PROBLEMAS DE TEORIA DOS NÚMEROS: DIVISIBILIDADE, CONGRUÊNCIAS, TEOREMA DE EULER-FERMAT

RICARDO BORTOLOTTI

Nestas notas, vamos abordar alguns problemas envolvendo divisibilidade, congruências e o Teorema de Euler. O principal problema que motiva estas notas é o Problema 2 da segunda fase da OBM-U de 2017:

Problema (Problema 2 - OBMU 2017, 2a fase)**.** *Fixados os inteiros positivos a e b, mostre que o conjunto dos divisores primos dos termos da sequência*

$$a_n = a \cdot 2017^n + b \cdot 2016^n$$

é infinito.

Motivados por este problema, vamos listar diversos fatos básicos de Teoria dos Números, incluindo definições, propriedades básicas e teoremas.

Definições.

(1) *Dizemos que d **divide** a (denotado por $d|a$) se existe algum inteiro k tal que $a = kd$.*
(2) *Dizemos que $a \equiv b (\mathrm{mod}\, m)$ (a **é congruente a** b **módulo** m) se m divide $b - a$.*
(3) *O **maior divisor comum** entre a e b (denotado por (a, b)) é o maior inteiro d que divide a e b ao mesmo tempo.*
(4) *Dizemos que p é um **número primo** se os únicos inteiros positivos que dividem p são 1 e p.*
(5) *Dizemos que a e b são **primos entre si** se o maior divisor comum entre a e b é igual a 1.*
(6) *A **função phi de Euler** é definida por $\varphi(n) = \#\{a | 1 \leq a \leq n, (a, n) = 1\}$ (isto é, $\varphi(n)$ é a quantidade de números menores que n que são primos entre si com n.*
   Em particular, se p é primo, então $\varphi(p^k) = p^{k-1}(p - 1)$.

Propriedades.

(1) *Se $d|a$ e $d|b$, então $d|ax + by$ para todos inteiros x, y.*
(2) *Se $d|a$, então $|d| \leq |d|$.*
(3) *Se $d|1$, então $d = 1$ ou $d = -1$.*
(4) *Se $d|ab$ e $mdc(d, a) = 1$, então $d|b$.*
(5) *Se $a \equiv b (\mathrm{mod}\, m)$ e $c \equiv d (\mathrm{mod}\, m)$, então $ax + cy \equiv bx + dy (\mathrm{mod}\, m)$, e $ac \equiv bd (\mathrm{mod}\, m)$ para todos inteiros x, y.*
(6) *Se $(c, m) = 1$ e $ac \equiv bc (\mathrm{mod}\, m)$, então $a \equiv b (\mathrm{mod}\, m)$.*
(7) *Se $a \equiv b (\mathrm{mod}\, m_1)$, $a \equiv b (\mathrm{mod}\, m_2)$ e $(m_1, m_2) = 1$, então $a \equiv b (\mathrm{mod}\, m_1 m_2)$.*
(8) *Se $a^x \equiv 1 (mod m)$ e $a^y \equiv 1 (mod m)$, então $a^{(x,y)} \equiv 1 (mod m)$.*
(9) *Se $(m, n) = 1$, então $\varphi(mn) = \varphi(m)\varphi(n)$.*
   Em particular $\varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1)$.
(10) *Se p é primo, então $(a + b)^p \equiv a^p + b^p (\mathrm{mod}\, p)$.*

Exercício 1. *Demonstre as propriedades acima.*

Teoremas.

(1) ***(Divisão euclideana)*** *Dados a, b inteiros, existem únicos inteiros q, r tais que $0 \leq r < |b|$ e $a = bq + r$.*
(2) ***(Bézout)*** *Dados a, b inteiros e $d = (a, b)$, então existem inteiros x, y tais que $d = ax + by$.*
(3) ***(Euclides)*** *Existem infinitos primos.*
(4) ***(Teorema Fundamental da Aritmética)*** *Todo número natural $n \geq 2$ pode ser escrito unicamente na forma*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

