Técnicas para problemas de mdc e divisibilidade

Andrey Chen

Técnica 1: Força bruta para cada fator primo

Lembramos que $v_p(n) := \max \alpha$ t.q. $p^\alpha | n$. Às vezes é útil contar os fatores primos diretamente.

Exemplo: A demonstração da irracionalidade de $\sqrt[n]{2}$. Se $\sqrt[n]{2} = \frac{p}{q}$ então $p^n = 2q^n$ e portanto $nv_2(p) = v_2(p^n) = v_2(2q^n) = 1 + nv_2(q)$ logo $n|1$, absurdo!

Outro exemplo: A demonstração de $mdc(a,b) \cdot mmc(a,b) = a \cdot b$. Sendo p um primo qualquer fixado, $\alpha = v_p(a), \beta = v_p(b)$, e assumindo s.p.g $\alpha \leq \beta$, temos que $v_p(mdc(a,b)) = \alpha$, $v_p(mmc(a,b)) = \beta \Rightarrow v_p(mdc(a,b)mmc(a,b)) = v_p(ab)$ e o resultado segue.

Agora alguns problemas para praticar!

1. a) Prove que $abc | mdc(a,b,c)mmc(a,b,c)^2$

   b) Prove que $abc = mdc(a,b,c)mmc(a,b,c)mmc(mdc(a,b), mdc(b,c), mdc(a,c))$

   c) Obtenha e demonstre uma expressão análoga para o produto de n variáveis.

2. Seja $S := \{2^n - 3 | n \in \mathbb{N}\}$. Prove que existe um subconjunto infinito $R \subset S$ tal que $mdc(x,y) = 1 \, \forall x \neq y \in R$.

   (Bônus: generalize o problema substituindo o 3 por um inteiro M fixo. Encontre condições simples para M funcionar.)

3. Prove que, para quaisquer $n, k > 1$, o racional $H_{n,k} := \frac{1}{n} + \frac{1}{n+1} + \ldots + \frac{1}{n+k}$ não é inteiro.

   (Bônus: generalize o problema colocando numeradores coprimos em cada fração. Que condições adicionais são necessárias?)

4. (Lifting the Exponent, ou LTE) a) Seja p primo ímpar, e a, b naturais com $p \nmid a, p | a - b$. Então $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$.

   b) Sejam a, b naturais com $2 \nmid a, 4 | a - b$. Então $v_2(a^n - b^n) = v_2(a - b) + v_2(n)$

   c) Encontre todas as trincas de inteiros não-negativos (x, y, z) tais que $3^x - 1 = 2^y 7^z$.

5. Prove que existem infinitos primos p que dividem algum número da forma $1! + 2! + \ldots + n!$ para $n \geq 1$.

6. Encontre todos os naturais n tais que existem x_n, y_n inteiros positivos satisfazendo $x_n^2 + y_n^2 = 2^n + 1$.

Técnica 2: Aritmética Polinomial

É importante lembrar que os polinômios de coeficientes racionais (ou reais, ou inteiros) formam um conjunto com propriedades similares aos inteiros. É possível fazer divisão com resto (no mínimo, para divisores mônicos), calcular mdc's e até usar o teorema fundamental da aritmética!

Exemplo: Vamos calcular $mdc(x^4-16, 2x^2-3x-2)$. Por brevidade, vamos omitir o mdc e denotar apenas os parêntesis. O algoritmo de Euclides nos dá $(x^4-16, 2x^2-3x-2) = (2x^2-3x-2, \frac{51}{8}x - \frac{51}{4}) = (\frac{51}{8}x - \frac{51}{4}, 0)$. Nos racionais, lembre que o mdc é mônico por definição, e portanto cortamos o fator $\frac{51}{8}$ para obter $x-2$.

Note que raízes comuns geram fatores comuns. Isso acontece por conta do seguinte lema importante:

Lema do resto: Seja $P(x)$ um polinômio e r um real. Então o resto da divisão de $P(x)$ por $x-r$ é $P(r)$.

Demonstração: Se $P(x) = (x-r)Q(x) + R(x)$ então $P(r) = 0 + R(r)$ e portanto $R(r) = P(r)$. Porém, R é constante pois $R = 0$ ou $degR < deg(x-r) = 1$. O lema segue.

Corolário importante: $P(r) = 0 \Leftrightarrow x - r | P(x)$.

