \cdot (n \cdot m) \\
&= ((n^k \cdot m^k) \cdot n) \cdot m \\
&= (n^k \cdot (m^k \cdot n)) \cdot m \\
&= (n^k \cdot (n \cdot m^k)) \cdot m \\
&= ((n^k \cdot n) \cdot m^k) \cdot m \\
&= (n^k \cdot n) \cdot (m^k \cdot m).
\end{aligned}$$

Hence

$$
\begin{aligned}
&(n \cdot m)^{k+1} \\
&= (n \cdot m)^k \cdot (n \cdot m) \\
&= (n^k \cdot m^k) \cdot (n \cdot m) \\
&= (n^k \cdot n) \cdot (m^k \cdot m) \\
&= n^{k+1} \cdot m^{k+1}.
\end{aligned}
$$

Qed. Qed.

Therefore every natural number is contained in P. □

Proposition 55. **(NN 01 04 857078)** For all n, m we have

$$n^m = 0 \iff (n = 0 \text{ and } m \neq 0).$$

Proof. (1) For all n, m if $n^m = 0$ then $n = 0$ and $m \neq 0$.
Proof. Define $P = \{$natural number m :for all natural numbers n if $n^m = 0$ then $n = 0$ and $m \neq 0\}$.

(BASE CASE) P contains 0. Indeed for all natural numbers n if $n^0 = 0$ then we have a contradiction.

(INDUCTION STEP) For all natural numbers m we have $m \in P \implies m + 1 \in P$.
Proof. Let m be a natural number. Assume $m \in P$.

For all natural numbers n if $n^{m+1} = 0$ then $n = 0$ and $m + 1 \neq 0$.
Proof. Let n be a natural number. Assume $n^{m+1} = 0$. Then $0 = n^{m+1} = n^m \cdot n$. Hence $n^m = 0$ or $n = 0$. We have $m + 1 \neq 0$ and if $n^m = 0$ then $n = 0$. Hence the thesis. Qed. Qed.

Thus every natural number is contained in P. Qed.

(2) For all n, m if $n = 0$ and $m \neq 0$ then $n^m = 0$.
Proof. Let n, m be natural numbers. Assume $n = 0$ and $m \neq 0$. Take a natural number k such that $m = k + 1$. Then

$$
\begin{aligned}
&n^m \\
&= n^{k+1} \\
&= n^k \cdot n \\
&= 0^k \cdot 0 \\
&= 0.
\end{aligned}
$$

Qed. □

5 Factorial

Signature 56. $n!$ is a natural number.

Axiom 57. **(1st factorial axiom)** $(0!) = 1$.

Axiom 58. **(2nd factorial axiom)** $((n+1)!) = n! \cdot (n+1)$.

Part II
Ordering

6 Ordering

6.1 Definitions and immediate consequences

Definition 59. $n < m$ iff there exists a nonzero natural number k such that $m = n + k$.

Let n is less than m stand for $n < m$. Let $n > m$ stand for $m < n$. Let n is greater than m stand for $n > m$. Let $n \nless m$ stand for n is not less than m. Let $n \ngtr m$ stand for n is not greater than m. Let n is positive stand for $n > 0$.

Definition 60. A predecessor of n is a natural number that is less than n.

Definition 61. A successor of n is a natural number that is greater than n.

Definition 62. $n \leq m$ iff there exists a natural number k such that $m = n + k$.

Let n is less than or equal to m stand for $n \leq m$. Let $n \geq m$ stand for $m \leq n$. Let n is greater than or equal to m stand for $n \geq m$. Let $n \nleq m$ stand for n is not less than or equal to m. Let $n \ngeq m$ stand for n is not greater than or equal to m.

Proposition 63. **(NN 02 01 206749)** $n \leq m$ iff $n < m$ or $n = m$.

Proof. Case $n \leq m$. Take a natural number k such that $m = n + k$. If $k = 0$ then $n = m$. If $k \neq 0$ then $n < m$. End.

Case $n < m$ or $n = m$. If $n < m$ then there is a positive natural number k such that $m = n + k$. If $n = m$ then $m = n + 0$. Thus if $n < m$ then there is a natural number k such that $m = n + k$. Hence the thesis. End. □

Proposition 64. **(NN 02 01 115117)** $0 < n$ iff $n \neq 0$.

Proof. Case $0 < n$. Take a positive natural number k such that $n = 0 + k = k$. Then we have $n \neq 0$. End.

Case $n \neq 0$. Take a natural number k such that $n = k + 1$. Then $n = 0 + (k + 1)$. $k + 1$ is positive. Hence $0 < n$. End. □

6.2 Basic properties

Proposition 65. **(NN 02 01 659871)** $n \not< n$.

Proof. Assume the contrary. Then we can take a positive natural number k such that $n = n + k$. Then we have $0 = k$. Contradiction. □

Proposition 66. **(NN 02 01 679789)** If $n < m$ then $n \neq m$.

Proof. Assume $n < m$. Take a positive natural number k such that $m = n + k$. If $n = m$ then $k = 0$. Hence $n \neq m$. □

Proposition 67. **(NN 02 01 710123)** If $n \leq m$ and $m \leq n$ then $n = m$.

Proof. Assume $n \leq m$ and $m \leq n$. Take natural numbers k, l such that $m = n + k$ and $n = m + l$. Then $m = (m + l) + k = m + (l + k)$. Hence $l + k = 0$. Therefore $l = 0 = k$. Then we have the thesis. □

Proposition 68. **(NN 02 01 662806)** If $n < m < k$ then $n < k$.

Proof. Assume $n < m < k$. Take positive natural numbers a, b such that $m = n + a$ and $k = m + b$. Then $k = (n + a) + b = n + (a + b)$. $a + b$ is positive. Hence $n < k$. □

Proposition 69. **(NN 02 01 394529)** If $n \leq m \leq k$ then $n \leq k$.

Proof. Case $n = m = k$. Obvious.

Case $n = m < k$. Obvious.

Case $n < m = k$. Obvious.

Case $n < m < k$. Obvious. □

Proposition 70. **(NN 02 01 161701)** If $n \leq m < k$ then $n < k$.

Proof. Assume $n \leq m < k$. If $n = m$ then $n < k$. If $n < m$ then $n < k$. □

Proposition 71. **(NN 02 01 807366)** If $n < m \leq k$ then $n < k$.

Proof. Assume $n < m \leq k$. If $m = k$ then $n < k$. If $m < k$ then $n < k$. □

Proposition 72. **(NN 02 01 802467)** If $n < m$ then $n + 1 \leq m$.

Proof. Assume $n < m$. Take a positive natural number k such that $m = n + k$.

Case $k = 1$. Then $m = n + 1$. Hence $n + 1 \leq m$. End.

