NÚMEROS INTEIROS E CRIPTOGRAFIA – UFRJ

GABARITO LISTA 5: TESTES DE COMPOSIÇÃO E PSEUDOPRIMOS

1. Ver gabarito das questões do livro.

2. (a) Fatorando 2665 temos que $2665 = 5 \cdot 13 \cdot 41$. Vamos calcular 3^{2664} módulo cada um dos fatores primos de 2665. Usando o teorema de Fermat, temos

$$3^{2664} \equiv (3^4)^{666} \equiv 1 \pmod 5$$
$$3^{2664} \equiv (3^{12})^{222} \equiv 1 \pmod{13}$$
$$3^{2664} \equiv (3^{40})^{66} \cdot 3^{24} \equiv (3^{12})^2 \equiv 40^2 \equiv (-1)^2 \equiv 1 \pmod{41}.$$

Portanto, $3^{2664} - 1$ é divisível por 5, e por 13 e por 41. Como estes números são primos distintos, segue que eles são dois a dois co-primos. Logo, $3^{2664} - 1$ é divisível pelo produto $5 \cdot 13 \cdot 41 = 2665$. Em outras palavras,

$$3^{2664} \equiv 1 \pmod{2665}.$$

(b) Um número n não pode ser pseudoprimo para uma base que seja um fator de n. Portanto, 2665 não é um pseudoprimo para a base 13, nem para a base 41.

3. Para decidir se 10585 é pseudoprimo forte precisamos aplicar o *teste forte de composição* e verificar se a saída é inconclusiva. Mas,

$$10584 = 2^3 \cdot 1323.$$

Já sabemos que

$$3^{1323} \equiv 8422 \pmod{10585}$$

mas isto ainda não nos permite calcular nada. Passamos, então, ao elemento seguinte da sequência, que é

$$3^{2 \cdot 1323} \equiv 8422^2 \equiv 10584 \pmod{10585}.$$

Como este número é congruente a -1 módulo 10585, a saída do teste forte de composição será inconclusivo. Portanto, 10585 é pseudoprimo forte para a base 3.

4. Como n é um pseudoprimo para a base 2, temos que $2^{n-1} \equiv 1 \pmod{n}$. Mas $n = pq$, de modo que $2^{n-1} \equiv 1 \pmod{p}$. Porém
$$n - 1 = p(q-1) + p - 1,$$
de modo que
$$1 \equiv 2^{n-1} \equiv 2^{p(q-1)} \cdot 2^{p-1} \pmod{p}.$$
Mas, pelo teorema de Fermat $2^{p-1} \equiv 1 \pmod{p}$ e $2^p \equiv 2 \pmod{p}$, donde
$$1 \equiv 2^{p(q-1)} \cdot 2^{p-1} \equiv 2^{q-1} \cdot 1 \pmod{p}.$$
Logo $2^{q-1} \equiv 1 \pmod{p}$ e o resto desejado é 1.

5. Como n é um pseudoprimo forte para a base 3, devemos ter que
$$3^q \equiv 1 \pmod{n}.$$
ou então que
$$3^{2^t q} \equiv -1 \pmod{n},$$
para algum $0 \leq t < k$. Contudo, se a primeira possiblidade ocorresse, 3 teria ordem menor ou igual do que q módulo n. Contudo, a ordem foi dada como sendo $2^{m+1}q$, que é sempre maior que q pois $m \geq 0$. Por outro lado, segue da segunda possibilidade que
$$3^{2^{t+1}q} \equiv (3^{2^t q})^2 \equiv 1 \pmod{n};$$
de modo que a ordem de 3 módulo n deve ser exatamente $2^t q$. Logo, levando em conta a hipótese, $t = m$. Finalmente, levando em conta as conclusões acima e o fato de 2 tem ordem $2^m q$ módulo n, obtemos
$$6^{2^m q} \equiv (2^{2^m q})(3^{2^m q}) \equiv 1 \cdot (-1) \equiv -1 \pmod{n};$$
donde segue que n é pseudoprimo forte para a base 6.

6. Basta verificar o que ocorre se calcularmos
$$2^{(2^p-1)-1} = (2^{2^{p-1}-1})^2$$
módulo $2^p - 1$. Contudo, pelo teorema de Fermat $2^{p-1} - 1 \equiv 0 \pmod{p}$. A propósito, note que o fato de $2^p - 1$ ser composto significa que $p \neq 2$, tornando possível a aplicação de Fermat acima. Em outras palavras, $2^{p-1} - 1 = rp$ para algum inteiro positivo r. Assim,
$$2^{(2^p-1)} - 1 \equiv (2^{2^{p-1}-1})^2 \equiv (2^p)^{2r} \pmod{2^p - 1}.$$
Como,
$$2^p \equiv 1 \pmod{2^p - 1},$$
concluímos que
$$2^{(2^p-1)} - 1 \equiv (2^p)^{2r} \equiv (1)^{2r} \equiv 1 \pmod{2^p - 1}.$$

Portanto, todas as vezes que $2^p - 1$ for composto, será um pseudoprimo para a base 2.

7. Seja $F(n) = 2^{2^n} + 1$ um número de Fermat composto. Para determinar se é pseudoprimo para a base 2 devemos calcular o resto de $2^{F(n)-1}$ por $F(n)$. Contudo, como $F(n) \equiv 0 \pmod{F(n)}$, obtemos
$$2^{2^n} \equiv -1 \pmod{F(n)}.$$
Por outro lado,
$$F(n) - 1 = 2^{2^n} = 2^{2^n - n} \cdot 2^n$$
de modo que
$$2^{F(n)-1} \equiv 2^{2^{2^n - n} \cdot 2^n} \equiv (2^{2^n})^{2^{2^n - n}} \equiv (-1)^{2^{2^n - n}} \equiv 1 \pmod{F(n)},$$
como queríamos mostrar.