Filipe Rodrigues de S. Moreira
Graduando em Engenharia Mecânica –
Instituto Tecnológico de Aeronáutica (ITA)
Agosto 2006

Congruências Lineares

Introdução

A idéia de se estudar congruências lineares pode vir a facilitar (e muito) a vida de um estudante, na hora de resolver questões de Teoria dos Números e até Polinômios. Esse assunto merece uma atenção especial, pois em geral os livros que estão no mercado, mostram do que se trata, porém vão logo para uma abordagem mais abrangente e acabam saindo do foco de um aluno que não se interessa pelo assunto como estudo puro e sim está apenas buscando, alternativamente, outra ferramenta para resolver questões de vestibulares mais rebuscados como IME e ITA. Esse artigo tem por objetivo atender a necessidade de bons alunos que não se interessam por Olimpíadas de Matemática (puro e simplesmente), mas querem descobrir novos métodos para tornar simples questões difíceis, que à priori exigiriam muito raciocínio e genialidade.

Definição da palavra e notação

Dizemos que dois números inteiros são congruentes, em relação a algum outro, quando deixam o mesmo resto na divisão por esse outro, ou seja, diz-se que "a é congruente a b módulo m" quanto tanto "a" quanto "b" deixam o mesmo resto na divisão por "m". Veja a notação usual: $a \equiv b \pmod{m}$. Aplicando!!!!

$12 \equiv 2 \pmod{5}$, pois 2 é o resto da divisão de 12 por 5.

$12 \equiv 7 \pmod{5}$, pois 7 e 12 deixam o mesmo resto na divisão por 5.

$24 \equiv 3 \pmod{7}$, pois 3 é o resto da divisão de 24 por 7.

$28 \equiv 1 \pmod{9}$, pois 1 é o resto da divisão de 28 por 9.

Veja esse último exemplo....sabe-se que $28 = 9.3 + 1$, mas por que não escrevermos que $28 = 9.4 - 8$? Sendo assim, o resto da divisão de 28 por 9 poderia ser "-8". De fato, na divisão Euclidiana, isso não é permitido, pois se trata do menor resto positivo, porém, podemos trabalhar com restos negativos na teoria de congruência, ou seja, é possível escrever que $28 \equiv -8 \pmod{9}$. Acredite! isso vai tornar a sua vida muito mais tranqüila na hora de resolver questões de teoria dos números.

Exercícios propostos

P1. Resolva as congruências abaixo:

a) $12 \equiv \quad \pmod{4}$	b) $32 \equiv \quad \pmod{3}$	c) $71 \equiv \quad \pmod{8}$
d) $38 \equiv \quad \pmod{13}$	e) $48 \equiv \quad \pmod{6}$	f) $27 \equiv \quad \pmod{11}$

Algumas propriedades de congruências

P_1 -) Sejam dois números inteiros tais que $a \equiv b \pmod{m}$ e outros dois inteiros tais que $c \equiv d \pmod{m}$. Assim, $a \pm c \equiv b \pm d \pmod{m}$.

Prova:
Se $a \equiv b \pmod m$ então $a = k.m + b$ (com $k \in Z$) e se $c \equiv d \pmod m$ então $c = t.m + d$ (com $t \in Z$) Logo temos que $(a \pm c) = (k \pm t).m + (b \pm d)$, logo $a \pm c \equiv b \pm d \pmod m$.

P_2 -) Sejam dois números inteiros tais que $a \equiv b \pmod m$ e outros dois inteiros tais que $c \equiv d \pmod m$. Assim, $a.c \equiv b.d \pmod m$.
Prova:
Se $a \equiv b \pmod m$ então $a = k.m + b$ (com $k \in Z$) e se $c \equiv d \pmod m$ então $c = t.m + d$ (com $t \in Z$) Logo temos que $a.c = \overbrace{k.t.m^2 + k.m.d + t.m.b}^{\text{múltiplo de } m} + b.d$, logo $a.c \equiv b.d \pmod m$.

