Theorem 15.1 (Well-ordering principle)**.** *Every non-empty subset A of $\mathbb{N}$ has a smallest element.*
$\forall A \in \mathcal{P}(\mathbb{N}).\ A \neq \emptyset \implies A$ *has a smallest element*
where "has a smallest element" means $\exists a_0 \in A.\ \forall a \in A.\ a_0 \leq a$.

Proof. Theorem 3.5.1 in textbook. (induction)

16 Divisibility

Definition 16.1. For any $a, d \in \mathbb{N}$, write $d \mid a$ (d (is a factor of|divides) a, a (is divisible by|a multiple of) d) iff $\exists k \in \mathbb{N}.\ d \cdot k = a$.

Examples. $\forall a, d \in \mathbb{N}$

- $a \mid a$ is true (because $a \cdot 1 = a$)
- $1 \mid a$ is true (because $1 \cdot a = a$)
- $d \mid 0$ is true (because $d \cdot 0 = 0$)
- $0 \mid a \implies a = 0$ (because only $0 \cdot 0 = 0$)

Lemma 16.2 (Divisibility implies ordering in $\mathbb{N}$)**.** *For any $a, d \in \mathbb{N}$, with $a \neq 0$. If $d \mid a$, then $d \leq a$.*

Proof.

1. Suppose $d \mid a \implies \exists k \in \mathbb{N}.\ d \cdot k = a$
2. Since $a \neq 0$ by hopothesis, $d \neq 0, k \neq 0$. So $k \in \mathbb{N} \setminus \{ 0 \} = S(\mathbb{N})$
3. so $\exists l \in \mathbb{N}.\ k = S(l)$
4. $a = d \cdot k = d \cdot (l + 1) = d \cdot l + d$
5. Since $d + d \cdot l = a$ and $d \cdot l \in \mathbb{N}$, $d \leq a$. □

Example. $\forall d \in \mathbb{N}.\ d \mid 1 \implies d = 1$.

Proof. $d \mid 1$, then by (division implies ordering) lemma, $d \leq 1$, so $d = 0 \vee d = 1$, but $0 \nmid 1$, so $d = 1$. □

Properties. Divisibility is reflexive, anti-symmetric and transitive. $\forall a, b, c \in \mathbb{N}$,

1. $\exists 1 \in \mathbb{N}.\ a \cdot 1 = a \implies a \mid a$
2. $a \mid b \wedge b \mid a \implies a \leq b \wedge b \leq a \implies a = b$ (by above lemma and anti-symmetry of ordering)
3. $a \mid b \wedge b \mid c \implies \exists l, m \in \mathbb{N}.\ a \cdot l = b, b \cdot m = c \implies a \cdot l \cdot m = c \implies a \mid c$

17 More Division

Theorem 17.1 (Division Algorithm)**.** *Let $a, d \in \mathbb{N}$ with $d > 0$. Then there exists $q \in \mathbb{N}$ and $r \in \{0, \ldots, d-1\}$ such that $a = qd + r$ in $\mathbb{N}$. Moreover, $q \in \mathbb{N}$ and $r \in \{0, \ldots, d-1\}$ are uniquely determined by $a, d \in \mathbb{N}$.*

Theorem (Uniqueness of q, r)**.** *Given $a, d \in \mathbb{N}, d > 0$, if $q, q' \in \mathbb{N}, r, r' \in \{0, \ldots, d-1\}$ such that*

$$a = qd + r = q'd + r' \tag{17.1.1}$$

then $q = q', r = r'$. (uniqueness)

Proof.

