

## Prime Numbers

ARITHMETIC\_10\_5450464558579712

**Definition 0.1.** Let  $n$  be a natural number.  $n$  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.

ARITHMETIC\_10\_3834705971511296

**Definition 0.2.**  $\mathbb{P}$  is the class of all prime numbers.

ARITHMETIC\_10\_7801379464675328

**Proposition 0.3.** Let  $n$  be a natural number such that  $n > 1$ . Then  $n$  is prime iff every divisor of  $n$  is a trivial divisor of  $n$ .

ARITHMETIC\_10\_3606185106210816

**Proposition 0.4.** Let  $n$  be a natural number such that  $n > 1$ . Then  $n$  has a prime divisor.

*Proof.* Define  $\Phi = \{n' \in \mathbb{N} \mid \text{if } n' > 1 \text{ then } n' \text{ has a prime divisor}\}$ .

Let us show that for every  $n' \in \mathbb{N}$  if  $\Phi$  contains all predecessors of  $n'$  then  $\Phi$  contains  $n'$ . Let  $n' \in \mathbb{N}$ . Assume that  $\Phi$  contains all predecessors of  $n'$ . We have  $n' = 0$  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  $\Phi$ . 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  $\Phi$  (by ARITHMETIC\_04\_3609801697263616).  $\square$

ARITHMETIC\_10\_463197419077632

**Definition 0.5.** Let  $n, m$  be natural numbers.  $n$  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.

ARITHMETIC\_10\_5776394594287616

**Proposition 0.6.** Let  $n, m$  be natural numbers.  $n$  and  $m$  are coprime iff  $n$  and  $m$  have no common prime divisor.

*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  $n$  and  $m$  have no common prime divisor. Assume that  $n$  and  $m$  are not coprime. 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.  $\square$

ARITHMETIC\_10\_7212152851005440

**Proposition 0.7.** Let  $n, m$  be natural numbers and  $p$  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.  $\square$

ARITHMETIC\_10\_8313676557713408

**Proposition 0.8.** Let  $n, m$  be natural numbers and  $p$  be a prime number. If  $p \mid n \cdot m$  then  $p \mid n$  or  $p \mid m$ .

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

Case  $p \mid n$ . Trivial.

Case  $p \nmid n$ . Define  $\Phi = \{k \in \mathbb{N} \mid k \neq 0 \text{ and } p \mid k \cdot m\}$ . Then  $p \in \Phi$  and  $n \in \Phi$ . Hence  $\Phi$  contains some natural number. Thus we can take  $a \in \Phi$  such that  $a \leq k$  for all  $k \in \Phi$ .

Let us show that  $a$  divides all elements of  $\Phi$ . Let  $k \in \Phi$ . Take natural numbers  $q, r$  such that  $k = (a \cdot q) + r$  and  $r < a$  (by ARITHMETIC\_08\_7743986617810944). Indeed  $a$  is nonzero. Then  $k \cdot m = ((q \cdot a) + r) \cdot m = ((q \cdot a) \cdot m) + (r \cdot m)$ . We have  $p \mid k \cdot m$ . Hence  $p \mid ((q \cdot a) \cdot m) + (r \cdot m)$ .

We can show that  $p \mid r \cdot m$ . We have  $p \mid a \cdot m$ . Hence  $p \mid (q \cdot a) \cdot m$ . Indeed  $((q \cdot a) \cdot m) = q \cdot (a \cdot m)$ . Take  $A = (q \cdot a) \cdot m$  and  $B = r \cdot m$ . Then  $p \mid A + B$  and  $p \mid A$ . Thus  $p \mid B$  (by ARITHMETIC\_07\_1076947887063040). Indeed

$p, A$  and  $B$  are natural numbers. Consequently  $p \mid r \cdot m$ . End.

Therefore  $r = 0$ . Indeed if  $r \neq 0$  then  $r$  is an element of  $\Phi$  that is less than  $a$ . Hence  $k = q \cdot a$ . Thus  $a$  divides  $k$ . End.

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