Engenharia dos Números

Ramyro Corrêa

1 Introdução

Em muitos problemas de Teoria dos Números, é normal o problema nos dar uma propriedade que é válida para todos os inteiros positivos n. Geralmente, ou queremos achar alguma contradição, ou queremos chegar em alguma família de soluções específica. Para isso, é importante escolher números "espertos" de modo que essa escolha implica no que nós queremos provar. Para realizar esse tipo de escolha, ferramentas como as abaixo são comuns:

- **Teorema Chinês dos Restos:** Se $d_1, d_2, ..., d_N$ são inteiros positivos dois a dois coprimos, e $a_1, a_2, ..., a_N$ são inteiros quaisquer, o sistema

$$X \equiv a_1 \pmod{d_1},$$

$$X \equiv a_2 \pmod{d_2},$$

$$...,$$

$$X \equiv a_N \pmod{d_N}$$

  tem solução única $\pmod{d_1 d_2 ... d_N}$.

  Muitas vezes, é comum tomarmos um produto de números primos e somarmos 1 (isso faz que esse número seja coprimo com todos os primos no produtório).

- **Indução esperta:** A ideia é usar indução forte e tomar um número esperto menor que n (em alguns problemas, é interessante tomar $\phi(n)$).

- **LTE:** Se p é um primo ímpar e a, b são inteiros tais que $p \not| a, b$ e $p | a - b$, então $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$, onde $v_p(m)$ é o maior número inteiro tal que $p^{v_p(m)}$ divide m. A fórmula é análoga para $v_p(a^n + b^n)$ se n é ímpar.

- **Teorema de Dirichlet:** Se a, b são inteiros positivos coprimos, então a progressão aritmética $a + nb$ contém infinitos números primos (em muitos casos tomamos $a = 1$).

- **Teorema de Zsigmondy:** Sejam $a > b \geq 1$ inteiros coprimos, e seja $n \geq 2$ um inteiro. Então, $a^n - b^n$ possui um fator primo que não divide $a^k - b^k$ para todo $1 \leq k \leq n - 1$, exceto quando $n = 2$ e $a + b$ é uma potência de 2, ou $(a, b, n) = (2, 1, 6)$.

2 Exemplos

Exemplo 1 Para todo inteiro positivo n, prove que existem n números consecutivos de modo que nenhum deles seja um número primo.

Solução: Quando pensamos em um número composto, é intuitivo pensarmos em um número com muitos divisores. Um dos primeiros números com muitos divisores que vem na cabeça é $n!$. Daí, quando somamos qualquer inteiro positivo $m \leq n$ a $n!$, o número $n!+m$ não é primo, pois $m|n!$ e $m|m$, logo $m|n!+m$. Então, os números $n!+2, n!+3, ..., n!+n$ não são primos e são consecutivos, mas só temos $n-1$ números consecutivos. Para adaptarmos, basta então considerarmos os números $(n+1)!+2, (n+1)!+3, ..., (n+1)!+n+1$, e o problema está resolvido!

Exemplo 2 Seja p um número primo e a um inteiro não divisível por p. A sequência $\{a_n\}_{n=1}^{\infty}$ satisfaz $a_1 = a$ e $a_{n+1} = a^{a_n}$ para todo $n \geq 1$ inteiro. Prove que $\{a_n\}_{n=1}^{\infty}$ é eventualmente constante módulo p.

Solução: Aqui, vamos generalizar o problema para qualquer n ao invés de somente para primos p. Provemos o problema por indução em n. Se $n = 1$, então a sequência é 0 módulo 1. Se $n = 2$, o problema também é obviamente válido. Agora, provemos para um n genérico. Por hipótese, sabemos que $\{a_n\}_{n=1}^{\infty}$ é eventualmente constante módulo $\phi(n)$. Isso significa que existe c e K tal que para todo $k \geq K$, temos que $a_k \equiv c \pmod{\phi(n)}$. Porém, pelo Teorema de Euler, temos que $a^{\phi(n)} \equiv 1 \pmod{n}$, o que significa que $a^k \equiv a^{k+l\phi(n)} \pmod{n}$, para qualquer l inteiro. Então o resto de a^k módulo n é igual a a^{k_0}, onde k_0 é o resto de k módulo $\phi(n)$. Portanto, para todo $k \geq K$

$$a_{k+1} = a^{a_k} \equiv a^c \pmod{n}$$

o que significa que para todo $k > K$, a_k é igual a a^c módulo n, que é constante, e o problema acabou!

Exemplo 3 (IMO SL 2007/N2) Sejam $b, n > 1$ inteiros. Suponha que para cada $k > 1$ inteiro existe um inteiro a_k tal que $b - a_k^n$ é divisível por k. Prove que $b = A^n$ para algum inteiro A.