P_3-) Sejam dois números inteiros tais que $a \equiv b \pmod m$. Logo sendo r outro número inteiro tem-se que $a \pm r \equiv b \pm r \pmod m$.
Prova:
Se $a \equiv b \pmod m$ então $a = k.m + b$, com $k \in Z$. Logo temos que $(a \pm r) = k.m + (b \pm r)$, logo $a \pm r \equiv b \pm r \pmod m$.

P_4 -) Sejam dois números inteiros tais que $a \equiv b \pmod m$. Logo sendo r outro número inteiro tem-se que $a.r \equiv b.r \pmod m$.
Prova:
Se $a \equiv b \pmod{.m}$ então $a = k.m + b$, com $k \in Z$. Logo temos que $a.r = k.m.r + b.r$, logo $a.r \equiv b.r \pmod m$.

P_5 -) Sejam dois números inteiros tais que $a \equiv b \pmod{.m}$. Seja n um número natural logo, $a^n \equiv b^n \pmod{.m}$.
Prova (exercício): Esse o resultado da propriedade P_2 e indução finita.

Veja que essas propriedades vão ajudar muito na hora da resolução de questões mais elaboradas, pois a partir de agora será possível substituir números grandes, pelos seus restos na divisão em questão.
Por exemplo: Calcular o resto da divisão de 2006^{2006} por 5.
Pela propriedade P_5, $2006^{2006} \equiv 1^{2006} = 1 \pmod{.5}$, logo o resto da divisão de 2006^{2006} por 5 é 1.

Veja a série de exemplos abaixo e aprenda a aplicar essa teoria:

E1) Calcular o resto da divisão de $(2006^{2006} + 2004^{2004})^{2005}$ por 5.
Solução:

$(2006^{2006}+2004^{2004})^{2005} \equiv (1^{2006}+(-1)^{2004})^{2005} \equiv 2^{2005}$. Como $16 = 2^4 \equiv 1 \pmod{5}$, podemos escrever $2^{2005} = (2^4)^{501}.2 \equiv (1)^{501}.2 = 2$. Logo $(2006^{2006}+2004^{2004})^{2005}$ deixa resto 2 na divisão por 5.

Observação: Veja que a vantagem dessa teoria é a possibilidade da substituição das bases pelos seus restos na divisão desejada. Nesse caso, 2006 foi substituído por 1 e 2004 o foi por (-1) que são seus respectivos restos na divisão por 5.

E2) Calcular o resto da divisão de $5^{131}+7^{131}+11^{131}+13^{131}$ por 9.

Solução:

$$5^{131}+7^{131}+11^{131}+13^{131} \equiv (-4)^{131}+(-2)^{131}+(2)^{131}+(4)^{131} = 0 \pmod{9}$$

E3) Calcular o resto da divisão de $N = 1^{2007}+2^{2007}+3^{2007}+\dots+2006^{2007}+2007^{2007}$ por 5.

Solução:

Vamos resolver essa questão por partes. Tome os 5 primeiros termos.

$$1^{2007}+2^{2007}+3^{2007}+4^{2007}+\overbrace{5^{2007}}^{\equiv 0} \equiv 1^{2007}+2^{2007}+(-2)^{2007}+(-1)^{2007} \equiv 0 \pmod{5}$$

Esse raciocínio se repete para cada grupo de cinco números consecutivos, contando a partir dos números da forma $5k+1,\ k \in Z$, assim, todas as parcelas até 2005^{2007} vão se anular na congruência módulo 5. Faltam então as duas últimas parcelas. Logo:

$$N \equiv 2006^{2007}+2007^{2007} \equiv 1+2^{2007} \equiv 1+2^3.(\overbrace{2^4}^{\equiv 1})^{501} \equiv 9 \equiv 4 \pmod{5}$$

E4) Determinar qual é o algarismo das unidades na representação decimal do número $N = (2006^{2007}+2005.2007^{2007})^{2007}$.

Solução:

Determinar o algarismo das unidades de um número qualquer é o mesmo que determinar o resto na divisão por 10, pois qualquer número inteiro N pode ser escrito sob a forma $N = 10k+b$, com k e b inteiros. Logo, fazendo congruência módulo 10:

$$N = (2006^{2007}+2005.2007^{2007})^{2007} \equiv (6^{2007}+5.(\overbrace{7^2}^{\equiv -1})^{1003}.7)^{2007} \equiv (6^{2007}-35)^{2007} \equiv (6^{2007}-5)^{2007}$$

Vamos estudar as potências de 6 na divisão por 10.

