

Congruências

Congruências.

Referência: Discrete Mathematics with Graph Theory
Edgar Goodaire e Michael Parmenter, 3rd ed 2006
Capítulo: 4

Aritmética horária

	0-24	0-12
5	5	5
17	17	5
8+6	14	2
16+3*7	13	1
10+3*8	10	10



		Registo com 8 bits							
250		1	1	1	1	1	0	1	0
251		1	1	1	1	1	0	1	1
252		1	1	1	1	1	1	0	0
253		1	1	1	1	1	1	0	1
254		1	1	1	1	1	1	1	0
255		1	1	1	1	1	1	1	1
0		0	0	0	0	0	0	0	0
1		0	0	0	0	0	0	0	1

Congruência

- ❑ **Definição:** seja $n > 1$ um número natural fixo. Dados inteiros a e b , diz-se que a é congruente com b módulo n e escreve-se $a \equiv b \pmod{n}$ se e só se $n | (a-b)$. O número n é o módulo da congruência.
- ❑ Exemplos:
 - $3 \equiv 17 \pmod{7}$ porque $3-17=-14$ é divisível por 7
 - $-2 \equiv 13 \pmod{3}$ porque $-2-13=-15$ é divisível por 3
- ❑ Propriedades da congruência em \mathbb{Z}
 - Reflexiva $a \equiv a \pmod{n}$ para todo o a
 - Simétrica se $a \equiv b \pmod{n}$ então $b \equiv a \pmod{n}$
 - Transitiva se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ então $a \equiv c \pmod{n}$
 - Portanto: **relação de equivalência**

Classes de congruência

- ❑ **Definição:** a classe de congruência $\text{mod } n$ de um inteiro a é o conjunto de todos os inteiros com que a é congruente $\text{mod } n$ e denota-se \bar{a}

$$\bar{a} = \{b \in \mathbb{Z} \mid a \equiv b(\text{mod } n)\}$$

- ❑ Ex: seja $n=5$; como $-8-17=-25$ é divisível por 5, -8 e 17 estão na mesma classe de congruência $-8 \in \overline{17}$, da mesma forma que $17 \in \overline{-8}$. Verifique que $\overline{-8} = \overline{17}$.

Exemplo

- ❑ Ex: determine todas as classes de congruência mod 5
- ❑ $\bar{0} = \{b \in \mathbb{Z} | b \equiv 0 \pmod{5}\} = \{b \in \mathbb{Z} | 5 \mid (b-0)\} = \{b \in \mathbb{Z} | b = 5k, k \in \mathbb{Z}\} = 5\mathbb{Z}$
- ❑ $\bar{1} = \{b \in \mathbb{Z} | b \equiv 1 \pmod{5}\} = \{b \in \mathbb{Z} | b = 5k + 1, k \in \mathbb{Z}\} = 5\mathbb{Z} + 1$
- ❑ $\bar{2} = \{b \in \mathbb{Z} | b = 5k + 2, k \in \mathbb{Z}\} = 5\mathbb{Z} + 2$
- ❑ $\bar{3} = \{b \in \mathbb{Z} | b = 5k + 3, k \in \mathbb{Z}\} = 5\mathbb{Z} + 3$
- ❑ $\bar{4} = \{b \in \mathbb{Z} | b = 5k + 4, k \in \mathbb{Z}\} = 5\mathbb{Z} + 4$
- ❑ Estas classes formam uma **partição** em \mathbb{Z}

$a \pmod n$

- ❑ **Proposição:** para inteiros a, b , e n ,

$$a \equiv b \pmod n \leftrightarrow \bar{a} = \bar{b}$$

- ❑ **Definição:** se $n > 1$ é um natural e a um inteiro, então $a \pmod n$ é o resto r , $0 \leq r < n$, da divisão de a por n

- ❑ **Proposição:** qualquer inteiro é congruente mod n com o seu resto da divisão por n . Assim, há n possíveis classes de congruência mod n correspondendo a cada um dos n possíveis restos

- $\bar{0} = n\mathbb{Z}$

- $\bar{1} = n\mathbb{Z} + 1$

- $\bar{2} = n\mathbb{Z} + 2$

- ...

