DIDATTICA EROGATA 2026/2027

Matematica (LM-40 R)

Dipartimento: MATEMATICA E FISICA
Codice CdS: 104652

INSEGNAMENTI

Primo semestre

20410882 - AC310 - ANALISI COMPLESSA *(- MATH-02/B - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*
Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CAPORASO LUCIA	72	
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CAPORASO LUCIA	72	
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CAPORASO LUCIA	72	

20410882 - AC310 - ANALISI COMPLESSA *(- MATH-02/B,MATH-02/B - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*
Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CAPORASO LUCIA	72	
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CAPORASO LUCIA	72	
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CAPORASO LUCIA	72	

20410882 - AC310 - ANALISI COMPLESSA *(- MATH-02/B,MATH-03/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*
Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CAPORASO LUCIA	72	
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CAPORASO LUCIA	72	
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CAPORASO LUCIA	72	

20410408 - AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*
Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	

20410445 - AL410 - ALGEBRA COMMUTATIVA *(- MATH-02/A - 9 CFU - 72 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*
Docenti:

Nominativo	Ore	Tipo incarico	Canale
TURCHET AMOS	60	Carico didattico	

Nominativo	Ore	Tipo incarico	Canale
TURCHET AMOS	12	Affidamento a titolo gratuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410445 AL410 - ALGEBRA COMMUTATIVA in Matematica LM-40 R TURCHET AMOS	72	
Mutuato da: 20410445 AL410 - ALGEBRA COMMUTATIVA in Matematica LM-40 R TURCHET AMOS	72	

20410408 - AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE *(- MATH-02/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	

20410609 - AM300 - ANALISI MATEMATICA 5 *(- MATH-03/A - 9 CFU - 72 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410609 AM300 - ANALISI MATEMATICA 5 in Matematica L-35 R HAUS EMANUELE	72	
Mutuato da: 20410609 AM300 - ANALISI MATEMATICA 5 in Matematica L-35 R HAUS EMANUELE	72	

20410876 - AM400-ISTITUZIONI DI ANALISI SUPERIORE *(- MATH-03/A - 9 CFU - 72 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
FEOLA ROBERTO	72	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410876 AM400-ISTITUZIONI DI ANALISI SUPERIORE in Matematica LM-40 R FEOLA ROBERTO	72	
Mutuato da: 20410876 AM400-ISTITUZIONI DI ANALISI SUPERIORE in Matematica LM-40 R FEOLA ROBERTO	72	

20410469 - AM430 - EQUAZIONI DIFFERENZIALI ORDINARIE *(- MATH-03/A - 6 CFU - 60 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BESSI UGO	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410469 AM430 - EQUAZIONI DIFFERENZIALI ORDINARIE in Matematica LM-40 R BESSI UGO	60	
Mutuato da: 20410469 AM430 - EQUAZIONI DIFFERENZIALI ORDINARIE in Matematica LM-40 R BESSI UGO	60	

20430011 - BL410-INTRODUZIONE ALLA BIOLOGIA *(- BIOS-08/A - 6 CFU - 48 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20440000 Introduzione alla Biologia in Scienze biologiche L-13 R BERARDINELLI FRANCESCO	48	
Fruito da: 20440000 Introduzione alla Biologia in Scienze biologiche L-13 R COLASANTI MARCO	48	
Fruito da: 20440000 Introduzione alla Biologia in Scienze biologiche L-13 R ROSSI MARIANNA NICOLETTA	48	

20410413 - AN410 - ANALISI NUMERICA 1 *(- MATH-05/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410413 AN410 - ANALISI NUMERICA 1 in Matematica L-35 R FERRETTI ROBERTO	72	
Mutuato da: 20410413 AN410 - ANALISI NUMERICA 1 in Matematica L-35 R FERRETTI ROBERTO	72	
Mutuato da: 20410413 AN410 - ANALISI NUMERICA 1 in Matematica L-35 R FERRETTI ROBERTO	72	
Mutuato da: 20410413 AN410 - ANALISI NUMERICA 1 in Matematica L-35 R FERRETTI ROBERTO	72	

20410439 - CH410- ELEMENTI DI CHIMICA *(- CHEM-03/A - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410066 CHIMICA E LABORATORIO in Scienze geologiche L-34 R TUTI SIMONETTA	60	

20410414 - CP410 - TEORIA DELLA PROBABILITÀ *(- MATH-03/B - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia*

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410414 CP410 - TEORIA DELLA PROBABILITÀ in Matematica L-35 R CANDELLERO ELISABETTA	72	

20410447 - CP410 - TEORIA DELLA PROBABILITÀ *(- MATH-03/B - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410414 CP410 - TEORIA DELLA PROBABILITÀ in Matematica L-35 R CANDELLERO ELISABETTA	72	
Fruito da: 20410414 CP410 - TEORIA DELLA PROBABILITÀ in Matematica L-35 R CANDELLERO ELISABETTA	72	
Fruito da: 20410414 CP410 - TEORIA DELLA PROBABILITÀ in Matematica L-35 R CANDELLERO ELISABETTA	72	

20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO A *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MEROLA FRANCESCA	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410625-1 CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO A in Matematica LM-40 R MEROLA FRANCESCA	60	
Mutuato da: 20410625-1 CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO A in Matematica LM-40 R MEROLA FRANCESCA	60	

20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO B *(- MATH-02/A - 3 CFU - 12 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MEROLA FRANCESCA	12	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410625-2 CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO B in Matematica LM-40 R MEROLA FRANCESCA	12	
Mutuato da: 20410625-2 CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO B in Matematica LM-40 R MEROLA FRANCESCA	12	

20430000 - FS410 - LABORATORIO DI DIDATTICA DELLA FISICA *(- PHYS-01/A - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
ORESTANO DOMIZIA	30	Carico didattico	
RICCI FEDERICA	30	Carico didattico	

20410436 - FS420 - MECCANICA QUANTISTICA *(- PHYS-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Matematica applicata e computazionale*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410015 MECCANICA QUANTISTICA in Fisica L-30 R LUBICZ VITTORIO	60	
Fruito da: 20410015 MECCANICA QUANTISTICA in Fisica L-30 R TARANTINO CECILIA	60	

20411068 - FS430 - TEORIA DEI CAMPI E GRAVITÀ *(- PHYS-02/A - 6 CFU - 48 ore - ITA)*

Curricula: *Matematica applicata e computazionale*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20430009 Teoria dei Campi e Gravità in Fisica LM-17 R FRANCIA DARIO	48	

20410429 - FS510 - METODO MONTECARLO *(- PHYS-01/A - 6 CFU - 60 ore - ITA)*

Curricula: *Matematica applicata e computazionale*

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410429 FS510 - METODO MONTECARLO in Fisica LM-17 R FRANCESCHINI ROBERTO	40	
Mutuato da: 20410429 FS510 - METODO MONTECARLO in Fisica LM-17 R BUSSINO SEVERINO ANGELO MARIA	20	

20411003 - FS520 – RETI COMPLESSE *(- INFO-01/A,INFO-01/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
GUARINO STEFANO	60	Contratto di insegnamento gratuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20411003 FS520 – RETI COMPLESSE in Matematica LM-40 R GUARINO STEFANO	60	
Mutuato da: 20411003 FS520 – RETI COMPLESSE in Matematica LM-40 R GUARINO STEFANO	60	

20411003 - FS520 – RETI COMPLESSE *(- INFO-01/A,PHYS-03/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
GUARINO STEFANO	60	Contratto di insegnamento gratuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20411003 FS520 – RETI COMPLESSE in Matematica LM-40 R GUARINO STEFANO	60	
Mutuato da: 20411003 FS520 – RETI COMPLESSE in Matematica LM-40 R GUARINO STEFANO	60	

20410449 - GE410 - GEOMETRIA ALGEBRICA 1 *(- MATH-02/B - 9 CFU - 72 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
LOPEZ ANGELO	60	Carico didattico	
LOPEZ ANGELO	12	Affidamento a titolo gratuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410449 GE410 - GEOMETRIA ALGEBRICA 1 in Matematica LM-40 R LOPEZ ANGELO	72	
Mutuato da: 20410449 GE410 - GEOMETRIA ALGEBRICA 1 in Matematica LM-40 R LOPEZ ANGELO	72	

20410465 - GE450 - TOPOLOGIA ALGEBRICA *(- MATH-02/B - 6 CFU - 60 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MASCARENHAS MELO ANA MARGARIDA	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410465 GE450 - TOPOLOGIA ALGEBRICA in Matematica LM-40 R MASCARENHAS MELO ANA MARGARIDA	60	
Mutuato da: 20410465 GE450 - TOPOLOGIA ALGEBRICA in Matematica LM-40 R MASCARENHAS MELO ANA MARGARIDA	60	

20411064 - IN401 - MODULO A: PROGRAMMAZIONE IN PYTHON *(- INFO-01/A - 3 CFU - 30 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
Da assegnare	30	Bando	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20411064-1 IN401 - MODULO A: PROGRAMMAZIONE IN PYTHON in Matematica LM-40 R		
Mutuato da: 20411064-1 IN401 - MODULO A: PROGRAMMAZIONE IN PYTHON in Matematica LM-40 R		

20411064 - IN401 - MODULO B: TECNICHE DI PROGRAMMAZIONE SCIENTIFICA *(- INFO-01/A - 3 CFU - 30 ore - ITA)*

Curricula: *Crittografia - Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
Da assegnare	30	Bando	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20411064-2 IN401 - MODULO B: TECNICHE DI PROGRAMMAZIONE SCIENTIFICA in Matematica LM-40 R		
Mutuato da: 20411064-2 IN401 - MODULO B: TECNICHE DI PROGRAMMAZIONE SCIENTIFICA in Matematica LM-40 R		

Dettaglio	Ore	Canale
Mutuato da: 20411064-2 IN401 - MODULO B: TECNICHE DI PROGRAMMAZIONE SCIENTIFICA in Matematica LM-40 R		

20410427 - IN490 - LINGUAGGI DI PROGRAMMAZIONE *(- INFO-01/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
LOMBARDI FLAVIO	72	Esperto di alta qualificazione retribuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410427 IN490 - LINGUAGGI DI PROGRAMMAZIONE in Matematica LM-40 R LOMBARDI FLAVIO	72	
Mutuato da: 20410427 IN490 - LINGUAGGI DI PROGRAMMAZIONE in Matematica LM-40 R LOMBARDI FLAVIO	72	

20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ *(- MATH-01/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
PEDICINI MARCO	60	Carico didattico	
PEDICINI MARCO	12	Affidamento a titolo gratuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410417 IN410-CALCOLABILITÀ E COMPLESSITÀ in Matematica LM-40 R PEDICINI MARCO	72	
Mutuato da: 20410417 IN410-CALCOLABILITÀ E COMPLESSITÀ in Matematica LM-40 R PEDICINI MARCO	72	
Mutuato da: 20410417 IN410-CALCOLABILITÀ E COMPLESSITÀ in Matematica LM-40 R PEDICINI MARCO	72	

20411002 - IN510 – QUANTUM COMPUTING MODULO A *(- IINF-05/A - 3 CFU - 27 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20830130-1 QUANTUM COMPUTING - I Modulo in Ingegneria informatica e dell'intelligenza artificiale LM-32 DI BATTISTA GIUSEPPE	27	
Fruito da: 20830130-1 QUANTUM COMPUTING - I Modulo in Ingegneria informatica e dell'intelligenza artificiale LM-32 DI BATTISTA GIUSEPPE	27	
Fruito da: 20830130-1 QUANTUM COMPUTING - I Modulo in Ingegneria informatica e dell'intelligenza artificiale LM-32 DI BATTISTA GIUSEPPE	27	

20411002 - IN510 – QUANTUM COMPUTING MODULO B *(- INFO-01/A - 3 CFU - 30 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
PEDICINI MARCO	30	Affidamento a titolo gratuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20411002_2 IN510 – QUANTUM COMPUTING MODULO B in Matematica LM-40 R PEDICINI MARCO	30	
Mutuato da: 20411002_2 IN510 – QUANTUM COMPUTING MODULO B in Matematica LM-40 R PEDICINI MARCO	30	

20410432 - IN550 – MACHINE LEARNING *(- INFO-01/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BONIFACI VINCENZO	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410432 IN550 – MACHINE LEARNING in Matematica LM-40 R BONIFACI VINCENZO	60	
Mutuato da: 20410432 IN550 – MACHINE LEARNING in Matematica LM-40 R BONIFACI VINCENZO	60	

20410621 - MC410 - DIDATTICA DELLA MATEMATICA *(- MATH-01/B - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BRUNO ANDREA	60	Carico didattico	

20410451 - LM410 -TEOREMI SULLA LOGICA 1 - MODULO A *(- MATH-01/A - 6 CFU - 48 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MAIELI ROBERTO	48	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410451-1 LM410 -TEOREMI SULLA LOGICA 1 - MODULO A in Matematica LM-40 R MAIELI ROBERTO	48	
Mutuato da: 20410451-1 LM410 -TEOREMI SULLA LOGICA 1 - MODULO A in Matematica LM-40 R MAIELI ROBERTO	48	
Mutuato da: 20410451-1 LM410 -TEOREMI SULLA LOGICA 1 - MODULO A in Matematica LM-40 R MAIELI ROBERTO	48	

