1 Modular arithmetic

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

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

Having seen Euclidean division we now can establish a new kind of arithmetic, called *modular arithmetic*. To do this we fix a natural number k and identify any two natural numbers if they have the same remainder when divided by k.

Definition 1.1. Let k be nonzero. $n \equiv m \pmod{k}$ iff $n \bmod k = m \bmod k$.

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

Proposition 1.2. Let m be nonzero. Then

$$n \equiv n \pmod{m}.$$

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

Proposition 1.3. Let m be nonzero. Then

$$n \equiv n' \pmod{m} \implies n' \equiv n \pmod{m}.$$

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

Proposition 1.4. Let m be nonzero. Then

$$(n \equiv n' \pmod{m} \text{ and } n' \equiv n'' \pmod{m}) \implies n \equiv n'' \pmod{m}.$$

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

Proposition 1.5. Let k be nonzero. 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 $(q \cdot k) + r < (q' \cdot k) + r$. 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

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

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

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

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

Proposition 1.6. Let k, k' be nonzero. Then

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

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. □

Corollary 1.7. Let k, k' be nonzero natural numbers. Then

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

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