- $\overline{n-1} = n\mathbb{Z} + (n-1)$

Substituir um inteiro fora da gama 0 a $n-1$ pelo resto da divisão por n e trabalhar só dentro da gama com $a \pmod n$

Exemplos

❑ Calcular

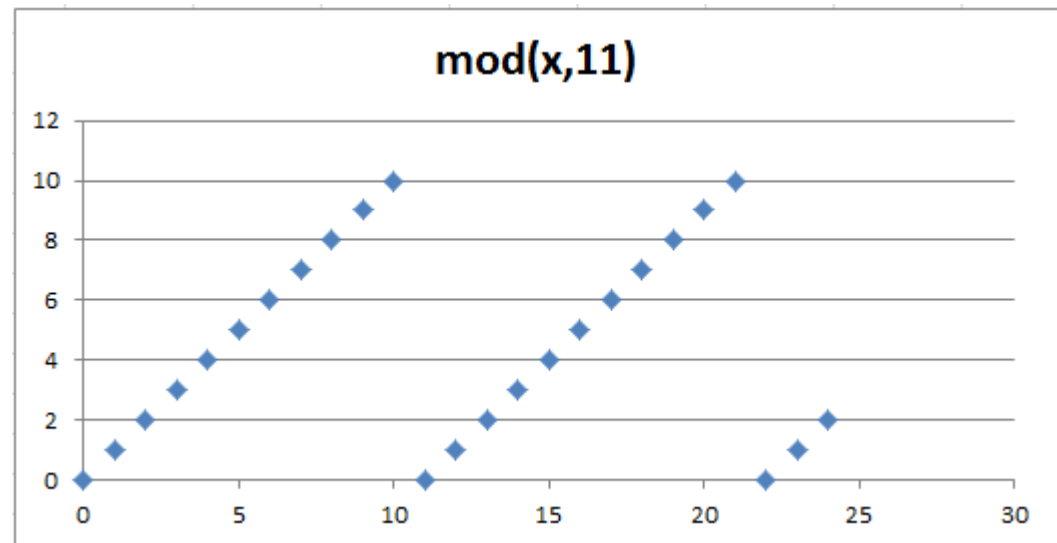
- $28 \pmod{6}$ 4
- $-17 \pmod{5}$ 3
- $-30 \pmod{9}$ 6
- $3958 \pmod{18}$ 16
- $-3958 \pmod{18}$ 2

❑ Esboce a função

$$y = x \pmod{n}$$

[Excel: $y = \text{mod}(x,n)$]