aonde $p_1, p_2, \cdots, p_k$ são números primos distintos, $k \geq 1$ e $\alpha_i \geq 1$ para todo i.
(5) ***(Euler)*** *Se a e m são primos entre si, então $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.*
(6) ***(Fermat)*** *Se p é primo e p não divide a, então $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.*
(7) ***(Pequeno teorema de Fermat)*** *Se p é primo, então $a^p \equiv a (\mathrm{mod}\, p)$.*
(8) ***(Wilson)*** *Se p é primo, então $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.*
(9) ***(Teorema chinês dos restos)*** *Se $m_1, \cdots, m_r$ são dois-a-dois primos entre si, então o sistema de equações*

$$\begin{aligned} x &\equiv b_1 (\mathrm{mod}\, m_1) \\ x &\equiv b_2 (\mathrm{mod}\, m_2) \\ &\vdots \\ x &\equiv b_r (\mathrm{mod}\, m_r) \end{aligned}$$

admite solução, que é única módulo $m_1 m_2 \cdots m_r$.

Exercício 2. *Demonstre os teoremas acima (se necessário, consulte algum livro de teoria dos números).*

1. Exercícios (não tão olímpicos)

Exercício 3. *Prove que $2222^{5555} + 5555^{2222}$ é um múltiplo de 7.*

Exercício 4. *Prove que $20^{15} - 1$ é um múltiplo de 31.*

Exercício 5. *Mostre que a equação $x^3 - 117y^3 = 5$ não possui soluções inteiras.*

Exercício 6. *Encontre os últimos dígitos de 3^{2018} na representação decimal.*

Exercício 7. *Encontre todos os inteiros positivos n tais que $2n^2 + 1 | n^3 + 9n - 17$.*

Dica: $|2n^2 + 1| \leq |n^3 + 9n - 17|$ só é válido para poucos valores de n, pois o polinômio de grau 3 cresce mais rápido que o polinômio de grau 2.

Exercício 8. *Determine todos os inteiros x, y tais que $13x + 5y = 1$.*

Exercício 9. *Mostre que* $2^{15}-1$ *e* $2^{10}+1$ *são primos entre si.*

Exercício 10. *Mostre que não existe um inteiro* m *tal que* $103|m^3-2$.

Exercício 11. *Mostre que* $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$ *não é um inteiro se* $n>1$.

2. Problemas com expoente n e o Teorema de Euler

Agora sim, vamos nos focar no tipo de problema que estamos interessados, que são aqueles com expoente n e que podem ser abordados utilizando o Teorema de Euler.

Problema 1 (P2 - OBMU 2017, 2a fase)**.** *Fixados os inteiros positivos* a *e* b*, mostre que o conjunto dos divisores primos dos termos da sequência*

$$a_n = a\cdot 2017^n + b\cdot 2016^n$$

é infinito.

Dica: Prove por absurdo: se $p_1,\cdots,p_r$ *são todos os primos que dividem algum* a_n*, considere* $N=\varphi(p_1^{\alpha_1})\cdots\varphi(p_1^{\alpha_r})$ *para alguma boa escolha de expoentes* $\alpha_1,\cdots,\alpha_r$*. Olhe para* $a_{Nk}(mod p_j^{\alpha_j})$ *e tente obter alguma contradição.*

Problema 2. *Seja* $n>1$*, prove que* n *não divide* 3^n-2^n.

Dica: Se $n>1$*, considere* p *o menor fator primo de* n*, então* $p|3^n-2^n$*. Pelo pequeno teorema de Fermat, também temos* $p|3^{p-1}-2^{p-1}$*. Conclua que* $p|3-2$ *e conclua o problema.*

Problema 3. *Seja* $n>1$*, prove que* n *não divide* 2^n-1.

Dica: A mesma do problema acima.

Problema 4 (P4 - IMO 2005)**.** *Consideremos a sequência infinita* $a_1,a_2,\cdots$ *definida por*

$$a_n = 2^n+3^n+6^n-1$$

para todos $n\geq 1$*. Determine todos os inteiros positivos que são primos entre si com todos os termos da sequência.*

Dica: Sabemos o valor de $a_p(\mathrm{mod}\, p)$*. Que tal investigar* a_{p-1} *ou* $a_{p-2}(\mathrm{mod}\, p)$*?*

O seguinte problema da OBMU também está relacionado com os teoremas de Wilson e o teorema de Euler.

