

Teoria de Números Computacional

folha 3

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 $2(p-3)! \equiv -1 \pmod{p}.$

10. Mostre que, para p primo,

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

11.  Escreva uma função que teste o recíproco do exercício anterior (conjectura-se que tal seja verdade).

12. Mostre que, para p primo ímpar,







$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

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.
16. Mostre que 91 é um pseudoprimo de base 3.
17. Mostre que 45 é um pseudoprimo de bases 17 e 19.
18. Mostre que $n = 161038 = 2 \cdot 73 \cdot 1103$ satisfaz a congruência $2^n \equiv 2 \pmod n$. O inteiro n é de facto o menor pseudoprimo par de base 2.
19. Mostre que se n é um pseudoprimo ímpar de base a então n é um pseudoprimo de base $n - a$.
20. Mostre que se n é um pseudoprimo de bases a e b então é um pseudoprimo de base ab .
21. Mostre que se n é um pseudoprimo de a mas não o é de base b , com $(a, n) = (b, n) = 1$, então n não é pseudoprimo de base ab .
22. Mostre que 25 é um pseudoprimo forte de base 7.
23.  Verifique se os ímpares seguintes passam o teste de Miller de base 2, construindo as respectivas sequências-B.
 - (a) 483
 - (b) 2159
 - (c) 417
 - (d) 111029769
 - (e) 2913
 - (f) 3873
24.  Mostre que 1387 é um pseudoprimo de base 2 mas que não é um pseudoprimo forte de base 2.
25.  Mostre que 1373653 é um pseudoprimo forte de bases 2 e 3.
26.  Mostre que 253260001 é um pseudoprimo forte de bases 2, 5 e 7.