1. Suppose for a contradiction that $r \neq r'$. By comparibility of natural numbers, either $r > r'$ or $r' > r$.

2. Without loss of generality, assume $r > r'$, then

$$\exists s \in \mathbb{N}, s \neq 0.\ r = r' + s$$

3. Then by (17.1.1), $qd + r' + s = q'd + r'$, then by cancellation law for addition,

$$qd + s = q'd \tag{17.1.2}$$

4. Because $s \in \mathbb{N}, s \neq 0$, $q'd > qd$, then by cancellation law for multiplication, $q' > q$, so

$$\exists t \in \mathbb{N}, t \neq 0.\ q' = q + t$$

5. By (17.1.2),

$$\begin{aligned}
qd + s &= (q + t) \cdot d \\
qd + s &= qd + td \\
s &= td && (\textit{cancellation property of addition}) \\
d &\mid s && (\textit{and } d > 0) \\
d &\leq s && (\textit{division implies ordering})
\end{aligned}$$

6. which shows $d \leq s \leq r \implies d \leq r$, a contradiction with requirement that $r \in \{0, \ldots, d-1\}$.

7. Hence $r = r'$, then by (17.1.1), $a = qd + r = q'd + r$.

8. $qd = q'd \implies q = q'$. *(by cancellation law of $+, \times$)*

9. $r = r'$ and $q = q'$, uniqueness of r, q shown. $\square$

Theorem (Existence of q, r)**.** *Given $a, d \in \mathbb{N}, d > 0, \exists q, r \in \mathbb{N}$ with $r < d$ such that $a = qd+r$.*

Proof.

1. Consider the following subset of $\mathbb{N}$:

$$S := \{ n \in \mathbb{N} : \exists q \in \mathbb{N}.\ a = qd + n \}$$

   [(S consists of all natural numbers of form $a - q \cdot d$ for various choices of q)]

2. Then $a = 0 \cdot d + a$, shows $a \in S$, in particular $S \neq \emptyset$, then by well-ordering principle,

$$\exists r \in S.\ \forall n \in S.\ r \leq n$$

3. This means $\exists q \in \mathbb{N}.\ a = qd + r$.

   Claim. $r < d$

   - Suppose for contradiction $r \geq d$, $\exists k \in \mathbb{N}.\ d + k = r$ $\qquad (k = r - d)$
   - Then $a = qd + d + k = (q + 1) \cdot d + k$
   - This shows that $k \in S$, then by fact that $r \in S$ is smallest, we must have $r \leq k$.
   - But $d + k = r \implies k \leq r$, so $r = k$ *(by anti-symmetry of ordering)*
   - then we have $d + r = r$, cancelling $+$, $d = 0$, a contradiction with $d > 0$.

4. So given any number a and factor d, there exists quotient q and remainder $r < d$ such that $a = qd + r$ □

Corollary 17.2. *Let $n \in \mathbb{N}$. Then $\neg$(n is even) $\iff$ ($\exists l \in \mathbb{N}.\ n = 2l + 1$)*

Proof.

1. Apply division algorithm to n with $d = 2$,

$$\exists q \in \mathbb{N}, r \in \{ 0, 1 \}.\ n = 2q + r$$

   and q, r above are uniquely defined by n. Either $r = 0$ exclusive or $r = 1$.

2. Case $r = 0$, then $n = 2q$ is even *(by definition)*

3. If n is odd, then $\exists l \in \mathbb{N}.\ n = 2l + 1$, then

$$2q + 0 = n = 2l + 1$$

   with $q, l \in \mathbb{N}$ and $0, 1 \in \{ 0, 1 \}$ a contradiction with uniqueness of remainder

4. Case $r = 1$, then $n = 2q + 1$ is odd

5. if n is even, then $\exists k \in \mathbb{N}.\ n = 2k$, again

$$2k + 0 = n = 2q + 1$$

   a contradiction with uniqueness of remainder. □

Prime numbers and factorisation

Definition 17.3. A <u>prime number</u> is a natural number, $p \in \mathbb{N}$ such that

- $p > 1$ (ie. $p \neq 0 \wedge p \neq 1$)
- $\forall d \in \mathbb{N}.\ d \mid p.\ d = 1 \vee d = p.$

  equivalently: $\forall r, s \in \mathbb{N}.\ p = r \cdot s$, one has $r = 1 \vee s = 1$.

