**Modularna Aritmetika**

Veoma često se traži da rešenje koje bi inače bilo veliki broj, bude ispisano po modulu **m**.

Moduo je u matematici definisan kao pozitivan ostatak pilikom celobrojnog deljenja jednog broja sa drugim.

Kao provera, modula pri deljenju broja **n** sa **m** mora da važi

**m** \* (**n** div **m**) + **n** mod **m** = **n ( I )**

SABIRANJE:

1. (**a**+**b**+**c**+…) mod **m** =
2. (**a** mod **m** + **b** mod **m** + **c** mod **m** …) mod **m** =
3. (…(((**a** mod **m** + **b** mod **m)** mod **m** + **c** mod **m)** mod **m** …) mod **m**

MNOŽENJE:

1. **a**\***b**\***c**\*… mod **m** =
2. **a** mod **m** \* **b** mod **m** \* **c** mod **m** \* d… mod **m** =

Koji od navedenih izraza upotrebiti zavisi od toga da li (**a**\***b**\***c**\*…) ili (**a+b+c+**…) izleće iz opsega tipa podatka kojim su promenljive definisane.

Takodje je bitno sagledati koliko je vreme kritično jer je **mod** operacija najsporija od svih operacija.

ODUZIMANJE:

1. (**a**-**b**-**c**-…) mod **m** =
2. (**a** mod **m** - **b** mod **m** - **c** mod **m** …) mod **m** =
3. (…(((**a** mod **m** - **b** mod **m)** mod **m** - **c** mod **m)** mod **m** …) mod **m**

**NAPOMENA: Ovo važi samo ako su brojevi koje delite pozitivni .**

**ZA NEGATIVNE BROJEVE NE VAŽI JEDNAKOST (I).**

Ako postoji opasnost da je broj koji delite negativan, tada ga je potrebno translirati u pozitini deo za neki proizvod delioca **m,** znači:

**a** < 0; **a** mod **m** = (**a**+**k**\***m**) mod **m**;

gde je k tako izabrano da (a+k\*m) predje u pozitivu a da pri tome ostanete u tipu podatka.

DELJENJE:

1. Ako je ikako moguće deljenje treba izbeći. Pod deljenjem se podrazumeva **DIV** operacija.
2. Ako nije moguće izbeći deljenje, tada ga treba odraditi pre nego sto se prvi **MOD m** odradi.
3. Ako ni to nije moguče, tada je postupak za deljenje sledeći:

(**A** div **B**) mod **m** = ( ( **A** mod **m** ) \* ( **Bm-2** mod **m** ) ) mod **m**    
  
ako je **m** prost broj

UGNJEŽDENO STEPENOVANJE

<http://stackoverflow.com/questions/4223313/finding-abc-mod-m>

Primeri zadataka:

[Super Bijeg](http://www.z-trening.com/tasks.php?show_task=5000000403)

[Trojke](http://www.z-trening.com/tasks.php?show_task=5000000125&lang=rs)

[Reli](http://www.z-trening.com/tasks.php?show_task=5000000102&lang=rs)

[Kvadratići Quals#2-2011](http://www.z-trening.com/tasks.php?show_task=5000001280&lang=rs)

[Z-Product – za deljenje](http://www.z-training.net/tasks.php?show_task=5000000340&lang=hr)

<http://www.codechef.com/problems/IITK2P10> - za ugnježdeno stepenovanje