Case $k \neq 1$. Then we can take a natural number l such that $k = l + 1$. Then $m = n + (l + 1) = (n + l) + 1 = (n + 1) + l$. l is positive. Thus $n + 1 < m$. End. □

Proposition 73. (NN 02 01 299356) For all n, m we have $n < m$ or $n = m$ or $n > m$.

Proof. Define $P = \{$natural number m :for all natural numbers n we have $n < m$ or $n = m$ or $n > m\}$.

(BASE CASE) P contains 0.

(INDUCTION STEP) For all natural numbers m we have $m \in P \implies m + 1 \in P$.
Proof. Let m be a natural number. Assume $m \in P$.

For all natural numbers n we have $n < m + 1$ or $n = m + 1$ or $n > m + 1$.
Proof. Let n be a natural number.

Case $n < m$. Obvious.

Case $n = m$. Obvious.

Case $n > m$. Take a positive natural number k such that $n = m + k$.

Case $k = 1$. Obvious.

Case$k \neq 1$. Take a natural number l such that $n = (m + 1) + l$. Hence $n > m + 1$. Indeed l is positive. End. End. Qed. Qed.

Thus every natural number is contained in P. □

Proposition 74. (NN 02 01 112345) $n \not< m$ iff $n \geq m$.

Proof. Case $n \not< m$. Then $n = m$ or $n > m$. Hence $n \geq m$. End.

Case $n \geq m$. Assume $n < m$. Then $n \leq m$. Hence $n = m$. Contradiction. End. □

6.3 Ordering and successors

Proposition 75. (NN 02 01 203608) If $n < m \leq n+1$ then $m = n+1$.

Proof. Assume $n < m \leq n + 1$. Take a positive natural number k such that $m = n + k$. Take a natural number l such that $n + 1 = m + l$. Then $n + 1 = m + l = (n + k) + l = n + (k + l)$. Hence $k + l = 1$.

We have $l = 0$.
Proof. Assume the contrary. Then $k, l > 0$.

Case $k, l = 1$. Then $k + l = 2 \neq 1$. Contradiction. End.

Case $k = 1 and l \neq 1$. Then $l > 1$. Hence $k + l > 1 + l > 1$. Contradiction. End.

Case $k \neq 1 and l = 1$. Then $k > 1$. Hence $k + l > k + 1 > 1$. Contradiction. End.

Case $k, l \neq 1$. Take natural numbers a, b such that $k = a+1$ and $l = b+1$. Indeed $k, l \neq 0$. Hence $k = a+1$ and $l = b+1$. Thus $k, l > 1$. Indeed a, b are positive. End. Qed.

Then we have $n + 1 = m + l = m + 0 = m$. □

Proposition 76. **(NN 02 01 126729)** If $n \leq m < n+1$ then $n = m$.

Proof. Assume $n \leq m < n+1$.

Case $n = m$. Obvious.

Case $n < m$. Then $n < m \leq n+1$. Hence $n = m$. End. □

Proposition 77. **(NN 02 01 408119)** $n + 1 \geq 1$.

Proof. Case $n = 0$. Obvious.

Case $n \neq 0$. Then $n > 0$. Hence $n + 1 > 0 + 1 = 1$. End. □

7 Ordering and addition

Proposition 78. **(NN 02 02 179654)** We have

$$n < m \iff n + k < m + k.$$

Proof. Case $n < m$. Take a positive natural number l such that $m = n+l$. Then $m + k = (n + l) + k = (n + k) + l$. Hence $n + k < m + k$. End.

Case $n + k < m + k$. Take a positive natural number l such that $m + k = (n + k) + l$. $(n + k) + l = n + (k + l) = n + (l + k) = (n + l) + k$. Hence $m + k = (n + l) + k$. Thus $m = n + l$. Therefore $n < m$. End. □

Corollary 79. **(NN 02 02 316437)** We have

$$n < m \iff k + n < k + m.$$

Proof. We have $k + n = n + k$ and $k + m = m + k$. Hence $k + n < k + m$ iff $n + k < m + k$. □

Corollary 80. **(NN 02 02 143631)** $n \leq m$ iff $k + n \leq k + m$.

Corollary 81. **(NN 02 02 598206)** $n \leq m$ iff $n + k \leq m + k$.

8 Ordering and multiplication

Proposition 82. **(NN 02 03 496205)** Assume $k \neq 0$. Then for all n, m we have
$$n < m \iff n \cdot k < m \cdot k.$$

Proof. Define $P = \{$natural number n :for all natural numbers m if $n \cdot k < m \cdot k$ then $n < m\}$.

Let us show that every natural number is contained in P. (BASE CASE) P contains 0.

(INDUCTION STEP) For all natural numbers n we have $n \in P \implies n + 1 \in P$. Proof. Let n be a natural number. Assume $n \in P$.

For all natural numbers m if $(n + 1) \cdot k < m \cdot k$ then $n + 1 < m$.
Proof. Let m be a natural number. Assume $(n + 1) \cdot k < m \cdot k$. Then $(n \cdot k) + k < m \cdot k$. Hence $n \cdot k < m \cdot k$. Thus $n < m$. Then $n + 1 \leq m$. If $n + 1 = m$ then $(n + 1) \cdot k = m \cdot k$. Hence the thesis. Qed. Qed.

Therefore every natural number is contained in P. End.

Let n, m be natural numbers.

Case $n < m$. Take a positive natural number l such that $m = n + l$. Then $m \cdot k = (n + l) \cdot k = (n \cdot k) + (l \cdot k)$. $l \cdot k$ is positive. Hence $n \cdot k < m \cdot k$. End.

Case $n \cdot k < m \cdot k$. Then $n < m$. Indeed n and m are contained in P. End. □

Corollary 83. **(NN 02 03 332119)** Assume $k \neq 0$. Then
$$n < m \iff k \cdot n < k \cdot m.$$

Proof. We have $k \cdot n = n \cdot k$ and $k \cdot m = m \cdot k$. Hence $k \cdot n < k \cdot m$ iff $n \cdot k < m \cdot k$. □

Proposition 84. **(NN 02 03 319805)** For all n, m we have
$$n, m > k \implies n \cdot m > k.$$

Proof. Define $P = \{$natural number n :for all natural numbers m if $n, m > k$ then $n \cdot m > k\}$.

(BASE CASE) P contains 0.

(INDUCTION STEP) For all natural numbers n we have $n \in P \implies n + 1 \in P$.
Proof. Let n be a natural number. Assume $n \in P$.

For all natural numbers m if $n + 1, m > k$ then $(n + 1) \cdot m > k$.
Proof. Let m be a natural number. Assume $n+1, m > k$. Then $(n+1) \cdot m =$

$(n \cdot m) + m$. If $n = 0$ then $(n \cdot m) + m = 0 + m = m > k$. If $n \neq 0$ then $(n \cdot m) + m > m > k$. Indeed if $n \neq 0 then n \cdot m > 0$. Indeed $m > 0$. Hence $(n + 1) \cdot m > k$. Qed. Qed.

