

Percorso: LM Plinio Seniore, dall'algebra modulare all'algoritmo di crittografia RSA con Python in Colab

Descrizione dell'attività

L'attività è articolata in tre fasi, per ciascuna di esse è previsto un Notebook Colab.

La documentazione relativa a Colab Google può essere reperita al seguente link

https://colab.research.google.com/?utm_source=scs-index

Il primo modulo "Introduzione a Python e l'algebra modulare"

[https://colab.research.google.com/drive/1uxJSCLDDTinTomX4PACtiwKFDdu-](https://colab.research.google.com/drive/1uxJSCLDDTinTomX4PACtiwKFDdu-Dt2g?usp=sharing)

[Dt2g?usp=sharing](https://colab.research.google.com/drive/1uxJSCLDDTinTomX4PACtiwKFDdu-Dt2g?usp=sharing) introduce all'uso del linguaggio Python inoltre sono riportati semplici esempi per familiarizzare con i comandi base e prepararsi alle sfide successive. Si descrive come importare moduli e/o librerie, il ciclo WHILE e le alternative con IF. Dal punto di vista matematico nel notebook si illustra l'algebra modulare e si propongono proposte di lavoro su semplici programmi. Per la sezione congetture/dimostrazioni si propone il gioco di Collatz.

Nel secondo modulo "Introduzione a Python, la primalità e MCD"

[https://colab.research.google.com/drive/1ewfQi7E6tfNLXFnPXS9p9bXayVuXR_Ck?usp=sha](https://colab.research.google.com/drive/1ewfQi7E6tfNLXFnPXS9p9bXayVuXR_Ck?usp=sharing)

[ring](https://colab.research.google.com/drive/1ewfQi7E6tfNLXFnPXS9p9bXayVuXR_Ck?usp=sharing) si approfondiscono alcuni aspetti del linguaggio Python come le stringhe e si introduce il ciclo FOR. Nel notebook si illustra la primalità e il crivello di Eratostene. Inoltre si introducono gli algoritmi di Euclide per il calcolo del MCD sia con il metodo delle sottrazioni successive sia con il metodo dei resti successivi. Per la sezione congetture/dimostrazioni si propone di scrivere un programma per verificare l'ipotesi di Goldback.

Nel terzo modulo "Le funzioni in Python e il sistema di crittografia RSA" si descrive l'algoritmo RSA e se ne propone una implementazione.

<https://colab.research.google.com/drive/10U8jhRghtYNRdFvpHfUft3AkVrwLweRb?usp=sharing>