Definition 17.4. A <u>composite number</u> is a natural number $n \in \mathbb{N}$ such that

- $n > 1$ (ie. $n \neq 0 \wedge n \neq 1$)
- n is <u>not prime</u>

  equivalently: $\exists d \in \mathbb{N}.\ d \mid n \wedge d \neq 1 \wedge d \neq n$

Theorem 17.5 (Existence of prime factors)**.** *Let $a \in \mathbb{N}$ with $a > 1$. Then $\exists p.\ p \mid a$ where p is a prime number.*

Proof.

1. Consider the subset
$$S := \{\, d \in \mathbb{N} : d > 1 \wedge d \mid a \,\}$$
   ie. S is set of all divisors of a which are > 1.

2. Then since $a > 1$ by given hypothesis, and $a \mid a$, we get $a \in S$, $S \neq \emptyset$. then by well-ordering principle
$$\exists p \in S.\ \forall d \in S.\ p \leq d$$

3. so we know $p \in \mathbb{N}, p > 1, p \mid a$.

   Claim. p is prime.

   - If not, $\exists r, s \in \mathbb{N}.\ (p = r \cdot s) \wedge (r \neq 1) \wedge (s \neq 1)$. *(defn of composite numbers)*
   - Then because $s \mid p$ and $p \mid a$, $s \mid a$.
   - because $p \in S \implies p > 1 \implies p \neq 0$, so $s \neq 0$, then $s > 1$, hence $s \in S$.

$$\begin{aligned} s = 1 \cdot s &< 2 \cdot s \\ 2 &\leq r \\ s < 2 \cdot s &\leq r \cdot s = p \\ s &< p \end{aligned}$$

   - because $2 \leq r$ and $1 < s \implies s \neq 0$.
   - $s < p$ contradicts with p being smallest in S.

4. So every natural number $a \in \mathbb{N}$ has prime factor(s) $p \in \mathbb{N}$ where $p \mid a$. □

Theorem 17.6 (Fundamental Theorem of Arithmatic or Unique Prime Factorisation property of $\mathbb{N}$)**.**
For any natural number $a \in \mathbb{N}$ with $a > 1$, there exists a (finitely many) sequence of prime numbers $p_1, \ldots, p_r$ such that $a = \prod_{i=1}^{r} p_i$.
Moreover, the primes $p_1, \ldots, p_r$ are unique up to reordering. ie if $q_1, \ldots, q_s$ is another sequence of primes such that $a = \prod_{i=1}^{r} q_i$, then $r = s$ (same number) and $q_1, \ldots, q_r$, up to re-ordering, matches $p_1, \ldots, p_r$.

Existence.

Proof.

1. Given $a \in \mathbb{N}$, $a > 1$, show: $\exists$ primes $p_1, \ldots, p_r$ such that $a = \prod_{i=1}^{r} p_i$.
2. For $a \in \mathbb{N}$, $a > 1$, let
$$Q(a) := \exists \text{ primes } p_1, \ldots, p_r.\ a = \prod_{i=1}^{r} p_i$$
3. Base case: $Q(2)$ is true because 2 is prime, so $a = 2$, can take $r = 1, p_1 = 2$.
4. Induction step: Assume $a > 1$ and $Q(2), \ldots, Q(a)$ true. then $Q(a+1)$ true because
5. $a + 1$ is either prime xor not prime
6. Case $a + 1$ is prime, then $Q(a + 1)$ is true (take $r = 1, p_1 = a + 1$)
7. Case $a + 1$ is not prime, then $a + 1 > 1$,
$$\exists r, s \in \mathbb{N}.\ a + 1 = r \cdot s, r \neq 1, s \neq 1.$$
(clear that $r \neq 0, s \neq 0$ either)
8. $r \mid (a+1) \implies r \leq a + 1$ and $s \neq 1 \implies r < a + 1 \implies r \leq a$
9. Symmetrically, $s \leq a$.
10. Then $r, s \in \{2, 3, \ldots, a\}$, so $Q(r), Q(s)$ are true by induction hypothesis.
11. Hence $\exists$ primes $p_1, \ldots, p_l$. $r = \prod_{i=1}^{l} p_i$.
and $\exists$ primes $p_{l+1}, \ldots, p_{l+m}$. $s = \prod_{i=l+1}^{l+m} p_i$.
12. Then $a + 1 = r \cdot s = \prod_{i=1}^{l} p_i \cdot \prod_{i=l+1}^{l+m} p_i$ is a product of primes.
13. by strong induction, $Q(a)$ true for all $a \geq 2$. □