Existe outra maneira de visualizar o lema do resto, e ela complementa a ideia de igualdade entre polinômios e números. Vamos aplicar congruência:

Demonstração 2: Note que $x \equiv r \,(mod\, x-r)$, por definição. Isso implica que $P(x) = \sum a_n x^n \equiv a_n r^n = P(r) \,(mod\, x-r)$ e portanto $x - r | P(x) - P(r)_\square$

Vamos abrir um pequeno parêntesis e comentar brevemente a utilidade de derivadas nesse tipo de análise.

Definição: (simplificada) A *derivada* de um polinômio $P(x) = \sum a_n x^n$ é o polinômio $P' = \sum n a_n x^{n-1}$.

Alguns exercícios simples para praticar essa ideia:

1. Prove que para quaisquer dois polinômios f, g vale a identidade $(fg)' = f'g + fg'$.

2. a) Prove que P tem uma raiz dupla se, e somente se, P e P' têm uma raiz comum.

   b) Prove que P tem uma raiz com multiplicidade n se, e somente se, P e suas primeiras $n-1$ derivadas têm todos uma mesma raiz comum.

3. Encontre todos os pares de reais a, b tais que $x^2 + ax + b$ é tangente à reta $2x + 3$.

Vamos voltar a estudar o mdc de polinômios. Convém agora olhar quem são os primos no conjunto dos polinômios.

Definição: Um polinômio não-constante f é *irredutível* sobre um conjunto S se $g|f$, $g \in S$ implica g constante ou $g \propto f$ (Em termos leigos, polinômios irredutíveis não têm fatores próprios)

Nos complexos, por conta do teorema fundamental da álgebra, os únicos irredutíveis sobre $\mathbb{C}[x]$ são os polinômios lineares.

Nos reais, por conta do mesmo resultado anterior, os irredutíveis são os polinômios lineares e os quadráticos com $\Delta < 0$.

Já nos outros conjuntos, temos exemplos mais interessantes. Seguem alguns exercícios para praticar.

4. Mostre que $x^3 - 2$ e $x^4 + 1$ são irredutíveis sobre $\mathbb{Q}[x]$.

5. Seja P um polinômio de coeficientes inteiros tal que $P(\sqrt{2}+\sqrt{5})$ é inteiro. Prove que $P(\pm\sqrt{2} \pm \sqrt{5})$ é inteiro para qualquer escolha de sinais.

6. Sejam P, Q polinômios de coeficientes racionais que são irredutíveis sobre $\mathbb{Q}$. Sejam α real, r racional tais que $P(\alpha) = 0 = Q(r - \alpha)$. Prove que $P^2 - Q^2$ admite raiz racional.

Vamos juntar tudo para os seguintes problemas.

7. Encontre todos os polinômios P tais que $P(n)|P(2n)$ para infinitos inteiros n.

8. Sejam α um real, f polinômio de coeficientes inteiros tais que $\alpha^3 - 21\alpha = (f(\alpha))^3 - 21f(\alpha) = 7$. Mostre que a sequência $\alpha, f(\alpha), \dots f^n(\alpha) \dots$ é eventualmente periódica.

9. Mostre que não existe um par de polinômios não-constantes P, Q tal que $P^{10} + P^9 = Q^{21} + Q^{20}$.

10. Seja $f(x)$ um polinômio irredutível sobre os inteiros, com $f(0) = 2021$. Mostre que $f(x^2)$ é irredutível. **(Dica que eu tenho que tirar: lema do ab=cd)**

Técnica 3: "Exagerando" nossas proposições

Algumas vezes é muito mais simples calcular um mdc de maneira implícita. O seguinte lema e exemplo ilustram bem essa possibilidade:

Lema: Para quaisquer a, b, c, temos que $mdc(a, b)|mdc(a, bc)$. Além do mais, $mdc(a, bc)|mdc(a, b)mdc(a, c)$.

A demonstração pode ser feita, por exemplo, por inspeção direta dos expoentes como na primeira seção.

Exemplo: Calcule $mdc(x^{12} - x^3 - 2x^2 - 1, x^4 - x^2 + 1)$.

Basta observar que $x^4 - x^2 + 1|x^6 - 1|x^{12} - 1$ e temos que $mdc(x^{12} - x^3 - 2x^2 - 1, x^4 - x^2 + 1)|mdc(x^{12} - x^3 - 2x^2 - 1, x^{12} - 1) = mdc(x^12 - 1, x^3 + 2x^2)|mdc(x^12 - 1, x^2)mdc(x^12 - 1, x + 2) = 1$. O único divisor mônico de 1 é 1 e o resultado segue.

Isso vai além de poupar trabalho em contas; chutar o valor do mdc permite uma rota direta por uma definição alternativa.