20410451 - LM410 -TEOREMI SULLA LOGICA 1 - MODULO B *(- MATH-01/A - 3 CFU - 24 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
TORTORA DE FALCO LORENZO	24	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410451-2 LM410 -TEOREMI SULLA LOGICA 1 - MODULO B in Matematica LM-40 R TORTORA DE FALCO LORENZO	24	
Mutuato da: 20410451-2 LM410 -TEOREMI SULLA LOGICA 1 - MODULO B in Matematica LM-40 R TORTORA DE FALCO LORENZO	24	
Mutuato da: 20410451-2 LM410 -TEOREMI SULLA LOGICA 1 - MODULO B in Matematica LM-40 R TORTORA DE FALCO LORENZO	24	

20410613 - LM430 - LOGICA E FONDAMENTI DELLA MATEMATICA *(- MATH-01/A - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
TORTORA DE FALCO LORENZO	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410613 LM430 - LOGICA E FONDAMENTI DELLA MATEMATICA in Matematica LM-40 R TORTORA DE FALCO LORENZO	60	
Mutuato da: 20410613 LM430 - LOGICA E FONDAMENTI DELLA MATEMATICA in Matematica LM-40 R TORTORA DE FALCO LORENZO	60	
Mutuato da: 20410613 LM430 - LOGICA E FONDAMENTI DELLA MATEMATICA in Matematica LM-40 R TORTORA DE FALCO LORENZO	60	

20410456 - MC420-DIDATTICA DELLA MATEMATICA *(- MATH-01/B - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MAGRONE PAOLA	60	Affidamento di incarico retribuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410456 MC420-DIDATTICA DELLA MATEMATICA in Matematica LM-40 R MAGRONE PAOLA	60	

20411076 - MC430 - LABORATORIO DI DIDATTICA DELLA MATEMATICA *(- MATH-01/A,MATH-01/B - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
FALCOLINI CORRADO	60	Affidamento di incarico retribuito	

20410617 - ME410 - ELEMENTI DI ALGEBRA SUPERIORE *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
Da assegnare	30	Bando	
TARTARONE FRANCESCA	30	Carico didattico	

20410618 - ME420 - FONDAMENTI E STORIA DELLA GEOMETRIA *(- MATH-02/B - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
LELLI CHIESA MARGHERITA	56	Carico didattico	
VERRA ALESSANDRO	4	Esperto di alta qualificazione (contratto gratuito, Art. 23 comma 1)	

20410555 - ST410-STATISTICA *(- MATH-03/B - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
CANDELLERO ELISABETTA	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410555 ST410-STATISTICA in Matematica LM-40 R CANDELLERO ELISABETTA	60	
Mutuato da: 20410555 ST410-STATISTICA in Matematica LM-40 R CANDELLERO ELISABETTA	60	
Mutuato da: 20410555 ST410-STATISTICA in Matematica LM-40 R CANDELLERO ELISABETTA	60	

20410627 - TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
PAPPALARDI FRANCESCO	45	Affidamento a titolo gratuito	
Da assegnare	15	Bando	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R PAPPALARDI FRANCESCO	45	
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R		
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R PAPPALARDI FRANCESCO	45	
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R		
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R PAPPALARDI FRANCESCO	45	
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R		

20410766 - TN520 - ALTEZZE ED EQUAZIONI DIOFANTEE *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BARROERO FABRIZIO	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410766 TN520 - ALTEZZE ED EQUAZIONI DIOFANTEE in Matematica LM-40 R BARROERO FABRIZIO	60	

Secondo semestre

20411075 - AL450 - TEORIA DELLE RAPPRESENTAZIONI *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
TURCHET AMOS	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20411075 AL450 - TEORIA DELLE RAPPRESENTAZIONI in Matematica LM-40 R TURCHET AMOS	60	
Mutuato da: 20411075 AL450 - TEORIA DELLE RAPPRESENTAZIONI in Matematica LM-40 R TURCHET AMOS	60	

20410757 - AM410 - MODULO B - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI *(- MATH-03/A - 3 CFU - 30 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BATTAGLIA LUCA	30	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410757_2 AM410 - MODULO B - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI in Matematica LM-40 R BATTAGLIA LUCA	30	
Mutuato da: 20410757_2 AM410 - MODULO B - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI in Matematica LM-40 R BATTAGLIA LUCA	30	

20410757 - AM410- MODULO A - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI *(- MATH-03/A - 3 CFU - 30 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BATTAGLIA LUCA	30	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410757_1 AM410- MODULO A - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI in Matematica LM-40 R BATTAGLIA LUCA	30	
Mutuato da: 20410757_1 AM410- MODULO A - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI in Matematica LM-40 R BATTAGLIA LUCA	30	

20410637 - AM450 - ANALISI FUNZIONALE *(- MATH-03/A - 9 CFU - 72 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BESSI UGO	60	Carico didattico	
BESSI UGO	12	Affidamento a titolo gratuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410637 AM450 - ANALISI FUNZIONALE in Matematica LM-40 R BESSI UGO	72	
Mutuato da: 20410637 AM450 - ANALISI FUNZIONALE in Matematica LM-40 R BESSI UGO	72	

20410428 - CR510 – CRITTOSISTEMI ELLITTICI *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
CAPUANO LAURA	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410428 CR510 – CRITTOSISTEMI ELLITTICI in Matematica LM-40 R CAPUANO LAURA	60	
Mutuato da: 20410428 CR510 – CRITTOSISTEMI ELLITTICI in Matematica LM-40 R CAPUANO LAURA	60	
Mutuato da: 20410428 CR510 – CRITTOSISTEMI ELLITTICI in Matematica LM-40 R CAPUANO LAURA	60	

20410420 - AN420 - ANALISI NUMERICA 2 *(- MATH-05/A - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
FERRETTI ROBERTO	60	Carico didattico	
REUVERS ROBIN JOHANNES PETRUS	12	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R FERRETTI ROBERTO	60	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R REUVERS ROBIN JOHANNES PETRUS	12	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R FERRETTI ROBERTO	60	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R REUVERS ROBIN JOHANNES PETRUS	12	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R FERRETTI ROBERTO	60	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R REUVERS ROBIN JOHANNES PETRUS	12	

20410420 - AN420 - ANALISI NUMERICA 2 *(- MATH-05/A - 9 CFU - 72 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
FERRETTI ROBERTO	60	Carico didattico	
REUVERS ROBIN JOHANNES PETRUS	12	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R FERRETTI ROBERTO	60	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R REUVERS ROBIN JOHANNES PETRUS	12	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R FERRETTI ROBERTO	60	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R REUVERS ROBIN JOHANNES PETRUS	12	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R FERRETTI ROBERTO	60	
Mutuato da: 20410420 AN420 - ANALISI NUMERICA 2 in Matematica LM-40 R REUVERS ROBIN JOHANNES PETRUS	12	

20411067 - CR530 – POST QUANTUM CRYPTOGRAPHY *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
Da assegnare	60	Bando	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20411067 CR530 – POST QUANTUM CRYPTOGRAPHY in Matematica LM-40 R		

20410410 - FM310 - ISTITUZIONI DI FISICA MATEMATICA *(- MATH-04/A - 9 CFU - 72 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410410 FM310 - ISTITUZIONI DI FISICA MATEMATICA in Matematica L-35 R GIULIANI ALESSANDRO	72	
Mutuato da: 20410410 FM310 - ISTITUZIONI DI FISICA MATEMATICA in Matematica L-35 R GIULIANI ALESSANDRO	72	
Mutuato da: 20410410 FM310 - ISTITUZIONI DI FISICA MATEMATICA in Matematica L-35 R GIULIANI ALESSANDRO	72	

20410441 - CP420-INTRODUZIONE AI PROCESSI STOCASTICI *(- MATH-03/B - 6 CFU - 10 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
CAPUTO PIETRO	10	Affidamento a titolo gratuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410441 CP420-INTRODUZIONE AI PROCESSI STOCASTICI in Matematica LM-40 R CAPUTO PIETRO	10	
Mutuato da: 20410441 CP420-INTRODUZIONE AI PROCESSI STOCASTICI in Matematica LM-40 R CAPUTO PIETRO	10	
Mutuato da: 20410441 CP420-INTRODUZIONE AI PROCESSI STOCASTICI in Matematica LM-40 R CAPUTO PIETRO	10	

20410556 - CP450 - METODI PROBABILISTICI E ALGORITMI ALEATORI *(- MATH-03/B - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20430033 METODI PROBABILISTICI E ALGORITMI ALEATORI in DATA SCIENCE LM-Data QUATTROPANI MATTEO	60	
Fruito da: 20430033 METODI PROBABILISTICI E ALGORITMI ALEATORI in DATA SCIENCE LM-Data QUATTROPANI MATTEO	60	
Fruito da: 20430033 METODI PROBABILISTICI E ALGORITMI ALEATORI in DATA SCIENCE LM-Data QUATTROPANI MATTEO	60	

Dettaglio	Ore	Canale
Fruito da: 20430033 METODI PROBABILISTICI E ALGORITMI ALEATORI in DATA SCIENCE LM-Data QUATTROPANI MATTEO	60	

20410416 - FM410-COMPLEMENTI DI MECCANICA ANALITICA - Modulo A *(- MATH-04/A - 3 CFU - 30 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410084 COMPLEMENTI DI MECCANICA ANALITICA - MOD A in Fisica L-30 R REUVERS Robin Johannes Petrus	30	
Fruito da: 20410084 COMPLEMENTI DI MECCANICA ANALITICA - MOD A in Fisica L-30 R REUVERS Robin Johannes Petrus	30	

20410416 - FM410-COMPLEMENTI DI MECCANICA ANALITICA - Modulo B *(- MATH-04/A - 3 CFU - 30 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410085 COMPLEMENTI DI MECCANICA ANALITICA - MOD. B in Fisica L-30 R MARCELLI GIOVANNA	30	
Fruito da: 20410085 COMPLEMENTI DI MECCANICA ANALITICA - MOD. B in Fisica L-30 R MARCELLI GIOVANNA	30	

20410875 - FM530 - METODI MATEMATICI PER IL MACHINE LEARNING *(- MATH-04/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20430032 METODI MATEMATICI PER IL MACHINE LEARNING in DATA SCIENCE LM-Data REUVERS ROBIN JOHANNES PETRUS	72	
Fruito da: 20430032 METODI MATEMATICI PER IL MACHINE LEARNING in DATA SCIENCE LM-Data REUVERS ROBIN JOHANNES PETRUS	72	
Fruito da: 20430032 METODI MATEMATICI PER IL MACHINE LEARNING in DATA SCIENCE LM-Data REUVERS ROBIN JOHANNES PETRUS	72	

20430001 - FM540 - METODI COMPUTAZIONALI PER MODELLI STOCASTICI *(- MATH-04/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
SCALA ANTONIO	60	Affidamento in convenzione	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20430001 FM540 - METODI COMPUTAZIONALI PER MODELLI STOCASTICI in Matematica LM-40 R Scala Antonio	60	
Mutuato da: 20430001 FM540 - METODI COMPUTAZIONALI PER MODELLI STOCASTICI in Matematica LM-40 R Scala Antonio	60	
Mutuato da: 20430001 FM540 - METODI COMPUTAZIONALI PER MODELLI STOCASTICI in Matematica LM-40 R Scala Antonio	60	

20411074 - FS401- MODULO A - ELEMENTI DI FISICA TEORICA CONTEMPORANEA *(- PHYS-02/A - 3 CFU - 30 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410023 ELEMENTI DI FISICA TEORICA CONTEMPORANEA in Fisica L-30 R LUBICZ VITTORIO	30	
Fruito da: 20410023 ELEMENTI DI FISICA TEORICA CONTEMPORANEA in Fisica L-30 R TARANTINO CECILIA	30	
Fruito da: 20410023 ELEMENTI DI FISICA TEORICA CONTEMPORANEA in Fisica L-30 R LUBICZ VITTORIO	30	
Fruito da: 20410023 ELEMENTI DI FISICA TEORICA CONTEMPORANEA in Fisica L-30 R TARANTINO CECILIA	30	

20411074 - FS401- MODULO B - RELATIVITÀ RISTRETTA *(- PHYS-02/A - 3 CFU - 30 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20430005 Relatività Ristretta in Fisica L-30 R MELONI DAVIDE	30	
Fruito da: 20430005 Relatività Ristretta in Fisica L-30 R MELONI DAVIDE	30	

20410434 - FS450 - ELEMENTI DI MECCANICA STATISTICA *(- PHYS-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Matematica applicata e computazionale*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20401806 ELEMENTI DI MECCANICA STATISTICA in Fisica L-30 R N0 RAIMONDI ROBERTO	60	