Uniqueness. (ad-hoc proof using wop, not (easily) generalisable to other context.)

Proof.

1. Suppose on contary that uniqueness of factorisation fails, consider the set
$$S := \{ a \in \mathbb{N} : a > 1, a \text{ has non-unique prime factors} \}$$
ie. assuming $S \neq \emptyset$.

2. By well-ordering principle, S has smallest element $a \in S$

3. So $a \in \mathbb{N}, a > 1, \exists$ primes $p_1, \ldots, p_r, q_1, \ldots, q_s$ such that $a = \prod_{i=1}^{r} p_i = \prod_{i=1}^{s} q_i$ and $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ are distinct even allowing permutation.

   Claim. None of p's appear among the q's.
$$\forall i \in \{ 1, \ldots, r \} . \forall j \in \{ 1, \ldots, s \} . p_i \neq q_j$$

   i. Suppose $\exists i \in \{ 1, \ldots, r \} . \exists j \in \{ 1, \ldots, s \} . p_i = q_j$, then
$$p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_r = \frac{a}{p_i} = \frac{a}{q_j} = q_1 \cdots q_{j-1} \cdot q_{j+1} \cdots q_r$$

   ii. Take a' as above expression, we have $a' < a$, and having non-unique prime factors, so $a' \in S$, a contradiction with smallest $a \in S$.

4. Without loss of generality, assume $p_1 < q_1$, so $\exists t \in \mathbb{N}.\ t \neq 0, p_1 + t = q_1$.

5. consider $b := t \cdot q_2 \cdots q_s$, t nonzero, so $b \geq 1$.

6. Also, $a = q_1 \cdot q_2 \cdots q_s$, so $b < a$, so $b \notin S$, ie b has the unique prime factorisation property

7. If $t = 1$, then $b = q_2 \cdots q_s$ must be <u>the</u> unique prime factorisation of b. Then by above claim, p_1 does not appear among $q_2, \ldots, q_s$. Yet,
$$\begin{aligned} b &= (q_1 - p_1) \cdot q_2 \cdots q_s \\ &= q_1 q_2 \cdots q_s - p_1 q_2 \cdots q_s \\ &= p_1 p_2 \cdots p_r - p_1 q_2 \cdots q_s \\ &= p_1 (p_2 \cdots p_r - q_2 \cdots q_s) \end{aligned}$$

8. So $p_1 \mid b$, which should appear in the prime factorisation of b, a contradiction, so $t \neq 1$.

9. So $t = q_1 - p_1 > 1$. Now $q_1 - p_1 \leq b \leq a$, so $q_1 - p_1 \notin S$. So $q_1 - p_1$ has unique prime factorasation, say
$$q_1 - p_1 = l_1 \cdots l_u$$
where $l_1, \ldots, l_u$ are primes.

10. By examination of $b = (q_1 - p_q) \cdot q_2 \cdots q_s = p_1(p_2 \cdots p_r - q_2 \cdots q_s)$, p_1 must appear in prime factor of b.

11. But $b = l_1 \cdots l_u \cdot q_1 \cdots q_s$ is also a prime factorisation of b, but

12. *I give up, this is useless.* □