$6^0 \equiv 1 \pmod{10}$

$6^1 \equiv 6 \pmod{10}$

$6^2 \equiv 36 \equiv 6 \pmod{10}$ *começa a repetir*

Logo qualquer potência (n > 0) de 6 deixa resto 6 na divisão por 10. Assim:

$N \equiv (6^{2007}-5)^{2007} \equiv (6-5)^{2007} \equiv 1 \pmod{10}$. Logo o algarismo das unidades de N é 1.

E5) Determinar qual é o algarismo das unidades na representação decimal do número $N = (22222^{55555}+55555^{22222})^{33333}+(33333^{77777}+77777^{33333})^{44444}$.

Solução:

Fazendo congruência módulo 10.

$N \equiv ((\underbrace{2^4}_{\equiv 1})^{13888}.2^3 + \underbrace{5^{22222}}_{\equiv 5})^{33333} + (\underbrace{3^2}_{\equiv -1})^{38888}.3 + (\underbrace{7^2}_{\equiv -1})^{16666}.7))^{44444} \equiv (8+5)^{33333} + (3+7)^{44444} \equiv$

$\equiv (3)^{33333} + (\underbrace{10}_{\equiv 0})^{44444} \equiv 3^{33333} \equiv (\underbrace{3^2}_{\equiv -1})^{16666}.3 \equiv 3$. Logo o algarismo das unidades de N é 3.

Teorema útil: Teorema de Fermat

Sejam *a* um número natural e *p* um número primo tais que mdc (*a*, *p*) = 1. Com essas condições pode-se afirmar que $a^{p-1} \equiv 1 \ (\text{mod}\ p)$.

Prova: Tomemos o conjunto $A = \{a,\ 2a,\ 3a,\ 4a,\ ...\ ,\ (p-1)a\}$.

Lema: Todos os elementos de *A* são incongruentes entre si (módulo *p*), dois a dois.

Provando o lema:

Suponha que existam dois elementos distintos de A tais que sejam congruentes entre si na divisão por p. Logo $ka - ta \equiv 0 \ (\text{mod}\ p) \Rightarrow k - t \equiv 0 \ (\text{mod}\ p)$, pois se tem que o mdc (*a*, *p*) = 1. Assim, $k \equiv t \ (\text{mod}\ p)$, mas como são menores que *p*, temos que $k = t$, mas isso é absurdo, pois por hipótese $k \neq t$.

Logo A tem (*p* – 1) elementos e todos são incongruentes entre si na divisão por *p*, temos que em A existem todos os possíveis restos (diferentes de zero) na divisão por *p*. Pela propriedade P_2, a multiplicação de todos os elementos de A é congruente à multiplicação de todos os restos, respectivos, na congruência módulo *p*.

$a.2a.3a.4a.\cdots.(p-1)a \equiv 1.2.3.\cdots.(p-1) \equiv (\text{mod}.\ p)$

$a^{p-1}(1.2.3.\cdots.(p-1)) \equiv 1.2.3.\cdots.(p-1) \equiv (\text{mod}.\ p)$ como $1.2.3.\cdots.(p-1)$ é primo com *p*, podemos cancelar os termos comuns de ambos os lados da congruência e assim:

$a^{p-1} \equiv 1 \ (\text{mod}.\ p)$

Corolário: Sejam *a* um número natural e *p* um número primo. $a^p \equiv a \ (\text{mod}.\ p)$.

Prova (exercício): É resultado direto do Teorema de Fermat. Sugestão: Abra em dois casos:

1º) *a* é primo com *p*.

2º) *a* é um inteiro qualquer múltiplo de *p*.

E6) (IME) Prove que os inteiros *k* e k^5 têm o mesmo algarismo das unidades.