Hence every natural number is contained in P. □

Corollary 85. **(NN 02 03 496763)** We have

$$n \leq m \implies k \cdot n \leq k \cdot m.$$

Corollary 86. **(NN 02 03 575338)** Assume $k \neq 0$. Then

$$k \cdot n \leq k \cdot m \implies n \leq m.$$

Corollary 87. **(NN 02 03 419208)** We have

$$n \leq m \implies n \cdot k \leq m \cdot k.$$

Corollary 88. **(NN 02 03 582576)** Assume $k \neq 0$. Then

$$n \cdot k \leq m \cdot k \implies n \leq m.$$

Proposition 89. **(NN 02 03 252473)** Let $k > 1$ and $m > 0$. Assume $n = k \cdot m$. Then $n > m$.

Proof. Take a natural number l such that $k = l + 2$. Then

$$n$$

$$= k \cdot m$$
$$= (l + 2) \cdot m$$
$$= (l \cdot m) + (2 \cdot m)$$
$$= (l \cdot m) + (m + m)$$
$$= ((l \cdot m) + m) + m$$
$$= ((l + 1) \cdot m) + m$$
$$\geq 1 + m$$
$$> m.$$

□

9 Ordering and exponentiation

Proposition 90. **(NN 02 04 770958)** Assume $k \neq 0$. Then for all n, m we have

$$n < m \iff n^k < m^k.$$

Proof. Define $P = \{\text{natural number } k' : \text{for all natural numbers } n, m \text{ if } n < m \text{ and } k' > 1 \text{ then } n^{k'} < m^{k'}\}$.

Let us show that every natural number is contained in P. (BASE CASE 1) P contains 0.

(BASE CASE 2) P contains 1.

(BASE CASE 3) P contains 2.
Proof. Let us show that for all natural numbers n, m if $n < m$ then $n^2 < m^2$. Let n, m be natural numbers. Assume $n < m$.

Case $n = 0$ or $m = 0$. Obvious.

Case $n, m \neq 0$. Then $n \cdot n < n \cdot m < m \cdot m$. Hence $n^2 = n \cdot n < n \cdot m < m \cdot m = m^2$. End. End. Qed.

(INDUCTION STEP) For all natural numbers k' we have $k' \in P \implies k' + 1 \in P$.
Proof. Let k' be a natural number. Assume $k' \in P$.

For all natural numbers n, m if $n < m$ and $k' + 1 > 1$ then $n^{k'+1} < m^{k'+1}$.
Proof. Let n, m be natural numbers. Assume $n < m$ and $k' + 1 > 1$. Then $n^{k'} < m^{k'}$. Indeed $k' \neq 0$ and $if k' = 1$ then $n^{k'} < m^{k'}$.

Case $k' \leq 1$. Then $k' = 0$ or $k' = 1$. Hence $k' + 1 = 1$ or $k' + 1 = 2$. Thus $k' + 1 \in P$. Therefore $n^{k'+1} < m^{k'+1}$. End.

Case $k' > 1$. Case $n = 0$. Then $m \neq 0$. Hence $n^{k'+1} = 0 < m^{k'} \cdot m = m^{k'+1}$. Thus $n^{k'+1} < m^{k'+1}$. End.

Case $n \neq 0$. Then $n^{k'} \cdot n < m^{k'} \cdot n < m^{k'} \cdot m$. Indeed $m^{k'} \neq 0$. Hence $n^{k'+1} = n^{k'} \cdot n < m^{k'} \cdot n < m^{k'} \cdot m = m^{k'+1}$. Thus $n^{k'+1} < m^{k'+1}$ (by NN 02 01 662806). End. End.

Hence the thesis. Indeed $k' \leq 1$ or $k' > 1$. Qed.

$k' + 1 \in P$. Qed.

Therefore every natural number is contained in P. End.

Define $Q = \{\text{natural number } k' : \text{for all natural numbers } n, m \text{ if } n \geq m \text{ then } n^{k'} \geq m^{k'}\}$.

Let us show that every natural number is contained in Q. (BASE CASE) Q contains 0.

(INDUCTION STEP) For all natural numbers k' we have $k' \in Q \implies$

$k' + 1 \in Q$.
Proof. Let k' be a natural number. Assume $k' \in Q$.

For all natural numbers n, m if $n \geq m$ then $n^{k'+1} \geq m^{k'+1}$.
Proof. Let n, m be natural numbers. Assume $n \geq m$. Then $n^{k'} \geq m^{k'}$. Hence $n^{k'} \cdot n \geq m^{k'} \cdot n \geq m^{k'} \cdot m$. Thus $n^{k'+1} = n^{k'} \cdot n \geq m^{k'} \cdot n \geq m^{k'} \cdot m = m^{k'+1}$. Therefore $n^{k'+1} \geq m^{k'+1}$ (by NN 02 01 394529). Qed.

Hence the thesis. Indeed $k' + 1$ is a natural number. Qed.

Thus every natural number is contained in Q. End.

Let n, m be natural numbers.

Case $n < m$. Case $k = 1$. Obvious.

Case$k \neq 1$. Then $k > 1$. Indeed $k < 1$ or $k = 1$ or $k > 1$. Hence $n^k < m^k$. Indeed n and m belong to P. End. End.

Case $n^k < m^k$. Then $n^k \not\geq m^k$. Hence $n \not\geq m$. Indeed n and m are contained in Q. Thus $n < m$. End. ☐

Corollary 91. (NN 02 04 537812) Assume $k \neq 0$. Then

$$n^k = m^k \implies n = m.$$

Proof. Assume $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $n^k < m^k$. If $m < n$ then $m^k < n^k$. Thus $n^k \neq m^k$. Hence the thesis. ☐

Corollary 92. (NN 02 04 707319) Assume $k \neq 0$. Then

$$n^k \leq m^k \iff n \leq m.$$

Proof. If $n^k < m^k$ then $n < m$. If $n^k = m^k$ then $n = m$.

If $n < m$ then $n^k < m^k$. If $n = m$ then $n^k = m^k$. ☐

Proposition 93. (NN 02 04 274623) Assume $k > 1$. Then for all n, m we have

$$n < m \iff k^n < k^m.$$

Proof. Define $P = \{$natural number m : for all natural numbers n if $k > 1$ and $n < m$ then $k^n < k^m\}$.

Let us show that every natural number is contained in P.

(BASE CASE) P contains 0.

(INDUCTION STEP) For all natural numbers m we have $m \in P \implies m + 1 \in P$.
Proof. Let m be a natural number. Assume $m \in P$.

For all natural numbers n if $k > 1$ and $n < m + 1$ then $k^n < k^{m+1}$.
Proof. Let n be natural numbers. Assume $k > 1$ and $n < m + 1$. Then

$n \leq m$. We have $k^m \cdot 1 < k^m \cdot k$. Indeed $k^m \neq 0$. If $n = m$ then $k^n = k^m < k^m \cdot k = k^{m+1}$. If $n < m$ then $k^n < k^m < k^m \cdot k = k^{m+1}$. Qed. Qed.