- $n=11, 0 \leq x \leq 24$

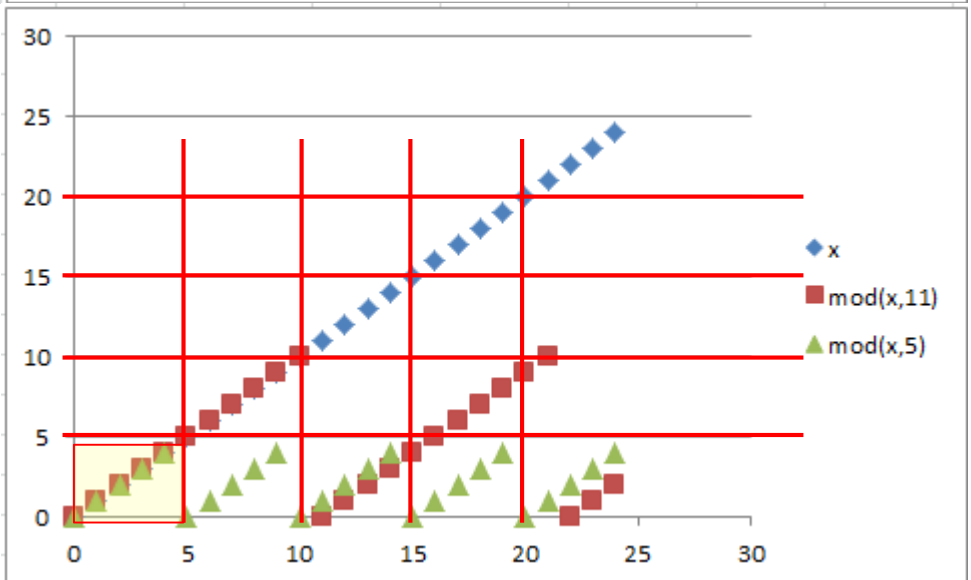
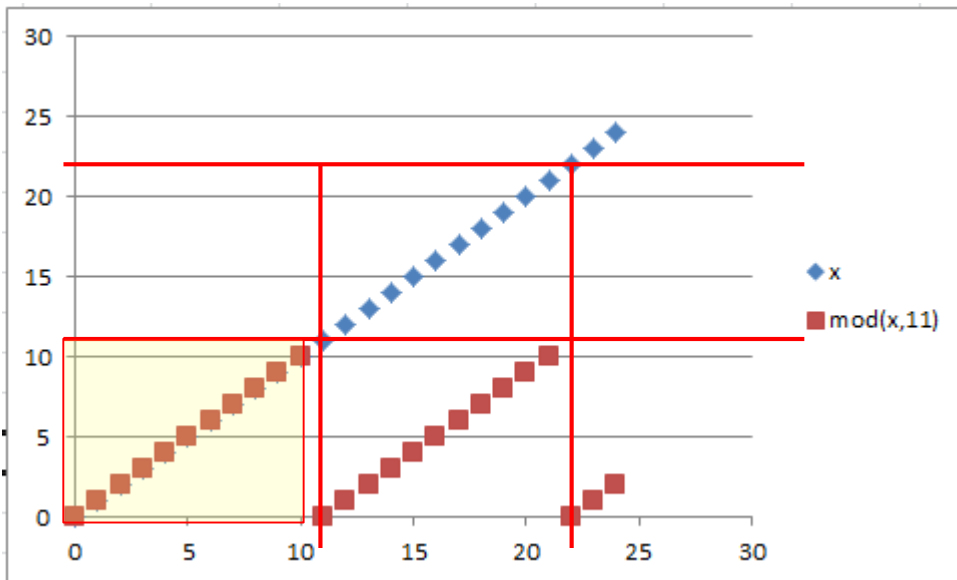
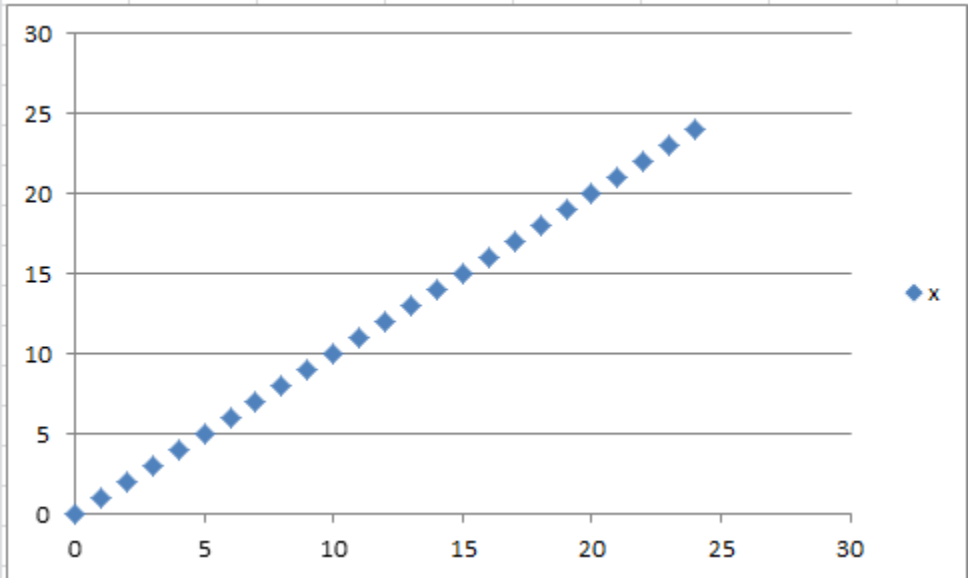


Exemplos

□ Esboce as funções

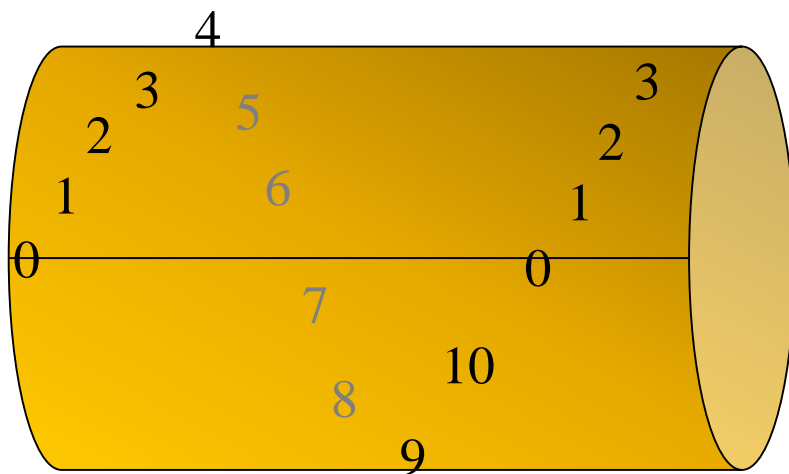
- $y = x$
- $y \equiv x \pmod{11}$
- $y \equiv x \pmod{5}$

