DIVISIBILIDADE E CONGRUÊNCIA

Semana Olímpica, N1, Recife – PE, julho de 2022
Tiago Sandino, tiagosandino1@gmail.com

Introdução

A motivação deste material é ser uma revisão dos principais conceitos de divisibilidade e uma introdução à teoria das congruências.

Os principais tópicos de divisibilidade serão brevemente expostos, isto é, sem demonstrações ou maiores detalhes, e acompanhados de bons, representativos e não tão difíceis problemas. Em seguida, será apresentada uma teoria pouco mais completa, porém ainda introdutória, de congruência.

Divisibilidade

Algoritmo da divisão. Dados inteiros a e b, com $b > 0$, existem únicos inteiros q e r tais que $a = qb + r$, com $0 \leq r < b$. Os inteiros q e r são chamados, respectivamente, o *quociente* e o *resto* da divisão de a por b.

O seguinte corolário é um pouco mais geral no sentido de que substitui a condição de $b > 0$ por apenas $b \neq 0$.

Corolário. Se a e b são inteiros, com $b \neq 0$, então existem únicos inteiros q e r tais que $a = qb + r$, com $0 \leq r < |b|$.

Quando formos falar de congruência, a restrição $0 \leq r < |b|$ vai ser irrelevante. O seguinte resultado já dá um gostinho disso.

Teorema dos Restos. A soma (o produto) de dois números quando divididos por um terceiro número tem o mesmo resto que a soma (o produto) de seus restos quando divididos por esse terceiro número.

Observe que nesse teorema, o resto da soma (e do produto) pode ser maior que o divisor. Esse teorema é útil quando não estamos interessados no quociente, mas apenas no resto, daí podemos até aplicar o algoritmo da divisão novamente para chegar em um resto menor que o divisor.

Veremos que, quando estivermos falando de congruência, o quociente não terá normalmente nenhuma importância e o resto pode até ser negativo.

Vamos ver alguns problemas importantes que podem ser resolvidos com esses resultados:

Problema 1. (OBM – 1998, 1ª Fase N2, P6/20). Qual é o dígito das unidades do número 3^{1998}?

Problema 2. Mostre que o quadrado de um número inteiro deixa apenas resto 0 ou 1 na divisão por 4.

Problema 3. Mostre que o quadrado de um inteiro ímpar pode sempre ser escrito na forma $8k + 1$.

Problema 4. Mostre que todo quadrado perfeito deixa resto 0 ou 1 na divisão por 3.

Problema 5. Mostre que o cubo de um número inteiro é de uma das formas: $9k$, $9k + 1$ ou $9k + 8$.

Problema 6. Mostre que a quarta potência de um inteiro é da forma $5k$ ou $5k + 1$.

Problema 7. Mostre que o cubo de um inteiro é da forma $7k$, $7k + 1$ ou $7k + 6$.

Problema 8. Mostre que todo número primo é da forma $6k + 1$ ou $6k + 5$.

É bem interessante olhar o caso em que $r = 0$ no algoritmo da divisão.

Definição. Um inteiro b é divisível por um inteiro $a \neq 0$, escreve-se $a|b$ (lê-se "a divide b"), se existe um inteiro c tal que $b = ac$. Escreve-se $a \nmid b$ quando a não divide b.

Se $a|b$, dizemos que a é um *divisor* de b, que b é um múltiplo de a e que a é um fator de b.

Note que $b = ac$ só implica $a|b$ quando $a \neq 0$. Note também que se $a|b$, então $-a|b$, pois $b = ac \Rightarrow b = (-a)(-c)$, o que nos leva a observar que os divisores de um número inteiro sempre aparecem aos pares, daí, quando falamos em divisores, muitas vezes estamos nos referindo apenas aos positivos.

Teorema. Para os inteiros a, b e c são válidas as seguintes afirmações:

a) $a|0$, $1|a$, $a|a$ (propriedade reflexiva);
b) $a|1$ se, e somente se, $a = \pm 1$;
c) Se $a|b$ e $c|d$, então $ac|bd$;
d) Se $a|b$ e $b|c$, então $a|c$ (propriedade transitiva);
e) $a|b$ e $b|a$ se, e somente se, $a = \pm b$ (a relação de divisão não comuta);
f) Se $a|b$, então $|a| \leq |b|$ ou $b = 0$ (propriedade da limitação);
g) Se $a|b$ e $a|c$, então $a|(bx + cy)$ para quaisquer inteiros x e y.