Hence every natural number is contained in P. End.

Define $Q = \{$natural number n : for all natural numbers m if $n \geq m$ then $k^n \geq k^m$ or $k \leq 1\}$.

Let us show that every natural number is contained in Q.

(BASE CASE) $0 \in Q$.

(INDUCTION STEP) For all natural numbers n we have $n \in Q \implies n + 1 \in Q$.
Proof. Let n be a natural number. Assume $n \in Q$.

For all natural numbers m if $n + 1 \geq m$ then $k^{n+1} \geq k^m$ or $k \leq 1$.
Proof. Let m be natural numbers. Assume $n + 1 \geq m$.

Case $n + 1 = m$. Obvious.

Case $n + 1 > m$. Then $n \geq m$. Hence $k^n \geq k^m$ or $k \leq 1$.

Case $k \leq 1$. Obvious.

Case $k^n \geq k^m$. We have $k^n \cdot 1 \leq k^n \cdot k$. Indeed $1 \leq k$ and $k^n \neq 0$. Hence $k^m \leq k^n = k^n \cdot 1 \leq k^n \cdot k = k^{n+1}$. End. End. Qed. Qed.

Thus every natural number is contained in Q. End.

Let n, m be natural numbers.

Case $n < m$. Then $k^n < k^m$. Indeed n and m are contained in P. End.

Case $k^n < k^m$. Then it is wrong that $k^n \geq k^m$ or $k \leq 1$. Hence $n \ngeq m$. Indeed n and m are contained in Q. Thus $n < m$. End. □

Corollary 94. **(NN 02 04 837306)** Assume $k > 1$. Then

$$k^n = k^m \implies n = m.$$

Proof. Assume $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $k^n < k^m$. If $m < n$ then $k^m < k^n$. Thus $k^n \neq k^m$. Hence the thesis. □

Corollary 95. **(NN 02 04 734298)** Assume $k > 1$. Then

$$n \leq m \iff k^n \leq k^m.$$

10 Induction

10.1 Least natural numbers

Let P denote a class.

Definition 96. A least natural number of P is a natural number n such that $n \in P$ and no natural number that is less than n belongs to P.

Lemma 97. Let n, m be least natural numbers of P. Then $n = m$.

Proof. Assume $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $n \notin P$ and if $m < n$ then $m \notin P$. Contradiction. Therefore $n = m$. □

Theorem 98. **(NN 02 05 124228)** Assume that P contains some natural number. Then P has a least natural number.

Proof. Assume the contrary. Define $Q = \{$natural number $n : n$ is less than any natural number m such that $m \in P\}$.

Let us show that every natural number belongs to Q.

(BASE CASE) Q contains 0.
Proof. If P contains 0 then 0 is the least natural number of P. Hence 0 is less than any natural number m such that $m \in P$. Therefore Q contains 0. Qed.

For all natural numbers n we have $n \in Q \implies n + 1 \in Q$.
Proof. Let n be a natural number. Assume $n \in Q$. Then n is less than any natural number m such that $m \in P$. Assume that Q does not contain $n+1$. Then we can take a natural number m such that $m \in P$ and $n + 1 \not< m$. Hence $n < m \leq n + 1$. Thus $m = n + 1$. Then $n + 1$ is the least natural number of P. Contradiction. Qed. End.

Then every natural number is less than any natural number n such that $n \in P$. Hence there is no natural number n such that $n \in P$. Contradiction. □

10.2 Induction via predecessors

Theorem 99. **(NN 02 05 167446)** Assume for all natural numbers n if P contains all predecessors of n then P contains n. Then P contains every natural number.

Proof. Assume the contrary. Take a natural number n such that P does not contain n. Define $Q = \{$natural number $k : k \notin P\}$. Then Q contains n. Thus we can take a least natural number m of Q. Hence Q does not contain any predecessor of m. Therefore P contains all predecessors of m. Thus P contains m. Contradiction. □

10.3 Induction above a certain number

Theorem 100. (NN 02 05 497603) Let k be a natural number such that $k \in P$. Suppose that for all natural numbers n such that $n \geq k$ we have $n \in P \implies n+1 \in P$. Then for every natural number n such that $n \geq k$ we have $n \in P$.

Proof. Define $Q = \{\text{natural number } n : \text{if } n \geq k \text{ then } n \in P\}$.

Let us show that every natural number belongs to Q.

(BASE CASE) We have $0 \in Q$.

(INDUCTION STEP) For all natural numbers n we have $n \in Q \implies n+1 \in Q$.
Proof. Let n be a natural number. Assume $n \in Q$.

If $n+1 \geq k$ then $n+1 \in P$.
Proof. Assume $n+1 \geq k$.

Case $n < k$. Then $n+1 = k$. Hence $n+1 \in P$. End.

Case $n \geq k$. Then $n \in P$. Hence $n+1 \in P$. End. Qed.

Thus we have $n+1 \in Q$. Qed. End.

Therefore Q contains every natural number. Hence the thesis. □

11 Standard exercises

Proposition 101. (NN 02 06 276270) We have

$$(n+1)^2 = (n^2 + (2 \cdot n)) + 1.$$

Proof. We have

$$\begin{aligned}
&(n+1)^2 \\
&= (n+1) \cdot (n+1) \\
&= ((n+1) \cdot n) + (n+1) \\
&= ((n \cdot n) + n) + (n+1) \\
&= (n^2 + n) + (n+1) \\
&= ((n^2 + n) + n) + 1 \\
&= (n^2 + (n+n)) + 1 \\
&= (n^2 + (2 \cdot n)) + 1.
\end{aligned}$$

□

Proposition 102. (NN 02 06 671464) For all n if $n \geq 3$ then

$$n^2 > (2 \cdot n) + 1.$$

Proof. Define $P = \{\text{natural number } n : n^2 > (2 \cdot n) + 1\}$.

(BASE CASE) P contains 3.

(INDUCTION STEP) For all natural numbers n such that $n \geq 3$ we have $n \in P \implies n + 1 \in P$.
Proof. Let n be a natural number. Suppose $n \geq 3$. Assume $n \in P$.

$(n^2 + (2 \cdot n)) + 1 > (((2 \cdot n) + 1) + (2 \cdot n)) + 1$. Indeed $n^2 + (2 \cdot n) > ((2 \cdot n) + 1) + (2 \cdot n)$.

$(2 \cdot (n + n)) + 1 > (2 \cdot (n + 1)) + 1$. Indeed $2 \cdot (n + n) > 2 \cdot (n + 1)$. Indeed $n + n > n + 1$ and $2 \neq 0$.

