

ESTRATTO

Salvatore Damantino, Emanuele Campeotto

Aritmetica modulare

Teoria e applicazioni

Indice

1	Congruenze	9
1.1	Relazione di congruenza modulo un intero n	10
1.2	Proprietà generali	13
1.3	Criteri di congruenza	24
1.4	Il Piccolo Teorema di Fermat	30
1.5	La funzione di Eulero e il teorema di Eulero	36
2	Congruenze lineari	49
2.1	Equazioni lineari	49
2.1.1	Inverso moltiplicativo e divisori dello zero	54
2.1.2	Un metodo alternativo	57
2.1.3	La legge di annullamento del prodotto	58
2.2	Il teorema di Wilson	58
2.3	Sistemi lineari	60
2.3.1	Il Teorema Cinese dei Resti	62
2.3.2	Caso generale	73
3	Ordine moltiplicativo e generatori	77
3.1	Ordine moltiplicativo modulo n	77
3.1.1	Lunghezza del periodo dei decimali periodici	85
3.1.2	Test di primalità di Lucas	87

3.2	Generators	88
3.2.1	Ordine moltiplicativo universale	96
4	Residui ed equazioni diofantee	101
4.1	Residui quadratici modulo un primo p	101
4.2	Equazioni diofantee non lineari	111
5	Approfondimenti	117
5.1	Il calendario perpetuo	117
5.2	Girone all'italiana	120
5.3	Terne pitagoriche	122
5.4	L'Ultimo Teorema di Fermat	130
5.5	Interi esprimibili come somma di due quadrati	133
5.6	Crittografia e sistema RSA	137
6	Problemi	143
7	Soluzioni	159
	Bibliografia	182
	Elenco dei simboli	187
	Indice analitico	189