# Programma di Algebra I
# A.A. 2018/2019

1. Assiomi di teoria degli insemi. Paradosso di Russel. Intersezione e unione di insiemi.
2. Insieme potenza. Coppie ordinate. Prodotto cartesiano.
3. Leggi di De Morgan.
4. Funzioni. Uguaglianza tra funzioni. Funzioni iniettive e suriettive.
5. Funzioni biiettive. Funzioni iniettive e suriettive tra insiemi finiti.
6. Teorema di Cantor.
7. Composizione di funzioni. Funzione identica. Inverse destre e sinistre.
8. Assioma di scelta. Inverse di funzioni iniettive e di funzioni suriettive.
9. Principio del minimo.
10. Divisione con resto.
11. Principio di induzione nella prima forma. Induzione nella seconda forma (solo enunciato).
12. Scrittura di un naturale in basi diverse.
13. Divisibilità in $\mathbb{Z}$. Associati. Definizione di massimo comun divisore.
14. Esistenza di un massimo comun divisore. Alcune proprietà del massimo comun divisore. Interi coprimi.
15. Algoritmo di Euclide. Esistenza di un minimo comune multiplo.
16. Equazioni diofantee lineari.

17. Primi e irriducibili. I primi sono irriducibili. In $\mathbb{Z}$ gli irriducibili sono primi.

18. Teorema di fattorizzazione in $\mathbb{Z}$. I primi di $\mathbb{Z}$ sono infiniti.

19. Per ogni primo $p \in \mathbb{N}$, $\sqrt{p}$ è irrazionale.

20. Terne pitagoriche.

21. Relazioni d'ordine e di equivalenza.

22. Massimo e minimo. Maggioranti e minoranti. Estremo superiore ed estremo inferiore. Elementi massimali e minimali.

23. Lemma di Zorn (solo enunciato).

24. Classi di equivalenza e insieme quoziente.

25. Trasversali. Esistenza di un trasversale. Equivalenza associata ad una funzione. Teorema di omomorfismo per insiemi.

26. Congruenze in $\mathbb{Z}$. Classi di congruenza.

27. Comportamento delle congruenze rispetto alle operazioni. Criteri di divisibilità per 9 e 11.

28. Piccolo teorema di Fermat.

29. Sistemi di congruenze.

30. Operazioni.

31. Anelli.

32. Regola dei segni.Potenze e multipli. Proprietà di multipli e potenze. Divisori di zero e nilpotenti.

33. Binomio di Newton.

34. Sottoanelli.

35. Numeri complessi. Quaternioni.

36. Ideali. Ideali di $\mathbb{Z}$.

37. Intersezioni e somme di ideali.

38. Ideale generato da un sottoinsieme.

39. Ideali generati da sottoinsiemi finiti in anelli commutativi. Ideali principali.

40. Morfismi di anelli. L'inverso di un isomorfismo è un isomorfismo.

41. Nucleo di un morfismo. Il nucleo è un ideale. Morfismi iniettivi.

42. Equivalenza associata ad un ideale.

43. Anelli quoziente. Proiezione canonica.

44. Quozienti di $\mathbb{Z}$. Elementi invertibili, nilpotenti e divisori di zero in $\mathbb{Z}/n\mathbb{Z}$.

45. Prodotti diretti di anelli. Ideali nei prodotti diretti di anelli.

46. Primo teorema di omomorfismo per anelli.

47. Caratteristica di un anello. Sottoanello fondamentale. Morfismo di Frobenius.

48. Teorema cinese dei resti. Funzione di Eulero.

49. Teorema di corrispondenza.

50. Serie formali e polinomi. Grado di un polinomio. Principio di identità dei polinomi e delle serie formali.

51. Principio di sostituzione. Valutazione. Teorema della divisione con resto per polinomi.

52. Teorema di Ruffini. Numero di zeri di un polinomio in un dominio.

53. Teorema di Wilson.

54. Divisibilità. Associati. Elementi associati in domini di integrità.

55. Primi e irriducibili. I primi di un dominio sono irriducibili. Esempi di irriducibili non primi in $\mathbb{Z}[i\sqrt{5}]$.

56. Definizione di UFD.

57. Caratterizzazione degli UFD.

58. Esempi di fattorizzazione non unica in $\mathbb{Z}[i\sqrt{17}]$.

59. Se $D$ è UFD allora $D[x]$ è UFD (solo enunciato).

60. PID. Le catene ascendenti nei PID sono stazionarie. I PID sono UFD.

61. Domini euclidei. I domini euclidei sono PID. L'anello $\mathbb{Z}[x]$ è UFD ma non PID.

62. Gli anelli $\mathbb{Z}[i]$ e $\mathbb{Z}[\sqrt{2}]$ sono domini euclidei.

63. Ideali primi. Un ideale è primo se e solo se l'anello quoziente non ha divisori di zero.

64. Ideali massimali. Un ideale $I$ dell'anello commutativo $A$ è massimale se e solo se $A/I$ è un campo. Quozienti di un PID. L'anello $\mathbb{Z}[x]$ non è un PID.

65. Se $p \in \mathbb{N}$ è un primo pari o congruo a 1 modulo 4, allora esistono $a, b \in \mathbb{Z}$ tali che $p = a^2 + b^2$.

66. Primi di $\mathbb{Z}[i]$.