Problema 5 (P3 - OBMU 2016, 2a fase)**.** *Seja* $k\geq 1$ *um inteiro. Definimos a sequência* $(a_n)_{n\geq 0}$ *por* $a_0=0$, $a_1=1$ *e*

$$a_{n+1} = ka_n + a_{n-1}$$

para $n=1,2,\cdots$*. Seja* p *um número primo ímpar. Denote por* $m(p)$ *o menor inteiro positivo* i *tal que* $p|a_i$*. Denote por* $T(p)$ *o menor inteiro positivo tal que para qualquer natural* j *temos* $p|a_{j+T(p)}-a_j$.

i) Mostre que $T(p)\leq m(p)(p-1)$.

ii) Se $T(p) = m(p)(p-1)$*, mostre que*

$$\prod_{1 \leq j \leq T(p)-1 j \neq 0 (\mathrm{mod}\, m(p))} a_j \equiv (-1)^{m(p)-1} (\mathrm{mod}\, p).$$

3. Problemas diversos de teoria dos números

Problema 6 (IMO 1959)**.** *Mostre que a fração* $\dfrac{21n+4}{14n+3}$ *é irredutível para todo inteiro positivo* n*.*

Problema 7. *Mostre que existe um inteiro positivo* n *tal que* 2^n *tenha mais de duas mil casas decimais e tenha entre suas* 2000 *últimas casas decimais* 1000 *zeros consecutivos.*

Dica: olhe para os números $2^{\varphi(5^{2000})}$ *e* $2^{2000+\varphi(5^{2000})}$*.*

Problema 8 (OBM 1991)**.** *Mostre que existe um número da forma* $199\cdots991$*, com mais de dois dígitos* 9*, que é múltiplo de* 1991*.*

Problema 9 (OBM 1998)**.** *Determine todos os primos que são a soma e a diferença de dois primos.*

Problema 10 (OBM)**.** *Encontre todas as soluções da equação* $n^a + n^b = n^c$*, para* n, a, b *e* c *estritamente positivos.*

Problema 11 (IMO 1994)**.** *Determine todos os pares de inteiros positivos* m *e* n *para os quais* $\dfrac{n^3+1}{mn+1}$ *é inteiro.*

Problema 12 (P4 - OBMU 2009, 1a fase)**.** *Determine a quantidade de números inteiros positivos* n *menores ou iguais a* $31!$ *tais que* $3^n + n$ *é divisível por* 31*.*

Dica: $3^n + n (\mathrm{mod}\, 31)$ *é periódica com período divisor de* $930 = 30 \cdot 31$*. Pelo teorema chinês dos restos, para cada* $0 \leq a \leq 29$ *e* $0 \leq b \leq 30$ *existe um único* $c \in [0, 929]$ *tal que* $3^c + c \equiv 3^a + b (\mathrm{mod}\, 31)$*.*

Problema 13 (P4 - OBMU 2007, 1a fase)**.** *Seja* a *um inteiro não-nulo. Prove que se* a *é uma* n*-ésima potência módulo* $4a^2$ *(ou seja, existe algum* b *inteiro tal que* $a - b^n$ *é um múltiplo de* $4a^2$*), então* a *é uma* n*-ésima potência.*

Dica: Se $a \equiv b^n (\mathrm{mod}\, 4a^2)$*, escreva* $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *e* $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$*. Então existe* k *tal que* $p_1^{\alpha_1} \cdots p_r^{\alpha_r} = p_1^{n\beta_1} \cdots p_r^{n\beta_r} + 4k p_1^{2\alpha_1} \cdots p_r^{2\alpha_r}$*, daonde podemos concluir que* $n\beta_j = \alpha_j$*.*

Problema 14 (P2 - OBMU 2001, 1a fase)**.** *Seja* $s(n)$ *a soma dos algarismos de* n*. Assim, por exemplo,* $s(77) = 14$ *e* $s(2001) = 3$*. Diga se existe um inteiro positivo* n *com* $s(n) = 10$ *e* $s(n^2) = 100$*. Se não existir, demonstre este fato. Se existir, dê um exemplo.*