Teoria de Números Computacional

1. 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.
2. Use o Teorema de Wilson para calcular o resto da divisão de $\frac{13!}{7!}$ por 7.
3. Qual o resto da divisão de $18!$ por 437?
4. Qual o resto da divisão de 5^{100} por 7?
5. Qual o resto da divisão de 6^{2000} por 11?
6. Qual o resto da divisão de $3^{999999999}$ por 7?
7. Qual o resto da divisão de $2^{1000000}$ por 17?
8. Mostre que se p é um primo ímpar então $2(p-3)! \equiv -1 \mod p$.
9. Mostre que, para p primo,
$$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \mod p.$$
10. Escreva uma função que teste o recíproco do exercício anterior (conjectura-se que tal seja verdade).
11. Mostre que, para p primo,
$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \mod p.$$
12. Use o método $p-1$-Pollard para encontrar um divisor de 689.
13. Use o método $p-1$-Pollard para encontrar um divisor de 7331117.
14. Construa uma função que encontre os primos de Wilson inferiores a 10000.
15. Implemente o método $p-1$-Pollard de factorização.
16. Implemente o algoritmo *Square & Multiply*.