Chapter 1

Prime numbers

File: `arithmetic/sections/09_primes.ftl.tex`

[readtex `arithmetic/sections/07_divisibility.ftl.tex`]

[readtex `arithmetic/sections/08_euclidean-division.ftl.tex`]

ARITHMETIC_10_5438991513944064

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

ARITHMETIC_10_8768240253665280

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

ARITHMETIC_10_5450464558579712

Definition 1.3. 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 1.4. $\mathbb{P}$ is the class of all prime numbers.

ARITHMETIC_10_8507257891323904

Proposition 1.5. $\mathbb{P}$ is a set.

ARITHMETIC_10_8020087063707648

Definition 1.6. Let n be a natural number. n is composite iff $n > 1$ and n has a nontrivial divisor.

ARITHMETIC_10_7801379464675328

Proposition 1.7. 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_3685624758403072

Proposition 1.8. 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. Indeed $3 \cdot m \neq 5$ for all $m \in \mathbb{N}$ such that $m \leq 5$. Indeed $3 \cdot 0, 3 \cdot 1, 3 \cdot 2, 3 \cdot 3, 3 \cdot 4, 3 \cdot 5 \neq 5$. 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. Indeed $3 \cdot m \neq 7$ for all $m \in \mathbb{N}$ such that $m \leq 7$. Indeed $3 \cdot 0, 3 \cdot 1, 3 \cdot 2, 3 \cdot 3, 3 \cdot 4, 3 \cdot 5, 3 \cdot 6, 3 \cdot 7 \neq 7$. 4 does not divide 7. 5 does not divide 7. Indeed $5 \cdot m \neq 7$ for all $m \in \mathbb{N}$ such that $m \leq 7$. Indeed $5 \cdot 0, 5 \cdot 1, 5 \cdot 2, 5 \cdot 3, 5 \cdot 4, 5 \cdot 5, 5 \cdot 6, 5 \cdot 7 \neq 7$. 6 does not divide 7. Therefore $k = 1$ or $k = 7$. Thus k is a trivial divisor of 7. End. $\square$

ARITHMETIC_10_2539250413207552

Proposition 1.9. 4, 6, 8 and 9 are compound.

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

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

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

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

ARITHMETIC_10_3606185106210816

Proposition 1.10. 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 Φ contains all predecessors of n' then Φ contains n'. Let $n' \in \mathbb{N}$. Assume that Φ 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 Φ. 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.

[prover vampire] Thus every natural number belongs to Φ (by **??**). □

ARITHMETIC_10_463197419077632

Definition 1.11. 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 1.12. 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. □

ARITHMETIC_10_7212152851005440

Proposition 1.13. 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. □

ARITHMETIC_10_8313676557713408

Proposition 1.14. Let n, m be natural numbers and p be a prime number. Then

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

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

Case $p \mid n$. Trivial.

Case $p \nmid n$. Define $\Phi = \{k \in \mathbb{N} \mid k \neq 0 \text{ and } p \mid k \cdot m\}$. Then $p \in \Phi$ and $n \in \Phi$. Hence Φ contains some natural number. Thus we can take a least element a of Φ regarding $<$.

Let us show that a divides all elements of Φ. Let $k \in \Phi$. Take natural numbers q, r such that $k = (a \cdot q) + r$ and $r < a$ (by **??**). 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 **??**). 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 Φ 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. $\square$