

Teoria de Números Computacional

folha vi

2º semestre, 2006/2007

1. Encontre um sistema reduzido de resíduos dos inteiros
(a) 6 (b) 9 (c) 10 (d) 14 (e) 16 (f) 17
2. Use o Teorema de Euler para encontrar o resto da divisão de 3^{100000} por 35.
3. Use o Teorema de Euler para encontrar o último algarismo de 7^{1000} na representação na base decimal.
4. Use o Teorema de Euler para encontrar o último símbolo na expansão hexadecimal de $5^{1000000}$.
5. Fazendo uso do Teorema de Euler, resolva as congruências lineares
(a) $5x \equiv 3 \pmod{14}$ (b) $4x \equiv 7 \pmod{15}$ (c) $3x \equiv 5 \pmod{16}$
6. Calcule $\phi(n)$ para $13 \leq n \leq 20$.
7. Calcule $\phi(n)$ com $n =$
(a) 100 (b) 256 (c) 1001 (d) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ (e) 10! (f) 20!
8. Mostre que existe uma infinidade de primos, usando a função ϕ de Euler.
[Sugestão: suponha que o conjunto \mathbb{P} dos números primos é finito, e considere $N = \prod_{p_i \in \mathbb{P}} p_i$.
Conclua que $\phi(N) = 1$.]
9. Lehmer conjecturou que n é primo se $\phi(n)$ divide $n - 1$. Teste a conjectura, usando o *pari/gp*.
[Sugestão: `for(i=2,N,n=2*i+1;if((n-1)%eulerphi(n)==0&&!isprime(n),print(n)))`, para N suficientemente grande.]
10. Encontre os primos p e q , sabendo que $n = pq = 14647$ e $\phi(n) = 14400$.
11. Encontre os primos p e q , sabendo que $n = pq = 4386607$ e $\phi(n) = 4382136$.
12. Suponha que um criptanalista encontra um certo $k < n$ que não é primo relativo com $n = pq$ usado no RSA. Mostre que o criptanalista pode quebrar a cifra. Calcule a probabilidade de tal acontecer.