Hence

$$\begin{aligned}
&(n+1)^2 \\
&= (n^2 + (2 \cdot n)) + 1 \\
&> (((2 \cdot n) + 1) + (2 \cdot n)) + 1 \\
&> ((2 \cdot n) + (2 \cdot n)) + 1 \\
&= (2 \cdot (n + n)) + 1 \\
&> (2 \cdot (n + 1)) + 1.
\end{aligned}$$

Thus $(n + 1)^2 > (2 \cdot (n + 1)) + 1$ (by NN 02 01 662806). Qed.

Therefore P contains every natural number n such that $n \geq 3$ (by NN 02 05 497603). $\square$

Proposition 103. (NN 02 06 205395) For all n if $n \geq 5$ then

$$2^n > n^2.$$

Proof. Define $P = \{\text{natural number } n : 2^n > n^2\}$.

(BASE CASE) P contains 5. Indeed $2^5 = 2 \cdot (2 \cdot (2 \cdot (2 \cdot 2))) = (5 \cdot 5) + 7 > 5 \cdot 5 = 5^2$.

(INDUCTION STEP) For all natural numbers n such that $n \geq 5$ we have $n \in P \implies n + 1 \in P$.
Proof. Let n be a natural number. Suppose $n \geq 5$. Assume $n \in P$. Then $2^n > n^2$.

(1) $2^n \cdot 2 > n^2 \cdot 2$ (by NN 02 03 496205). Indeed $2 \neq 0$.

(2) $n^2 \cdot 2 = n^2 + n^2$.

(3) $n^2 + n^2 > n^2 + ((2 \cdot n) + 1)$. Indeed $n^2 > (2 \cdot n) + 1$.

(4) $n^2 + ((2 \cdot n) + 1) = (n + 1)^2$.

Hence

$$2^{n+1}$$

$$= 2^n \cdot 2$$

$$> n^2 \cdot 2$$

$$= n^2 + n^2$$

$$> n^2 + ((2 \cdot n) + 1)$$

$$= (n+1)^2.$$

Thus $2^{n+1} > (n+1)^2$. Qed.

Therefore P contains every natural number n such that $n \geq 5$ (by NN 02 05 497603). $\square$

Proposition 104. **(NN 02 06 527159)** For all n if $n \geq 2$ then

$$n^n > n!.$$

Proof. Define $P = \{\text{natural number } n : n^n > n!\}$.

(BASE CASE) P contains 2.

(INDUCTION STEP) For all natural numbers n such that $n \geq 2$ we have $n \in P \implies n+1 \in P$.
Proof. Let n be a natural number. Suppose $n \geq 2$. Assume $n \in P$.

(1) $(n+1)^n \cdot (n+1) > n^n \cdot (n+1)$ (by NN 02 03 496205). Indeed $(n+1)^n > n^n$ and $n+1 \neq 0$. Indeed $n+1 > nandn \neq 0$.

(2) $n^n \cdot (n+1) > n! \cdot (n+1)$ (by NN 02 03 496205). Indeed $n^n > n!$ and $n+1 \neq 0$.

Hence

$$(n+1)^{n+1}$$

$$= (n+1)^n \cdot (n+1)$$

$$> n^n \cdot (n+1)$$

$$> n! \cdot (n+1)$$

$$= (n+1)!.$$

Thus $(n+1)^{n+1} > (n+1)!$. Qed.

Therefore P contains every natural number n such that $n \geq 2$ (by NN 02 05 497603). $\square$

Proposition 105. **(NN 02 06 493411)** For all n if $n \geq 4$ then

$$n! > 2^n.$$

Proof. Define $P = \{\text{natural number } n : n! > 2^n\}$.

(BASE CASE) P contains 4.
Proof.

$$
\begin{aligned}
&(4!) \\
&= 4 \cdot (3 \cdot 2) \\
&= 2 \cdot (2 \cdot (3 \cdot 2)) \\
&= 3 \cdot (2 \cdot (2 \cdot 2)) \\
&> 2 \cdot (2 \cdot (2 \cdot 2)) \\
&= 2^4.
\end{aligned}
$$

Qed.

(INDUCTION STEP) For all natural numbers n such that $n \geq 4$ we have $n \in P \implies n+1 \in P$.
Proof. Let n be a natural number. Suppose $n \geq 4$. Assume $n \in P$. Then $n! > 2^n$.

(1) $0 \neq n+1 > 2$. Indeed $n > 1$.

(2) $n! \cdot (n+1) > 2^n \cdot (n+1)$ (by NN 02 03 496205).

(3) $2^n \cdot (n+1) > 2^n \cdot 2$ (by NN 02 03 332119). Indeed $2^n \neq 0$.

Hence

$$
\begin{aligned}
&((n+1)!) \\
&= n! \cdot (n+1) \\
&> 2^n \cdot (n+1) \\
&> 2^n \cdot 2 \\
&= 2^{n+1}.
\end{aligned}
$$

Thus $(n+1)! > 2^{n+1}$. Qed.

Therefore P contains every natural number n such that $n \geq 4$ (by NN 02 05 497603). $\square$

Part III
Divisibility

12 Divisibility

12.1 Definitions

Definition 106. n divides m iff there exists a natural number k such that $n \cdot k = m$.

Let $n \mid m$ stand for n divides m. Let m is divisible by n stand for n divides m. Let $n \nmid m$ stand for n does not divide m.

Definition 107. A factor of n is a natural number that divides n.

Let a divisor of n stand for a factor of n.

Definition 108. n is even iff n is divisible by 2.

Definition 109. n is odd iff n is not divisible by 2.

12.2 Basic properties

Proposition 110. **(NN 03 01 148842)** Every natural number divides 0.

Proof. Let n be a natural number. We have $n \cdot 0 = 0$. Hence $n \mid 0$. □

Proposition 111. **(NN 03 01 295259)** Every natural number that is divisible by 0 is equal to 0.

Proof. Let n be a natural number. Assume $0 \mid n$. Take a natural number k such that $0 \cdot k = n$. Then we have $n = 0$. □

Proposition 112. **(NN 03 01 856465)** 1 divides every natural number.

Proof. Let n be a natural number. We have $1 \cdot n = n$. Hence $1 \mid n$. □

Proposition 113. **(NN 03 01 258975)** Every natural number n divides n.

Proof. Let n be a natural number. We have $n \cdot 1 = n$. Hence $n \mid n$. □

Proposition 114. **(NN 03 01 211137)** Every natural number that divides 1 is equal to 1.

Proof. Let n be a natural number. Assume $n \mid 1$. Take a natural number k such that $n \cdot k = 1$. Suppose $n \neq 1$. Then $n < 1$ or $n > 1$.

Case $n < 1$. Then $n = 0$. Hence $0 = 0 \cdot k = n \cdot k = 1$. Contradiction. End.