Vamos para mais uma rodada de problemas!

Problema 9. (OBM – 1998, 1ª Fase N2, P8/20). O número $1234a6$ é divisível por 7. O algarismo a vale:

A) 0 B) 2 C) 5 D) 6 E) 8

Problema 10. (OBM – 1999, 1ª Fase N2, P12/20). Quantos são os possíveis valores inteiros de x para que $\frac{x+99}{x+19}$ seja um número inteiro?

A) 5 B) 10 C) 20 D) 30 E) 40

Vamos aumentar um pouco o nível.

Problema 11. (Albânia, N3, 2018, P1/6). Ache todos os primos p tais que $p + 2$ e $p^2 + 2p - 8$ também sejam primos.

Problema 12. Prove que se a é um inteiro ímpar, então $32|(a^2 + 3)(a^2 + 7)$.

Problema 13. Prove que se a e b são números inteiros ímpares, então $16|a^4 + b^4 - 2$.

Problema 14. Para p e q inteiros positivos, prove que $2^p + 1 = q^2$ implica $p = q = 3$.

Problema 15. (OCM, N2, 2000, P. 4). Encontre as soluções inteiras da equação $y^2 - 3 = x(3y - 6)$.

Problema 16. Vinte entediados estudantes se revezam na seguinte tarefa, em um corredor do colégio há vinte armários numerados de um a vinte. O primeiro estudante passa por todos abrindo todos. O segundo passa por todos fechando os armários de números 2, 4, 6, 8, 10, 12, ..., 20. O terceiro passa pelos armários abrindo, caso esteja fechado, ou fechando, caso esteja aberto, os de números 3, 6, 9, ...,

18. E assim por diante, de forma que o i-ésimo estudante fecha, caso esteja aberto, ou abre, caso esteja fechado, os armários múltiplos de i. Quantos armários estarão abertos após essa operação toda?

Problema 17. (AIME 1986). Qual é o maior inteiro positivo n para o qual $n^3 + 100$ é divisível por $n + 10$?

Problema 18. (IMO – 1959. P1). Provar que a fração $\frac{21n+4}{14n+3}$ é irredutível para qualquer número natural n.

Problema 19. Prove que para todos os inteiros positivos n: $n^5 - 5n^3 + 4n$ é divisível por 120.

Problema 20. (Eslovênia, 1994, Third Grade, P1/4). Seja n um número natural. Prove que: se $2n + 1$ e $3n + 1$ são quadrados perfeitos, então n é divisível por 40.

Problema 21. Prove que para todos os inteiros positivos n: $n^2 + 3n + 5$ não é divisível por 121.

Vamos falar agora de um dos conceitos mais importantes da Teoria dos Números, o de máximo divisor comum. Logo após, mais uma bateria de problemas.

Definição (MDC). Sejam a e b inteiros dados, com ao menos um deles diferente de zero. O *máximo divisor comum* de a e b, denotado por $mdc(a, b)$, é um inteiro positivo d que satisfaz:

a) $d|a$ e $d|b$;
b) Se $c|a$ e $c|b$, então $c \leq d$.

Teorema (Bachet-Bézout). Dados os inteiros a e b, não sendo ambos nulos, existem inteiros x e y tais que

$$mdc(a, b) = ax + by$$

e mais ainda, o $mdc(a, b)$ é o menor número nesse formato.

Note que, mesmo após esse último teorema, ainda não temos um método para calcular mdc's. Falaremos em breve do Algoritmo de Euclides que é um método para isso.

O que você deve reter, principalmente, do teorema anterior é que o mdc de dois números é a menor combinação linear deles.

Corolário. Se a e b são inteiros dados, de modo que, pelo menos, um deles é diferente de zero, então o conjunto

$$T = \{ax + by | x, y \in \mathbb{Z}\}$$

é precisamente o conjunto de todos os múltiplos de $d = mdc(a, b)$.

Definição. Dois inteiros a e b, não sendo ambos iguais a zero, são ditos *primos relativos* ou *primos entre si* quando $mdc(a, b) = 1$.

Teorema. Sejam a e b inteiros, não sendo ambos iguais a zero. Então a e b são primos relativos se e somente se existem inteiros x e y tais que $1 = ax + by$.

Corolário. Se o $mdc(a,b) = d$, então o $mdc(a/d\,, b/d) = 1$.

