O Seminário Diagonal é um seminário de estudantes, para todos os interessados em Matemática, sobre Matemática no sentido lato. Iniciou-se no ano lectivo 2000–01 em vários pontos do país, incluindo o Instituto Superior Técnico onde decorreram 14 sessões.

Dado o sucesso da iniciativa, a organização no IST entendeu oportuno editar uma compilação de textos escritos por alunos, a propósito dos seminários que aí apresentaram. Assim, esses artigos estão acessíveis a partir de

`http://www.math.ist.utl.pt/diagonal/`

desde Novembro de 2001. Segue-se a lista dos respectivos resumos.

A Organização Diagonal IST 2000–01

Habilidades com Somatórios

Luís Cruz-Filipe (5º ano da LMAC[1])

Alguns quebra-cabeças relativamente simples criam por vezes a necessidade de calcular somas pouco atraentes. Neste apontamento introduzem-se técnicas elegantes que permitem resolver alguns somatórios sem esforço recorrendo, nomeadamente, à introdução de uma notação diferente da habitual.

Análise Real(mente) Infinitesimal

João Pedro Boavida (5º ano da LMAC)

Entre as hipóteses inconscientes na prática matemática habitual, conta-se a possibilidade de provar/refutar o que é verdadeiro/falso num número *finito* de passos. Assim, o conjunto de fórmulas $\{\varepsilon < 1, \varepsilon < \frac{1}{2}, \varepsilon < \frac{1}{3}, ...\}$ a respeito de um real $\varepsilon > 0$ não pode ser refutado, pelo que deveria existir algum número ε satisfazendo-as, que seria realmente infinitesimal.

Esta observação aparentemente inocente será o nosso ponto de partida para explorar a Matemática Não-Standard.

Computação Quântica

Alexandre P. Lourenço Francisco (4º ano da LMAC)

Quando falamos em Computação Quântica e em Computadores Quânticos, todos pensamos em máquinas ultra rápidas. No entanto não é apenas o tempo de processamento que está em causa. Ao nível da computação teórica têm ocorrido algumas surpresas, estudam-se novos algoritmos estruturalmente diferentes dos usuais e a complexidade parece não obedecer aos padrões clássicos. Contudo, para o utilizador comum, a surpresa maior virá a ocorrer aquando do primeiro computador quântico utilizável: os códigos criptográficos até então seguros serão facilmente quebrados. Teremos deste modo como objecto de discussão estes e outros pontos associados à Computação Quântica, tais como o processamento de informação, o hardware, os novos algoritmos e a sua complexidade.

Criptologia; Contratos e Dinheiro Virtuais

Pedro Miguel Adão (4º ano da LMAC)

Quando queríamos guardar alguma coisa usávamos os cofres; quando queríamos que uma carta chegasse ao destino sem ser aberta, usávamos lacre; quando queríamos garantir que um destinatário recebia uma carta, enviávamo-la com aviso de recepção.

Hoje em dia, no mundo em que vivemos, será possível ter segurança? Podemos ter um cofre na Internet para guardar dinheiro virtual? Podemos assinar documentos

[1] Trata-se do ano curricular (da Licenciatura em Matemática Aplicada e Computação, do IST) frequentado em 2000–01.

virtuais sem que ninguém falsifique a nossa assinatura? Podemos enviar *e-mails* lacrados? Podemos enviar *e-mails* com aviso de recepção?

Estas e outras questões são o tema deste artigo.

Criptografia e Jogos por Telefone *Tiago Reis (2º ano da LMAC)*

Será possível que duas pessoas lancem uma moeda ao ar ao telefone? Poderá isto ser feito sem que a pessoa que escolhe cara ou coroa, no caso de perder, não duvide nem um pouco da honestidade do lançamento? Neste artigo veremos qual a solução para este problema e até que ponto é fiável.

Veremos por fim o que é um algoritmo de encriptação de chave pública, isto é, um algoritmo em que tanto a chave como o próprio algoritmo são públicos. E o que é e como funciona o algoritmo RSA, amplamente difundido.

O Teorema de Pitágoras *Luís Russo (3º ano da LMAC)*

Sabia que Pitágoras não foi o primeiro a descobrir o Teorema de Pitágoras? Sabia que são conhecidas cerca de 380 demonstrações independentes deste resultado que tem fascinado gerações pela sua simplicidade? A abordagem destas questões, bem como algumas curiosidades históricas com elas relacionadas, constitui o tema deste artigo.

Um Passeio Pouco Aleatório *João Pedro Boavida (5º ano da LMAC)*

Normalmente não nos apercebemos como é frequente que fenómenos que em pequena escala são totalmente deterministas se revelem verdadeiramente aleatórios na escala 'de todos os dias'. Basta pensar na trajectória de um grão de poeira, ou na imagem de um raio nos céus.

Neste artigo vamos descrever o movimento browniano e usá-lo como modelo de ruído em equações diferenciais, o que, como veremos, nos trará algumas surpresas. No final, um passeio curto por Monte-Carlo para explorar algumas propriedades das funções harmónicas.

Grupos, Variedades e Relatividade *Patrícia Engrácia (3º ano da LMAC)*

Os grupos estão muito relacionados com a geometria: há grupos que são espaços geométricos muito ricos e há estruturas geométricas a que podemos associar grupos. Também na física as perspectivas de observadores distintos se relacionam por acção de elementos de grupos.

Neste artigo vamos olhar para alguns exemplos e brincar um pouco com a relatividade de Einstein.