Solução:

Veja que qualquer número pode ser escrito na forma $x = 10t + b$. Se e k^5 têm o mesmo algarismo das unidades então são da forma $k = 10t + b$ e $k^5 = 10m + b$, logo a diferença entre eles é da forma $k^5 - k = 10(m-t)$, múltiplo de 10. Assim sendo, provar que ambos tem o mesmo algarismo das unidades é equivalente a provar que a diferença $k^5 - k$ é múltiplo de 10. Basta então provarmos que essa diferença é múltiplo de 2 e de 5, simultaneamente.

Fatorando: $k^5 - k = k(k^4 - 1) = k(k^2 - 1)(k^2 + 1) = (k-1) \overbrace{k(k+1)}^{\text{inteiros consecutivos}} (k^2 + 1)$. Na fatoração aparece o produto de dois inteiros consecutivos, logo um deles é par e assim o produto é par, portanto, múltiplo de 2.

Veja que 5 é primo e *k* é inteiro, logo pelo corolário do teorema de Fermat, $k^5 \equiv k \ (\text{mod}.5)$, logo $k^5 - k \equiv 0 \ (\text{mod}.5)$, portanto, essa diferença é múltiplo de 5.

Visto é a diferença $k^5 - k$ é par e é múltiplo de 5, logo ela é múltiplo de 10. cqd

Aplicação de congruências a Polinômios

Assim como a idéia de se associar a divisão euclidiana à notação em módulo é real e útil com números inteiros, podemos também utilizá-la para polinômios, veja alguns exemplos:
Ex. $P(x) = x^4 - 1 \equiv 0 \ (\text{mod}.\, x^3 + x^2 + x + 1)$ pois fatorando $x^4 - 1$, tem-se que $x^4 - 1 = (x-1)(x^3 + x^2 + x + 1)$, ou seja, $x^4 - 1$ deixa resto zero na divisão por $x^3 + x^2 + x + 1$.

Ex. $P(x) = x^4 + x - 1 \equiv x \ (\text{mod}.\, x^2 - 1)$, pois dividindo $x^4 + x - 1$ por $x^2 - 1$ tem-se resto x.

E6) Calcular o resto da divisão de $P(x) = x^5 + x + 1$ por $x^3 - 1$.
Solução:
Temos que $x^3 - 1 \equiv 0 \ (\text{mod}.\, x^3 - 1)$, logo somando 1 em ambos os lados da congruência chega-se que $x^3 \equiv 1 \ (\text{mod}.\, x^3 - 1)$. $P(x) = x^5 + x + 1 \equiv x^2.(\overbrace{x^3}^{\equiv 1}) + x + 1 \equiv x^2 + x + 1$.
Logo o resto da divisão de $P(x)$ por $x^3 - 1$ é $x^2 + x + 1$.

E7) Calcular o resto da divisão de $P(x) = x^{10} + 3x^8 + x^7 - x^3 + x^2 + 2x - 1$ por $x^3 + x$.
Solução:
Temos que $x^3 + x \equiv 0 \ (\text{mod}.\, x^3 + x)$, logo somando (-$x$) em ambos os lados da congruência chega-se que $x^3 \equiv -x \ (\text{mod}.\, x^3 - 1)$.

$$x^{10} + 3x^8 + x^7 - x^3 + x^2 + 2x - 1 \equiv x.(\overbrace{x^3}^{\equiv =x})^3 + 3x^2(\overbrace{x^3}^{\equiv =x})^2 + x.(\overbrace{x^3}^{\equiv =x})^2 - (\overbrace{x^3}^{\equiv =x}) + x^2 + 2x - 1 \equiv$$
$$\equiv x.(-x)^3 + 3x^2(-x)^2 + x.(-x)^2 - (-x) + x^2 + 2x - 1 \equiv -x^4 - 3x^4 - x^3 + x + x^2 + 2x - 1 \equiv$$
$$\equiv -4x^4 - x^3 + x^2 + 3x - 1 \equiv -4x.(x^3) - (x^3) + x^2 + 3x - 1 \equiv -4x.(-x) - (-x) + x^2 + 3x - 1 \equiv$$
$$\equiv 4x^2 + x + x^2 + 3x - 1 \equiv 5x^2 + 4x - 1.$$

Logo o resto da divisão de $P(x)$ por $x^3 + x$ é $5x^2 + 4x - 1$.
Obs.: Veja que a vantagem da congruência é poder substituir as potências grandes de x por outros termos que são exatamente o resto da divisão dessa potência pelo módulo em questão.

