# Matematiche complementari II

Prof. Marco Antonio Pellegrini

***OBIETTIVO DEL CORSO E RISULTATI DI APPRENDIMENTO ATTESI***

L’insegnamento si propone di fornire agli studenti le nozioni di base di Teoria dei Numeri, affrontando sia problemi classici propri di questa disciplina sia considerandone alcune applicazioni in ambito crittografico, mantenendo un approccio storico-didattico.

Al termine dell’insegnamento, lo studente che avrà partecipato attivamente alle lezioni avrà consolidato le proprie conoscenze algebriche e appreso i concetti di base della Teoria dei Numeri e di Crittografia.

***PROGRAMMA DEL CORSO***

- Interi: il corso inizia con un breve ripasso dei concetti visti nel corso di Algebra riguardo gli interi e le classi di resto modulo *n*. In particolare, parleremo di divisibilità e dell’algoritmo euclideo, di equazioni diofantee e di fattorizzazione unica. Vedremo anche alcuni risultati riguardanti i primi di Mersenne, i primi di Fermat e i numeri perfetti, i criteri di divisibilità, la risoluzioni di congruenze lineari, la funzione di Eulero.

- Interi di Gauss: studieremo l’anello degli interi di Gauss, allo scopo di determinare quali interi possono essere scritti come somma di due quadrati. Vedremo poi come gli interi di Gauss possono essere utilizzati per costruire terne pitagoriche.

- Crittografia a chiave simmetrica: vedremo alcuni risultati riguardanti i cifrari affini, cifrari a blocchi, il cifrario di Vigenère e i cifrari a flusso.

Crittografia a chiave pubblica: studieremo il sistema crittografico RSA e il problema della firma digitale.

- Ultimo teorema di Fermat: proveremo questo teorema, nel caso di quarte potenze, seguendo la dimostrazioni di Fermat basata sul metodo della discesa infinita.

***BIBLIOGRAFIA***

La referenza principale sono le dispense fornite dal docente sulla piattaforma Blackboard. Per un approfondimento degli argomenti visti, si consigliano:

J. Kraft, L. Washington, *An introduction to Number Theory with Cryptography, Second Edition,* Chapman and Hall/CRC, 2018.

M. Cozzens, S.J. Miller, *The Mathematics of Encryption, AMS*, 2013.

***DIDATTICA DEL CORSO***

Il corso di compone di lezioni alla lavagna. Gli studenti trovano numerosi esercizi nei libri indicati in Bibliografia.

***METODO E CRITERI DI VALUTAZIONE***

L’esame si compone di una prova orale, dalla durata media di 30-35 minuti, nella quale viene saggiata la preparazione teorica e la capacità espositiva e argomentativa dello studente. Durante tale prova, verrà chiesto allo studente di descrivere alcuni concetti visti nel corso, provandone alcuni risultati.

Il voto finale (espresso in trentesimi) terrà conto dell'efficacia, chiarezza e correttezza espositiva del candidato.

***AVVERTENZE E PREREQUISITI***

Si presuppone che lo studente abbia già nozioni di base di Algebra, solitamente acquisite durante il primo anno del corso di Laurea Triennale in Matematica.

*Orario e luogo di ricevimento degli studenti*

Il docente riceve nel proprio studio presso il Dipartimento di Matematica e Fisica, compatibilmente con i vari impegni didattici. E’ anche possibile utilizzare la piattaforma Blackboard per il ricevimento “a distanza”. Si consiglia in ogni caso di fissare un appuntamento scrivendo a [marcoantonio.pellegrini@unicatt.it](mailto:marcoantonio.pellegrini@unicatt.it).