Corolário. Se $a|c$ e $b|c$, com $mdc(a,b) = 1$, então $ab|c$.

Teorema (Lema de Euclides). Se $a|bc$, com $mdc(a,b) = 1$, então $a|c$.

Notação Alternativa. Em um contexto onde fique claro, podemos trocar a notação $mdc(a,b)$ por simplesmente (a,b).

Para praticar, usaremos essa notação no teorema seguinte.

Teorema. Para a, b e x inteiros, temos:

$$(a,b) = (a, b + ax).$$

E, vamos a mais alguns problemas!

Problema 22. Prove que para algum inteiro positivo n e para todo inteiro a, $mdc(a, a+n)$ divide n; consequentemente $mdc(a, a+1) = 1$, ou seja, dois números consecutivos são relativamente primos.

Problema 23. Para todo inteiro a, mostre que $mdc(2a+1, 9a+4) = 1$.

Problema 24. (Hungria, 1894, P1/3). Demonstre que as expressões $2x + 3y$ e $9x + 5y$ são divisíveis por 17 para os mesmos valores inteiros de x e y.

Obs.: Esse é o primeiro problema da primeira prova de olimpíada de matemática.

Problema 25. (Austrália, 2006). Ache todos os inteiros positivos m e n tais que $1 + 5 \cdot 2^m = n^2$.

Vamos continuar a teoria.

Lema. Se $a = qb + r$, então $mdc(a,b) = mdc(b,r)$.

Algoritmo de Euclides. Com $0 \leq r < b$, aplicando o algoritmo da divisão sucessivas vezes, podemos montar uma sequência de restos decrescentes (pois $r < b$) e finita (pois $0 \leq r$).

Antes de mostrar a execução do Algoritmo de Euclides, vamos mostrar como obter uma solução geral de uma equação diofantina linear e encontrar a solução inicial de um exemplo usando o Algoritmo de Euclides.

Teorema. A equação diofantina linear $ax + by = c$ tem soluções se, e somente se $d|c$, em que $d = mdc(a,b)$. Se x_0, y_0 é uma solução particular desta equação, então todas as soluções são dadas por

$$x = x_0 + \left(\frac{b}{d}\right)t, \quad y = y_0 - \left(\frac{a}{d}\right)t.$$

em que t é um inteiro qualquer.

Problema 26. Resolva a equação $5x + 22y = 18$.

Problema 27. Resolva a equação $172x + 20y = 1000$. Ache uma solução positiva.

Problema 28. Sendo $mdc(a, b) = 1$, prove o que segue:

a) $mdc(a + b, a - b) = 1$ ou 2.
b) $mdc(2a + b, a + 2b) = 1$ ou 3.
c) $mdc(a + b, a^2 + b^2) = 1$ ou 2.

A seguir, um resultado simples, porém bem relevante.

Teorema (Teorema Fundamental da Aritmética). Todo inteiro positivo $n > 1$ ou é um número primo ou é um produto de números primos; esta representação é única, fora a ordem na qual os fatores ocorrem.

Corolário. Um inteiro positivo $n > 1$ pode ser escrito de maneira única na *forma canônica*

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

em que, para $i = 1, 2, \dots, r$, cada k_i é um inteiro positivo e cada p_i é um primo, com $p_1 < p_2 < \cdots < p_r$.

Problema 29. Considere $n \in \mathbb{N}$ e $\theta(n) =$ número de primos que dividem n. Prove que $n \geq 2^{\theta(n)}$.

CONGRUÊNCIA

Definição. Seja n um inteiro positivo dado. Diz-se que os inteiros positivos a e b são 'congruentes módulo n', simbolizado por:

$$a \equiv b \ (mod\ n)$$

se n divide a diferença $a - b$, ou seja, desde que $a - b = kn$ para algum inteiro k. Quando $n \nmid (a - b)$ dizemos que a é incongruente a b módulo n, e escrevemos $a \not\equiv b \ (mod\ n)$.

Observa-se também que quaisquer dois inteiros são congruentes módulo 1. Por isso, costuma-se assumir $n > 1$. Veja também que dois inteiros são congruentes módulo 2 se são ambos pares ou ambos ímpares.