20410461 - FS460 - DIDATTICA DELLA FISICA *(- PHYS-06/B - 6 CFU - 64 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410502 DIDATTICA DELLA FISICA in Fisica LM-17 R	64	

20410566 - FS470 - PRINCIPI DI ASTROFISICA *(- PHYS-05/A - 6 CFU - 60 ore - ITA)*

Curricula: *Matematica applicata e computazionale*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410499 Principi di Astrofisica in Fisica L-30 R LA FRANCA FABIO	60	
Fruito da: 20410499 Principi di Astrofisica in Fisica L-30 R MATT GIORGIO	60	

20410411 - GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE *(- MATH-02/B - 9 CFU - 72 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R PONTECORVO MASSIMILIANO	60	
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R SUPINO PAOLA	12	
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R PONTECORVO MASSIMILIANO	60	
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R SUPINO PAOLA	12	

20410425 - GE460 - TEORIA DEI GRAFI *(- MATH-02/B - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MASCARENHAS MELO ANA MARGARIDA	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410425 GE460 - TEORIA DEI GRAFI in Matematica LM-40 R MASCARENHAS MELO ANA MARGARIDA	60	
Mutuato da: 20410425 GE460 - TEORIA DEI GRAFI in Matematica LM-40 R MASCARENHAS MELO ANA MARGARIDA	60	
Mutuato da: 20410425 GE460 - TEORIA DEI GRAFI in Matematica LM-40 R MASCARENHAS MELO ANA MARGARIDA	60	
Mutuato da: 20410425 GE460 - TEORIA DEI GRAFI in Matematica LM-40 R MASCARENHAS MELO ANA MARGARIDA	60	

20410462 - GE510 - GEOMETRIA ALGEBRICA 2 *(- MATH-02/B - 6 CFU - 60 ore - ITA)*

Curricula: *Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
SCHAFFLER LUCA	60	Carico didattico	

20411007 - GL410 - INTRODUZIONE ALLA GEOLOGIA *(- GEOS-02/C - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20411005-2 INTRODUZIONE ALLA GEOLOGIA in Scienze della Natura e dell'Ambiente L-32 R CIFELLI FRANCESCA	60	
Fruito da: 20411005-2 INTRODUZIONE ALLA GEOLOGIA in Scienze della Natura e dell'Ambiente L-32 R MATTEI MASSIMO	60	

20410442 - IN420 - TEORIA DELL'INFORMAZIONE *(- INFO-01/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BONIFACI VINCENZO	60	Carico didattico	
BONIFACI VINCENZO	12	Affidamento a titolo gratuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410442 IN420 - TEORIA DELL'INFORMAZIONE in Matematica LM-40 R BONIFACI VINCENZO	72	
Mutuato da: 20410442 IN420 - TEORIA DELL'INFORMAZIONE in Matematica LM-40 R BONIFACI VINCENZO	72	

20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA *(- MATH-06/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
LIVERANI MARCO	48	Esperto di alta qualificazione retribuito	
Da assegnare	24	Bando	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410626 IN440 - OTTIMIZZAZIONE COMBINATORIA in Matematica LM-40 R LIVERANI MARCO	48	
Mutuato da: 20410626 IN440 - OTTIMIZZAZIONE COMBINATORIA in Matematica LM-40 R		
Mutuato da: 20410626 IN440 - OTTIMIZZAZIONE COMBINATORIA in Matematica LM-40 R LIVERANI MARCO	48	
Mutuato da: 20410626 IN440 - OTTIMIZZAZIONE COMBINATORIA in Matematica LM-40 R		
Mutuato da: 20410626 IN440 - OTTIMIZZAZIONE COMBINATORIA in Matematica LM-40 R LIVERANI MARCO	48	
Mutuato da: 20410626 IN440 - OTTIMIZZAZIONE COMBINATORIA in Matematica LM-40 R		

20410424 - IN450- ALGORITMI PER LA CRITTOGRAFIA *(- INFO-01/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
PEDICINI MARCO	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410424 IN450- ALGORITMI PER LA CRITTOGRAFIA in Matematica LM-40 R PEDICINI MARCO	60	
Mutuato da: 20410424 IN450- ALGORITMI PER LA CRITTOGRAFIA in Matematica LM-40 R PEDICINI MARCO	60	

20410426 - IN480 - CALCOLO PARALLELO E DISTRIBUITO *(- INFO-01/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
LOMBARDI FLAVIO	72	Affidamento in convenzione	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410426 IN480 - CALCOLO PARALLELO E DISTRIBUITO in Matematica LM-40 R LOMBARDI FLAVIO	72	
Mutuato da: 20410426 IN480 - CALCOLO PARALLELO E DISTRIBUITO in Matematica LM-40 R LOMBARDI FLAVIO	72	

20411014 - IN580- ETHICAL HACKING *(- IINF-03/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20810554 ETHICAL HACKING in Ingegneria delle Telecomunicazioni LM-27 CARLI MARCO	60	
Fruito da: 20810554 ETHICAL HACKING in Ingegneria delle Telecomunicazioni LM-27 CARLI MARCO	72	

20411014 - IN580- ETHICAL HACKING *(- IINF-03/A - 9 CFU - 72 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20810554 ETHICAL HACKING in Ingegneria delle Telecomunicazioni LM-27 CARLI MARCO	60	
Fruito da: 20810554 ETHICAL HACKING in Ingegneria delle Telecomunicazioni LM-27 CARLI MARCO	72	

20430002 - IN590 - NATURAL LANGUAGE PROCESSING *(- INFO-01/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Matematica applicata e computazionale*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
Da assegnare	60	Bando	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20430002 IN590 - NATURAL LANGUAGE PROCESSING in Matematica LM-40 R		

20410592 - LM400 - INTRODUZIONE ALLA LOGICA *(- PHIL-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410592 LM400 - INTRODUZIONE ALLA LOGICA in Matematica L-35 R ABRUSCI VITO MICHELE	60	
Mutuato da: 20410592 LM400 - INTRODUZIONE ALLA LOGICA in Matematica L-35 R ABRUSCI VITO MICHELE	60	

20410455 - LM420 - TEOREMI SULLA LOGICA 2 *(- MATH-01/A - 6 CFU - 60 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20710122 TEOREMI SULLA LOGICA, 2 in Scienze filosofiche LM-78 R TORTORA DE FALCO LORENZO	60	
Fruito da: 20710122 TEOREMI SULLA LOGICA, 2 in Scienze filosofiche LM-78 R TORTORA DE FALCO LORENZO	60	

20410529 - LM510 - TEORIE LOGICHE 1 *(- MATH-01/A - 6 CFU - 36 ore - ITA)*

Curricula: *Matematica applicata e computazionale - Teorico*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20710091 TEORIE LOGICHE 1 - LM in Scienze filosofiche LM-78 R MAIELI ROBERTO	36	
Fruito da: 20710091 TEORIE LOGICHE 1 - LM in Scienze filosofiche LM-78 R MAIELI ROBERTO	36	

20410456 - MC420-DIDATTICA DELLA MATEMATICA *(- MATH-01/B - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MAGRONE PAOLA	60	Affidamento di incarico retribuito	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410456 MC420-DIDATTICA DELLA MATEMATICA in Matematica LM-40 R MAGRONE PAOLA	60	

20411076 - MC430 - LABORATORIO DI DIDATTICA DELLA MATEMATICA *(- MATH-01/A,MATH-01/B - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
FALCOLINI CORRADO	60	Affidamento di incarico retribuito	

20410617 - ME410 - ELEMENTI DI ALGEBRA SUPERIORE *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
Da assegnare	30	Bando	
TARTARONE FRANCESCA	30	Carico didattico	

20410619 - ME430 - FONDAMENTI E STORIA DELL'ANALISI MATEMATICA *(- MATH-03/A - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MATALONI SILVIA	30	Esperto di alta qualificazione retribuito	
BIASCO LUCA	18	Affidamento a titolo gratuito	
BIASCO LUCA	12	Carico didattico	

20410438 - MF410 - FINANZA COMPUTAZIONALE *(- STAT-04/A - 9 CFU - 60 ore - ITA)*

Curricula: *Matematica applicata e computazionale*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 21201730 FINANZA COMPUTAZIONALE in Finanza e impresa LM-16 R CESARONE FRANCESCO	60	

20411069 - MS411-MECCANICA STATISTICA *(- MATH-04/A - 6 CFU - 60 ore - ITA)*

Curricula: *Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
GIULIANI ALESSANDRO	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20411069 MS411-MECCANICA STATISTICA in Matematica LM-40 R GIULIANI ALESSANDRO	60	
Mutuato da: 20411069 MS411-MECCANICA STATISTICA in Matematica LM-40 R GIULIANI ALESSANDRO	60	
Mutuato da: 20411069 MS411-MECCANICA STATISTICA in Matematica LM-40 R GIULIANI ALESSANDRO	60	

20410627 - TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI *(- MATH-02/A - 6 CFU - 60 ore - ITA)*

Curricula: *Crittografia - Didattica e comunicazione scientifica - Matematica applicata e computazionale - Teorico*

Docenti:

Nominativo	Ore	Tipo incarico	Canale
PAPPALARDI FRANCESCO	45	Affidamento a titolo gratuito	
Da assegnare	15	Bando	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R PAPPALARDI FRANCESCO	45	
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R		
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R PAPPALARDI FRANCESCO	45	
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R		
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R PAPPALARDI FRANCESCO	45	
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R		

INCARICHI DIDATTICI DEL CORSO DI LAUREA

Nominativo	Tot.Ore	Tipo incarico	Ore	Attivita didattica
BARROERO FABRIZIO	60	Carico didattico	60	20410766 - TN520 - ALTEZZE ED EQUAZIONI DIOFANTEE
BATTAGLIA LUCA	60	Carico didattico	30	20410757 - AM410 - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI
		Carico didattico	30	20410757 - AM410 - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI
BESSI UGO	132	Carico didattico	60	20410469 - AM430 - EQUAZIONI DIFFERENZIALI ORDINARIE
		Affidamento a titolo gratuito	72	20410637 - AM450 - ANALISI FUNZIONALE
		Carico didattico	48	20410637 - AM450 - ANALISI FUNZIONALE
BIASCO LUCA	30	Carico didattico	12	20410619 - ME430 - FONDAMENTI E STORIA DELL'ANALISI MATEMATICA
		Affidamento a titolo gratuito	12	20410619 - ME430 - FONDAMENTI E STORIA DELL'ANALISI MATEMATICA
BONIFACI VINCENZO	132	Affidamento a titolo gratuito	72	20410442 - IN420 - TEORIA DELL'INFORMAZIONE
		Carico didattico	48	20410442 - IN420 - TEORIA DELL'INFORMAZIONE
		Carico didattico	60	20410432 - IN550 – MACHINE LEARNING
BRUNO ANDREA	60	Carico didattico	60	20410621 - MC410 - DIDATTICA DELLA MATEMATICA
CANDELLERO ELISABETTA	60	Carico didattico	60	20410555 - ST410-STATISTICA
CAPUANO LAURA	60	Carico didattico	60	20410428 - CR510 – CRITTOSISTEMI ELLITTICI
CAPUTO PIETRO	10	Affidamento a titolo gratuito	10	20410441 - CP420-INTRODUZIONE AI PROCESSI STOCASTICI
FALCOLINI CORRADO	60	Affidamento di incarico retribuito	60	20411076 - MC430 - LABORATORIO DI DIDATTICA DELLA MATEMATICA
FEOLA ROBERTO	72	Carico didattico	72	20410876 - AM400-ISTITUZIONI DI ANALISI SUPERIORE
FERRETTI ROBERTO	60	Carico didattico	60	20410420 - AN420 - ANALISI NUMERICA 2
GIULIANI ALESSANDRO	60	Carico didattico	60	20411069 - MS411-MECCANICA STATISTICA
GUARINO STEFANO	60	Contratto di insegnamento gratuito	60	20411003 - FS520 – RETI COMPLESSE
LELLI CHIESA MARGHERITA	56	Carico didattico	56	20410618 - ME420 - FONDAMENTI E STORIA DELLA GEOMETRIA
LIVERANI MARCO	48	Esperto di alta qualificazione retribuito	48	20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA
LOMBARDI FLAVIO	144	Affidamento in convenzione	72	20410426 - IN480 - CALCOLO PARALLELO E DISTRIBUITO
		Esperto di alta qualificazione retribuito	72	20410427 - IN490 - LINGUAGGI DI PROGRAMMAZIONE
LOPEZ ANGELO	72	Carico didattico	48	20410449 - GE410 - GEOMETRIA ALGEBRICA 1
		Affidamento a titolo gratuito	72	20410449 - GE410 - GEOMETRIA ALGEBRICA 1
MAGRONE PAOLA	60	Affidamento di incarico retribuito	60	20410456 - MC420-DIDATTICA DELLA MATEMATICA
MAIELI ROBERTO	48	Carico didattico	48	20410451 - LM410 -TEOREMI SULLA LOGICA 1
MASCARENHAS MELO ANA MARGARIDA	120	Carico didattico	60	20410465 - GE450 - TOPOLOGIA ALGEBRICA
		Carico didattico	60	20410425 - GE460 - TEORIA DEI GRAFI
MATALONI SILVIA	30	Esperto di alta qualificazione retribuito	30	20410619 - ME430 - FONDAMENTI E STORIA DELL'ANALISI MATEMATICA
MEROLA FRANCESCA	72	Carico didattico	60	20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA
		Carico didattico	12	20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA
ORESTANO DOMIZIA	30	Carico didattico	30	20430000 - FS410 - LABORATORIO DI DIDATTICA DELLA FISICA
PAPPALARDI FRANCESCO	45	Affidamento a titolo gratuito	45	20410627 - TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI
PEDICINI MARCO	162	Carico didattico	48	20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ
		Affidamento a titolo gratuito	72	20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ
		Carico didattico	60	20410424 - IN450- ALGORITMI PER LA CRITTOGRAFIA
		Affidamento a titolo gratuito	30	20411002 - IN510 – QUANTUM COMPUTING
REUVERS ROBIN JOHANNES PETRUS	12	Carico didattico	12	20410420 - AN420 - ANALISI NUMERICA 2
RICCI FEDERICA	30	Carico didattico	30	20430000 - FS410 - LABORATORIO DI DIDATTICA DELLA FISICA
SCALA ANTONIO	60	Affidamento in convenzione	60	20430001 - FM540 - METODI COMPUTAZIONALI PER MODELLI STOCASTICI
SCHAFFLER LUCA	60	Carico didattico	60	20410462 - GE510 - GEOMETRIA ALGEBRICA 2
TARTARONE FRANCESCA	30	Carico didattico	30	20410617 - ME410 - ELEMENTI DI ALGEBRA SUPERIORE
TORTORA DE FALCO LORENZO	84	Carico didattico	24	20410451 - LM410 -TEOREMI SULLA LOGICA 1
		Carico didattico	60	20410613 - LM430 - LOGICA E FONDAMENTI DELLA MATEMATICA
TURCHET AMOS	132	Carico didattico	48	20410445 - AL410 - ALGEBRA COMMUTATIVA
		Affidamento a titolo gratuito	72	20410445 - AL410 - ALGEBRA COMMUTATIVA
		Carico didattico	60	20411075 - AL450 - TEORIA DELLE RAPPRESENTAZIONI
VERRA ALESSANDRO	4	Esperto di alta qualificazione (contratto gratuito, Art. 23 comma 1)	4	20410618 - ME420 - FONDAMENTI E STORIA DELLA GEOMETRIA
DOCENTE NON DEFINITO	294	Bando	60	20411067 - CR530 – POST QUANTUM CRYPTOGRAPHY
		Bando	30	20411064 - IN401 - PROGRAMMAZIONE SCIENTIFICA
		Bando	30	20411064 - IN401 - PROGRAMMAZIONE SCIENTIFICA
		Bando	24	20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA

