Provas de

Teoria dos Números

01/2006

UNIVERSIDADE DE BRASÍLIA
DEPARTAMENTO DE MATEMÁTICA -IE

Brasília, 26 de maio de 2006.

$1^{\underline{a}}$ prova em TEORIA DOS NÚMEROS

$1^{\underline{o}}$ período de 2006
Turma **B** (noturno)

NOME: MATRÍCULA:

RESOLVAM 05 (CINCO) DOS SEGUINTES PROBLEMAS

1) Seja $n \in \mathbb{N}$. Elaborar uma *fórmula fechada* para

$$Q_n = \sum_{k=2n}^{3n} k = 2n + (2n+1) + (2n+2) + \ldots + (3n-1) + 3n\,.$$

2) *Determinar os primos* p para os quais

$$p + 18\,145 \quad \text{seja um } \textit{número triangular}.$$

3) Sejam $a = 10\,187$ e $b = 12\,017$.

   a) Empregar o algoritmo Euclidiano para determinar $d = \mathrm{mdc}(a, b)$ e $m = \mathrm{mmc}(a, b)$.

   b) Deteminar as soluções da equação Diofantina

   $$10\,187x + 12\,017y = 183 \cdot 10^5\,.$$

   que satisfazem $x > y > 0$.

4) Escrever o número $n = 93\,347$ como *diferença de dois quadrados* de todas as maneiras possíveis.

5) Seja p um primo e $n \in \mathbb{N}$.

   Determinar *a maior potência de* p *que divide* $(p^n)!$.

6) Decompor $n = 34\,527\,367$ como *produto de três números primos.*

7) Determinar *todos os triplos Pitagóricos* - primitivos e não-primitivos - da forma

$$(\ \cdot\ ,\ \cdot\ ,\ 125\,)\,.$$

UNIVERSIDADE DE BRASÍLIA
DEPARTAMENTO DE MATEMÁTICA -IE

Brasília, 04 de julho de 2006.

$2^{\underline{a}}$ prova em TEORIA DOS NÚMEROS

$1^{\underline{o}}$ semestre de 2006

Turma B (noturno)

NOME: MATRÍCULA:

RESOLVAM 05 (CINCO) DOS SEGUINTES PROBLEMAS

1) Mostrar: Os números
$$n = 4757 \cdot 2^k$$
são *deficientes* para $0 \leq k \leq 4$ e *abundantes* para $k \geq 5$.
Sugestão : Cuidado, 4757 não é primo!

2) Determinar *todas as soluções* (incongruentes) da congruência
$$923x \equiv 221 \mod 1079 .$$

3) Determinar *todos os números* $n \in \mathbb{Z}$ com $|n| \leq 4 \cdot 10^5$ que deixam os restos $8,\ 11,\ 19,\ 40$ quando divididos por $13,\ 15,\ 28,\ 53$ respectivamente.

4) Seja $p > 2$ um número primo e $a \in \mathbb{Z}$ com $p \nmid a$. Mostrar:

a) $a^{\frac{p+3}{2}} \equiv \pm a^2 \mod p$ *sempre*.

b) $a^{\frac{p+3}{2}} \equiv +a^2 \mod p$ se a é um *resto quadrático* $\mod p$.

c) $a^{\frac{p+3}{2}} \equiv -a^2 \mod p$ se a é um *resto não-quadrático* $\mod p$.

5) Mostrar: *Existem infinitos primos* p da forma
$$p = 10k - 1 \quad (k = 1, 2, 3, \ldots) .$$
Sugestão : Supondo que $\{p_1 = 19,\ p_2 = 29,\ p_3 = 59,\ p_4,\ \ldots,\ p_r\}$ fosse o conjunto de *todos* estes primos, considerar o número
$$N = (2p_1p_2 \ldots p_r)^2 - 5 \in \mathbb{N}.$$

i) Porquê todo divisor primo q de N é $\equiv \pm 1 \mod 10$?
ii) Porquê $q \notin \{p_1, p_2, \ldots, p_r\}$ para todos estes q?
iii) Porquê existe entre estes q pelo menos um que é $\equiv -1 \mod 10$?
iv) Porquê i) - iii) mostram a afirmação ?

6) Mostrar: $\left(\frac{-1}{181}\right) = +1$, porém $\left(\frac{7}{181}\right) = \left(\frac{17}{181}\right) = -1$ e conseqüentemente $\left(\frac{\pm 119}{181}\right) = +1$. *Resolver as congrências*
$$x^2 \equiv -1, \quad x^2 \equiv 119 \ \text{e}\ x^2 \equiv -119 \mod 181.$$

UNIVERSIDADE DE BRASÍLIA
DEPARTAMENTO DE MATEMÁTICA -IE

Brasília, 25 de julho de 2006.

$3^{\underline{a}}$ prova em TEORIA DOS NÚMEROS

$1^{\underline{o}}$ semestre de 2006
Turma B (noturno)

NOME: MATRÍCULA:

RESOLVAM 05 (CINCO) DOS SEGUINTES PROBLEMAS

1) a) Mostrar (ou verificar na tabela) que $p = 5\,153$ é um número primo $\equiv 1 \mod 4$. Escreva-o como *soma de dois quadrados*.

b) Escreva $n = 13\,369$ como *soma de dois quadrados de duas maneiras essencialmente distintas*.

2) a) Escrever $n = 39\,996$ como *soma de quatro quadrados* e
$\frac{n}{2} = 19\,998$ como *soma de três quadrados*.
Porquê n não pode ser escrito como soma de três quadrados?

b) Escrever $n = 7\,387$ como *soma de três quadrados*. Porquê n não pode ser escrito como soma de dois quadrados?

3) Determinar a *decomposição primária* de $\varphi\left(\binom{17}{8}^2\right)$.

4) Seja $p = 71$. *Preencher a tabela*

a	1	2	3	4	5	6	7
$a^2 \equiv ? \mod 71$							
$a^5 \equiv ? \mod 71$							
$a^7 \equiv ? \mod 71$							
$a^{10} \equiv ? \mod 71$							
$a^{14} \equiv ? \mod 71$							
$a^{35} \equiv ? \mod 71$							
$\mathbf{o}_{71}(a) = ?$							

Qual é a *menor raíz primitiva* mod 71 ?

5) Determinar *todas as raízes primitivas* $r \mod 31$ com $1 \leq r \leq 30$ e *todas as raízes primitivas* $r \mod 62$ com $1 \leq r \leq 61$.

6) *Mostrar:*

$$\varphi(n) = \frac{n}{3} \iff n = 2^a \cdot 3^b \ \ com\ \ a, b \geq 1\ .$$