Se $a = q \cdot n + r$, $0 \leq r < n$, então $a \equiv r \ (mod\ n)$. Como há n escolhas para r, vemos que todo inteiro é congruente módulo n a exatamente um dos valores 0, 1, 2, ..., $n - 1$; em particular $a \equiv 0 \ (mod\ n)$ se, e somente se $n|a$. O conjunto dos n inteiros 0, 1, 2, ..., $n - 1$ é chamado de *o conjunto dos menores resíduos não negativos módulo* n. Em geral, diz-se que um conjunto de n inteiros a_1, a_2, ..., a_n forma um *conjunto (sistema) completo de resíduos módulo* n se cada inteiro é congruente módulo n a um e apenas um dos a_k. Por exemplo, $-12, -4, 11, 13, 22, 82, 91$ é conjunto completo de resíduos módulo 7.

Obs.: Quaisquer n inteiros formam um conjunto completo de resíduos módulo n se e somente se não há dois inteiros que sejam congruentes módulo n.

Teorema. Para inteiros arbitrários a e b, $a \equiv b \ (mod\ n)$ se e somente se a e b deixam o mesmo resto não negativo quando divididos por n.

Demonstração.

($\Rightarrow$) $a \equiv b \ (mod\ n) \Rightarrow a = b + kn$ para algum $k \in \mathbb{Z}$. Se $b = qn + r$, onde $0 \leq r < n$, $a = b + kn = qn + r + kn = (q + k)n + r$. Logo, a e b têm o mesmo resto.

($\Leftarrow$) Se $a = q_1 n + r$ e $b = q_2 n + r$, $0 \leq r < n$, então $a - b = (q_1 - q_2)n$. De onde, $n|a - b$, ou $a \equiv b \ (mod\ n)$.

Teorema (Propriedades da Relação de Congruência). Seja $n > 1$ um inteiro fixo e a, b, c e d inteiros arbitrários. Então as seguintes propriedades são válidas:

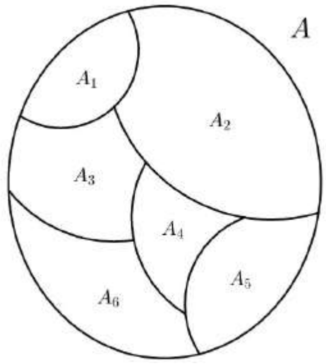
a) $a \equiv a \ (mod\ n)$, propriedade reflexiva;
b) Se $a \equiv b \ (mod\ n)$, então $b \equiv a \ (mod\ n)$, propriedade simétrica;
c) Se $a \equiv b \ (mod\ n)$ e $b \equiv c \ (mod\ n)$, então $a \equiv c \ (mod\ n)$, propriedade transitiva;
d) Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$, então $a + c \equiv b + d \ (mod\ n)$ e $ac \equiv bd \ (mod\ n)$;
e) Se $a \equiv b \ (mod\ n)$, então $a + c \equiv b + c \ (mod\ n)$ e $ac \equiv bc \ (mod\ n)$;
f) Se $a \equiv b \ (mod\ n)$, então $a^k \equiv b^k \ (mod\ n)$, $\forall k \in \mathbb{Z}$.

Há ainda outra propriedade que mostraremos em breve. Mas antes disso, vamos ver uma implicação das propriedades a, b e c.

Congruência como Relação de Equivalência e os Anéis de Classes de Congruência

Quando uma relação binária (entre dois entes matemáticos) apresenta as propriedades reflexiva, simétrica e transitiva, diz-se que essa relação é uma relação de equivalência. Devido a isso, podemos *particionar* o conjunto dos inteiros em *classes de equivalência*. Vamos explicar melhor esses dois termos em itálico.

1) Uma "família" de subconjuntos, A_1, A_2, ..., A_n de um conjunto A é uma *partição* quando:
   a. Nenhum desses subconjuntos é vazio;
   b. A união deles é o próprio A;
   c. São subconjuntos disjuntos, ou seja, não possuem elementos em comum.



A ideia de partição pode ser bem compreendida por meio do diagrama ao lado, onde particionamos o conjunto A em uma família com seis subconjuntos.

2) Classes de Equivalência: na relação de equivalência congruência módulo n, a classe de equivalência de um inteiro a é o conjunto $\overline{a_n} = \{\dots, a-2n, a-n, a, a+n, a+2n, \dots\}$. O conjunto de todas as classes de equivalência de uma congruência módulo n é denotado por $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}/n$. Dois números inteiros são congruentes módulo n se, e somente se, pertencem à mesma classe de equivalência.

