

MA 14 - Aritmética

Ementa

Os números inteiros. Aplicações da indução. Divisão nos inteiros. Representação dos números inteiros. Algoritmo de Euclides. Aplicações do máximo divisor comum. Números primos. Números especiais. Congruências. Os teoremas de Euler e Wilson. Congruências lineares e classes residuais. Congruências quadráticas. Noções de criptografia.

Referência Bibliográfica

1. HEFEZ, A.; FERNANDEZ, C.S. **Introdução à álgebra linear**. SBM, 2016 (Coleção PROFMAT).
2. HEFEZ, A. **Exercícios resolvidos de Aritmética**. SBM, 2016 (Coleção PROFMAT).
3. PROFMAT, **MA14 – Aritmética**. Disponível em: <<http://www.profmatt-sbm.org.br/ma14>>. Acesso: 04 jan. 2017.

Programa

1. Números inteiros: a adição e a multiplicação. Ordenação dos inteiros. Princípio da boa ordenação
2. Aplicação da indução: definição por recorrência. Binômio de Newton. Aplicações lúdicas
3. Divisão nos inteiros: divisibilidade. Divisão euclidiana. A aritmética na Magna Grécia
4. Representação dos números inteiros: sistema de numeração. Jogo de Nim
5. Algoritmo de Euclides: máximo divisor comum. Propriedades do MDC
6. Algoritmo de Euclides: algoritmo de Euclides estendido. Mínimo múltiplo comum. A equação pitagórica
7. Aplicações do máximo divisor comum: equações diofantinas lineares
8. Aplicações do máximo divisor comum: expressões binômias. Números de Fibonacci
9. Números primos: teorema fundamental da aritmética. Sobre a distribuição dos números primos
10. Números primos: pequeno teorema de Fermat
11. Números primos: o renascimento da Aritmética
12. Números especiais: primos de Fermat, de Mersenne e em PA

13. Números especiais: números perfeitos
14. Números especiais: decomposição do fatorial em primos. A equação $E_p(x!) = \alpha$
15. Congruências: aritmética dos restos. aplicações
16. Congruências: congruências e números binomiais. O calendário
17. Os teoremas de Euler e de Wilson: teorema de Euler. Teorema de Wilson
18. Congruências lineares e classes residuais: resolução de congruências lineares. Teorema chinês dos restos
19. Congruências lineares e classes residuais: Classes residuais
20. Congruências quadráticas: congruências quadráticas. Resíduos quadráticos
21. Congruências quadráticas: somas de quadrados
22. Congruências quadráticas: lei da reciprocidade quadrática
23. Noções de criptografia: as origens da criptografia
24. Noções de criptografia: o advento dos computadores. A grande revolução: O sistema RSA