E8) (IME) Provar que $P(x) = x^{999} + x^{888} + x^{777} + ... + x^{111} + 1$ é divisível pelo polinômio $D(x) = x^9 + x^8 + x^7 + ... + x^1 + 1$.
Solução:
Sabemos que $x^{10} - 1 = (x-1)(x^9 + x^8 + x^7 + ... + x + 1)$, logo escrevendo na notação de módulo temos que $x^{10} - 1 \equiv 0 (\text{mod}.\, x^9 + x^8 + x^7 + ... + x + 1)$ ou ainda podemos escrever que $x^{10} \equiv 1 (\text{mod}.\, x^9 + x^8 + x^7 + ... + x + 1)$. Assim, podemos substituir todas as potências de x^{10}, no polinômio original pelo número "1".

$P(x) = x^{999} + x^{888} + x^{777} + ... + x^{111} + 1 = x^9.(\overbrace{x^{10}}^{\equiv 1})^{99} + x^8.(\overbrace{x^{10}}^{\equiv 1})^{88} + ... + x.(\overbrace{x^{10}}^{\equiv 1})^{11} + 1 \equiv$
$\equiv x^9 + x^8 + ... + x + 1 \equiv 0 \pmod{x^9 + x^8 + ... + x + 1}$. Logo, $P(x)$ é divisível por $D(x)$.

Aplicação de congruência em fatoração de polinômios

Assim como essa ferramenta poderosa pode ser útil para determinar resto de divisões entre polinômios, podemos utilizá-la para determinar fatores de alguns polinômios que se quer obter a fatoração. Na verdade essa parte da teoria está atrelada à outra, denominada raízes da unidade. Seja o polinômio $P(x) = x^n - 1$. Resolvendo a equação $x^n - 1 = 0$, chega-se que $x = cis\left(\frac{2k\pi}{n}\right)$, ou seja, essas raízes representam números complexos que compõem os vértices de um n-ágono regular inscrito numa circunferência de raio unitário, logo se pode dizer que essas raízes são potências do complexo x, mostrado acima. Veja a fatoração: $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + ... + x + 1)$. Com base nesse resultado chega-se que $x^n - 1 \equiv 0 \pmod{(x^{n-1} + x^{n-2} + ... + x + 1)}$, logo $x^n \equiv 1 \pmod{(x^{n-1} + x^{n-2} + ... + x + 1)}$. Essa congruência pode ser muito útil em muitos problemas de fatoração, veja um exemplo:

E9) Fatorar $q(x) = x^5 + x + 1$.
Solução:
Vamos fazer a congruência de $q(x) = x^5 + x + 1$ no módulo $x^3 - 1$. $x^3 - 1 \equiv 0 \pmod{x^3 - 1}$, logo se chega que $x^3 \equiv 1 \pmod{x^3 - 1}$.

Com isso $q(x) = x^5 + x + 1 \equiv \overbrace{x^3}^{\equiv 1}.x^2 + x + 1 \equiv x^2 + x + 1 \pmod{x^3 - 1}$, mas como $x^2 + x + 1$ é fator de $x^3 - 1$, concluímos que se tivéssemos feito congruência módulo $x^2 + x + 1$, a congruência teria dado zero, assim, $x^2 + x + 1$ é um fator de $q(x)$. Fazendo então a divisão longa entre os polinômios $q(x)$ e $x^2 + x + 1$, chega-se que o resto é zero e o produto entre o divisor e o quociente já é a forma fatorada desse polinômio $q(x) = x^5 + x + 1$. Logo: $x^5 + x + 1 = (x^3 - x^2 + 1)(x^2 + x + 1)$.

E10) Fatorar $q(x) = x^7 + x^5 + x^2 + 1$.
Solução:
Vamos fazer a congruência de $q(x) = x^7 + x^5 + x^2 + 1$ no módulo $x^4 - 1$. $x^4 - 1 \equiv 0 \pmod{x^4 - 1}$, logo se chega que $x^4 \equiv 1 \pmod{x^4 - 1}$.