Case $n > 1$. We have $k \neq 0$. Indeed if $k = 0$ then $1 = n \cdot k = n \cdot 0 = 0$. Hence $k \geq 1$. Take a positive natural number l such that $n = 1 + l$. Then $1 < 1 + l = n = n \cdot 1 \leq n \cdot k$. Hence $1 < n$. Contradiction. End. ☐

Proposition 115. **(NN 03 01 364584)** We have

$$(n \mid m \text{ and } m \mid k) \implies n \mid k.$$

Proof. Assume $n \mid m$ and $m \mid k$. Take natural numbers l, l' such that $n \cdot l = m$ and $m \cdot l' = k$. Then $n \cdot (l \cdot l') = (n \cdot l) \cdot l' = m \cdot l' = k$. Hence $n \mid k$. ☐

Proposition 116. **(NN 03 01 710814)** We have

$$n \mid m \implies k \cdot n \mid k \cdot m.$$

Proof. Assume $n \mid m$. Take a natural number l such that $n \cdot l = m$. Then $(k \cdot n) \cdot l = k \cdot (n \cdot l) = k \cdot m$. Hence $k \cdot n \mid k \cdot m$. ☐

Proposition 117. **(NN 03 01 382863)** Assume $k \neq 0$. Then

$$k \cdot n \mid k \cdot m \implies n \mid m.$$

Proof. Assume $k{\cdot}n \mid k{\cdot}m$. Take a natural number l such that $(k{\cdot}n){\cdot}l = k{\cdot}m$. Then $k \cdot (n \cdot l) = k \cdot m$. Hence $n \cdot l = m$. Thus $n \mid m$. ☐

Proposition 118. **(NN 03 01 210721)** If $k \mid n$ and $k \mid m$ then $k \mid (n' \cdot n) + (m' \cdot m)$ for all natural numbers n', m'.

Proof. Assume $k \mid n$ and $k \mid m$. Let n', m' be natural numbers. Take natural numbers l, l' such that $k \cdot l = n$ and $k \cdot l' = m$. Then

$$\begin{aligned}
&k \cdot ((n' \cdot l) + (m' \cdot l')) \\
&= (k \cdot (n' \cdot l)) + (k \cdot (m' \cdot l')) \\
&= ((k \cdot n') \cdot l) + ((k \cdot m') \cdot l') \\
&= (n' \cdot (k \cdot l)) + (m' \cdot (k \cdot l')) \\
&= (n' \cdot n) + (m' \cdot m).
\end{aligned}$$

☐

Corollary 119. We have

$$(k \mid n \text{ and } k \mid m) \implies k \mid n + m.$$

Proof. Assume $k \mid n$ and $k \mid m$. Take $n' = 1$ and $m' = 1$. Then $k \mid (n' \cdot n) + (m' \cdot m)$ (by NN 03 01 210721). $(n' \cdot n) + (m' \cdot m) = n + m$. Hence $k \mid n + m$. □

Proposition 120. (NN 03 01 695362) Assume $k \mid n$ and $k \mid n + m$. Then $k \mid m$.

Proof. Case $k = 0$. Obvious.

Case $k \neq 0$. Take a natural number l such that $n = k \cdot l$. Take a natural number l' such that $n + m = k \cdot l'$. Then $(k \cdot l) + m = k \cdot l'$. We have $l' \geq l$. Indeed if $l' < l$ then $n + m = k \cdot l' < k \cdot l = n$. Hence we can take a natural number l'' such that $l' = l + l''$. Then $(k \cdot l) + m = k \cdot l' = k \cdot (l + l'') = (k \cdot l) + (k \cdot l'')$ (by NN 01 03 539933). Thus $m = (k \cdot l'')$. Therefore $k \mid m$. End. □

Proposition 121. (NN 03 01 376821) Let n, m be nonzero. If $m \mid n$ then $m \leq n$.

Proof. Assume $m \mid n$. Take a natural number k such that $m \cdot k = n$. If $k = 0$ then $n = m \cdot k = m \cdot 0 = 0$. Thus $k \geq 1$. Assume $m > n$. Then $n = m \cdot k \geq m \cdot 1 = m > n$. Hence $n > n$. Contradiction. □

13 Euclidean division

Proposition 122. (NN 03 02 332233) For all natural numbers n, m such that m is nonzero there exist natural numbers q, r such that

$$n = (m \cdot q) + r$$

and $r < m$.

Proof. (1) Define $P = \{$natural number n : for all nonzero natural numbers m there exist natural numbers q, r such that $r < m$ and $n = (m \cdot q) + r\}$.

(BASE CASE) P contains 0. Proof. Take $q = 0$ and $r = 0$. Then for all nonzero natural numbers m we have $r < m$ and $0 = (m \cdot q) + r$. Hence $0 \in P$. Qed.

(INDUCTION STEP) For all natural numbers n: $n \in P \implies n + 1 \in P$. Proof. Let n be a natural number. Assume $n \in P$.

Let us show that for all nonzero natural numbers m there exist natural numbers q, r such that $r < m$ and $n + 1 = (m \cdot q) + r$. Let m be a nonzero natural number. Take natural numbers q', r' such that $r' < m$ and $n = (m \cdot q') + r'$ (by 1). Indeed $n \in P$. We have $r' + 1 < m$ or $r' + 1 = m$.

Case $r'+1 < m$. Take natural numbers q, r such that $q = q'$ and $r = r'+1$. Then $r < m$ and $n+1 = ((q' \cdot m) + r') + 1 = (q' \cdot m) + (r'+1) = (q \cdot m) + r$. End.

Case $r' + 1 = m$. Take natural numbers q, r such that $q = q' + 1$ and $r = 0$. Then $r < m$ and $n + 1 = ((q' \cdot m) + r') + 1 = (q' \cdot m) + (r' + 1) = (q' \cdot m) + m = (q' + 1) \cdot m = (q \cdot m) + r$. End. End. Qed.

Then P contains every natural number. Let n, m be a natural numbers such that m is nonzero. Then $n \in P$. Hence the thesis (by 1). □

Lemma 123. Let m be nonzero. Let q, q', r, r' be natural numbers such that $n = (m \cdot q) + r$ and $n = (m \cdot q') + r'$ and $r, r' < m$. Then $q = q'$ and $r = r'$.

Proof. We have $(m \cdot q) + r = (m \cdot q') + r'$.

Case $q \geq q'$ and $r \geq r'$. Take natural numbers q'', r'' such that $q = q' + q''$ and $r = r' + r''$. Then $(m \cdot (q' + q'')) + (r' + r'') = (m \cdot q') + r'$. We have $(m \cdot (q'+q'')) + (r'+r'') = (m \cdot (q'+q'')) + (r''+r') = ((m \cdot (q'+q'')) + r'') + r'$. Hence $((m \cdot (q'+q'')) + r'') + r' = (m \cdot q') + r'$. Thus $(m \cdot (q'+q'')) + r'' = m \cdot q'$. We have $m \cdot (q' + q'') = (m \cdot q') + (m \cdot q'')$. Hence $((m \cdot q') + (m \cdot q'')) + r'' = (m \cdot q') + ((m \cdot q'') + r'') = m \cdot q'$. Thus $(m \cdot q'') + r'' = 0$. Therefore $r'' = 0$ and $m \cdot q'' = 0$. Consequently $q'' = 0$. Indeed $m \neq 0$. Then we have $q = q' + 0 = q'$ and $r = r' + 0 = r'$. End.

