ARITMÉTICA MODULAR E ALGUMAS APLICAÇÕES

Edite M. Cordeiro, emc@ipb.pt
Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança

A Aritmética Modular (por vezes designada de aritmética do relógio) envolve o conceito de congruência modular, relação entre dois números que, divididos por um terceiro, deixam o mesmo resto.
Na abordagem que propomos, serão observadas propriedades da congruência modular e noções como divisibilidade, número primo, factorização em primos e máximo divisor comum. A aplicação destes conceitos a números razoavelmente grandes será feita com recurso ao sistema computacional GAP (Groups, Algorithms, Programming).
Todas estas noções aparecem de forma natural em contextos diversos. Referiremos fenómenos periódicos e códigos de identificação numérica como, por exemplo, o número do cartão do cidadão. Serão também observadas aplicações à criptografia, dando especial destaque ao algoritmo RSA.