Universidade do Minho
Departamento de Matemática L.C.C. – 3° ano

Teoria de Números Computacional

trabalho de grupo — 2° semestre, 2008/2009

O problema do logaritmo discreto

Dado um natural n, seja $\mathbb{Z}_n^*$ o grupo dos elementos de $\mathbb{Z}_n$ que são unidades. Recorde que $\#\mathbb{Z}_n^* = \phi(n)$, e que $a^{\phi(n)} \equiv 1 \mod n$, para $a \in \mathbb{Z}_n^*$. Ou seja, a ordem de a, $\mathrm{ord}_n(a)$, é não superior a $\phi(n)$. Pelo Teorema de Lagrange, $\mathrm{ord}_n(a) \mid \phi(n)$. Um elemento $a \in \mathbb{Z}_n^*$ diz-se *primitivo módulo* n se $\mathbb{Z}_n^* = \langle a \rangle$, ou de forma equivalente, se $\mathrm{ord}_n(a) = \phi(n)$. No caso de a ser um elemento primitivo, então para qualquer $b \in \mathbb{Z}_n^*$ existe $0 \leq x \leq n-1$ para o qual $b \equiv a^x \mod n$. O elemento x é denotado $\log_a b$ e denominado por *logaritmo discreto de b na base a*. O problema do logaritmo discreto não é mais que resolver a equação $b \equiv a^x \mod n$ em ordem a x.

No caso de n ser primo, então $\phi(n) = n-1$. Assim, $a \in \mathbb{Z}_n \setminus \{0\}$ é primitivo se e só se $\mathrm{ord}_n(a) = n-1$. Por exemplo, dado o primo $n = 383$, obtemos $\mathbb{Z}_n^* = \langle 5 \rangle$ mas $\langle 2 \rangle$ é um subgrupo próprio de $\mathbb{Z}_n^*$.

```
? n=383
  = 383
? znprimroot(n)
  = Mod(5, 383)
? znorder(Mod(2,n))
  = 191
? znorder(Mod(5,n))
  = 382
```

A proposta de trabalho

Explore o algoritmo "Shanks' baby-step giant-step" para resolver o problema do logaritmo discreto, descrito, por exemplo, em [1] e em [3]. Implemente-o no pari/gp, construindo um *script*. Por fim, faça uma breve descrição desta solução para o problema num documento que não tenha mais que 5 páginas onde deve explicar as opções que tomou na implementação do algoritmo. Organize esse documento escrito como ditam as regras: sumário, introdução, corpo do trabalho, conclusões, bibliografia, anexos (se existentes). Seja claro e sucinto na sua exposição. Evite, a todo o custo, erros na escrita. Sugerimos que leia atentamente o documento [2].

Código de honra:
Não está vedada qualquer comunicação entre grupos. No entanto, cada grupo deve submeter os **seus** documentos, da **sua** autoria. Evite colagens às referências bibliográficas.

Referências

[1] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press.

[2] Eduardo M. de Sá, *Como Escrever um Texto. Parte I - Estrutura*, obtido de `http://www.mat.uc.pt/~emsa/EscreverTexto/ComoEscrever-Estrutura.pdf` a 4 de Maio de 2009.

[3] Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press.