Nominativo	Tot.Ore	Tipo incarico	Ore	Attivita didattica
		Bando	60	20430002 - IN590 - NATURAL LANGUAGE PROCESSING
		Bando	30	20410617 - ME410 - ELEMENTI DI ALGEBRA SUPERIORE
		Bando	30	20410617 - ME410 - ELEMENTI DI ALGEBRA SUPERIORE
		Bando	15	20410627 - TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI
		Bando	15	20410627 - TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI
Totale ore	**2509**			

CONTENUTI DIDATTICI

20410445 - AL410 - ALGEBRA COMMUTATIVA

Docente: TURCHET AMOS

Italiano

Prerequisiti

Conoscenze e risultati studiati nei corsi AL110 e AL210

Programma

Anelli e ideali, ideali massimali e ideali primi, nilradicale e radicale di Jacobson, spettro di un anello. Moduli, moduli finitamente generati e Lemma di Nakayama, successioni esatte, prodotto tensoriale, restrizione ed estensione degli scalari. Anelli e moduli di frazioni, localizzazione. Serie di composizione e lunghezza di un modulo. Condizioni sulle catene. Anelli Noetheriani, Teorema della Base di Hilbert. Estensioni intere, teoremi di Lying Over, Going-up. Teorema di Normalizzazione di Noether e Teorema degli zeri di Hilbert. Dimensione di Krull e Teorema dell'ideale principale di Krull. Grado di trascendenza. Dimensione di anelli Noetheriani locali. Anelli regolari.

Testi

M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1996. A. Gathmann, Commutative Algebra, Lecture notes. A. Chambert-Loir, (Mostly) Commutative Algebra, Springer Cham, 2021

Bibliografia di riferimento

M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1996. A. Gathmann, Commutative Algebra, Lecture notes. A. Chambert-Loir, (Mostly) Commutative Algebra, Springer Cham, 2021 D. Eisenbud, Commutative Algebra with a view toward Algebraic Geometry, Springer-Verlag, 1995.

Modalità erogazione

Lezioni in presenza

Modalità di valutazione

Esoneri o prova scritta su esercizi e prova orale consistente di un seminario più una parte standard su teoremi e dimostrazioni.

English

Prerequisites

Knowledge and results from the courses AL110 and AL210

Programme

Rings and ideals, maximal ideals and prime ideals, nilradical and Jacobson radical, spectrum of a ring. Modules, finitely generated modules and Nakayama's Lemma, exact sequences, tensor product, restriction and extension of scalars. Rings and modules of fractions, localization. Composition series and length of a module. Chain conditions. Noetherian rings, Hilbert's Basis Theorem. Integral extensions, Lying Over and Going-up theorems. Noether normalization theorem and Hilbert's Nullstellensatz. Krull dimension and Krull's principal ideal theorem. Transcendence degree. Dimension of local Noetherian rings. Regular rings.

Reference books

M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1996. A. Gathmann, Commutative Algebra, Lecture notes. A. Chambert-Loir, (Mostly) Commutative Algebra, Springer Cham, 2021

Reference bibliography

M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1996. A. Gathmann, Commutative Algebra, Lecture notes. A. Chambert-Loir, (Mostly) Commutative Algebra, Springer Cham, 2021 D. Eisenbud, Commutative Algebra with a view toward Algebraic Geometry, Springer-Verlag, 1995.

Study modes

In classroom lectures

Exam modes

-

20410876 - AM400-ISTITUZIONI DI ANALISI SUPERIORE

Docente: FEOLA ROBERTO

Italiano

Prerequisiti

Calcolo in una e più variabili, Teoria della misura di Lebesgue

Programma

Teoria della misura, misure esterne, costruzione di misure di Borel sui reali. Teoria dell'integrazione, teoremi di passaggio al limite, convergenza in media e in misura, integrazione sugli spazi prodotto. Misure di Radon, regolarità, funzionali lineari positivi sulle funzioni continue, Teorema di rappresentazione di Riesz. Misure con segno, teoremi di decomposizione, differenziazione di misure, funzioni a

variazione limitata, Teorema fondamentale del calcolo. Spazi Lp, proprietà di base, spazi duali, teoremi di densità. Cenni di teoria geometrica della misura.

Testi

G. Folland - "Real Analysis" - Wiley

Bibliografia di riferimento

G. Folland - "Real Analysis" - Wiley

Modalità erogazione

Lezioni frontali.

Modalità di valutazione

Esercizi assegnati a casa (tre assegnazioni in totale) e prova orale sul programma del corso.

English

Prerequisites

Calculus in one and more variables, Lebesgue measure theory

Programme

Measure theory, outer measures, construction of Borel measures. Integration theory, limit theorems, convergence in mean and in measure, integration on product spaces. Radon measures, regularity, positive linear functionals, Riesz representation theorem. Signed measures, decomposition theorems, differentiation, BV functions, fundamental theorem of calculus. Lp spaces, basic properties, dual spaces, density theorems. Introduction to geometric measure theory

Reference books

G. Folland - "Real Analysis" - Wiley

Reference bibliography

G. Folland - "Real Analysis" - Wiley

Study modes

Lectures.

Exam modes

-

20410757 - AM410 - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI

(AM410 - MODULO B - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI)

Docente: BATTAGLIA LUCA

Italiano

Prerequisiti

Programma

Testi da definire

Testi

Testi da definire

Bibliografia di riferimento

Testi da definire

Modalità erogazione

Testi da definire

Modalità di valutazione

Testi da definire

English

Prerequisites

Programme

-

Reference books

-

Reference bibliography

-

Study modes

-

Exam modes

-

20410757 - AM410 - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI

(AM410- MODULO A - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI)

Docente: BATTAGLIA LUCA

Italiano

Prerequisiti

Programma

Testi da definire

Testi

Testi da definire

Bibliografia di riferimento

Testi da definire

Modalità erogazione

Testi da definire

Modalità di valutazione

Testi da definire

English

Prerequisites

Programme

-

Reference books

-

Reference bibliography

-

Study modes

-

Exam modes

-

20410447 - CP410 - TEORIA DELLA PROBABILITÀ

Docente: CANDELLERO ELISABETTA

Italiano

Prerequisiti

E' preferibile che lo studente abbia compreso ed assimilato i contenuti principali dei corsi CP210, AM110, AM120, AM210, AM220, AM300/AM310. Non e' richiesto che tali esami siano stati verbalizzati, tuttavia nel corso verranno utilizzati strumenti introdotti in tali corsi.

Programma

Testi da definire

Testi

D. Williams, Probability with martingales R. Durrett, Probability: Theory and examples

Bibliografia di riferimento

D. Williams, Probability with martingales R. Durrett, Probability: Theory and examples

Modalità erogazione

Preferibilmente in presenza

Modalità di valutazione

La prova scritta (in alternativa, le prove in itinere) consisteranno di soli esercizi. Durata prevista: 2 ore. Per la prova orale si iniziera' con domande relative agli eventuali errori commessi nello scritto e successivamente verranno richieste alcune delle dimostrazioni dei risultati fondamentali visti in clas

English

Prerequisites

Students should have understood and be familiar with the main concepts introduced in the courses CP210, AM110, AM120, AM210, AM220, AM300/AM310. However, students are not required to have passed such exams to attend CP410.

Programme

-

Reference books

D. Williams, Probability with martingales R. Durrett, Probability: Theory and examples

Reference bibliography

D. Williams, Probability with martingales R. Durrett, Probability: Theory and examples

Study modes

Preferably in person

Exam modes

-

20410556 - CP450 - METODI PROBABILISTICI E ALGORITMI ALEATORI

Docente: Quattropani Matteo

Italiano

Prerequisiti

Un corso di probabilità elementare: - Funzioni di distribuzione/densità di variabili aleatorie - Variabili aleatorie notevoli: Bernoulliane, Binomiali, Poisson, Geoemetriche, Esponenziali, Gaussiane - Valore atteso/varianza - Legge debole dei grandi numeri

Programma

Metodi: - Metodo probabilistico (metodo del momento primo e del momento secondo, lemma locale di Lovasz) - Stime di concentrazione (es. disuguaglianze di Chernoff, Hoeffding, Bernstein, Azuma, McDiarmid) - Pairwise independence - Martingale (introduzione, cf. CP410) - Catene di Markov (introduzione, cf. CP420) Modelli ed esempi: - Algoritmi aleatori e analisi del caso medio (es. quicksort, routing su reti sparse, Johnson-Linderstrauss, balls-into-bins, funzioni di Hashing, Prophet/Secretary inequalities, randomized rounding, stochastic bandits) - Grafi aleatori (es. Erdos-Reyni e preferential attachment) - Passeggiate aleatorie su grafi (es. PageRank, cover times, algoritmo di Wilson) - Sistemi stocastici multi-agente (es. contact process, voter model)

Testi

Le lezioni saranno tratte principalmente da questi testi: - Michael Mitzenmacher e Eli Upfal, Probability and computing: randomized algorithm and probabilistic analysis - Noga Alon e Joel Spencer, The probabilistic method - Sebastién Roch, Modern discrete probability: an essential toolkit Alla fine di ogni lezione saranno condivisi con gli studenti gli appunti relativi

Bibliografia di riferimento

Altri libri di riferimento: - David Levin e Yuval Peres, Markov chains and mixing times - Rajev Motwani e Prabhakar Raghavan, Randomized algorithms - Devdatt Dubhashi e Alessandro Panconesi, Concetration of measure for the analysis of randomized algorithms

Modalità erogazione

Le lezioni saranno di tipo frontale, alla lavagna. Le lezioni verranno trasmesse in streaming e registrate per consentire agli/alle studenti lavoratori/lavoratrici di poterne usufruire in differita.

Modalità di valutazione

L'esame orale verterà sugli argomenti presentati a lezione.