Solução: Esse é aquele tipo de problema em que temos que forçar o lado direito da divisibilidade a ser algo fixo, assim podemos tomar o lado esquerdo da divisibilidade suficientemente grande, o que obriga o lado direito a ser igual a 0. Mas como fazer isso nesse problema? Façamos o básico:

Seja $b = p_1^{e_1} p_2^{e_2} ... p_t^{e_t}$ a fatoração de b em primos. Tomando k para ser um p_i^m, temos que $p_i^m | b - a_{p_i^m}^n$. Como $p_i | b$, então $p_i | a_{p_i^m}^n$. Além disso, temos que

$m = \nu_{p_i}(p_i^m) \leq \nu_{p_i}(b - a^n_{p_i^m})$ $(*)$. Suponha que $\nu_{p_i}(b) \neq \nu_{p_i}(a^n_{p_i^m})$. Tomando m suficientemente grande, $\nu_{p_i}(b - a^n_{p_i^m})$ também tem que crescer, por $(*)$. Mas como $\nu_{p_i}(b) = e_i$ é fixo, e $\nu_{p_i}(b) \neq \nu_{p_i}(a^n_{p_i^m})$, isso não pode acontecer, o que é um absurdo. Logo $e_i = \nu_{p_i}(b) = \nu_{p_i}(a^n_{p_i^m}) = n\nu_{p_i}(a_{p_i^m})$, então $n|e_i$ para todo $i = 1, 2, ..., t$. Isso implica que $b = A^n$ para algum A inteiro, como queríamos!

Exemplo 4 (IMO SL 2005/N6) Sejam a, b inteiros positivos tais que $a^n + n|b^n + n$ para todos os inteiros positivos n. Prove que $a = b$.

Solução: Assim como o exemplo anterior, a ideia desse problema é forçar o lado direito da divisibilidade a ser algo fixo, de modo que possamos forçar o lado esquerdo a crescer, obrigando o lado direito a ser 0. Por óbvio, como $a^n + n|b^n + n$, então $a^n + n|b^n + n - (a^n + n) = b^n - a^n$. Então, se o lado direito da divisibilidade for 0, temos $a = b$, como queremos.

Quando temos variáveis nos expoentes, é sempre interessante introduzir números primos, pois temos mais controle do problema olhando módulo p. Esse caso não é diferente. Veja que, pelo Teorema de Fermat, se p é um primo coprimo com a, e $N - 1$ é um múltiplo de $p - 1$, então para p dividir $a^N + N \equiv a + N \pmod{p}$, basta tomarmos $N \equiv -a \pmod{p}$. Mas esse N existe pelo Teorema Chinês, isto é, um N tal que $N \equiv 1 \pmod{p-1}$ e $N \equiv -a \pmod{p}$. Portanto, tome esse N. Temos que $p|a^N + N|b^n + n \implies p|b^N + N - (a^N + N) = b^N - a^N$. Porém, pelo Teorema de Fermat, como $p - 1|N - 1$, temos que $b^N - a^N \equiv b - a \pmod{p}$. Daí, como p apenas é um número primo coprimo com a, b, podemos tomá-lo para ser arbitrariamente grande, o que implica que $b - a = 0 \implies a = b$, como queríamos!

Exemplo 5 (IMO 2000/5)

Determine se existe um inteiro positivo n com exatamente 2000 fatores primos distintos tal que $n|2^n + 1$.

Solução: A resposta é sim.

O primeiro passo desse problema é perceber que n deve ser um número ímpar, caso contrário um número par estaria dividindo um número ímpar, uma contradição. Daí, como n é ímpar, então $2^n + 1$ é um múltiplo de 3. Agora vamos à parte divertida:

Se p é um primo que divide n e $n|2^n + 1$, então $\nu_p(n) \leq \nu_p(2^n + 1)$. Tomando $p = 3$, podemos usar o LTE: $\nu_3(n) \leq \nu_3(2^n + 1) = \nu_3(n) + \nu_3(2 + 1) = \nu_3(n) + 1$. De fato, para todo e inteiro positivo, $3^e|2^{3^e k} + 1$, para todo k inteiro positivo, pelo fato mencionado acima. Então, se escolhermos um inteiro positivo k (não divisível por 3) com exatamente 1999 fatores primos distintos tal que $k|2^{3^e k} + 1$, temos que $3^e k|2^{3^e k} + 1$, o que acaba com o problema, pois basta tomar $n = 3^e k$.

