# Folhas de exercícios IV

Fernando Ferreira

*Introdução à Teoria dos Números*
2018/2019

1. Na aula teórica afirmámos que 561 é um número de Carmichael mas não o verificámos.

   (a) Note que $561 = 3 \cdot 11 \cdot 17$. Use o pequeno teorema de Fermat para mostrar que, para todo $a \in \mathbb{Z}$,

   $$a^{561} \equiv a \pmod 3, \qquad a^{561} \equiv a \pmod{11}, \qquad a^{561} \equiv a \pmod{17}.$$

   (b) Diga por que é que estas congruências mostram que 561 é um número de Carmichael.

   (c) Use a ideia da alínea anterior para mostrar que 1729 é um número de Carmichael.

2. Encontre um inteiro $a$ tal que $102^{70} + 1 \equiv a^{37} \pmod{113}$. (Calcule mesmo $102^{70} \bmod 113$. Se quiser use o SAGE.)

3. Tente o teste de Miller-Rabin para 561 com as bases 4, 5 e 7. (Sei bem que este e o próximo exercício são um bocado tolos...)

4. Tente o teste de Miller-Rabin para 1105 com as bases 2, 3 e 4.

5. Qual é a ordem de 3 módulo 11? Qual é a ordem de 2 módulo 17? (Veja à mão.)

6. Mostre que 5 é uma raiz primitiva módulo 6.

7. Seja $p$ primo ímpar tal que $(p-1)/2$ também é primo. (A um primo assim chama-se um *primo seguro*. Os primos $(p-1)/2$ chamam-se *primos Sophie Germain*.) Mostre que os elementos de $(\mathbb{Z}/p\mathbb{Z})^*$ têm ordens 1, 2, $(p-1)/2$ ou $p-1$.

8. Seja $G$ um grupo comutativo e $a$ e $b$ elementos de $G$ com ordens $n$ e $m$ respetivamente. Suponha que $n \perp m$. Mostre que a ordem de $ab$ é $nm$. (Veja no livro, p. 42, ou consulte os seus apontamentos de Álgebra.)

9. Quantas raizes primitivas módulo 23 é que existem? E módulo 27? E módulo 50? E módulo 21?

10. Seja $K$ um corpo finito. Mostre que o grupo $(K \setminus \{0\}, \cdot)$ é cíclico. (Sugestão: adapte a demonstração de que, se $p$ é primo, então existem raízes primitivas módulo $p$.)

11. Seja $G$ um grupo cíclico finito de cardinalidade $n$. Mostre que $G$ tem $\varphi(n)$ geradores. (Sugestão: mostre que se $a$ gera $G$, então $a^k$ gera $G$ se, e somente se, $k \perp n$. Use a relação de Bézout.)

12. Porque é que os números quadrados são exceção na conjetura de Artin?

13. Seja dado $k \geq 3$.

    (a) Verifique que 8 não tem raízes primitivas.

    (b) Mostre que não há raízes primitivas módulo $2^k$.

    (c) Calcule $\varphi(2^k)$.

    (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. (Sugestão: use a alínea anterior e o exercício 8 da Folha III.)

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

15. Seja $p$ um número primo e $g$ uma raiz primitiva módulo $p$.

    (a) Mostre que a aplicação $\log_g : \mathbb{Z}_p^* \mapsto \mathbb{Z}_{p-1}$ que a cada $\overline{a} \in \mathbb{Z}_p^*$ faz corresponder $\overline{k} \in \mathbb{Z}_{p-1}$ tal que $g^k \equiv a \pmod{p}$ está bem definida.

    (b) Mostre que $\log_g(h_1 h_2) = \log_g(h_1) + \log_g(h_2)$, para todos $h_1, h_2 \in \mathbb{Z}_p^*$.

    (c) Mostre que $\log_g(h^n) = n \log_g h$, para todos $h \in \mathbb{Z}_p^*$ e $n \in \mathbb{Z}$.

16. Calcule $\log_2(13)$ para o primo 23. (Estamos a abusar da notação.)

17. Alice e Bob 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 Alice é $n = 153$.

    (a) Qual é a chave pública de Alice?

    (b) Bob pretende enviar secretamente a mensagem $M = 351$ à Alice e, para isso, escolhe secretamente a chave efémera $k = 197$. Que par de números é que Bob envia publicamente a Alice?

    (c) Apresente os cálculos de Alice para ler a mensagem que Bob lhe enviou.

18. 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 $1 < g < p$. Alice escolhe secretamente um número $1 < n < p$ e dá a conhecer $a \coloneqq ng \pmod{p}$. Bob também escolhe secretamente um número $1 < m < p$ e dá a conhecer $b \coloneqq mg \pmod{p}$. A chave secreta é $nmg \pmod{p}$, que tanto Alice como Bob podem calcular facilmente (porquê?). Por que é que esta troca de chaves não é segura?

19. Através do método de fatorização de Fermat, fatorize (a) 8633, (b) 809009, (c) 92296873 e (d) 4601.

20. Tente o teste de Miller-Rabin para 172947529 com as testemunhas 17, 3 e 23 (muitas contas... use o SAGE).

21. Alice vai combinar com Bob uma chave secreta usando o sistema de Diffie-Hellman. Escolhem o primo 3793 e $g = 7$. Alice toma como chave secreta um número natural $n < 3783$ e diz a Bob que $7^n \equiv 454 \pmod{3793}$. Bob escolhe aleatoriamente o número 1208 e toma-o como a sua chave secreta. Qual é a chave secreta que ambos combinaram?

22. Alice publica a sua chave pública RSA: (2038667,103), onde $n = 2038667$ é produto de dois primos distintos e $e = 103$ é o expoente encriptador. [Para fazer este exercício e o próximo utilize uma calculadora ou um computador.]

    (a) Bob quer enviar a mensagem $M = 892383$ à Alice. Que cifra é que ele envia?

    (b) Alice sabe que 1301 divide 2038667. Encontre o expoente decifrador $d$ da Alice.

    (c) Faça os cálculos que permitem à Alice obter $M$ a partir da cifra enviada por Bob.

    (d) Alice também recebe a cifra 317730 de Bob. Decifre esta mensagem.

23. Neste exercício, $n$ é o produto de dois primos distintos. Calcule estes primos (usando um método descrito na aula) sabendo que

    (a) $n = 352717$ e $\varphi(n) = 351520$.

    (b) $n = 172205490419$ e $\varphi(n) = 172204660344$.

24. O número 1433811615146881 é produto de dois primos distintos, próximos um do outro. Encontre estes dois primos.