English

Prerequisites

An elementary probability course: - Distribution/density functions of random variables - Notable random variables: Bernoulli, Binomial, Poisson, Geometric, Exponential, Gaussian - Expected value / variance - Weak law of large numbers

Programme

Methods: - Probabilistic method (first moment method, second moment method, Lovász Local Lemma) - Concentration bounds (e.g., Chernoff, Hoeffding, Bernstein, Azuma, McDiarmid inequalities) - Pairwise independence - Martingales (introduction, cf. CP410) - Markov chains (introduction, cf. CP420) Models and examples: - Randomized algorithms and average-case analysis (e.g., quicksort, routing on sparse networks, Johnson–Lindenstrauss, balls-into-bins, hashing functions, Prophet/Secretary inequalities, randomized rounding, stochastic bandits) - Random graphs (e.g., Erd#s–Rényi and preferential attachment) - Random walks on graphs (e.g., PageRank, cover times, Wilson’s algorithm) - Stochastic multi-agent systems (e.g., contact process, voter model)

Reference books

The lectures will be based primarily on the following books: - Michael Mitzenmacher e Eli Upfal, Probability and computing: randomized algorithm and probabilistic analysis - Noga Alon e Joel Spencer, The probabilistic method - Sebastién Roch, Modern discrete probability: an essential toolkit At the end of each lecture, the corresponding notes will be shared with the students.

Reference bibliography

Other reference books: - David Levin e Yuval Peres, Markov chains and mixing times - Rajev Motwani e Prabhakar Raghavan, Randomized algorithms - Devdatt Dubhashi e Alessandro Panconesi, Concetration of measure for the analysis of randomized algorithms

Study modes

Lectures will be traditional, board-based. They will be streamed live and recorded so that working students can access them asynchronously.

Exam modes

-

20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA

(CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO A)

Docente: MEROLA FRANCESCA

Italiano

Prerequisiti

Conoscenze di base di algebra.

Programma

Introduzione alla crittografia. Cenni storici. Definizione di crittosistema. Cifrari classici. Introduzione alla crittoanalisi. Introduzione alla crittografia a chiave pubblica. Il crittosistema RSA. Test di primalità. Algoritmi di fattorizzazione. Alcuni attacchi all'RSA. Il problema del logaritmo discreto. Scambio della chiave di Diffie-Hellman. Il crittosistema di Elgamal. il crittosistema di Massey-Omura. Firma digitale. Cenni su alcuni protocolli crittografici.

Testi

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Bibliografia di riferimento

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Modalità erogazione

lezioni in presenza: ci sarà anche probabilmente la possibilità di seguire online

Modalità di valutazione

prova scritta: di norma 4 esercizi teorico/pratici, durata di norma 2 ore e 30. prova orale: facoltativa per una votazione <=26

English

Prerequisites

Basic knowledge of algebra.

Programme

Introduction to cryptography. Classic ciphers. Introduction to cryptanalysis. Introduction to public-key cryptography. The RSA cryptosystem. Primality tests. Factorization algorithms. Some attacks on the RSA. The discrete logarithm problem. Diffie-Hellman key exchange. Elgamal cryptosystem. Massey-Omura cryptosystem. Digital signatures. Overview of some cryptographic protocols.

Reference books

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Reference bibliography

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Study modes

In-person classes: there will also probably be the possibility of attending online

Exam modes

-

20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA

(CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO B)

Docente: MEROLA FRANCESCA

Italiano

Prerequisiti

Conoscenze di base di algebra.

Programma

Argomenti avanzati di crittografia.Fra le possibilità: Protocolli, firme, crittografia PostQuantum.

Testi

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Bibliografia di riferimento

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Modalità erogazione

lezioni in presenza: ci sarà anche probabilmente la possibilità di seguire online

Modalità di valutazione

prova scritta: di norma 4 esercizi teorico/pratici, durata di norma 2 ore e 30. prova orale: facoltativa per una votazione <=26

English

Prerequisites

Basic knowledge of algebra.

Programme

Advanced topics in cryptography. Amongst the possibilities: Protocols, Digital signatures, PostQuantum Cryptography

Reference books

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Reference bibliography

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Study modes

In-person classes: there will also probably be the possibility of attending online

Exam modes

-

20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ

Docente: PEDICINI MARCO

Italiano

Prerequisiti

Non ci sono prerequisiti.

Programma

1) Computabilità, complessità e rappresentabilità: - Introduzione ai problemi di decisione, procedure algoritmiche e non algoritmiche, computazioni deterministiche, procedure discrete, nozione di alfabeto, di parola. Decidibilità e semidecidibilità di un insieme. Computazioni deterministiche, finitarie e discrete. Algoritmi formali: definizione formale di algoritmo, configurazioni di input, di output, funzione di transizione. Esempio di formalizzazione di un algoritmo. Decidibilità per automa finito. Rappresentazione degli automi mediante matrici. Monoide libero delle parole. Semianelli formali. Automi Finiti Non-deterministici. Linguaggi Regolari. Equivalenza tra automi deterministici e quelli non-deterministici. - Macchine di Turing: definizione, decidibilità per macchina di Turing, tempo di arresto, spazio di arresto. Costo della computazione. Complessità: caso peggiore e caso medio. Indipendenza del tempo di decisione da un numero finito di configurazioni di input. Funzioni di complessità, classi di complessità DTIME e DSPACE (deterministic time e space). Inclusione DTIME(T (n)) # DSPACE(T(n)) # DTIME(2^{cT(n)}). Pumping Lemma per gli insiemi decidibili in tempo lineare. Simulazione di algoritmi, simulazione della macchina di Turing a seminastro, simulazione di una macchina multinastro. Macchine di Turing speciali. Teorema di Speedup lineare per macchine di Turing con alfabeto esteso. Valutazione del coefficente di accelerazione in relazione agli alfabeti. Decidibilità di insiemi di numeri naturali. Indipendenza dalla rappresentazione. Considerazioni sulla complessità. - Turing calcolabilità: definizione di funzione Turing calcolabile, funzioni caratteristiche di insiemi Turing decidibili, la classe delle funzioni Turing calcolabili è chiusa per composizione, coppia, ricorsione primitiva e minimizzazione. Esempi di funzioni Turing calcolabili. Funzioni Ricorsive: equivalenza tra Turing computabilità e funzioni ricorsive. Funzione di Ackermann ([1] capp. 1,2,3,4,5 e [4] cap. 1). - Funzioni costruibili in tempo. Nozione di T-orologio. Esempi di alcune funzioni costruibili in tempo. Chiusura per composizione. - Macchine di Turing non-deterministiche: caratterizzazione mediante la decidibilità di insiemi proiezione. Definizione della classe delle funzioni non-deterministiche polinomiali. Problemi NP-completi. 2) Lambda calcolo e programmazione funzionale: - Programmazione dichiarativa: cenni storici sul lambda calcolo, definizioni di base, i termini del lambda calcolo, la sostituzione semplice. Relazioni sui lambda termini. Congruenze, passaggio al contesto. #-equivalenza. L'#-equivalenza passa al contesto. Chiusura transitiva di una relazione, proprietà di Church-Rosser. Quozientamento dei lambda-termini rispetto all'alpha equivalenza. - Definizione di beta-redesso e di beta-riduzione. Teorema di Church-Rosser per la beta-riduzione. Forme normali per beta-riduzione. Strategie di beta-riduzione. Strategia normalizzante: riduzione di sinistra (left most-outer most). Riduzione di testa. Termini Risolubili. Forme Normali di Testa. Teorema di caratterizzazione della risolubilità. - Rappresentazione delle funzioni ricorsive: teorema di lambda definibilità. Esistenza del punto fisso per il lambda termini. Punto Fisso di Church ed punto fisso di Curry. - Rappresentazione di altri tipi di dato nel lambda-calcolo: coppie, liste, alberi, soluzione di equazioni ricorsive su lambda-termini ([2] capp. 1, 2, 5).

Testi

[1] DEHORNOY, P., COMPLEXITÈ ET DECIDABILITÈ. SPRINGER-VERLAG, (1993). [2] KRIVINE, J.-L., LAMBDA CALCULUS: TYPES AND MODELS. #ELLIS HORWOOD, (1993). [3] SIPSER,M., INTRODUCTION TO THE THEORY OF COMPUTATION.THOMSON COURSE TECHNOLOGY, (2006).

Bibliografia di riferimento

G. Lolli, Hilbert e la logica, Le Matematiche, [S.l.], v. 55, n. 3, p. 93-126, mar. 2005. ISSN 2037-5298. Dexter C. Kozen, Theory of Computation, Springer-Verlag (2006). G. Ausiello, G. Gambosi, F. d'Amore Linguaggi, Modelli, Complessità Aho, Hopcroft, Ullman, Design and Analysis of Computer Programming. A. Bernasconi, B. Codenotti, Introduzione alla complessità computazionale, Springer-Verlag. H. Hermes, Enumerability, Decidability, Computability, Die Grundlehren der Mathematichen Wissenshaften in Einzeldarstellungen, n. 127, Springer-Verlag. F. Cardone and J. R. Hindley, History of Lambda-calculus and Combinatory Logic, from Swansea University Mathematics Department Research Report No. MRRS-05-06.

Modalità erogazione

Lezione frontale in aula.

Modalità di valutazione

L'esame consiste di due parti: un esame scritto, sostituibile con due prove in itinere (il voto finale viene calcolato pesando la prima prova al 35% e la seconda al 65%) e una prova orale opzionale, prevista per supplire alle insufficienze lievi (a partire dal 15, compreso) o per migliorare il voto ottenuto allo scritto.

English

Prerequisites

There is no required background.

Programme

1) Computability, complexity and representability: - Introduction to decision problems, algorithmic and non-algorithmic procedures, deterministic computations, discrete procedures, the notion of alphabet, of speech. Decidability and semi-decidability of a set. Deterministic, finitary and discrete computations. Formal algorithms: formal definition of algorithm, configurations of input, output, transition function. Example of formalization of an algorithm. Decidability for finished automata. Representation of the automata by matrices. Free Monoid of words. Formal semi-rings. Non-deterministic finite automata. Regular Languages. Equivalence between deterministic and non-deterministic automata. - Turing machines: definition, decidability for Turing machine, stopping time, stopping space. Cost of computation. Complexity: worst-case and average case. Independence of decision time from a finite number of input configurations. Complexity functions, complexity classes DTIME and DSPACE (deterministic time and space). Inclusion DTIME (T (n)) # DSPACE (T (n)) # DTIME (2 ^ {cT (n)}). Pumping Lemma. Simulation of algorithms, simulation of the half tape Turing machine, simulation of a multi-tape machine. Special Turing machines. Linear Speedup theorem for Turing machines with an extended alphabet. Evaluation of acceleration coefficient in relation to alphabets. Decisions of natural number sets. Independence from representation. Considerations concerning complexity. - Turing computability: definition of Turing computable function, characteristic functions of Turing decidable sets, the class of Turing computable functions is closed by composition, concatenation, primitive recursion and minimization. Examples of Turing computable functions. Recursive Functions: equivalence between Turing computability and recursive functions. Ackermann function ([1] chapter 1,2,3,4,5 and [4] chapter 1). - Time-constructible functions. The notion of T-clock. Examples of some time constructible function. Closure by composition. - Non-deterministic Turing machines: characterization through the decidability of projection sets. Definition of the class of polynomial non-deterministic functions. NP-complete problems. 2) Lambda calculus and functional programming: - Declarative programming: a historical outline on the lambda calculus, basic definitions, the terms of the lambda calculus, the simple substitution. Relations on the lambda terms. Congruences, transition to the context. #-equivalence. alpha-equivalence passes to the context. The transitive closure of a relationship, owned by Church-Rosser. Listing of lambda-terms concerning alpha-equivalence. - Definition of beta-reduction and beta-equivalence. Church-Rosser's theorem for beta-reduction. Normal forms for beta-reduction. Beta-reduction strategies. Normalizing strategy: left reduction (left most-outer most). Head reduction. Soluble Terms. Head Normal Forms. Solvability characterization theorem. - Representation of the recursive functions: lambda definability theorem. Existence of the fixed point for the lambda terms. Church Fixed Point and Curry fixed point. - Representation of other data types in the lambda-calculus: pairs, lists, trees, the solution of recursive equations on lambda-terms ([2] chapters 1, 2, 5).

Reference books

[1] DEHORNOY, P., COMPLEXITÈ ET DECIDABILITÈ. SPRINGER-VERLAG, (1993). [2] KRIVINE, J.-L., LAMBDA CALCULUS: TYPES AND MODELS. #ELLIS HORWOOD, (1993). [3] SIPSER,M., INTRODUCTION TO THE THEORY OF COMPUTATION.THOMSON COURSE TECHNOLOGY, (2006).

Reference bibliography

G. Lolli, Hilbert e la logica, Le Matematiche, [S.l.], v. 55, n. 3, p. 93-126, mar. 2005. ISSN 2037-5298. Dexter C. Kozen, Theory of Computation, Springer-Verlag (2006). G. Ausiello, G. Gambosi, F. d'Amore Linguaggi, Modelli, Complessità Aho, Hopcroft, Ullman, Design and Analysis of Computer Programming. A. Bernasconi, B. Codenotti, Introduzione alla complessità computazionale, Springer-Verlag. H. Hermes, Enumerability, Decidability, Computability, Die Grundlehren der Mathematichen Wissenshaften in Einzeldarstellungen, n. 127, Springer-Verlag. F. Cardone and J. R. Hindley, History of Lambda-calculus and Combinatory Logic, from Swansea University Mathematics Department Research Report No. MRRS-05-06.

