Folha **G** de exercícios

Fernando Ferreira

Introdução à Teoria dos Números
Março de 2017

1. Seja dado $k \geq 3$.
   (a) Verifique que 8 não tem raízes primitivas.
   (b) Calcule $\varphi(2^k)$.
   (c) Mostre que 2^k não tem raízes primitivas. (Raciocine por absurdo e use sistematicamente D5.)
   (d) Mostre que $5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$.
   (e) Mostre que $(\mathbb{Z}/2^k\mathbb{Z})^*$ é gerado por -1 e 5. (Use a alínea anterior e o exercício D11.)

2. Heloísa vai combinar com Abelardo uma chave secreta usando o sistema de Diffie-Hellman. Escolhem o primo 53 e $g = 2$. Heloísa toma como chave secreta $n = 29$. Qual é a chave pública de Heloísa? Entretanto, Heloísa recebe a chave pública de Abelardo, que é 12. Qual é a chave secreta que ambos combinaram?

3. Heloísa e Abelardo vão comunicar secretamente usando o sistema de encriptação pública ElGamal. O primo que escolhem é 467 e o elemento módulo 467 escolhido é $g = 2$. A chave secreta de Heloísa é $n = 153$.
   (a) Qual é a chave pública de Heloísa?
   (b) Abelardo pretende enviar secretamente a mensagem $M = 351$ à Heloísa e, para isso, escolhe secretamente a chave efémera $k = 197$. Que par de números é que Abelardo envia publicamente a Heloísa?
   (c) Apresente os cálculos de Heloísa para ler a mensagem que Abelardo lhe enviou.

4. Considere a seguinte variante simplificada da troca de chaves de Diffie-Hellman. Esta variante, tal como o original, baseia-se na escolha dum primo grande p e num elemento $1 < g < p$. Heloísa escolhe secretamente um número $1 < n < p$ e dá a conhecer $a := ng \pmod{p}$. Abelardo também escolhe secretamente um número $1 < m < p$ e dá a conhecer $b := mg \pmod{p}$. A chave secreta é $nmg \pmod{p}$, que tanto Heloísa como Abelardo podem calcular facilmente (porquê?). Por que é que esta troca de chaves não é segura?