Case $q \geq q'$ and $r < r'$. Take a natural number q'' such that $q = q' + q''$. Take a nonzero natural number r'' such that $r' = r + r''$. Then $(m \cdot (q' + q'')) + r = (m \cdot q') + (r + r'')$. We have $(m \cdot q') + (r + r'') = (m \cdot q') + (r'' + r) = ((m \cdot q') + r'') + r$. Hence $(m \cdot (q' + q'')) + r = ((m \cdot q') + r'') + r$. Thus $m \cdot (q' + q'') = (m \cdot q') + r''$. We have $m \cdot (q' + q'') = (m \cdot q') + (m \cdot q'')$. Hence $(m \cdot q') + (m \cdot q'') = (m \cdot q') + r''$. Thus $m \cdot q'' = r'' < r' < m$. Therefore $q'' = 0$. Indeed if $q'' \geq 1$ then $m \cdot q'' \geq m$. Consequently $q = q' + 0 = q'$. Hence we have $(m \cdot q) + r = (m \cdot q) + r'$. Thus $r = r'$. End.

Case $q < q'$ and $r \geq r'$. Take a nonzero natural number q'' such that $q' = q + q''$. Take a natural number r'' such that $r = r' + r''$. Then $(m \cdot q) + (r' + r'') = (m \cdot (q + q'')) + r'$. We have $(m \cdot q) + (r' + r'') = (m \cdot q) + (r'' + r') = ((m \cdot q) + r'') + r'$. Hence $((m \cdot q) + r'') + r' = (m \cdot (q + q'')) + r'$. Thus $(m \cdot q) + r'' = m \cdot (q + q'')$. We have $m \cdot (q + q'') = (m \cdot q) + (m \cdot q'')$. Hence $(m \cdot q) + r'' = (m \cdot q) + (m \cdot q'')$. Thus $m > r > r'' = m \cdot q''$. Therefore $q'' = 0$. Indeed if $q'' \geq 1$ then $m \cdot q'' \geq m$. Consequently $q' = q + 0 = q$. Hence we have $(m \cdot q) + r = (m \cdot q) + r'$. Thus $r = r'$. End.

Case $q < q'$ and $r < r'$. Take nonzero natural numbers q'', r'' such that $q' = q + q''$ and $r' = r + r''$. Then $(m \cdot (q + q'')) + (r + r'') = (m \cdot q) + r$. We have $(m \cdot (q+q'')) + (r+r'') = (m \cdot (q+q'')) + (r''+r) = ((m \cdot (q+q'')) + r'') + r$. Hence $((m \cdot (q + q'')) + r'') + r = (m \cdot q) + r$. Thus $(m \cdot (q + q'')) + r'' = m \cdot q$. We have $m \cdot (q + q'') = (m \cdot q) + (m \cdot q'')$. Hence $((m \cdot q) + (m \cdot q'')) + r'' =$

$(m \cdot q) + ((m \cdot q'') + r'') = m \cdot q$. Thus $(m \cdot q'') + r'' = 0$. Therefore $r'' = 0$ and $m \cdot q'' = 0$. Consequently $q'' = 0$. Indeed $m \neq 0$. Then we have $q' = q + 0 = q$ and $r' = r + 0 = r$. End. $\square$

Definition 124. Let m be nonzero. $n \mod m$ is the natural number r such that $r < m$ and there exists a natural number q such that $n = (m \cdot q) + r$.

Let the remainder of n over m stand for $n \mod m$.

Definition 125. Let m be nonzero. $n \operatorname{div} m$ is the natural number q such that $n = (m \cdot q) + r$ for some natural number r that is less than m.

Let the quotient of n over m stand for $n \operatorname{div} m$.

Definition 126. Let k be nonzero. $n \equiv m (\mathrm{mod}\ k)$ iff $n \mod k = m \mod k$.

Let n and m are congruent modulo k stand for $n \equiv m (\mathrm{mod}\ k)$.
Let n', n'' denote natural numbers.

Proposition 127. **(NN 03 02 188421)** Let m be nonzero. Then

$$n \equiv n (\mathrm{mod}\ m).$$

Proof. We have $n \mod m = n \mod m$. $n \equiv n (\mathrm{mod}\ m)$. $\square$

Proposition 128. **(NN 03 02 880545)** Let m be nonzero. Then

$$n \equiv n' (\mathrm{mod}\ m) \implies n' \equiv n (\mathrm{mod}\ m).$$

Proof. Assume $n \equiv n' (\mathrm{mod}\ m)$. Then $n \mod m = n' \mod m$. Hence $n' \mod m = n \mod m$. Thus $n' \equiv n (\mathrm{mod}\ m)$. $\square$

Proposition 129. **(NN 03 02 310316)** Let m be nonzero. Then

$$(n \equiv n' (\mathrm{mod}\ m) \text{ and } n' \equiv n'' (\mathrm{mod}\ m)) \implies n \equiv n'' (\mathrm{mod}\ m).$$

Proof. Assume $n \equiv n' (\mathrm{mod}\ m)$ and $n' \equiv n'' (\mathrm{mod}\ m)$. Then $n \mod m = n' \mod m$ and $n' \mod m = n'' \mod m$. Hence $n \mod m = n'' \mod m$. Thus $n \equiv n'' (\mathrm{mod}\ m)$. $\square$

14 Primes

14.1 Definitions

Definition 130. A trivial divisor of n is a divisor m of n such that $m = 1$ or $m = n$.

Definition 131. A nontrivial divisor of n is a divisor m of n such that $m \neq 1$ and $m \neq n$.

Definition 132. n is prime iff $n > 1$ and n has no nontrivial divisors.

Let n is compound stand for n is not prime. Let a prime number stand for a natural number that is prime.

Definition 133. n is composite iff $n > 1$ and n has a nontrivial divisor.

14.2 Basic properties

Proposition 134. (NN 03 03 357744) Let $n > 1$. Then n is prime iff every divisor of n is a trivial divisor of n.

Proposition 135. (NN 03 03 175431) 2 and 3 are prime.

Proof. Let us show that 2 is prime. Let k be a divisor of 2. Then $0 < k \leq 2$. Hence $k = 1$ or $k = 2$. Thus k is a trivial divisor of 2. End.

Let us show that 3 is prime. Let k be a divisor of 3. Then $0 < k \leq 3$. Hence $k = 1$ or $k = 2$ or $k = 3$.