Study modes

Lectures.

Exam modes

-

20410442 - IN420 - TEORIA DELL'INFORMAZIONE

Docente: BONIFACI VINCENZO

Italiano

Prerequisiti

Elementi di probabilità discreta. [CP210 Introduzione alla Probabilità]

Programma

1. Introduzione alla teoria dell'informazione Trasmissione affidabile dell'informazione. Contenuto informativo secondo Shannon. Misure di informazione. Entropia, mutua informazione, divergenza informazionale. Compressione dati. Correzione d'errore. Teoremi di elaborazione dei dati. Disuguaglianze fondamentali. Diagrammi d'informazione. Divergenza informazionale e massima verosimiglianza. 2. Codifica di sorgente e compressione dati Sequenze tipiche. Tipicità in probabilità. Proprietà di equipartizione asintotica. Codifica a blocco e a lunghezza variabile. Tasso di codifica. Teorema della codifica di sorgente. Compressione dati senza perdita. Codice di Huffman. Codici universali. Compressione Ziv-Lempel. 3. Codifica di canale Capacità di canale. Canali discreti senza memoria. Informazione trasportata da un canale. Criteri di decodifica. Teorema della codifica di canale con rumore. 4. Ulteriori codici ed applicazioni Spazio di Hamming. Codici lineari. Matrice generatrice e matrice di controllo. Codici ciclici. Codici hash.

Testi

F. Fabris. Teoria dell'informazione, codici, cifrari. Bollati Boringhieri, 2001.

Bibliografia di riferimento

T.M. Cover, J.A. Thomas. Elements of Information Theory. Wiley, 1991.
 V. Guruswamy, A. Rudra, M. Sudan. Essential Coding Theory. Bozza disponibile online, 2019.
 R.E. Blahut. Algebraic Codes for Data Transmission. Cambridge University Press, 2003.
 D.J.C. MacKay. Information Theory, Inference and Learning Algorithms. Cambridge University Press, 2004.

Modalità erogazione

Lezioni frontali con esercitazioni frontali.

Modalità di valutazione

Esame orale.

English

Prerequisites

Elements of discrete probability. [CP210 Introduzione alla Probabilità]

Programme

1. Introduction to information theory. Reliable transmission of information. Shannon's information content. Measures of information. Entropy, mutual information, informational divergence. Data compression. Error correction. Data processing theorems. Fundamental inequalities. Information diagrams. Informational divergence and maximum likelihood. 2. Source coding and data compression Typical sequences. Typicality in probability. Asymptotic equipartitioning property. Block codes and variable length codes. Coding rate. Source coding theorem. Lossless data compression. Huffman code. Universal codes. Ziv-Lempel compression. 3. Channel coding Channel capacity. Discrete memoryless channels. Information transmitted over a channel. Decoding criteria. Noisy channel coding theorem. 4. Further codes and applications Hamming space. Linear codes. Generating matrix and check matrix. Cyclic codes. Hash codes.

Reference books

T.M. Cover, J.A. Thomas. Elements of Information Theory. Wiley, 1991.
 R.E. Blahut. Algebraic Codes for Data Transmission. Cambridge University Press, 2003.

Reference bibliography

T.M. Cover, J.A. Thomas. Elements of Information Theory. Wiley, 1991.
 V. Guruswamy, A. Rudra, M. Sudan. Essential Coding Theory. Online draft, 2019.
 R.E. Blahut. Algebraic Codes for Data Transmission. Cambridge University Press, 2003.
 D.J.C. MacKay. Information Theory, Inference and Learning Algorithms. Cambridge University Press, 2004.

Study modes

Frontal lectures with recitations.

Exam modes

-

20410424 - IN450- ALGORITMI PER LA CRITTOGRAFIA

Docente: PEDICINI MARCO

Italiano

Prerequisiti

Nozioni elementari di teoria dei numeri, probabilità discreta ed algebra lineare, programmazione di base.

Programma

1. Crittografia Classica - Crittosistemi di base: cifratura per sostituzione, per traslazione, per permutazione, affine, di Vigenère, di Hill. Cifratura a flusso (sincrona e asincrona), Linear feedback shift registers (LFSR) su campi finiti, Cifrario autokey. Cifrari prodotto. Crittoanalisi di base: classificazione degli attacchi; crittoanalisi per i cifrari affini, per la cifratura a sostituzione (analisi delle frequenze), per la cifratura di Vigenere: Kasiski test, indice di coincidenza; crittoanalisi del cifrario di Hill e degli LFSR: attacchi algebrici, cube attack. 2. Applicazione della Teoria di Shannon alla crittografia - Sicurezza dei cifrari: sicurezza computazionale, sicurezza dimostrabile, sicurezza incondizionata. Richiami di calcolo delle probabilità: variabili aleatorie discrete, probabilita congiunta, probabilita condizionata, variabili aleatorie indipendenti, Teorema di Bayes. Variabili aleatorie associate a crittosistemi. Sistemi di cifratura a sicurezza perfetta. Crittosistema di Vernam. Entropia. Codici di Huffman. Spurious Keys e Unicity distance. 3. Cifrari a blocchi - Schemi di cifratura iterativi;

Reti di Sostituzione-Permutazione (SPN); Crittoanalisi lineare per SPN: Piling-Up Lemma, approssimazione lineare di S- boxes, attacchi lineari a S-boxes; Crittoanalisi differenziale per SPN; Cifrari di tipo Feistel; DES: descrizione e analisi; AES: descrizione; Cenni sui campi finiti: operazioni su campi finiti, algoritmo di Euclide generalizzato per il calcolo del mcd e degli inversi; Modi operativi per i cifrari a blocchi. 4. Funzioni Hash e Codici per l'autenticazione di messaggi - Funzioni di hash e integrità dei dati. Funzioni di hash sicure: resistenza alla controimmagine, resistenza alla seconda controimmagine, resistenza alla collisione. Il modello dell'oracolo random: funzioni di hash ideali, proprietà di indipendenza. Algoritmi randomizzati, collisione sul problema della seconda controimmagine, collisione sul problema della controimmagine. Funzioni di hash iterate; la costruzione di Merkle-Damgard. Algoritmo di Hash Sicuro (SHA-1). Codici di Autenticazione (MAC): codici di autenticazione nidificati (HMAC).

Testi

[1] Antoine Joux, Algorithmic Cryptanalysis, (2010) CRC Press. [2] Douglas Stinson, Cryptography: Theory and Practice, 3rd edition, (2006) Chapman and Hall/CRC. [3] Delfs H., Knebl H., Introduction to Cryptography, (2007) Springer Verlag.

Bibliografia di riferimento

[-] Serge Vaudenay, A Classical Introduction to Cryptography, Applications for Communications Security (2006) Springer-Verlag. [-] Th. Baigneres, P. Junod, Y. Lu, J. Monnerat, S. Vaudenay A Classical Introduction to Cryptography Exercise Book Springer Verlag (2006). [-] S. Mangano, Mathematica Cookbook ISBN: 9789863470106 Publisher: O'Reilly (2014). [-] Schneier, Applied Cryptography (2006) Chapman and Hall/CRC. [-] Katz, Lindell, Introduction to Modern Cryptography (2006) Chapman and Hall/CRC. [-] Rudolf Lidl, Harald Niederreiter, Finite Fields, 2nd edition, In Encyclopedia of Mathematics and its Applications, (2007) Cambridge University Press.

Modalità erogazione

Lezioni in aula e sessioni di programmazione al laboratorio informatico.

Modalità di valutazione

Esame scritto e valutazione del progetto di programmazione.

English

Prerequisites

Basic number theory, basic discrete probability theory, basic linear algebra, basic computer programming.

Programme

1. Classic Cryptography - Basic cryptosystems: encryption by substitution, by translation, by permutation, affine cryptosystem, by Vigenère, by Hill. Stream encryption (synchronous and asynchronous), Linear feedback shift registers (LFSR) on finite fields, Autokey cypher. Product cyphers. Basic cryptanalysis: classification of attacks; cryptoanalysis for affine cyphers, for substitution cypher (frequency analysis), for Vigenere cypher: Kasiski test, coincidence index; cryptoanalysis of Hill's cypher and LFSR: algebraic attacks, cube attack. 2. Application of Shannon theory to cryptography - Security of cyphers: computational security, provable security, unconditional security. Basics of probability: discrete random variables, joint probability, conditional probability, independent random variables, Bayes' theorem. Random variables associated with cryptosystems. Perfect secrecy for encryption systems. Vernam cryptosystem. Entropy. Huffman codes. Spurious Keys and Unicity distance. 3. Block cyphers - iterative encryption schemes; Substitution-Permutation Networks (SPN); Linear cryptanalysis for SPN: Piling-Up Lemma, linear approximation of S-boxes, linear attacks on S-boxes; Differential cryptanalysis for SPN; Feistel cyphers; DES: description and analysis; AES: description; Notes on finite fields: operations on finite fields, Euclid's generalized algorithm for the computation of the GCD and inverse; Operating modes for block cyphers. 4. Hash functions and codes for message authentication - Hash functions and data integrity. Safe hash functions: resistance to the pre-image, resistance to the second pre-image, collision resistance. The random oracle model: ideal hash functions, properties of independence. Randomized algorithms, collision on the problem of the second pre-image, collision on the problem of the pre-image. Iterated hash functions; the construction of Merkle-Damgard. Safe Hash Algorithm (SHA-1). Authentication Codes (MAC): nested authentication codes (HMAC).

Reference books

[1] Antoine Joux, Algorithmic Cryptanalysis, (2010) CRC Press. [2] Douglas Stinson, Cryptography: Theory and Practice, 3rd edition, (2006) Chapman and Hall/CRC. [3] Delfs H., Knebl H., Introduction to Cryptography, (2007) Springer Verlag.

Reference bibliography

[-] Serge Vaudenay, A Classical Introduction to Cryptography, Applications for Communications Security (2006) Springer-Verlag. [-] Th. Baigneres, P. Junod, Y. Lu, J. Monnerat, S. Vaudenay A Classical Introduction to Cryptography Exercise Book Springer Verlag (2006). [-] S. Mangano, Mathematica Cookbook ISBN: 9789863470106 Publisher: O'Reilly (2014). [-] Schneier, Applied Cryptography (2006) Chapman and Hall/CRC. [-] Katz, Lindell, Introduction to Modern Cryptography (2006) Chapman and Hall/CRC. [-] Rudolf Lidl, Harald Niederreiter, Finite Fields, 2nd edition, In Encyclopedia of Mathematics and its Applications, (2007) Cambridge University Press.

Study modes

Lectures and programming sessions in the computer laboratory.

Exam modes

-

20411002 - IN510 – QUANTUM COMPUTING

(IN510 – QUANTUM COMPUTING MODULO A)

Docente: DI BATTISTA GIUSEPPE

Italiano

Prerequisiti

Non ci sono particolari prerequisiti.

Programma

Qubit, coppie di qubit, registri, porte logiche con uno o piu' qubit, no cloning theorem, l'operatore di Hadamard, teletrasporto, computazioni reversibili, l'algoritmo di Bernstein Vazirani, l'algoritmo di Shor, amplitude amplification e l'algoritmo di Groover, teoria della complessità e quantum computing

Testi

Slides del docente.

Bibliografia di riferimento

I testi consigliati (per sola consultazione) sono: E. G. Rieffel, W. H. Polak Quantum Computing: a Gentle Introduction MIT Press N. S. Yanofsky, M. A. Mannucci Quantum Computing for Computer Scientists Cambridge

Modalità erogazione

Lezioni in aula.

Modalità di valutazione

Scritto di circa un'ora.

English

Prerequisites

None.

Programme

Qubit, pairs of qubits, registries, logic functions, no cloning theorem, Hadamard operator, teleportation, reversible computations, Bernstein Vazirani algorithm, Shor algorithm, amplitude amplification and the Groover algorithm, complexity theory and quantum computing

Reference books

Slides by the teacher.

Reference bibliography

The recommended texts (for consultation only) are: E. G. Rieffel, W. H. Polak Quantum Computing: a Gentle Introduction MIT Press N. S. Yanofsky, M. A. Mannucci Quantum Computing for Computer Scientists Cambridge

Study modes

Lecture in class.

Exam modes

-

20411002 - IN510 – QUANTUM COMPUTING

(IN510 – QUANTUM COMPUTING MODULO B)

Docente: PEDICINI MARCO

Italiano

Prerequisiti

Algebra Lineare. Calcolabilità e Complessità.

Programma

Elementi di Algebra Lineare: Spazi di Hilbert, Prodotti e prodotti tensore, matrici, spazi complessi e prodotto scalare, grafi, somma dei cammini nel grafo. Funzioni booleane, quantum bits e fattibilità computazionale. Matrici speciali: Hadamard Matrices, Fourier Matrices, Computazioni reversibili e matrici di permutazione, matrici diagonali, riflessioni. Vettori di inizializzazione, controllo e copia di stati di base. Algoritmi: Phil Algorithm, Deutsch’s Algorithm, Superdense Coding and Teleportation. The Deutsch-Jozsa Algorithm. Simon’s Algorithm. Shor’s Algorithm, Quantum Part of the Algorithm, Analysis of the Quantum Part, Continued Fractions. FactoringIntegers: Basic Number Theory, Periods Give the Order, Factoring. Grover’s Algorithm: The binary case, the general case, with k Unknowns, Grover Approximate Counting.