Devido a esse comportamento e propriedades, podemos entender congruência como uma "aritmética de relógio", onde cada número marcado representa uma classe de equivalência e as operações binárias apresentadas nas propriedades resultam sempre em elementos desse "relógio".

Teorema (uma última propriedade). Se $ca \equiv cb\ (mod\ n)$, então $a \equiv b\ (mod\ \ n/d)$, em que $d = mdc(c, n)$.

Demonstração. $ca \equiv cb\ (mod\ n) \Rightarrow c(a-b) = kn$, com $k \in \mathbb{Z}$. Se $d = mdc(c, n)$, sejam $c = rd$ e $n = sd$, com r, $s \in \mathbb{Z}$ e $mdc(r, s) = 1$. Então $c(a-b) = kn \Rightarrow r(a-b) = ks \Rightarrow s|a-b \Rightarrow a \equiv b\ (mod\ s)$, ou seja, $a \equiv b\ (mod\ n/d)$.

Obs.: Não precisa estabelecer que $c \not\equiv 0\ (mod\ n)$, pois isso implicaria em $mdc(c, n) = n$, de onde $ca \equiv cb\ (mod\ n) \Rightarrow a \equiv b\ (mod\ 1)$, o que é trivial no sentido de que não contribui para nada.

Na prática, evita-se usar essa propriedade. Quando temos uma congruência do tipo $ax \equiv b\ (mod\ n)$, procuramos um $\bar{a}$ tal que $\bar{a}a \equiv 1\ (mod\ n)$ e, ao multiplicar os dois lados de $ax \equiv b\ (mod\ n)$ por $\bar{a}$, obtemos $x \equiv \bar{a}b\ (mod\ n)$. Esse $\bar{a}$ é chamado de o inverso multiplicativo módulo n de a.

Nos problemas a seguir, há a possibilidade de usar certos "atalhos" em alguns dos problemas, mas tente evitar ou use-os apenas para conferir um possível caminho alternativo. Assim, você ganhará uma noção muito boa nas operações aritméticas envolvendo congruência.

De qualquer forma, já que toquei no assunto, aqui vão os dois atalhos:

Teorema (Pequeno Teorema de Fermat). Seja p um primo e suponha $a \in \mathbb{Z}$ tal que $p \nmid a$. Então $a^{p-1} \equiv 1\ (mod\ p)$.

A demonstração desse teorema usa o conceito já citado de conjunto completo de resíduos. Se quisermos um refinamento, retiramos desse conjunto os números que não são relativamente primos com o módulo. À quantidade de elementos que sobram nesse conjunto, chamamos $\phi(n)$, onde n é o módulo, que nesse caso não precisa mais ser primo. Podemos enunciar então:

Teorema (Teorema de Euler). Seja $n \in \mathbb{Z}$ e $a \in \mathbb{Z}$ tal que $n \nmid a$. Então $a^{\phi(n)} \equiv 1\ (mod\ n)$.

Para não dizer que enunciei esses dois teoremas lindos à toa, segue o problema abaixo.

Problema. (USAJMO, 2013, P. 1/6). Existem inteiros a e b tais que $a^5b + 3$ e $ab^5 + 3$ são ambos cubos perfeitos?

PROBLEMAS FÁCEIS

1. Mostrar que $41|2^{20}-1$.

2. Qual é o resto, após a divisão por 12, da soma $\sum_{k=1}^{100} k!$?

3 (China, 2004). Quando um número de três dígitos é dividido por 2, 3, 4, 5 e 7, os restos são todos iguais a 1. Ache o menor e o maior valor possíveis para esse número.

4. É sabido que 2726, 4472, 5054, 6412 possuem o mesmo resto quando divididos por um certo número natural m de dois dígitos. Ache o valor de m.

5 (China, 2000). Ache o resto de 3^{2000} dividido por 13.

6 (Singapura, 2001). Ache o menor inteiro positivo k tal que $2^{69}+k$ é divisível por 127.

7 (Singapura, 2003). Qual é o resto de $6^{273}+8^{273}$ dividido por 49?

8. Ache o resto que o número $2005^{2007^{2009}}$ deixa ao ser dividido por 7.

9 (Singapura, 1997). Ache o menor inteiro positivo n tal que $1000 \leq n \leq 1100$ e $1111^n+1222^n+1333^n+1444^n$ é divisível por 10.

