1 Primes

[readtex `arithmetic/sections/01_arithmetic/04_exponentiation.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/04_ordering-and-exponentiation.ftl.tex`]

[readtex `arithmetic/sections/02_ordering/05_induction.ftl.tex`]

[readtex `arithmetic/sections/03_divisibility/01_divisibility.ftl.tex`]

[readtex `arithmetic/sections/03_divisibility/02_euclidean-division.ftl.tex`]

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

1.1 Definitions

Let us turn back to the notion of divisibility. We will now investigate natural numbers which cannot be decomposed into a product of two (non-trivial) smaller numbers. Such numbers are called *prime*.

Definition 1.1. A trivial divisor of n is a divisor m of n such that $m = 1$ or $m = n$.

Definition 1.2. A nontrivial divisor of n is a divisor m of n such that $m \neq 1$ and $m \neq n$.

Definition 1.3. 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 1.4. n is composite iff $n > 1$ and n has a nontrivial divisor.

Proposition 1.5. Let $n > 1$. Then n is prime iff every divisor of n is a trivial divisor of n.

Let us have a look at what the first few prime numbers are.

Proposition 1.6. 2, 3, 5 and 7 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. Therefore $k = 1$ or

$k = 3$. Thus k is a trivial divisor of 3. End.

Let us show that 5 is prime. Let k be a divisor of 5. Then $0 < k \leq 5$. Hence $k = 1$ or $k = 2$ or $k = 3$ or $k = 4$ or $k = 5$. 2 does not divide 5. 3 does not divide 5. 4 does not divide 5. Therefore $k = 1$ or $k = 5$. Thus k is a trivial divisor of 5. End.

Let us show that 7 is prime. Let k be a divisor of 7. Then $0 < k \leq 7$. Hence $k = 1$ or $k = 2$ or $k = 3$ or $k = 4$ or $k = 5$ or $k = 6$ or $k = 7$. 2 does not divide 7. 3 does not divide 7. 4 does not divide 7. 5 does not divide 7. 6 does not divide 7. Therefore $k = 1$ or $k = 7$. Thus k is a trivial divisor of 7. End. □

Proposition 1.7. 4, 6, 8 and 9 are compound.

Proof. $4 = 2 \cdot 2$. Hence 2 divides 4. Thus 4 is compound.

$6 = 2 \cdot 3$. Hence 2 divides 6. Thus 6 is compound.

$8 = 2 \cdot 4$. Hence 2 divides 8. Thus 8 is compound.

$9 = 3 \cdot 3$. Hence 3 divides 9. Thus 9 is compound. □

Proposition 1.8. 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 $p = 2$. □

An important fact about primes is that every natural number has a prime divisor. From this the *fundamental theorem of arithmetic* can be derived, namely the assertion that every natural number has a unique decomposition into prime factors.

Proposition 1.9. Every natural number that is greater than 1 has a prime divisor.

Proof. Define

$$P = \{\, n \in \mathbb{N} \mid \text{if } n > 1 \text{ then } n \text{ has a prime divisor} \,\}.$$

Let us show that (1) 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 **??**, 1). □

Proposition 1.10. Let n be composite. Then n has a nontrivial divisor m such that $m^2 \leq n$.

Proof. Define

$$A = \{\, m \in \mathbb{N} \mid m \text{ is a nontrivial divisor of } n \,\}.$$

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 $m^2 \leq n$. □

Let us now have a look at natural numbers which have no (non-trivial) common divisor. Such numbers are called *coprime*.

Definition 1.11. 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 1.12. 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. □

Proposition 1.13. 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. □

Proposition 1.14. 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

$$N = \{\, x \in \mathbb{N} \mid x \neq 0 \text{ and } p \mid x \cdot m \,\}.$$

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 $x = (n' \cdot q) + r$ and $r < n'$ (by **??**). Indeed n' is nonzero. 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 **??**). 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. □

Proposition 1.15. 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

$$P = \left\{ n \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{for all natural numbers } m \text{ if } n \text{ and } m \text{ are nonzero and} \\ k \cdot m^2 = n^2 \text{ then } k \text{ is compound} \end{array} \right\}.$$

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. k is a nontrivial divisor of n^2. Hence k divides n. Take a natural number l such that $k \cdot l = n$.

(2) Then $m^2 = k \cdot l^2$ (by **??**). Indeed $k \cdot m^2 = (k \cdot l)^2 = k \cdot (k \cdot l^2)$.

(3) m is an element of P.
Proof. We have $n^2 > m^2$ (by **??**). 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.

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

(5) 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 2, 3, 4, 5). Contradiction. End.

Thus P contains every natural number (by **??**). Hence the thesis (by 1). End. □