Teoria e História de Números
Teste 2

Jorge Nuno Silva

10 de Janeiro de 2008

1. Prove que

   (a) $\lfloor \frac{n}{2} \rfloor - \lfloor -\frac{n}{2} \rfloor = n\,, \quad \forall n \in \mathbb{N}$.
   (b) $\lfloor x+n \rfloor = \lfloor x \rfloor + n\,, \forall x \in \mathbb{R}\ \forall n \in \mathbb{Z}$.

   Resolução:

   (a) Se n é par tem-se $n = 2k$ para algum k tem-se $\lfloor \frac{n}{2} \rfloor = k$ e vem:

   $$\lfloor \frac{n}{2} \rfloor - \lfloor -\frac{n}{2} \rfloor = k - (-k) = 2k = n\,.$$

   Se n é ímpar, $n = 2k+1$, tem-se $\lfloor \frac{n}{2} \rfloor = k$ e $\lfloor -\frac{n}{2} \rfloor = -k-1$ e vem:

   $$\lfloor \frac{n}{2} \rfloor - \lfloor -\frac{n}{2} \rfloor = k - (-k-1) = 2k+1 = n\,.$$

   (b) Seja $\lfloor x \rfloor = k$ e $x = k + \theta$ onde $0 \leqslant \theta < 1$. Então $\lfloor x+n \rfloor = \lfloor k+\theta+n \rfloor = k+n$.

2. Determine o dia da semana do dia em que nasceu.

   Resolução:

   Trata-se de aplicar a fórmula

   $$w \equiv d + \lfloor 2.6m - 0.2 \rfloor - 2c + y + \lfloor \frac{c}{4} \rfloor + \lfloor \frac{y}{4} \rfloor$$

   em que a congruência acima é módulo 6 (Domingo=0, ..., Sábado=6), d é o dia do mês, m é a ordem do mês (Março=1, ..., Fevereiro=12), c é o século ($c \geqslant 16$) e y é o ano ($0 \leqslant y < 100$, se $m = 11$ ou $m = 12$, y é o ano anterior ao real.)

3. Mostre que existe uma infinidade de inteiros n tais que $\varphi(n)$ é um quadrado perfeito.

   Resolução:

   Considere os números da forma $u_k = 2^{2k+1}$. Tem-se $\varphi(u_k) = 2^{2k} = (2^k)^2$.

4. Mostre que se se o inteiro n tem r factores primos ímpares, então $2^r|\varphi(n)$.

   Resolução:

   Se $n = 2^k p_1^{k_1} \cdots p_r^{k_r}$, onde os p_is são primos ímpares (se n for ímpar não se considera o factor inicial 2^k), então, como φ é multiplicativa, tem-se
$$\varphi(n) = 2^{k-1} p_1^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1)$$
   como todos os factores $p_1 - 1$ sãp pares, a conclusão segue-se.

5. Use o Teorema de Euler para mostrar que se $(a, n) = (a - 1, n) = 1$, então
$$a^{\varphi(n)-1} + \cdots + a^2 + a + 1 \equiv 0 \quad (mod\ n)\,.$$

   Resolução:

   Use-se a identidade
$$a^{\varphi(n)} - 1 = (a - 1)(a^{\varphi(n)-1} + \cdots + a^2 + a + 1)$$
   e as hipóteses.

6. Prove que, seja qual for o inteiro positivo a, tanto a como a^{4n+1} terminam no mesmo dígito.

   Resolução:

   Queremos mostrar que $a^{4n+1} \equiv a$ módulo 10. Note que $\varphi(10) = 4$ e aplique o Teorema de Euler.

7. Mostre que se a tem ordem hk módulo n, então a^h tem ordem k módulo n.

   Resolução:

   Claro que $(a^h)^k = a^{hk} \equiv 1$ módulo n. Se $(a^h)^s \equiv 1$ módulo n, com $s < k$ então $a^{hs} \equiv 1$ o que contraria o facto de a ordem de a ser hk, porque $hs < hk$.

8. Mostre que 2 é raiz primitiva de 19 mas não de 17.

   Resolução:

   Calculem-se as potências de 2 módulo 19 e 17. Basta considerar os expoentes divisores de 18 e 16, respectivamente.

9. Dado que 3 é raiz primitiva de 43, determine todos os inteiros positivos menores que 43 cuja ordem módulo 43 é 6.

   Resolução:

   A ordem de 3^h é $\frac{42}{(h,42)}$. Para este número ser 6 tem-se $h = 7$ ou $h = 35$. As soluções são então, módulo 43, 3^7 e 3^{35}, que são, módulo 43, 37 e 7, respectivamente.

10. Use uma tabela de índices para uma raiz primitiva módulo 11 para resolver a congruência $7x^3 \equiv 3 \ (mod\, 11)$.

    Resolução:

    A tabela de índices relativa à raiz primitiva 2:

número	1	2	3	4	5	6	7	8	9	10
índice	10	1	8	2	4	9	7	3	6	5

    A congruência dada é equivalente a $ind(7x^3) \equiv ind(3)$ módulo 10, isto é, $3ind(x) \equiv 1$ módulo 10. Donde, consultando a tabela, $ind(x) \equiv 7$ módulo 10, donde $x \equiv 7$ módulo 11.