Lema: $mdc(a, b)$ é o único inteiro positivo d com a seguinte propriedade:

- $d|a\,, d|b$
- Se $n|a\,, n|b$ então $n|d$

A demonstração é simples e fica a cargo do leitor.

Para uma aplicação do lema, considere o seguinte exemplo:

Exemplo: Prove que, para todos $a, b > 0$, vale $mdc(2^a - 1, 2^b - 1) = 2^{mdc(a,b)} - 1$.

Demonstração: Como $2^x - 1|2^{kx} - 1$, por fatoração direta, temos que $2^{mdc(a,b)} - 1|2^a - 1, 2^b - 1$.

Por outro lado, se $d|2^a - 1, 2^b - 1$ então $d|2^a - 2^b$ e portanto, como d é ímpar, $d|2^{|a-b|} - 1$. Seguindo o algoritmo de Euclides nos expoentes obtemos diretamente que $d|2^{mdc(a,b)} - 1$. Como $2^{mdc(a,b)} - 1$ é positivo, temos pelo lema que este é o mdc pedido, conforme queríamos demonstrar.

Não devemos esquecer do importante teorema de Bezout-Bachet!

Exemplo: Mostre que a fração $\frac{21n+4}{14n+3}$ é sempre irredutível.

Demonstração: Basta ver que $3 \cdot (14n+3) - 2 \cdot (21n+4) = 1$. Pelo teorema de Bezout-Bachet, isso implica que $mdc(14n + 3, 21n + 4) = 1$ e acabamos.

Outro tipo de "exagero" bem comum é a desigualdade básica para divisibilidades. Frequentemente acontece em problemas de uma simples cota limitar fortemente as possibilidades para as variáveis.

Lema: Se $a|b$ então $b = 0$ ou $|a| \leq |b|$.

Exemplo: Encontre todos os pares de inteiros (m, n) com $m^4 + n^4|m^3n + mn^3 - 1$.

Demonstração: Se $m^4+n^4|m^3n+mn^3-1$ então $m^4+n^4 \leq |m^3n+mn^3-1|$. O lado esquerdo é igual a $m^3n + mn^3 - 1$ se m, n têm o mesmo sinal, e igual a $-mn^3 - m^3n + 1$ se m, n têm sinais diferentes.

No primeiro caso, temos que $m^4+n^4 \leq m^3n+mn^3-1 \Leftrightarrow (m-n)(m^3-n^3) \leq -1$, que é impossível, ou $m^3n + mn^3 = 1$.

No segundo caso, temos $m^4+n^4 \leq -mn^3-m^3n+1 \Leftrightarrow (m+n)(m^3+n^3) \leq 1$, ou novamente $m^3n + mn^3 = 1$.

Como $(m \pm n)(m^3 \pm n^3)$ é sempre não-negativo, já que as parcelas têm o mesmo sinal, sobram os casos:

- $(m + n)(m^3 + n^3) = 0$ e portanto $m = -n$ que nos dá $2n^4| - 2n^4 - 1$ que não tem solução.
- $m^3n + mn^3 = 1 \Leftrightarrow mn(m^2 + n^2) = 1$ e portanto $m^2 + n^2 = 1$ que nos dá os pares $(0, \pm 1), (\pm 1, 0)$
- $(m + n)(m^3 + n^3) = 1$ e portanto $m + n = \pm 1$, $m^2 - mn + n^2 = 1 \Rightarrow (m + n)^2 - 3mn = 1$, de onde $3mn = 0$, que dá os casos já vistos antes.

Portanto esses são todos os pares.
Agora vamos juntar tudo para esses problemas.

1. (Lema de ab=cd) a) Sejam a, b, c, d tais que $ab = cd$, $mdc(a, c) = 1 = mdc(b, d)$. Então $a = d$ e $b = c$. Ou seja, se tivermos duas categorias de números sem fator comum, digamos esquerda e direita, então a decomposição de um inteiro em esquerda vezes direita é única (se existir).

   b) Sejam a, b, c, d inteiros tais que $ab = cd$. Mostre que existem inteiros x, y, z, w tais que $a = xy, b = zw, c = xz, d = yw$.

2. O n-ésimo polinômio ciclotômico $\Phi_n(x)$ é definido recursivamente por $\Phi_1(x) := x - 1$ e $\prod_{d|m} \Phi_d(x) = x^m - 1$ para todo $m > 1$.

   Mostre que $mdc(\Phi_n(x), \Phi_k(x)) = 1$ se $n \neq k$.