2 does not divide 3. Proof. Assume the contrary. Take a natural number l such that $3 = 2 \cdot l$. If $l = 0$ then $3 = 2 \cdot 0 = 0$. If $l = 1$ then $3 = 2 \cdot 1 = 2$. If $l \geq 2$ then $3 = 2 \cdot l \geq 2 \cdot 2 = 4 > 3$. Hence it is wrong that $3 = 2 \cdot l$. Contradiction. Qed.

Therefore $k = 1$ or $k = 3$. Thus k is a trivial divisor of 3. End. ☐

Proposition 136. (NN 03 03 520376) Let p be a prime number. If p is even then $p = 2$.

Proof. Assume that p is even. Then 2 divides p. Hence 2 is a trivial divisor of p. Thus $p = 2$. ☐

Proposition 137. (NN 03 03 130748) Every natural number that is greater than 1 has a prime divisor.

Proof. Define $P = \{$natural number n :if $n > 1$ then n has a prime divisor $\}$.

Let us show that for every natural number n if P contains all predecessors of n then P contains n. Let n be a natural number. Assume that P contains all predecessors of n. $n = 0$ or $n = 1$ or n is prime or n is composite.

Case $n = 0$ or $n = 1$. Trivial.

Case n is prime. Obvious.

Case n is composite. Take a nontrivial divisor m of n. Then $1 < m < n$. m is contained in P. Hence we can take a prime divisor p of m. Then we have $p \mid m \mid n$. Thus $p \mid n$. Therefore p is a prime divisor of n. End. End.

Thus every natural number belongs to P (by NN 02 05 167446). ☐

Proposition 138. **(NN 03 03 306779)** Let n be composite. Then n has a nontrivial divisor m such that $m^2 \leq n$.

Proof. Define $A = \{\text{natural number } m : m \text{ is a nontrivial divisor of } n\}$. A contains some natural number. Hence we can take a least natural number m of A. Consider a natural number k such that $m \cdot k = n$. Then $m \leq k$. Indeed if $k < m$ then k is the least natural number of A. Hence $m^2 = m \cdot m \leq m \cdot k = n$. Therefore $m^2 \leq n$. $\square$

Definition 139. n and m are coprime iff for all nonzero natural numbers k such that $k \mid n$ and $k \mid m$ we have $k = 1$.

Let n and m are relatively prime stand for n and m are coprime. Let n and m are mutually prime stand for n and m are coprime. Let n is prime to m stand for n and m are coprime.

Proposition 140. **(NN 03 03 356588)** n and m are coprime iff for no prime number p we have $p \mid n$ and $p \mid m$.

Proof. Case n and m are coprime. Let p be a prime number such that $p \mid n$ and $p \mid m$. Then p is nonzero and $p \neq 1$. Contradiction. End.

Case for no prime number p we have $p \mid n$ and $p \mid m$. Let k be a nonzero natural number such that $k \mid n$ and $k \mid m$. Assume that $k \neq 1$. Consider a prime divisor p of k. Then $p \mid k \mid n, m$. Hence $p \mid n$ and $p \mid m$. Contradiction. End. $\square$

Proposition 141. **(NN 03 03 691058)** Let p be a prime number. If p does not divide n then p and n are coprime.

Proof. Assume $p \nmid n$. Suppose that p and n are not coprime. Take a nonzero natural number k such that $k \mid p$ and $k \mid n$. Then $k = p$. Hence $p \mid n$. Contradiction. $\square$

Proposition 142. **(NN 03 03 703692)** Let p be a prime number. Then

$$p \mid n \cdot m \implies (p \mid n \text{ or } p \mid m).$$

Proof. Assume $p \mid n \cdot m$.

Case $p \mid n$. Trivial.

Case $p \nmid n$. Define $N = \{\text{natural number } x : x \neq 0 \text{ and } p \mid x \cdot m\}$. We have $p \in N$ and $n \in N$. Hence N contains some natural number. Thus we can take a least natural number n' of N.

Let us show that n' divides all elements of N. Let $x \in N$. Take natural numbers q, r such that $x = (q \cdot n') + r$ and $r < n'$. Then $x \cdot m = ((q \cdot n') + r) \cdot m = ((q \cdot n') \cdot m) + (r \cdot m)$. We have $p \mid x \cdot m$. Hence $p \mid ((q \cdot n') \cdot m) + (r \cdot m)$. Thus $p \mid r \cdot m$ (by NN 03 01 695362). Indeed $p \mid ((q \cdot n') \cdot m) = (q \cdot (n' \cdot m))$.

Indeed $p \mid n' \cdot m$. Therefore $r = 0$. Indeed if $r \neq 0$ then r is an element of N that is less than n'. Hence $x = q \cdot n'$. Thus n' divides x. End.

Then we have $n' \mid p$ and $n' \mid n$. Hence $n' = p$ or $n' = 1$. Thus $n' = 1$. Indeed if $n' = p$ then $p \mid n$. Then $1 \in N$. Therefore $p \mid 1 \cdot m = m$. End. $\square$

Proposition 143. **(NN 03 03 119851)** Let k be nonzero. Then for all nonzero n, m if $k \cdot m^2 = n^2$ then k is compound.

Proof. Case $k = 1$. Obvious.

Case $k > 1$. (1) Define $P = \{$natural number n :for all natural numbers m if n and m are nonzero and $k \cdot m^2 = n^2$ then k is compound$\}$.

Let us show that for all natural numbers n if P contains all predecessors of n then P contains n. Let n be a natural number. Presume that P contains all predecessors of n.

Let m be a natural number. Assume that n and m are nonzero and $k \cdot m^2 = n^2$.

Suppose that k is prime. Then k divides n^2 and k divides n. Take a natural number l such that $k \cdot l = n$.

(1) Then $m^2 = k \cdot l^2$ (by NN 01 03 169506). Indeed $k \cdot m^2 = (k \cdot l)^2 = k \cdot (k \cdot l^2)$.

(2) m is an element of P. Proof. We have $n^2 > m^2$ (by NN 02 03 252473). Indeed $k \cdot m^2 = n^2$ and $k > 1$ and $m^2 > 0$. Hence $m < n$. Indeed if $n \leq m$ then $n^2 \leq m^2$. Thus $m \in P$. Qed.

(3) m is nonzero. Indeed $m = 0 \implies n^2 = k \cdot 0^2 = k \cdot 0 = 0$ and $n^2 = 0 \implies n = 0$.

(4) l is nonzero. Indeed $l = 0 \implies m^2 = k \cdot 0^2 = k \cdot 0 = 0$ and $m^2 = 0 \implies m = 0$.

Therefore k is compound (by 1, 2, 3, 4). Contradiction. End.

Thus P contains every natural number (by NN 02 05 167446). Hence the thesis (by 1). End. $\square$