Universidade do Minho

2006/2007	1° Semestre ☐	2° Semestre ☒	Anual ☐
Disciplina: Teoria dos Números Computacional Cursos: MCC MAT CC	Docente José Pedro Patricio 204059		

Aula	Sumário
Teórica nº 1 2007-02-22 Quinta-Feira 8:00-10:00	Apresentação do docente e da disciplina. Algumas revisões de teoria de números elementar. O algoritmo de Euclides estendido; demonstração do teorema que fundamenta o algoritmo. Vantagens relativamente ao algoritmo de Euclides "clássico". Exemplos. O Docente _____

Aula	Sumário
Teórica nº 2 2007-03-01 Quinta-Feira 8:00-10:00	Revisões: o mmc de sua relação com o mdc, resolução da equação diofantina $ax + by = c$, números primos e algumas propriedades, TFA. Exemplo e verificação de um anel que não é domínio de factorização única. Prova em como a raiz quadrada de 2 não é racional. Prova em como as raizes de polinímios em $Z[x]$ são ou inteiras ou irracionais. Teste de primalidade de n à custa da divisibilidade pelos primos não superiores $[n]$. O crivo de Eratóstenes. O Docente _____

Aula	Sumário
Teórica nº 3 2007-03-08 Quinta-Feira 8:00-10:00	Distribuição dos números primos: a função $\pi(x)$, a aproximação de Legendre, as conjecturas de Gauss, o enquadramento de Chebyshev (e melhoramentos de Sylvester). Resultado de Hadamard e Vallée-Poussin: o Teorema dos Números Primos. Brevíssima referência à função zeta de Riemann. Factorização de Fermat. Números de Fermat: a conjectura de Fermat, prova em como F_5 é composto (e portanto a conjectura de Fermat é falsa), prova em como números de Fermat distintos são primos relativos, demonstração alternativa do Teorema de Euclides. O Docente _____

Universidade do Minho

2006/2007	1° Semestre ☐	2° Semestre ☒	Anual ☐
Disciplina: Teoria dos Números Computacional Cursos: MCC MAT CC	Docente José Pedro Patricio 204059		

Aula	Sumário
Teórica nº 4 2007-03-15 Quinta-Feira 8:00-10:00	Revisões sobre congruência e sobre congruências lineares. O teorema chinês dos resíduos e sua aplicação no cálculo de uma soma num computador que admite palavras menores que 100. Demonstração do Teorema de Wilson. O Docente _____

Aula	Sumário
Teórica nº 5 2007-03-22 Quinta-Feira 8:00-10:00	Prova do recípropoco do teorema de Wilson; o recípropoco do teorema de Wilson como teste determinístico de primalidade (computacionalmente pouco eficiente). Demonstração do Pequeno Teorema de Fermat (PTF); sua aplicação na resolução de algumas congruências lineares. Os algoritmos ρ-Pollard e $p-1$-Pollard de factorização. O Docente _____

Aula	Sumário
Teórica nº 6 2007-03-29 Quinta-Feira 8:00-10:00	O algoritmo (p-1)-Pollard: continuação da aula anterior; exemplos. "Square and multiply"para cálculo de exponenciação modular. Pseudo-primos de base b: definição e exemplos. Exemplo de Sarrus: prova em como 341 é um pseudo-primo de base 2. Demonstração da existência de uma infinidade de pseudo-primos de base 2. O Docente _____

Universidade do Minho

2006/2007	1° Semestre ☐	2° Semestre ☒	Anual ☐
Disciplina: Teoria dos Números Computacional Cursos: MCC MAT CC	Docente José Pedro Patricio 204059		

Aula	Sumário
Teórica nº 7 2007-04-12 Quinta-Feira 8:00-10:00	Definição de pseudo-primos absolutos, ou números de Carmichael. Prova em como 561 é número de Carmichael. Teste de pseudo-primalidade forte. Teste de primalidade probabilístico de Miller-Selfridge-Rabin. Prova em como 561 não passa o teste de Miller. Demonstração em como um número primo passa o teste de Miller, e em como de facto o teste de Miller é de primalidade. Prova em como o teste de Miller é mais forte do que o de pseudo-primalidade. Definição de pseudo-primo forte. Demonstração da existência de uma infinidade de pseudo-primos fortes de base 2. O Docente _____