Testi

Richard J. Lipton, Kenneth W. Regan Introduction to Quantum Algorithms via Linear Algebra, Second Edition, ISBN 9780262045254, (2021), MIT Press

Bibliografia di riferimento

Testi da definire

Modalità erogazione

Corso di Letture.

Modalità di valutazione

L'esame consiste nella presentazione di un seminario su un tema da concordare con il docente.

English

Prerequisites

Linear Algebra. Computability and Complexity

Programme

Basic Linear Algebra: Hilbert Spaces, Products and Tensor Products, Matrices, Complex Spaces and Inner Products, Matrices, Graphs, and Sums Over Paths. Boolean Functions, Quantum Bits, and Feasibility: Feasible Boolean Functions, Quantum Representation of Boolean Arguments Quantum Feasibility. Special Matrices: Hadamard Matrices, Fourier Matrices, Reversible Computation and Permutation Matrices, Feasible Diagonal Matrices, Reflections. Tricks: Start Vectors, Controlling and Copying Base States, The Copy-Uncompute Trick, Superposition Tricks, Flipping a Switch, Measurement Tricks, Partial Transforms. Algorithms: Phil's Algorithm: Phil Measures Up, Quantum Mazes versus Circuits versus Matrices. Deutsch's Algorithm: Superdense Coding and Teleportation. The Deutsch-Jozsa Algorithm. Simon's Algorithm. Shor's Algorithm, Quantum Part of the Algorithm, Analysis of the Quantum Part, Continued Fractions. FactoringIntegers: Basic Number Theory, Periods Give the Order, Factoring. Grover's Algorithm: The binary case, the general case, with k Unknowns, Grover Approximate Counting.

Reference books

Richard J. Lipton, Kenneth W. Regan Introduction to Quantum Algorithms via Linear Algebra, Second Edition, ISBN 9780262045254, (2021), MIT Press

Reference bibliography

-

Study modes

Lectures.

Exam modes

-

20410432 - IN550 – MACHINE LEARNING

Docente: BONIFACI VINCENZO

Italiano

Prerequisiti

Conoscenza del linguaggio di programmazione Python. [IN400a Programmazione in Python] Elementi di probabilità discreta, algebra lineare ed analisi matematica.

Programma

1. Apprendimento automatico. Tipi di apprendimento. Funzioni di costo. Minimizzazione del rischio empirico. Generalizzazione ed overfitting. 2. Ottimizzazione di modelli. Funzioni convesse. Discesa del gradiente. Discesa stocastica del gradiente. 3. Regressione. Regressione lineare. Basi di funzioni. Selezione dei predittori. Regolarizzazione. 4. Classificazione. Modelli generativi. Nearest neighbor. Regressione logistica. Support vector machines. Reti neurali. 5. Combinazione di modelli. Alberi di decisione. Boosting. Bagging. 6. Apprendimento non supervisionato. Clustering K-means. Clustering gerarchico. Analisi delle componenti principali. 7. Applicazione dei metodi nel linguaggio di programmazione Python. Esempi d'uso delle librerie NumPy, Pandas, SciKit-Learn, e PyTorch.

Testi

J. Watt, R. Borhani, A. Katsaggelos. Machine Learning Refined. Cambridge University Press, 2nd edition, 2020.

Bibliografia di riferimento

A. Géron. Hands-On Machine Learning with SciKit-Learn, Keras, and Tensorflow. O'Reilly, 3rd edition, 2022.
 M. Mohri, A. Rostamizadeh, A. Talwalkar. Foundations of Machine Learning. MIT Press, 2nd edition, 2018.
 S. Shalev-Shwartz, S. Ben-David. Understanding Machine Learning. Cambridge University Press, 2014.
 G. James, D. Witten, T. Hastie, R. Tibshirani. Introduzione all'apprendimento statistico. Piccin, 2020.
 K.P. Murphy. Probabilistic Machine Learning. MIT Press, 2022.
 T. Hastie, R. Tibshirani, J. Friedman. Gli elementi dell'apprendimento statistico. Piccin, 2025.
 C.M. Bishop. Pattern Recognition and Machine Learning. Springer, 2006.

Modalità erogazione

Lezioni teoriche frontali ed esercitazioni di laboratorio nel linguaggio di programmazione Python. Per il diario delle lezioni si consulti il sito web del docente: http://ricerca.mat.uniroma3.it/users/vbonifaci/in550.html Le lezioni saranno in presenza e verranno anche trasmesse e registrate.

Modalità di valutazione

L'esame si compone di due parti: un progetto software ed un esame orale. Nella parte di progetto software, gli studenti identificheranno ed analizzeranno un dataset utilizzando le metodologie presentate durante le lezioni, preparando un quaderno Python interattivo (Jupyter) ed una presentazione. L'esame orale consisterà, oltre che nella discussione del progetto, in domande su tutto il programma del corso.

English

Prerequisites

Knowledge of the Python programming language. [IN400a Programmazione in Python] Elements of discrete probability, linear algebra and real analysis.

Programme

1. Machine learning. Types of learning. Loss functions. Empirical risk minimization. Generalization and overfitting. 2. Model optimization. Convex functions. Gradient descent. Stochastic gradient descent. 3. Regression. Linear regression. Basis functions. Feature selection. Regularization. 4. Classification. Generative models. Nearest neighbor. Logistic regression. Support vector machines. Neural networks. 5. Ensemble methods. Decision trees. Boosting. Bagging. 6. Unsupervised learning. K-means clustering. Hierarchical clustering. Principal component analysis. 7. Application of the methods using the Python language. Examples using the NumPy, Pandas, SciKit-Learn, and PyTorch libraries.

Reference books

J. Watt, R. Borhani, A. Katsaggelos. Machine Learning Refined. Cambridge University Press, 2nd edition, 2020.

Reference bibliography

A. Géron. Hands-On Machine Learning with SciKit-Learn, Keras, and Tensorflow. O'Reilly, 3rd edition, 2022.
 M. Mohri, A. Rostamizadeh, A. Talwalkar. Foundations of Machine Learning. MIT Press, 2nd edition, 2018.
 S. Shalev-Shwartz, S. Ben-David. Understanding Machine Learning. Cambridge University Press, 2014.
 G. James, D. Witten, T. Hastie, R. Tibshirani. An Introduction to Statistical Learning. Springer, 2nd edition, 2013.
 K.P. Murphy. Probabilistic Machine Learning. MIT Press, 2022.
 T. Hastie, R. Tibshirani, J. Friedman. The Elements of Statistical Learning. Springer, 2nd edition, 2008.
 C.M. Bishop. Pattern Recognition and Machine Learning. Springer, 2006.

Study modes

Frontal theoretical lectures and programming labs based on the Python programming language. For the class diary see the teacher's webpage: http://ricerca.mat.uniroma3.it/users/vbonifaci/in550.html The lectures will be in presence, and at the same time they will be streamed and recorded.

Exam modes

-

20410451 - LM410 -TEOREMI SULLA LOGICA 1

(LM410 -TEOREMI SULLA LOGICA 1 - MODULO A)

Docente: MAIELI ROBERTO

Italiano

Prerequisiti

nessun requisito specifico

Programma

Parte 1: Alcune nozioni preliminari. Relazioni d'ordine e alberi, definizioni induttive, dimostrazioni per induzione, assioma di scelta e lemma di K#nig. Parte 2: Dimostrabilità e soddisfacibilità Linguaggio formale del primo ordine: alfabeto, termini , formule, sequenti. Strutture per un linguaggio del primo ordine: strutture, termini e formule a parametri in una struttura, valutazione di termini, formule e sequenti. Calcolo dei sequenti per la logica del primo ordine: il calcolo dei sequenti LK di Gentzen. Sequenti derivabili e derivazioni. Correttezza delle regole di LK. Analisi canonica e teorema fondamentale: costruzione dellanalisi canonica (con e senza tagli) e dimostrazione del teorema fondamentale dellanalisi canonica. Conseguenze del teorema fondamentale dell'analisi canocica: teoremi di completezza, eliminabilit del taglio, compattezza, L"owenheim-Skolem. Parte 3: Verso la teoria della dimostrazione: il teorema di eliminazione del taglio. La procedura di eliminazione del taglio. Definizione dei passi elementari di eliminazione del taglio. Prima strategia dimostrativa (riduzione a grandi passi). Seconda strategia dimostrativa (rovesciamento delle derivazioni). Cenni sulla complessit\`a della procedura di eliminazione del taglio. Qualche conseguenza immediata del teorema di eliminazione del taglio.

Testi

V. Michele Abrusci e Lorenzo Tortora de Falco, Logica. Vol. 1 Dimostrazioni e modelli al primo ordine, Springer, 2014
https://sites.google.com/view/lm410/home

Bibliografia di riferimento

V. Michele Abrusci e Lorenzo Tortora de Falco, Logica. Vol. 1 Dimostrazioni e modelli al primo ordine, Springer, 2014
https://sites.google.com/view/lm410/home

Modalità erogazione

Il corso prevede Didattica frontale; Discussioni con gli studenti e dibattiti sugli argomenti trattati; Esercitazioni; La frequenza non è obbligatoria ma è vivamente raccomandata. Nel caso di un prolungamento dell’emergenza sanitaria da COVID-19 verranno valutate le modalità di svolgimento delle attività didattiche. Si cercherà di limitare l’inevitabile danno agli studenti dovuto ad un’eventuale necessità di tenere il corso a distanza preservando, per quanto possibile, l’interattività durante le lezioni. E' presvisto lo streaming sincrono delle lezioni senza registrazione delle lezioni svolte in aula.

Modalità di valutazione

Esame scritto e/o orale, di durata variabile, in media tra 45 e 60 minuti. Nel caso di misure restrittive dovute alla emergenza sanitaria da COVID-19 verranno valutate le modalità di svolgimento degli esami. Si cercherà di limitare l’inevitabile danno agli studenti dovuto ad un’eventuale necessità di tenere gli esami a distanza.

English

Prerequisites

No specific prerequisite

Programme

Part 1: Some preliminary notions. Order relations and trees, inductive definitions, proofs by induction, axiom of choice and K#nig's

lemma. Part 2: Provability and satisyability. First order formal language: alphabet, terms, formulas, sequents. Structures for first order languages: structures, terms and formulas with parameters in a structure, value of terms, formulas and sequents. The calculus of sequents for first order logic: Gentzen's LK. Derivable sequents and derivations. Correctness of the rules of LK. Canonical analysis and fundamental theorem: construction of the canonical analysis (with and without cuts) and proof of the fundamental theorem of the canonical analysis. Consequences of the fundamental theorem: completeness theorem, compactness theorem, eliminability of cuts, L"owenheim-Skolem's theorem. Part 3: Towards proof-theory: the cut-elimination theorem. The cut-elimination procedure. Definition of the elementary steps of cut-elimination. First proof strategy (big reduction steps). Second proof strategy (reversion of derivations). The complexity of the cut-elimination procedure (sketch). Some immediate consequences of the cut-elimination theorem.

Reference books

V. Michele Abrusci e Lorenzo Tortora de Falco, Logica. Vol. 1 Dimostrazioni e modelli al primo ordine, Springer, 2014
https://sites.google.com/view/lm410/home

Reference bibliography

V. Michele Abrusci e Lorenzo Tortora de Falco, Logica. Vol. 1 Dimostrazioni e modelli al primo ordine, Springer, 2014
https://sites.google.com/view/lm410/home

Study modes

This course includes Face-to-face lectures; Discussions with students and debates on the discussed topics; Exercices; Attendance is not mandatory but strongly recommended. In case of health emergency due to COVID-19 the way lectures will be given will depend on the conditions. In such a potential framework all the possible efforts will be done to limit the unavoidable damages related to the necessity to switch to online courses and interaction during the lessons will be preserved as much as possible. Lessons held in classroom will be streamed in real time but not recorded.

