Università degli Studi di Verona

Modelli Biologici Discreti
a.a. 2014/2015

Docente: Zsuzsanna Lipták

Verona, 17 Nov. 2014

Solution of exercise 5 of the first batch of exercises (on discrete maths).

Modular arithmetic: Prove the fundamental property of the modular congruence using the definitions.

If $x \equiv x'(\text{mod } m)$ and $y \equiv y'(\text{mod } m)$, then
$(x+y) \equiv (x'+y')(\text{mod } m)$ and $(x \cdot y) \equiv (x' \cdot y')(\text{mod } m)$.

1. By definition, $x \equiv x'(\text{mod } m)$ implies that $x - x' \in m\mathbb{Z}$, i.e., there is a $k \in \mathbb{Z}$ such that $x - x' = km$. Similarly, since $y \equiv y'(\text{mod } m)$, there is a $k' \in \mathbb{Z}$ s.t. $y - y' = k'm$. Therefore,

$$(x+y) - (x'+y') = (x-x') + (y-y') = km + k'm = (k+k')m \in m\mathbb{Z},$$

since $k + k' \in \mathbb{Z}$. Thus, by definition, $(x+y) \equiv (x'+y')(\text{mod } m)$.

2. Let $x = km + r_1$, where $k, r_1 \in \mathbb{Z}$ and $0 \leq r_1 < m$. Note that this r_1, the remainder after division by m, is unique. Since $x' \equiv x(\text{mod } m)$, therefore $x' = k'm + r_1$ for some $k' \in \mathbb{Z}$, i.e. x' has the same remainder as x modulo m. Similarly, since $y \equiv y'(\text{mod } m)$, both have the same remainder r_2 modulo m; say $y = \ell m + r_2$, and $y' = \ell' m + r_2$. Now we have

$$\begin{aligned}
(x \cdot y) - (x' \cdot y') &= (km + r_1)(\ell m + r_2) - (k'm + r_1)(\ell' m + r_2) \\
&= (k\ell m^2 + kmr_2 + r_1\ell m + r_1r_2) - (k'\ell' m^2 + k'mr_2 + r_1\ell' m + r_1r_2) \\
&= ((k\ell m + kr_2 + r_1\ell)m + r_1r_2) - ((k'\ell' m + k'r_2 + r_1\ell')m + r_1r_2) \\
&= \underbrace{(k\ell m + kr_2 + r_1\ell - k'\ell' m - k'r_2 - r_1\ell')}_{:=K} m + \underbrace{(r_1r_2 - r_1r_2)}_{=0} \\
&= Km \quad \in m\mathbb{Z},
\end{aligned}$$

since $K = k\ell m + kr_2 + r_1\ell - k'\ell' m - k'r_2 - r_1\ell' \in \mathbb{Z}$, because it is a sum of integers. So by definition, $(x \cdot y) \equiv (x' \cdot y')(\text{mod } m)$.