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

Teoria de Números Computacional

folha iv — 2° semestre, 2008/2009

1. Use o método ρ–Pollard para factorizar n, usando x_0 e $f(x)$ como
   (a) $x_0 = 2, f(x) = x^2 + 1, n = 4453$;
   (b) $x_0 = 2, f(x) = x^2 - 1, n = 3953$;
   (c) $x_0 = 3, f(x) = x^2 - 1, n = 3953$.
2. Agrupando os inversos,
   (a) mostre que $11 \mid (10! + 1)$,
   (b) mostre que $13 \mid (12! + 1)$,
   (c) calcule o resto da divisão de $16!$ por 19.
3. Use o Teorema de Wilson para calcular o resto da divisão de $\frac{13!}{7!}$ por 7.
4. Qual o resto da divisão de $18!$ por 437?
5. Qual o resto da divisão de 5^{100} por 7?
6. Qual o resto da divisão de 6^{2000} por 11?
7. Qual o resto da divisão de $3^{999999999}$ por 7?
8. Qual o resto da divisão de $2^{1000000}$ por 17?
9. Mostre que se p é um primo ímpar então $2(p-3)! \equiv -1 \mod p$.
10. Mostre que, para p primo,
$$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \mod p.$$
11. Escreva uma função que teste o recíproco do exercício anterior (conjectura-se que tal seja verdade).
12. Mostre que, para p primo,
$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \mod p.$$

13. Use o método $p-1$-Pollard para encontrar um divisor de:

    (a) 689

    (b) 78621

    (c) 127621

    (d) 8971121

    (e) 12733331

    (f) 98712139726389721

    (g) 37318179102120757

    (h) 7331117.

14. Implemente o método $p-1$-Pollard de factorização.

15. Construa uma função que encontre os primos de Wilson inferiores a 1000.