Exam modes

-

20410529 - LM510 - TEORIE LOGICHE 1

Docente: MAIELI ROBERTO

Italiano

Prerequisiti

è consigliato che lo studente abbia già seguito un corso di logica di base

Programma

Dimostrazioni (Sequent Proofs) ********** Deduzione Naturale (ND) Il Calcolo dei Sequenti per la Logica Intuizionista (LJ) e Logica Classia (LK) L'eliminazione dei Tagli per LJ ed LK Il calcolo dei sequenti della Logica Lineare (LL) Il teorema di Eliminazione dei Tagli per LL Il Teorema di Focalizzazione delle dimostrazioni di LL Reti dimostrative (Proof Nets) ********** (stutture dimostrative, correttezza, normalizzazione, adeguatezza, sequenzializzazione, focalizzazione, complessità) Reti puramente moltiplicative Reti moltplicative-additive Reti moltiplicative-esponenziali Semantica Denotazionale

Testi

Libri, aricoli, APPUNTI E SLIDES DISPONIBILI SULLA PAGINA WEB DEL CORSO https://sites.google.com/view/lm510/

Bibliografia di riferimento

J.-Y. Girard, Proofs and Types AA.VV., Handbook of Linear Logic V. Danos and L. Regnier, The structure of Multiplicatives O. Laurent, Sequentialization of Multiplicative Proof Nets J.-M. Andreoli and R. Maieli, Focusing and proof nets in linear and non-commutative logic R. Maieli, Cut Elimination for Monomial Proof Nets of the Purely Multiplicativeand Additive Fragment of Linear Logic D. Mazza, Attack of the Exponentials C. Retoré, On the relation between coherence semantics and multiplicative proof nets

Modalità erogazione

LEZIONI CON ESERCITAZIONI in presenza in aula ed in streaming

Modalità di valutazione

domande ed esercizi sui temi affrontati a lezione con una esposizione in forma seminariale

English

Prerequisites

it is recommended that the student has already taken a basic course in logic

Programme

Sequent Calculus Proofs ********** Natural Deduction Sequent Calculus for Classical Logic (LK) and Intuitionistic Logic (LJ) Cut elimination for LK and LJ sequent proofs Sequent calculus for Linear Logic(LL) Cut Elimination Theorem for LL Focusing Theorem for LL proofs Proof Nets ********** (proof-structures, correctness, normalization, adequacy, sequentialization, focusing, complexity) Pure Multiplicative Proof Nets Multiplicative and Additive Proof Nets Multiplicative and Exponenial Proof Nets

Reference books

Handbooks, papers, NOTES AND SLIDES AVAILABLE ON THE COURSE WEB PAGE https://sites.google.com/view/lm510/

Reference bibliography

J.-Y. Girard, Proofs and Types AA.VV., Handbook of Linear Logic V. Danos and L. Regnier, The structure of Multiplicatives O. Laurent,

Sequentialization of Multiplicative Proof Nets J.-M. Andreoli and R. Maieli, Focusing and proof nets in linear and non-commutative logic R. Maieli, Cut Elimination for Monomial Proof Nets of the Purely Multiplicativeand Additive Fragment of Linear Logic D. Mazza, Attack of the Exponentials C. Retoré, On the relation between coherence semantics and multiplicative proof nets

Study modes

LECTURES WITH EXERCISES in classroom and by streaming

Exam modes

-

20410619 - ME430 - FONDAMENTI E STORIA DELL'ANALISI MATEMATICA

Docente: BIASCO LUCA

Italiano

Prerequisiti

Corsi di base di analisi

Programma

Storia del calcolo infinitesimale. I greci e il calcolo di aree e volumi. Gli indivisibili di Cavalieri. Cartesio, Fermat. La nascita del calcolo: Newton e Leibniz. Gli sviluppi del calcolo, i Bernoulli, de l'Hopital, Euler e Lagrange. Il padre dell'analisi matematica: Cauchy. Weiersrtass. L'integrale di Riemann. L'assiomatica dei reali: Cantor e Dedekind. L'integrale di Lebesgue. Lo studio qualitativo delle equazioni differenziali: Poincare. L'analisi funzionale: Hilbert, Banach e von Neumann.

Testi

E. Giusti, Analisi Matematica 1 E. Giusti Piccola storia del calcolo infinitesimale dall'antichità al Novecento

Bibliografia di riferimento

Testi da definire

Modalità erogazione

5 ore di didattica frontale a settimana.

Modalità di valutazione

prova scritta con esercizi e successiva prova orale

English

Prerequisites

Basic calculus

Programme

History of infinitesimal calculus. The Greeks and the calculation of areas and volumes. Cavalieri's indivisibles. Descartes, Fermat. The birth of calculus: Newton and Leibniz. The development of calculus: the Bernoullis, de l'Hôpital, Euler, and Lagrange. The father of mathematical analysis: Cauchy. Weierstrass. The Riemann integral. The axiomatization of the real numbers: Cantor and Dedekind. The Lebesgue integral. The qualitative study of differential equations: Poincaré. Functional analysis: Hilbert, Banach, and von Neumann.

Reference books

E. Giusti, Analisi Matematica 1 E. Giusti Piccola storia del calcolo infinitesimale dall'antichità al Novecento

Reference bibliography

-

Study modes

5 hours of frontal teaching a week

Exam modes

-

20410555 - ST410-STATISTICA

Docente: CANDELLERO ELISABETTA

Italiano

Prerequisiti

Avere seguito un corso base di teoria della probabilita' e di analisi matematica in piu' variabili

Programma

Programma di massima: - Variabili casuali e la loro distribuzione, funzione generatrice dei momenti, media, varianza e covarianza. Modello di campionamento casuale e modello statistico. - Statistica: concetto, esempi, statistica sufficiente e minimale. - Stimatori puntuali: definizione e proprieta' desiderate, momenti, massima verosimiglianza e Bayes + Metodi computazionali. Metodi per miglioramento di uno stimatore (es. Cramer-Rao) - Intervalli di confidenza - Verifica d'ipotesi - Metodi non parametrici: goodness-of-fit, tabella di contingenza, Kolmogorov-Smirnov e test tramite graduatoria. - Analisi della varianza (ANOVA) e test F - Regressione

Testi

Introduzione alla Statistica, S.M. Ross, Apogeo - Maggioli Editore. testo aggiuntivo: Luca Leuzzi, Enzo Marinari, Giorgio Parisi CALCOLO DELLE PROBABILITÀ: un trattatello per principianti volenterosi

Bibliografia di riferimento

Testi da definire

Modalità erogazione

Le lezioni si terranno in aula con scrittura sulla lavagna o su tablet

Modalità di valutazione

La valutazione in itinere consiste nel risolvere in circa 10 giorni e per quattro volte durante il corso una serie di quesiti di carattere pratico (esercizi) e teorico. Ciascuno foglio riceve un voto da 0 a 10. L'esame finale consiste di 4 esercizi, ciascuno articolato in 2 o 3 quesiti a carattere teorico e pratico. Il voto finale e' il massimo tra il voto dell'esame finale e 2/3 x (voto esame finale) + 1/3 x media dei voti dei fogli di esercizi

English

Prerequisites

A basic course in probability theory and in multivariable calculus

Programme

- Random variables and their distribution, moment generating function, mean variance and covariance. - Random sampling model and statistical model. - Statistics: concept, examples, sufficient statistics. - Point estimators: definition and desired properties, moments, maximum likelihood and Bayes + computational methods. Methods for improving an estimator (for example Cramer-Rao) - Confidence intervals - Hypothesis testing - Non-parametric methods: goodness-of-fit, contingency table, Kolmogorov-Smirnov and ranking tests. - Analysis of variance (ANOVA) and F. - Regression

Reference books

Statistical Inference, Casella e Berger, 2nd Edition, Duxbury Advanced Series. Additional reference: Luca Leuzzi, Enzo Marinari, Giorgio Parisi CALCOLO DELLE PROBABILITÀ: un trattatello per principianti volenterosi

Reference bibliography

-

Study modes

Lectures will take place in a lecture room either on the blackboard or on a tablet

Exam modes

-

20410627 - TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI

Docente: PAPPALARDI FRANCESCO

Italiano

Prerequisiti

AL110. E' utile familiarità con il linguaggio matematico con speciale riguardo all'algebra di base

Programma

Divisione, fattorizzazione, alcune proprietà elementari dei numeri primi, alcuni risultati e problemi riguardanti i primi. Funzioni aritmetiche: La funzione numero di divisori. La funzione di Moebius. La funzione di Eulero. La convoluzione Dirichlet. Congruenze: Sistemi Completi di residui, alcuni Congruenze interessanti, alcune congruenze lineari, congruenze polinomiali, radici primitive, il teorema di Gauss. RESIDUI Quadratici: i simboli di Legendre. Reciprocità quadratica. I simboli di Jacobi.La distribuzione dei residui quadratici. Somme di quadrati di interi: somme di due quadrati. Numero di rappresentazioni. Somme di quattro quadrati. Somme di tre quadrati. TEORIA ELEMENTARE DEI NUMERI PRIMI: il teorema di Euclide rivisitato. La funzione Von Mangoldt. Teorema di Tchebycheff. Alcuni risultati di Mertens

Testi

Chen, W; ELEMENTARY NUMBER THEORY. https://rutherglen.science.mq.edu.au/wchen/lnentfolder/lnent.html Chowdhury, F.; Chowdhury, M. R. Essentials of Number Theory. Pi Publications, Dhaka, Bangladesh, 2005. ISBN 984-32-2836-7 Hardy, G. H.; Wright, E. M. An introduction to the theory of numbers. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979. xvi+426 pp. ISBN: 0-19-853170-2; 0-19-853171-0 Davenport, H. Aritmetica superiore. Un'introduzione alla teoria dei numeri. Editore: Zanichelli, 1994. 199 pp. ISBN: 8808091546 Gioia, A. A. The theory of numbers. An introduction. Reprint of the 1970 original. Dover Publications, Inc., Mineola, NY, 2001. xii+207 pp. ISBN: 0-486-41449-3 Rosen, K. H. Elementary number theory and its applications. Fourth edition. Addison-Wesley, Reading, MA, 2000. xviii+638 pp. ISBN: 0-201-87073-8 Tattersall, J. J. Elementary number theory in nine chapters. Cambridge University Press, Cambridge, 1999. viii+407 pp. ISBN: 0-521-58531-7

Bibliografia di riferimento

Gioia, A. A. The theory of numbers. An introduction. Reprint of the 1970 original. Dover Publications, Inc., Mineola, NY, 2001. xii+207 pp. ISBN: 0-486-41449-3 Rosen, K. H. Elementary number theory and its applications. Fourth edition. Addison-Wesley, Reading, MA, 2000. xviii+638 pp. ISBN: 0-201-87073-8 Tattersall, J. J. Elementary number theory in nine chapters. Cambridge University Press, Cambridge, 1999. viii+407 pp. ISBN: 0-521-58531-7

Modalità erogazione

60 ore in presenza

Modalità di valutazione

scritto di due ore con esercizi pratici e teorici

English

Prerequisites

AL110. It is auspicable to be able to use mathematical notions especially that of basic algebra

Programme

Division, Factorization, Some Elementary Properties of Primes, Some Results and Problems Concerning Primes. ARITHMETIC FUNCTIONS: The Divisor Function. The Moebius Function. The Euler Function. Dirichlet Convolution CONGRUENCES: Sets of Residues,Some Interesting Congruences, Some Linear Congruences, Some Polynomial Congruences, Primitive Roots, the Theorem of Gauss. QUADRATIC RESIDUES: The Legendre Symbol. Quadratic Reciprocity. The Jacobi Symbol.The Distribution of Quadratic Residues. SUMS OF INTEGER SQUARES: Sums of Two Squares. Number of Representations. Sums of Four Squares. Sums of Three Squares. ELEMENTARY PRIME NUMBER THEORY: Euclid's Theorem Revisited. The Von Mangoldt Function. Tchebycheff's Theorem. Some Results of Mertens

Reference books

Chen, W; ELEMENTARY NUMBER THEORY. https://rutherglen.science.mq.edu.au/wchen/lnentfolder/lnent.html Chowdhury, F.; Chowdhury, M. R. Essentials of Number Theory. Pi Publications, Dhaka, Bangladesh, 2005. ISBN 984-32-2836-7 Hardy, G. H.; Wright, E. M. An introduction to the theory of numbers. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979. xvi+426 pp. ISBN: 0-19-853170-2; 0-19-853171-0 Davenport, H. Aritmetica superiore. Un'introduzione alla teoria dei numeri. Editore: Zanichelli, 1994. 199 pp. ISBN: 8808091546 Gioia, A. A. The theory of numbers. An introduction. Reprint of the 1970 original. Dover Publications, Inc., Mineola, NY, 2001. xii+207 pp. ISBN: 0-486-41449-3 Rosen, K. H. Elementary number theory and its applications. Fourth edition. Addison-Wesley, Reading, MA, 2000. xviii+638 pp. ISBN: 0-201-87073-8 Tattersall, J. J. Elementary number theory in nine chapters. Cambridge University Press, Cambridge, 1999. viii+407 pp. ISBN: 0-521-58531-7

Reference bibliography

Gioia, A. A. The theory of numbers. An introduction. Reprint of the 1970 original. Dover Publications, Inc., Mineola, NY, 2001. xii+207 pp. ISBN: 0-486-41449-3 Rosen, K. H. Elementary number theory and its applications. Fourth edition. Addison-Wesley, Reading, MA, 2000. xviii+638 pp. ISBN: 0-201-87073-8 Tattersall, J. J. Elementary number theory in nine chapters. Cambridge University Press, Cambridge, 1999. viii+407 pp. ISBN: 0-521-58531-7

Study modes

60 hours of frontal lectures

Exam modes

-