All occurring letters denote integers.

Divisibility:

!!! $a \mid bc$ and $a \nmid b$ do **NOT** imply $a \mid c$,

e.g. $15 \mid 3 \cdot 20$, but $15 \nmid 3$ and $15 \nmid 20$.

Correct versions:

(i) $a \mid bc,\ (a,b) = 1 \Rightarrow a \mid c$.

(ii) a is a prime, $a \mid bc,\ a \nmid b \Rightarrow a \mid c$.

!!! $a \mid c$ and $b \mid c$ do **NOT** imply $ab \mid c$,

e.g. $6 \mid 12,\ 4 \mid 12$, but $24 \nmid 12$.

Correct versions:

(i) $a \mid c,\ b \mid c$, and $(a,b) = 1 \Rightarrow ab \mid c$ (where (a,b) denotes the greatest common divisor of a and b).

(ii) $a \mid c$ and $b \mid c \Rightarrow [a,b] \mid c$ (where $[a,b]$ denotes the least common multiple of a and b).

The above properties can be deduced e.g. from the unique prime factorization theorem (UFT).

Congruence:

If $m \mid a - b$ where $m > 0$, i.e. a and b give the same remainder upon division by m, then we say that "a is *congruent* to b modulo m" and denote it by $a \equiv b \pmod{m}$.

The congruence relation is reflexive, symmetric, and transitive, and congruences can be added, subtracted, and multiplied.

We cannot divide congruences even if the quotients are integers: e.g. $24 \equiv 14 \pmod{10}$ and $2 \equiv 2 \pmod{10}$, but $24/2 = 12 \not\equiv 14/2 = 7 \pmod{10}$.

Correct versions:

(i) $ac \equiv bc \pmod{m}$ and $(c,m) = 1 \Rightarrow a \equiv b \pmod{m}$.

(ii) $ac \equiv bc \pmod{m} \iff a \equiv b \pmod{m/(c,m)}$.

Euler's function $\varphi(n)$

$\varphi(n)$ is defined as the number of integers coprime to n in $\{1, 2, \ldots, n\}$.

If the standard form of n is $n = p_1^{k_1} \ldots p_r^{k_r}$ where p_j are distinct primes and $k_j > 0$, then $\varphi(n) = p_1^{k_1-1}(p_1 - 1) \ldots p_r^{k_r-1}(p_r - 1)$.

Euler–Fermat Theorem

$(c,m) = 1 \Rightarrow c^{\varphi(m)} \equiv 1 \pmod{m}$.

An important special case if Fermat's Little Theorem:

If p is a prime and $p \nmid c$, then $c^{p-1} \equiv 1 \pmod{p}$

An alternative form is: $c^p \equiv c \pmod{p}$ for every c.

Linear Diophantine equations and linear congruences

A *linear Diophantine equation* (in two variables) is $Ax + By = C$ where A, B, C are given integers, A and B are not both zero, and we are looking for integer solutions in x and y.

It is solvable iff $(A,B) \mid C$, and in this case there are infinitely many solutions.

A *linear congruence* is $ax \equiv b \pmod{m}$, and we are looking for pairwise incongruent solutions in x.

It is solvable iff $(a,m) \mid b$, and in this case there are (a,m) pairwise incongruent solutions.

The equation $Ax + By = C$ can be transformed into the congruence $Ax \equiv C \pmod{|B|}$ or into $By \equiv C \pmod{|A|}$ (if B and A are not zero, resp.)

Conversely, the congruence $ax \equiv b \pmod{m}$ can be transformed into the equation $ax - my = b$.