Fermat e Eulero

Per quello che avete studiato nelle prime videolezioni, l'insieme delle classi resto modulo n ha una struttura di anello rispetto all'aritmetica (somma e prodotto) che vi avete definito. Ciò vuol dire, semplicemente, che sapete sommare e moltiplicare le classi. Ricordo che, date due classi (due elementi di $\mathbb{Z}_n$), la somma di tali classi è la classe della somma di due qualsiasi loro rappresentanti e, analogamente, il loro prodotto è la classe del prodotto di qualsiasi due rappresentanti. Le stesse regole si estendono alle potenze, sicché, se denotiamo con $\overline{a}$ la classe di a, valgono sinteticamente le regole:

- $\overline{a}+\overline{b} = \overline{a+b}$; inoltre a e b possono essere sostituiti con a' e b', rispettivamenti congrui ad a e b modulo n, senza che il risultato cambi: $\forall q,\, s,\, t \in \mathbb{Z},\ \overline{a+qn} + \overline{b+sn} = \overline{a+b+tn}$.
- $\overline{a}\overline{b} = \overline{ab}$; inoltre, valgono le stesse considerazioni viste sopra;
- per ogni intero non negativo s, $\overline{a^s} = \overline{a}^s$ e valgoo le stesse considerazioni viste sopra.

In moltissimi esercizi, è richiesto il calcolo della classe $\overline{a}^s$ per qualche s. Oltre all'inviduale creatività, vi sono tre risultati che consentono un tale conto:

1. la moltiplicatività della funzione ϕ di Eulero (leggete i primi due paragrafi di questa pagina fino al paragarafo *Andamento asintotico* escluso).
2. Il Teorema di Eulero-Fermat (leggete per intero questa cortissima pagina).
3. Il cosiddétto Piccolo Teorema di Fermat (leggete per intero questa altrettanto corta pagina). Tale teorema può vedersi come un corollario del Teorema di Eulero-Fermat.

I fatti suddetti sono discussi e dimostrati nelle videolezioni successive alla terza, nell'ambito della Teoria dei Gruppi. Sebbene io incoraggi ogni forma di ulteriore approfondimento, le poche righe contenute nelle pagine di Wikipedia che vi ho indicato sopra, sono più che bastevoli a risolvere gli esercizi di aritmetica che potrebbero capitarvi all'esame.