

Teoria de Números Computacional

teste I

28 abril '08

1. Mostre que 8911 é um pseudoprimo absoluto.
2. Mostre que 7957 é um pseudoprimo fraco de base 2.
3. Verifique se 74665 é um pseudoprimo forte de base 2.
4. Use a factorização de Fermat para encontrar um divisor não trivial de 14647.
5. Use o método $(p - 1)$ -Pollard para encontrar um divisor não trivial de 14647.
6. Use o método ρ -Pollard para encontrar um divisor de 1458943, usando a sequência pseudo-aleatória dada por $x_0 = 2$ e gerada da forma usual por $f(x) = x^2 + 1$.
7. Use o algoritmo estendido de Euclides para encontrar uma solução particular de $77x + 48y = 1$.
8. Numa máquina que opera com números inferiores a 1000, calcule $3243 + 71261$.
9. Mostre que $a^{12} \equiv 1 \pmod{35}$ se $(a, 35) = 1$.
10. Mostre que $\pi(x)$ é assintótico a $\frac{x}{\log x - a}$ para qualquer escolha de a .

Sugestão: mostre que $\frac{\pi(x)}{x} \rightarrow_{x \rightarrow +\infty} 0$ e recorde que $\pi(x) \sim \frac{x}{\log x}$.

Cotação:

cada questão: 2 valores