3. Calcule $mdc(a^n + 1, a^m + 1)$, onde $a > 1$.

4. a) Mostre que, para todos $a, n > 1$ inteiros, vale $n|\phi(a^n - 1)$.

   b) Mostre que não existe inteiro n para o qual $n|2^n - 1$.

   c) Encontre todos os inteiros n tais que $n^2|2^n + 1$.

   d) Encontre todos os pares de inteiros positivos (n, p) com p primo, $n \leq 2p$ e tais que $n^{p-1}|(p - 1)^n + 1$.

5. a) Encontre todos os pares de inteiros positivos (x, y) com $xy^2+y+7|x^2y+x+y$.

   b) Encontre todos os pares de inteiros positivos (a, b) com $2ab^2-b^3+1|a^2$.

   c) Encontre todas as triplas de inteiros positivos (a, b, c) com $(a - 1)(b - 1)(c - 1)|abc - 1$.

6. Sejam x, y inteiros positivos com $2^n y - 1|x^{2^n} - 1$ para todo $n \geq 1$. Mostre que $x = 1$.

   (Bônus: você consegue fazer o problema com $2^n y + 1$ ao invés de $2^n y - 1$?)

Problemas miscelâneos

Aqui vale de tudo, até o que não está na lista! Essa é a seção de bônus para quem quer alguns problemas extras para pensar.

1. Sejam $p_1 = 2, p_2 = 3, \ldots$ os primos. Para cada n, mostre que existem infinitas $n + 1$-uplas $(y, x_1, \ldots, x_n)$ de inteiros positivos tais que $y^2 = x_1^{p_1} + x_2^{p_2} + \ldots + x_n^{p_n}$.

2. Sejam a, b inteiros positivos tais que $a^n + n|b^n + n$ para todo $n > 0$. Prove que $a = b$.

3. Mostre que para qualquer sequência crescente de inteiros positivos a_n satisfazendo $0 < a_{k+1} - a_k \leq 2021$, existem infinitos pares de índices distintos (x, y) com $a_x | a_y$.

4. Uma fração é dita *egípcia* se tiver numerador 1. Prove que, para todo k, existem infinitas progressões aritméticas de tamanho k, compostas apenas de frações egípcias.

5. Sejam m, a, b, c, d inteiros quaisquer, com $a, m > 1$ e $mdc(c, m) = 1$.

   a) Prove que existe n inteiro positivo tal que $m | a^n - n$.

   b) Prove que existe n inteiro positivo tal que $m | a^n + n$.

   c) Prove que existe n inteiro positivo tal que $m | b \cdot a^n + cn + d$.

6. a) Mostre que para todo inteiro positivo k, existe um inteiro positivo $S(k)$ tal que todo $n > 0$ se escreve como soma de no máximo $S(k)$ potências k-ésimas perfeitas.

   b) Encontre o menor valor possível de $S(3)$.

7. a) Mostre que $mdc(n, \lfloor n\sqrt{2} \rfloor) < \sqrt[4]{8}\sqrt{n}$.

   b) Mostre que a constante acima é a melhor possível.

8. Dado $n := \prod p_i^{\alpha_i}$, defina $\overline{n} = \prod \alpha_i p_i^{\alpha_i - 1}$.
   Prove que existem infinitos n com $\overline{n+1} = \overline{n} + 1$.

9. a) Mostre que existem infinitas potências de 2 com pelo menos 1000 zeros nos seus últimos 2021 dígitos.

   b) Mostre que existe uma potência de 2 que tem apenas 1's e 2's nos últimos 2021 dígitos.

   c) Prove que existe uma potência de 2 cujos primeiros 2021 dígitos são todos 7.

   d) Prove que não existem duas potências de 2 compostas do mesmo multiconjunto de dígitos (excluindo zeros à esquerda), mas em ordens diferentes.

   e) Prove que existem infinitas potências de 2 cuja soma dos dígitos é maior que a soma dos dígitos da próxima potência de 2 (ou seja, $s(2^n) > s(2^{n+1})$

10. Encontre todas as soluções inteiras positivas de $a^3 + 2b^3 + 4c^3 - 6abc = 1$.

11. (Complemento do famoso problema do Gugu)

    a) Sejam a, b, c inteiros positivos tais que $a \cdot 4^n + b \cdot 6^n + c \cdot 9^n$ é sempre quadrado perfeito para todo n. Prove que existem x, y inteiros com $a = x^2, b = 2xy, c = y^2$.

    b) Sejam $a, b > 1$ inteiros tais que $a^n - 1 | b^n - 1$ para todo n. Prove que b é uma potência de a.

    c) Sejam $a, b > 1$ inteiros tais que $(a^n - 1)(b^n - 1)$ é quadrado perfeito para todo n, Mostre que $a = b$.