Aula	Sumário
Teórica nº 8 2007-04-19 Quinta-Feira 8:00-10:00	Alguns factos que permitem verificar que o teste de Miller é, em alguns casos, um teste de primalidade determinístico. O Teorema do teste de primalidade probabilístico de Rabin, à custa do teste de Miller. A função ϕ de Euler: definição e alguns exemplos. Sistemas reduzidos de resíduos: definição e prova de alguns resultados. Demonstração do Teorema de Euler. Definição de função aritmética, multiplicativa e absolutamente multiplicativa. Demonstração de que a imagem, por uma função multiplicativa, do produto de potências de primos distintos iguala o produto das imagens, pela mesma função, das potências dos primos. Prova em como $\phi(p) = p - 1$ se e só se p é primo. O Docente _____

Universidade do Minho

2006/2007	1° Semestre ☐	2° Semestre ☒	Anual ☐
Disciplina: Teoria dos Números Computacional Cursos: MCC MAT CC	Docente José Pedro Patricio 204059		

Aula	Sumário
Teórica nº 9 2007-05-03 Quinta-Feira 8:00-10:00	Demonstração de $\phi(p^a) = p^a - p^{a-1}$, para p primo. Prova em como ϕ é multiplicativa. Um exemplo. Corolário: $\phi(pq) = (p-1)(q-1)$, onde p, q são primos distintos. Prova de uma fórmula de cálculo de ϕ de um número à custa da sua factorização em primos. Prova em como $\phi(n)$ é par, para $n > 2$. Prova em como $\sum_{d\|n} \phi(d) = n$. Prova em como $2^m - 1$ primo implica que m é primo, mas que o recíproco é falso. Números de Mersenne, primos de Mersenne. Teste de Lucas-Lehmer. O projecto GIMPS. O Docente _____

Aula	Sumário
Teórica nº 10 2007-05-10 Quinta-Feira 8:00-10:00	Descrição da cifra de chave pública RSA. Prova em como a função de encriptação tem inversa à esquerda. Para n=pq, cálculo da probabilidade de $(x, n) \neq 1$. Algumas considerações sobre a implementação (e alguns cuidados a ter) de uma chave pública RSA. Prova em como calcular $\phi(n)$ é equivalente a factorizar n. O Docente _____

Aula	Sumário
Teórica nº 11 2007-05-24 Quinta-Feira 8:00-10:00	Ordem de a módulo m. Sua relação com $\phi(m)$ e algumas propriedades. Raiz primitiva. Demonstração do teorema dos índices. O número de raizes primitivas. Propriedades dos índices. A cifra de chave pública ElGamal. O Docente _____

Universidade do Minho

2006/2007	1° Semestre ☐	2° Semestre ☒	Anual ☐
Disciplina: Teoria dos Números Computacional Cursos: MCC MAT CC	Docente José Pedro Patricio 204059		

Aula	Sumário
Teórica nº 12 2007-05-30 Quarta-Feira 14:00-16:00	Enunciado do teste de primalidade de Lucas-Lehmer. Prova em como o teste de Lucas-Lehmer é determinístico. Um exemplo e um corolário. Definição de resíduo quadrático.Prova em como a congruência quadrática tem 0 ou 2 soluções. Número de resíduos quadráticos e de não-resíduos quadráticos. A caracterização de resíduos quadráticos à custa da paridade do índice. O símbolo de Legendre. Enunciado e prova do Critério de Euler. O Docente _____

Aula	Sumário
Teórica nº 13 2007-05-31 Quinta-Feira 8:00-10:00	Algumas propriedades do símbolo de Legendre. O estudo dos casos em que -1 é resíduo quadrático de p. O Lema de Gauss: enunciado e um exemplo. Lei da Reciprocidade Quadrática: enunciado e uma aplicação. O símbolo de Jacobi. Algumas propriedades e um exemplo. A Lei da Reciprocidade Quadrática para o símbolo de Jacobi: enunciado e um exemplo de aplicação. Pseudo-primos de Euler: definição e suas relações com os pseudo-primos fortes e fracos. O teste probabilístico de primalidade de Solovay-Strassen. Um algoritmo para cálculo do símbolo de Jacobi sem uso da factorização em primos. Exemplo. Preenchimento dos inquéritos de avaliação da disciplina. O Docente _____