Modular Arithmetics

Quotients and Remainders

ARITHMETIC_08_8621463798022144

Definition 0.1. Let n, m be natural numbers such that $m \neq 0$. $n \operatorname{div} m$ 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 $n \operatorname{div} m$.

ARITHMETIC_08_3560980160184320

Definition 0.2. Let n, m be natural numbers such that $m \neq 0$. $n \bmod m$ 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 $n \bmod m$.

Basic Properties

ARITHMETIC_08_5448561831444480

Definition 0.3. Let n, m, k be natural numbers such that $k \neq 0$. $n \equiv m \pmod{k}$ iff $n \bmod k = m \bmod k$.

Let n and m are congruent modulo k stand for $n \equiv m \pmod{k}$.

ARITHMETIC_08_3818318544764928

Proposition 0.4. Let n, k be natural numbers such that $k \neq 0$. Then $n \equiv n \pmod{k}$.

Proof. We have $n \bmod k = n \bmod k$. Hence $n \equiv n \pmod{k}$. □

ARITHMETIC_08_2337210737098752

Proposition 0.5. Let n, m, k be natural numbers such that $k \neq 0$. If $n \equiv m \pmod{k}$ then $m \equiv n \pmod{k}$.

Proof. Assume $n \equiv m \pmod{k}$. Then $n \bmod k = m \bmod k$. Hence $m \bmod k = n \bmod k$. Thus $m \equiv n \pmod{k}$. □

ARITHMETIC_08_7464329746055168

Proposition 0.6. Let n, m, l, k be natural numbers such that $k \neq 0$. If $n \equiv m \pmod{k}$ and $m \equiv l \pmod{k}$ then $n \equiv l \pmod{k}$.

Proof. Assume $n \equiv m \pmod{k}$ and $m \equiv l \pmod{k}$. Then $n \bmod k = m \bmod k$ and $m \bmod k = l \bmod k$. Hence $n \bmod k = l \bmod k$. Thus $n \equiv l \pmod{k}$. □

ARITHMETIC_08_2034122983735296

Proposition 0.7. Let n, m, k be natural numbers such that $k \neq 0$. Assume $n \geq m$. Then $n \equiv m \pmod{k}$ iff $n = (k \cdot x) + m$ for some natural number x.

Proof. Case $n \equiv m \pmod{k}$. Then $n \bmod k = m \bmod k$. Take a natural number r such that $r < k$ and $n \bmod k = r = m \bmod k$. Take a nonzero natural number l such that $k = r + l$. Consider natural numbers q, q' such that $n = (q \cdot k) + r$ and $m = (q' \cdot k) + r$.

Then $q \geq q'$.
Proof. Assume the contrary. Then $q < q'$. Hence $q \cdot k < q' \cdot k$. Thus $(q \cdot k) + r < (q' \cdot k) + r$ (by `ARITHMETIC_04_7354062662008832`). Indeed $q \cdot k$ and $q' \cdot k$ are natural numbers. Therefore $n < m$. Contradiction. Qed.

Take a natural number x such that $q = q' + x$.

Let us show that $n = (k \cdot x) + m$. We have

$$(k \cdot x) + m$$

$$= (k \cdot x) + ((q' \cdot k) + r)$$
$$= ((k \cdot x) + (q' \cdot k)) + r$$
$$= ((k \cdot x) + (k \cdot q')) + r$$
$$= (k \cdot (q' + x)) + r$$
$$= (k \cdot q) + r$$
$$= n.$$

End. End.

Case $n = (k \cdot x) + m$ for some natural number x. Consider a natural number x such that $n = (k \cdot x) + m$. Take natural numbers r, r' such that $n \bmod k = r$ and $m \bmod k = r'$. Then $r, r' < k$. Take natural numbers q, q' such that $n = (k \cdot q) + r$ and $m = (k \cdot q') + r'$. Then

$$(k \cdot q) + r$$

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

Hence $r = r'$. Thus $n \bmod k = m \bmod k$. Therefore $n \equiv m \pmod{k}$. End. ☐

ARITHMETIC_08_2988318228742144

Proposition 0.8. Let n, m, k, k' be natural numbers such that $k, k' \neq 0$. If $n \equiv m \pmod{k \cdot k'}$ then $n \equiv m \pmod{k}$.

Proof. Assume $n \equiv m \pmod{k \cdot k'}$.

Case $n \geq m$. We can take a natural number x such that $n = ((k \cdot k') \cdot x) + m$. Then $n = (k \cdot (k' \cdot x)) + m$. Hence $n \equiv m \pmod{k}$. End.

Case $m \geq n$. We have $m \equiv n \pmod{k \cdot k'}$. Hence we can take a natural number x such that $m = ((k \cdot k') \cdot x) + n$. Then $m = (k \cdot (k' \cdot x)) + n$. Thus $m \equiv n \pmod{k}$. Therefore $n \equiv m \pmod{k}$. End. ☐

ARITHMETIC_08_5895145169879040

Corollary 0.9. Let n, m, k, k' be natural numbers such that $k, k' \neq 0$. If $n \equiv m \pmod{k \cdot k'}$ then $n \equiv m \pmod{k'}$.

Proof. Assume $n \equiv m \pmod{k \cdot k'}$. Then $n \equiv m \pmod{k' \cdot k}$. Hence $n \equiv m \pmod{k'}$. ☐

ARITHMETIC_08_5984712287846400

Proposition 0.10. Let n, k be natural numbers such that $k \neq 0$. Then $n + k \equiv n \pmod{k}$.

Proof. Take $r = n \bmod k$ and $r' = (n + k) \bmod k$. Consider a $q \in \mathbb{N}$ such that $n = (k \cdot q) + r$ and $r < k$. Consider a $q' \in \mathbb{N}$ such that $n + k = (k \cdot q') + r'$ and $r' < k$. Then $(k \cdot q') + r' = n + k = ((k \cdot q) + r) + k = (k + (k \cdot q)) + r = (k \cdot (q + 1)) + r$. Hence $r = r'$. Consequently $n \bmod k = (n + k) \bmod k$. Thus $n + k \equiv n \pmod{k}$. ☐