10. Prove que para qualquer natural ímpar n, o número $1^{2007}+2^{2007}+\cdots+n^{2007}$ não é divisível por $n+2$.

11 (Singapura, 2001). Escreva os últimos quatro dígitos do número 7^{128}.

12. Determine os números primos p tais que 2^p+p^2 é primo.

PROBLEMAS MÉDIOS

1 (Austrian Beginner's Competition, 2015, P1/4). Sejam a, b, c inteiros tais que $a^3+b^3+c^3$ é divisível por 18. Prove que abc é divisível por 6.

2 (Letônia, 1994). Resolva a equação $1!+2!+3!+\cdots+n!=m^3$ no conjunto dos naturais.

3 (Olimpíada de Maio, 2020, N2, P2/5). a) Determinar se existem inteiros positivos a, b e c, não necessariamente distintos, tais que $a+b+c=2020$ e $2^a+2^b+2^c$ é um quadrado perfeito. b) Determinar se existem inteiros positivos a, b e c, não necessariamente distintos, tais que $a+b+c=2020$ e $3^a+3^b+3^c$ é um quadrado perfeito.

4 (Olimpíada Australiana de Matemática, 2016, P1/8). Ache todos os inteiros positivos n tais que 2^n+7^n é um quadrado perfeito.

5 (Peru, N1, 2017, Fase 4/4, P.2/4). Um conjunto formado por números inteiros positivos é chamado de *super-divisível* se a soma de seus elementos é divisível por cada um dos elementos do conjunto. Determine quantos elementos, no mínimo, pode ter um conjunto super-divisível que contém os números 3, 14 e 21.

Observação: Leve em conta que um conjunto pode ter elementos repetidos.

6 (Singapura, 2011). Determine os dois últimos dígitos de 7^{5^6}.

7 (USAJMO, 2011). Ache todos os inteiros positivos n tais que $2^n + 12^n + 2011^n$ é um quadrado perfeito.

8. Sabendo que $641 = 2^7 \cdot 5 + 1$, prove que $641|2^{32} + 1$.

9 (Crux Mathematicorum, v48n2, pag. 63). Prove que há infinitos inteiros positivos k tais que k^k pode ser expresso como a soma dos cubos de dois inteiros positivos.

10 (Crux Mathematicorum, v48n2, pag. 64). Ache todos os pares (x, y) de inteiros positivos que satisfazem a equação $x^2 - 2x + 29 = 7^x y$.

11 (Mathematical Reflexions, 2022, vol. 1). Sejam k, m, n inteiros tais que $k + m + n = 1$. Prove que $(k^2 + m^2 + n^2 + 7)^2 + (kmn - 4)^2$ não pode ser o quadrado de um inteiro ímpar.

12 (Lista Cone Sul, 2007). Encontre todas as triplas (m, p, q) onde m é um inteiro positivo, p e q são primos positivos e que satisfazem: $2^m p^2 + 1 = q^5$.

13 (OBM, N2, 2011, P. 1). Num tabuleiro 3×3 escrevemos os números de 1 a 9, um em cada casa. Em seguida, achamos a soma dos números de cada linha, de cada coluna e de cada diagonal e contamos o número de somas que são múltiplos de três. Por exemplo, no tabuleiro abaixo as 8 somas (as três linhas, as três colunas e as duas diagonais) são números múltiplos de 3.

1	2	3
4	5	6
7	8	9

É possível que nenhuma das 8 somas seja um múltiplo de 3?

Lembre-se de que você deve justificar sua resposta.

14 (OBM, 2011, N2, P. 4). Esmeralda escreveu uma lista de números inteiros positivos em uma folha de papel. Renan percebeu que todos os números da lista e todas as somas de qualquer quantidade de números distintos da lista não eram divisíveis por nenhum quadrado perfeito diferente de 1. Qual a quantidade máxima de números na lista de Esmeralda?

15 (Hanoi Open MC, Senior, 2014, Q4). Ache o menor inteiro positivo n tal que $2^n + 2^8 + 2^{11}$ é um quadrado perfeito.

A) 8 B) 9 C) 11 D) 12 E) NDA

PROBLEMAS DIFÍCEIS

1 (Kvant, M 274). Ache os menores números das formas:

a) $|11^k - 5^l|$
b) $|36^k - 5^l|$
c) $|53^k - 37^l|$