O fato de escolhermos potências de 3 não é à toa. Veja que para todo $1 \leq i \leq e$,

$2^{3^i}+1|2^{3^e}+1$. Então, se para cada fator $2^{3^i}+1$ conseguirmos associar um primo p_i tal que $p_i|2^{3^i}+1$, de modo que todos esses primos sejam distintos, conseguimos muitos fatores primos distintos. E é possível fazer tal escolha pelo Teorema de Zsigmondy! Então, tomando $e > 2000$, conseguimos selecionar os primos $p_1, p_2, ..., p_{1999}$ de modo que para todo $1 \leq i \leq 1999$, $p_i|2^{3^i}+1|2^{3^e}+1|2^{3^e k}+1$, onde $k = p_1 p_2 ... p_{1999}$. Então, $n = 3^e k$ possui exatamente 2000 fatores primos distintos e satisfaz $n|2^n+1$.

3 Problemas

Problema 1. (USAMO 2017/1) Prove que existem infinitos pares de inteiros positivos coprimos $a, b > 1$ satisfazendo $a+b|a^b+b^a$.

Problema 2. (OBM 2011/4) Existem inteiros positivos $a_< a_2 < ... < a_{2011}$ tais que o $mdc(a_i, a_j) = a_j - a_i$ para todos $1 \leq i < j \leq 2011$?

Problema 3. (OBM 2014/2) Encontre todos os inteiros n, $n > 1$, com a seguinte propriedade: para todo k, $0 \leq k < n$, existe um múltiplo de n cuja a soma dos dígitos deixa resto k na divisão por n.

Problema 4. (Cone Sul 2013/5) Seja $d(k)$ o número de divisores positivos de um inteiro k. Um inteiro positivo n é dito balanceado se $d(n-1) \leq d(n) \leq d(n+1)$ ou $d(n-1) \geq d(n) \geq d(n+1)$. Mostre que existem infinitos números balanceados.

Problema 5. (IMO SL 2014/N4) Seja $n > 1$ um inteiro. Prove que existem infinitos inteiros $k \geq 1$ tais que

$$\lfloor \frac{n^k}{k} \rfloor$$

é um número ímpar.

OBS: Dado um número real x, definimos $\lfloor x \rfloor$ como sendo o maior inteiro que não supera x. Por exemplo, $\lfloor 3,4 \rfloor = 3$ e $\lfloor -2,8 \rfloor = 2$.

Problema 6. (USA TST 2007/4) Determine se existem inteiros positivos a, b tais que a não divide $b^n - n$ para todos os inteiros positivos n.

Problema 7. (China TST 2018/2/4) Sejam k, M inteiros positivos tais que $k-1$ não é livre de quadrados. Prove que existe um real positivo α tal que $\lfloor \alpha k^n \rfloor$ são relativamente primos entre si para todo inteiro positivo n.

OBS: Dado um número real x, definimos $\lfloor x \rfloor$ como sendo o maior inteiro que não supera x. Por exemplo, $\lfloor 3,4 \rfloor = 3$ e $\lfloor -2,8 \rfloor = 2$.

Problema 8. (OBM 2015/3)

Seja $n > 1$ um inteiro positivo e $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ sua fatoração em primos. Então, definimos a falsa derivada de n como sendo

$$f(n) = \alpha_1 p_1^{\alpha_1 - 1} \alpha_2 p_2^{\alpha_2 - 1} ... \alpha_k p_k^{\alpha_k - 1}$$

. Prove que existem infinitos inteiros positivos n tais que $f(n) = f(n-1) + 1$.

4 Dicas e soluções

Problema 1. Teste o par $(n, n+2)$ para um n genérico e veja em quais casos esse par funciona.

Problema 2.

- Faça indução em n;
- Veja uma condição necessária e suficiente para termos $mdc(a_i, a_j) = a_j - a_i$;
- Procure um inteiro positivo N tal que se tomarmos $b_i = a_i + N$, a condição do problema continua sendo válida;
- Escolha N de modo que conseguimos adicionar ele ao conjunto $\{b_1, b_2, ..., b_n\}$ e, consequentemente, completar a hipótese;
- Conclua o problema.

Problema 3.

- A resposta é todo n não divisível por 3;
- Prove e use o lema que se $S(N)$ denota a soma dos dígitos de N, então, para todo k inteiro positivo e $1 \leq N \leq 10^k - 1$, $S(N(10^k - 1) = 9k$;
- Juntamente com o lema acima, use o fato de que 9 e n são coprimos e conclua o problema.

Problema 4.

- Assuma que o problema não seja válido;

- Encontre um conjunto de números N tal que $d(N)$ seja pequeno;
- Use o Teorema de Dirichlet para conseguir estimar $d(p-1)$ ou $d(p+1)$.