Com isso $q(x) = x^7 + x^5 + x^2 + 1 \equiv \overbrace{x^4}^{\equiv 1}.x^3 + \overbrace{x^4}^{\equiv 1}.x + x^2 + 1 \equiv x^3 + x + x^2 + 1 \pmod{x^4 - 1}$, mas como $x^3 + x + x^2 + 1$ é fator de $x^4 - 1$, concluímos que se tivéssemos feito congruência módulo $x^3 + x + x^2 + 1$, a congruência teria dado zero, assim, $x^3 + x + x^2 + 1$ é um fator de $q(x)$. Fazendo então a divisão longa entre os polinômios $q(x)$ e $x^3 + x + x^2 + 1$, chega-se que o resto é zero e o produto entre o divisor e o quociente já é a forma fatorada desse polinômio $q(x) = x^7 + x^5 + x^2 + 1$. Logo: $x^7 + x^5 + x^2 + 1 = (x^4 - x^3 + x^2 - x + 1)(x^3 + x^2 + x + 1)$.

Exercícios propostos

P2) Mostre que $3.5^{2n+1}+2^{3n+1}$ é divisível por 17, para todo $n \in \mathbb{N}$.

P3) Mostre que $63!$ deixa resto $61!$ na divisão por 71.

P4) Achar o resto da divisão de:
a) $2^{50}+41^{65}$ por 7
b) $243^{2000}+451^{2002}$ por 6
c) $1001^{999}.50005^{888}+1458^{333}$ por 11

P5) Achar o resto da divisão por 5 do produto $74892^{359}\times 6379^{207}\times 9538^{179}\times 3785^{723}$.

P6) Achar o algarismo das unidades do inteiro:
a) 2^{1000}
b) $2007^{2007}+2006^{2006}$
c) $1001^{999}.50005^{888}+1458^{333}$

P7) Calcular o resto da divisão de $1^{2007}+2^{2007}+3^{2007}+...+50^{2007}$ por 5.

P8) Calcular o resto da divisão do número $(111^{111}+222^{222}+333^{333})^{444}$ por 7.

*P9) Calcular os dois últimos algarismos do número $\sum_{k=1}^{99}(n+k)^4$, em que n é um inteiro não negativo.

P10) Mostre que $11^{10}-1$ é divisível por 100.

P11)
a) O número $123456789(10)(11)(12)(13)(14)$ está escrito na base 15. Qual o resto da divisão desse número por 7.
b) O número $N=\left(1234567(10)(11)(12)(13)(14)(15)(16)(17)...\right)_8$ está escrito na base 8. Sabe-se que N tem 2007 algarismos. Determine o resto da divisão de N por 8.
c) Determine um critério de divisibilidade por 7 de um número escrito na base 8.
d) Demonstre que os critérios de divisibilidade por 11, 9 e 8 de um número na base 10.

P12) Prove que, pra todo inteiro n:
a) $3^{6n}-2^{6n}$ é divisível por 35 (n > 0);
b) n^5-5n^3+4n é divisível por 120;

P13) Mostre que se um número ímpar é quadrado perfeito então ele pode ser escrito como soma de dois quadrados.

P14) Sejam a, b, c três números consecutivos. Mostre que o cubo do maior não pode ser escrito como soma dos cubos dos menores.

P15) Fatorar:
a) $q(x)=x^5+x^4+1$

b) $q(x) = x^7 + x^6 + x + 1$
c) $q(x) = x^8 - x^7 + x^4 + x + 1$
d) $q(x) = x^{10} + x^7 - x^4 + x + 2$
e) $q(x) = 2007x^8 + 2006x^7 - 2005x^4 - 2006x^2 + 1$

P16) Prove que o polinômio $(a+b+c)^{3333} - a^{3333} - b^{3333} - c^{3333}$ é divisível pelo polinômio $(a+b+c)^3 - a^3 - b^3 - c^3$.

P17) (IME) que o produto $N = (a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$ é múltiplo de 12, para quaisquer inteiros a, b, c, d.