O espaço como que se enrola e volta a zero ao atingir o módulo ficando confinado a $n \times n$ (relógio)

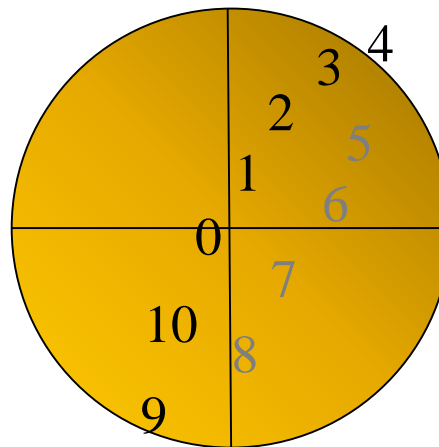


Aplicar o módulo

❑ No eixo dos yy



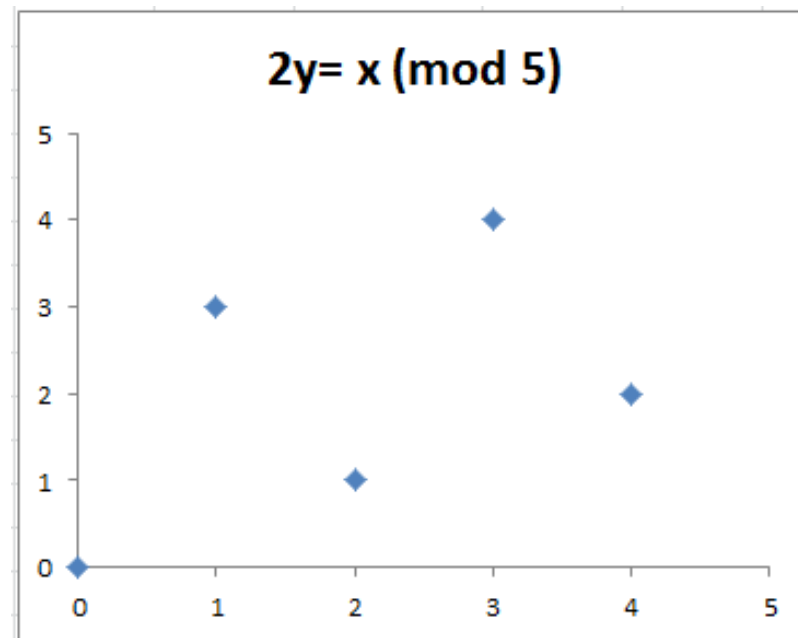
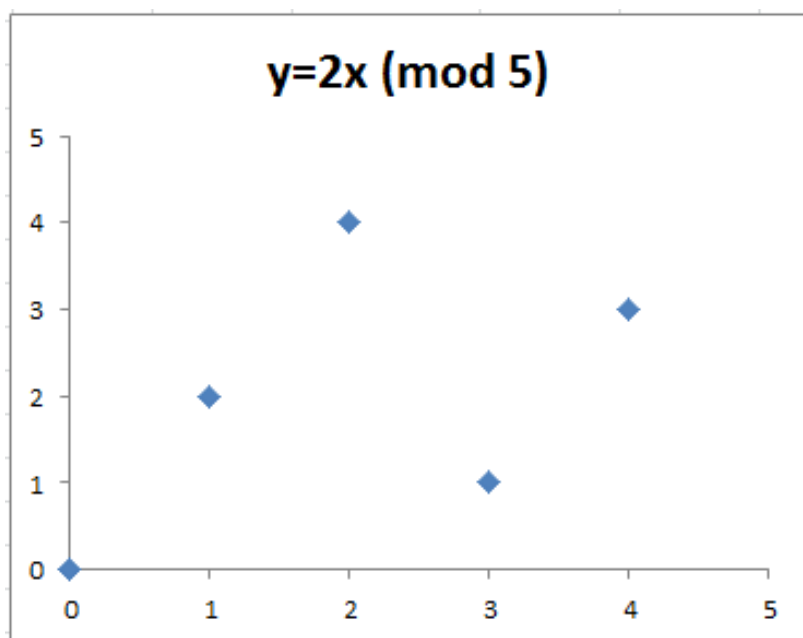
Nos eixos dos xx e dos yy



