Modular Arithmetic In $\mathbb{Z}$

Definition : --
for $n, a \in \mathbb{Z} \times \mathbb{Z}^+$ *we define amodn the reminder when a is divided by n. n is called the modulus.*
so the equation $a = q{*}n + r$ *with* $q = \left\lfloor \frac{a}{n} \right\rfloor$ *and* $0 \leqslant r < n$
became $a = \left\lfloor \frac{a}{n} \right\rfloor {*}n + (a \bmod n)$ *with* $r = (a \bmod n) \in \{0, 1, ..., n-1\}$
we say that a and b are congruent modulo n, if $a \bmod n = b \bmod n$ *and we can write it as* $a \equiv b \pmod{n}$
as result $a \equiv 0 \pmod{n}$ *means* $n|a$*, which is abvious case where* $r = 0$
----

1) $a \equiv b \pmod{n}$*, then* $n|a-b$

Proof :
$a = q{*}n + a \bmod n$ *and* $b = q'{*}n + b \bmod n$ *because a and b are congruent modulo n,*
$a - b = (q - q')n$*, hence* $n|a-b$

2) $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$

Proof :
$a \equiv b \pmod{n} \Leftrightarrow (a \bmod n) = (b \bmod n) \Leftrightarrow (b \bmod n) = (a \bmod n) \Leftrightarrow b \equiv a \pmod{n}$

3) *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$*, then* $a \equiv c \pmod{n}$

Proof :
$a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n} \Leftrightarrow (a \bmod n) = (b \bmod n)$ *and* $(b \bmod n) = (c \bmod n)$
$\Leftrightarrow a \equiv c \pmod{n}$

4) *for* $n > 0$ $a \bmod n = a$ *if and only if* $0 \leqslant a < n$

Proof :
$\Longrightarrow a \bmod n = a$ *this is direct* $0 \leqslant a \bmod n < n$*, hence* $0 \leqslant a < n$
$\Longleftarrow$ $0 \leqslant a < n$ *meaning that* $a = q{*}n + r$ *with* $r = a \bmod n$
this is true for $q = 0$ *and* $a = r = a \bmod n$

5) *for* $n > 0$, $\forall k \in \mathbb{Z}$ $(a + k{*}n) \bmod n = a \bmod n$

$Proof:$

$$\exists q, r \in \mathbb{Z}\ \ a = q*n + r \Leftrightarrow for\ k \in \mathbb{Z}\ \ a + kn = (q+k)*n + r\ with\ r = a \bmod n\ for\ q' = (q+k)$$
$$\Leftrightarrow a + kn = q'*n + a \bmod n$$

$hence\ \forall k \in \mathbb{Z}\ \ (a + k*n) \bmod n = a \bmod n$

6) $for\ n > 0,\ [(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

$Proof:$

$\exists q, q', r, r' \in \mathbb{Z}\ \ a = q*n + r\ \ and\ \ b = q'*n + r'\ with\ r = a \bmod n\ and\ r' = b \bmod n$

$$\begin{aligned}(a+b) \bmod n &= ((q+q')*n + r + r') \bmod n \\ &= (\ r + r') \bmod n \\ &= \ [(a \bmod n) + (b \bmod n)] \bmod n\end{aligned}$$

7) $for\ n > 0,\ [(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

$Proof:$

$\exists q, q', r, r' \in \mathbb{Z}\ \ a = q*n + r\ \ and\ \ b = q'*n + r'\ with\ r = a \bmod n\ and\ r' = b \bmod n$

$$\begin{aligned}(a-b) \bmod n &= ((q-q')*n + r - r') \bmod n \\ &= (\ r - r') \bmod n \\ &= \ [(a \bmod n) - (b \bmod n)] \bmod n\end{aligned}$$

8) $for\ n > 0,\ [(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

$Proof:$

$\exists q, q', r, r' \in \mathbb{Z}\ \ a = q*n + r\ \ and\ \ b = q'*n + r'\ with\ r = a \bmod n\ and\ r' = b \bmod n$

$$\begin{aligned}(a \times b) \bmod n &= ((q*q'*n + q*r' + q'*r)*n + r \times r') \bmod n \\ &= (\ r \times r') \bmod n \\ &= [(a \bmod n) \times (b \bmod n)] \bmod n\end{aligned}$$

9) $for\ n > 0, \forall a \in \mathbb{Z}\ \ \ \exists k \in \mathbb{Z}/n\mathbb{Z},\ \ (a+k) \equiv 0 \bmod n$

$Proof:$

$$\exists q, r \in \mathbb{Z}\ \ a = q*n + r\ \ \Leftrightarrow\ \ a - r = q*n\ so\ we\ take\ k = \ -r$$
$$\Leftrightarrow\ \ a + k = q*n\ implying\ that\ n | a + k$$

$hence\ (a+k) \equiv 0 \bmod n,\ in\ case\ k \in \mathbb{Z}/n\mathbb{Z},\ we\ call\ k\ the\ additive\ inverse\ of\ a\ and\ we\ give\ it\ the\ symbole\ (-a)$

10) $for\ n > 0, for\ a \in \mathbb{Z}\ \ and\ \ gcd(a, n) = 1\ then\ \exists k \in \mathbb{Z}/n\mathbb{Z},\ \ (a \times k) \equiv 1 \bmod n\ we\ call\ k\ the\ multiplicative\ inverse\ and\ we\ give\ it\ the\ symbole\ a^{-1}$

$Proof:$

$i\ will\ proof\ why\ gcd(a,n)\ need\ to\ be\ 1,\ for\ n>0\ and\ a\in\mathbb{Z}\ suppose\ that\ gcd(a,n)>1\ and$
$\exists k\in\mathbb{Z}/n\mathbb{Z},\ \ (a\times k)\equiv 1 \bmod n$
$we\ have\ \exists q,r\in\mathbb{Z}\ \ a=q*n+r\ by\ the\ inverse\ definition\ ka=q'*n+1\ meaning\ that$
$ka-q'*n=1\ which\ contradict\ the\ fact\ that\ gcd(a,n)>1,\ hence\ we\ need\ gcd(a,n)=1$