# Lista 6 - MAC105

**João Gabriel Basi - N° USP: 9793801**

1. (a) Partindo da implicação (1)$a \equiv b \Rightarrow a \simeq b$ (ou seja, $\equiv$ é um refinamento de $\simeq$, já que $\equiv \subseteq \simeq$) se, para todo $a, b \in A$, $a \equiv b \Leftrightarrow a, b \in [a]_\equiv$ e $a \simeq b \Leftrightarrow a, b \in [a]_\simeq$ podemos substituir na implicação (1) e teremos que $a, b \in [a]_\equiv \Rightarrow a, b \in [a]_\simeq$. Com isso, podemos deduzir que $[a]_\equiv \subseteq [a]_\simeq$.

   (b) Se $a \equiv b \Rightarrow a \simeq b$, sempre haverá uma classe $[a]_\simeq$ correspondente para cada classe $[a]_\equiv$, com $a \in A$, pois $\equiv$ é um refinamento de $\simeq$. Além disso, nunca haverá mais de uma classe em $\simeq$ correspondente à mesma classe de $\equiv$, pois ambas são relações de equivalência, concluindo que a função está bem definida.

   (c) Se $m|n$, então, quando $a\ mod\ n$ atinge seus valores mínimo e máximo, $a\ mod\ m$ também atinge, sincronizando os valores dos módulos, pois $m$ é múltiplo de $n$. Já quando $m$ não divide $n$, isso não ocorre, então um mesmo valor em $\mathbb{Z}_n$ pode ter mais de um valor em $\mathbb{Z}_m$. Exemplificando, temos:

   | $\mathbb{Z}$ | $\mathbb{Z}_n = \mathbb{Z}_6$ | $\mathbb{Z}_m = \mathbb{Z}_3$ | $\mathbb{Z}_m = \mathbb{Z}_4$ |
   |---|---|---|---|
   | 0 | 0 | 0 | 0 |
   | 1 | 1 | 1 | 1 |
   | 2 | 2 | 2 | 2 |
   | 3 | 3 | 0 | 3 |
   | 4 | 4 | 1 | 0 |
   | 5 | 5 | 2 | 1 |
   | 6 | 0 | 0 | 2 |

   Podemos ver que $f(0\ mod\ 6) = f(0) = 0\ mod\ 3 = 0\ mod\ 4 = 0$, porém, para $f(6\ mod\ 6) = f(0) = 6\ mod\ 3 = 0$ mas $f(6\ mod\ 6) = f(0) = 7\ mod\ 4 = 3$ contradizendo o valor anterior de $f(0) = 0\ mod\ 4 = 0$. Concluindo que a função não está bem definida se $m$ não divide $n$, mas está bem definida se $m|n$.

2. Manipulando um pouco a combinação temos $\binom{p}{i} = \frac{p!}{i!(p-i)!} = p\frac{(p-1)!}{i!(p-i)!}$. Como $\binom{p}{i}$ tem que ser inteiro e $p$ não tem mais divisores além de 1 (sendo que $\frac{p}{1} = p$) e $p$ (que não tem como aparecer no denominador pois $i \leqslant p-1$), o valor de $\frac{(p-1)!}{i!(p-i)!} = k$ sempre será um inteiro para qualquer $p$ primo, então como $\binom{p}{i} = pk$, $p|\binom{p}{i}$, então $\binom{p}{i} \equiv 0\ mod\ p$, concluindo a demonstração.

5. Para $x^2 \equiv x\ mod\ 100$ temos 25 e 76;
   Para $x^2 \equiv x\ mod\ 1000$ temos 625 e 376;
   Para $x^2 \equiv x\ mod\ 10000$ temos 9376.