Problema 5.
- Tome k como sendo um primo $p > n$. Dessa forma, $\lfloor \frac{n^p}{p} \rfloor = \lfloor \frac{n^p - n}{p} + \frac{n}{p} \rfloor = \frac{n^p - n}{p}$, que é um inteiro, pelo Pequeno Teorema de Fermat;
- Separe o problema em n par e n ímpar e tente adaptar a ideia acima. O caso n ímpar não é difícil. Tente você mesmo! Se n for par, tome p um primo que divide $n-1$ e $k = p^t \implies \lfloor \frac{n^{p^t}}{p^t} \rfloor = \lfloor \frac{n^{p^t} - 1}{p^t} \rfloor$. Como isso conclui esse caso?

Problema 6.
- Generalize o exemplo 2 e veja como que isso acaba com o problema.

Problema 7.
- Esse problema não é fácil! O primeiro passo é enxergar α na base k, pois temos mais controle ao multiplicarmos α por k^n.
- Tente construir um α no qual os dígitos na base k fiquem controláveis. Uma maneira disso é tomar $\alpha = [N, ddd...]_k$, onde N é um inteiro e $d < k$ é um inteiro positivo, pois daí temos que $\alpha = N + d(\frac{1}{k} + \frac{1}{k^2} + \frac{1}{k^3} + ...) = N + d\frac{1}{k-1} = N + \frac{d}{k-1}$.
- Então, $\lfloor k^n \alpha \rfloor = \lfloor k^n N + d\frac{k^n}{k-1} \rfloor$. Como $k^n N$ é inteiro e $k-1 | k^n - 1$, temos que tal parte inteira é igual a $k^n N + \frac{d(k^n-1)}{k-1} = \frac{k^{n+1}N - k^n N + dk^n - d}{k-1}$. Agora, vamos tentar escolher um d mais esperto em função de k. Tomemos $d = \frac{k-1}{l}$ para algum l inteiro positivo que divide $k-1$. Dessa forma, $\lfloor k^n \alpha \rfloor = k^n N + \frac{k^n - 1}{l} = \frac{k^n(Nl+1)-1}{l}$.
- A partir de agora, como estamos lidando com divisibilidades, é interessante tomar $l = p$, onde p é um número primo. Pelo enunciado, existe um $p | k-1$ tal que $p^2 | k-1$. Tome esse primo em específico. Agora, o próximo passo é escolher um N de modo que $\frac{k^n(Np+1)-1}{p}$ seja coprimo com M. Dito isso, é interessante tomar tal N de modo que o denominador de $\frac{k^n(Np+1)-1}{p}$ seja constante. Você pode fazer isso tomando um divisor primo q de M e usando o Teorema Chinês dos Restos. Mas e se $p | M$?
- Force o numerador de $\frac{k^n(Np+1)-1}{p}$ a não ser divisível por p^2 e conclua o problema.

Problema 8.

- Fixe um inteiro positivo k e encontre um par de números coprimos a,b tal que $f(a)=k$ e $f(b)=k-1$. Pelo Teorema de Bézout, existem inteiros positivos c,d tais que $ac-bd=1$.
- Veja que se c,d forem livre de quadrados, $f(ac)=f(a)=k$ e $f(ac-1)=f(bd)=f(b)=k-1$. Portanto, se encontrarmos infinitos c,d livre de quadrados que satisfazem $ac-bd=1$, o problema acabou.
- Lembre-se que se c_0,d_0 é a solução minimal de $ac-bd=1$, então as soluções (c,d) dessa equação são dadas por $(c,d)=(bk+c_0,ak+d_0)$, para todo k inteiro positivo.
- Portanto, queremos provar que existem infinitos pares de inteiros positivos tais que $bk+c_0$ e $ak+d_0$ são livre de quadrados.
- É um fato conhecido que $\sum_{p\text{primo}}\frac{1}{p^2}<-\frac{1}{1^2}+\frac{1}{2^2}+\sum_{n>0}\frac{1}{n^2}-\sum_{2|n}\frac{1}{n^2}=-\frac{1}{1^2}+\frac{1}{2^2}+\frac{\Pi^2}{6}-\frac{1}{4}\frac{\Pi^2}{6}=\frac{3}{4}\frac{\Pi^2}{6}<-\frac{3}{4}+\frac{5}{4}=\frac{1}{2}$, ou seja, a densidade dos inteiros positivos livres de quadrados é maior que $\frac{1}{2}$.
- Adapte a prova acima para as progressões aritméticas $bk+c_0$ e $ak+d_0$. Se para todo k suficientemente grande, no máximo um dentre $bk+c_0$ e $ak+d_0$ for livre de quadrados, a densidade dos números livre de quadrados em ambas as PAs seria menor do que $\frac{1}{2}$.
- Veja como o fato apontado acima é um absurdo e conclua o problema.