❑ Ao atingir o módulo volta a zero

Redução ao espaço modular

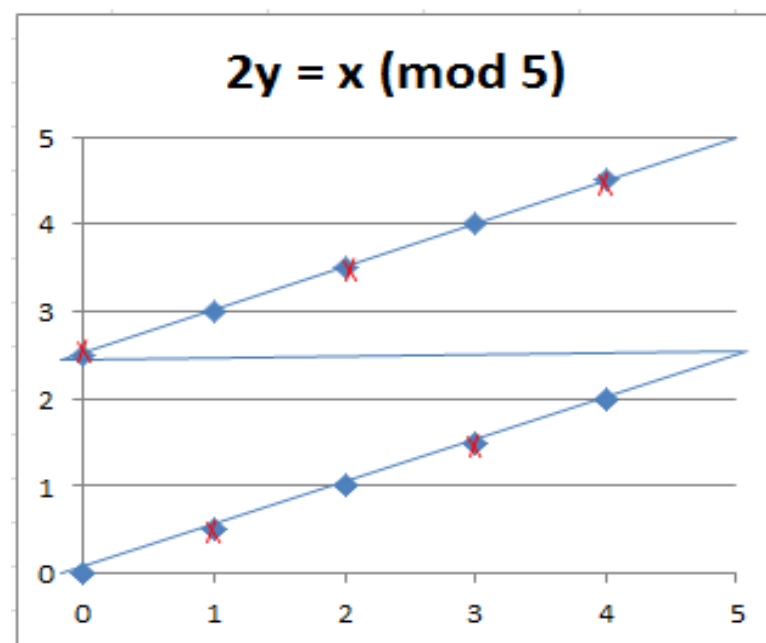
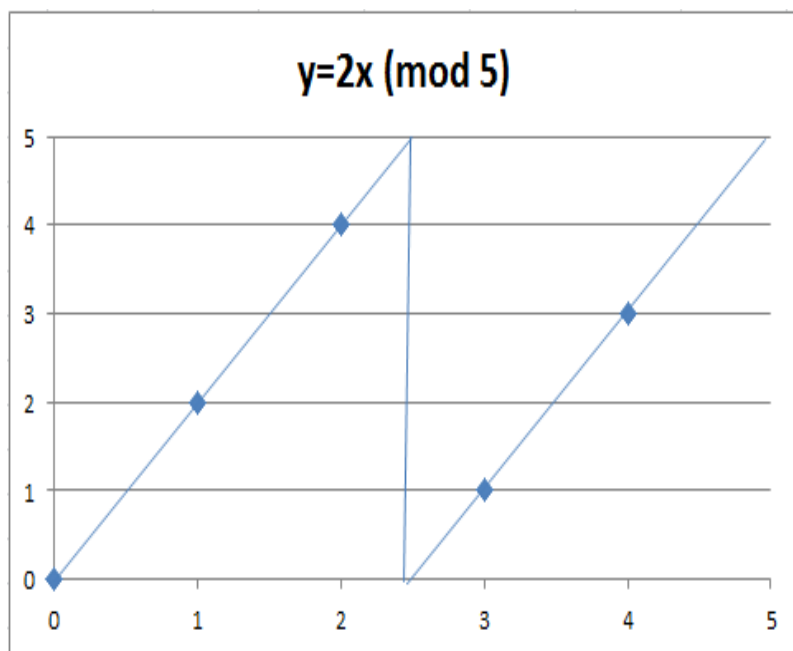
- ❑ Esboce $y \equiv 2x \pmod{5}$ e $2y \equiv x \pmod{5}$ mas colocando no eixo horizontal $x \pmod{5}$



- A distribuição de pontos é um pouco obscura

Redução ao espaço modular

- ❑ Esboce $y \equiv 2x \pmod{5}$ e $2y \equiv x \pmod{5}$ mas colocando no eixo horizontal $x \pmod{5}$



- Nota ao 2º caso: os pontos marcados com **x** não fazem parte da função porque não são inteiros; é necessário ir até $x=10$ para marcar os pontos todos

Equações

□ $2x \equiv 0 \pmod{4}$

- R: 0, 2, 4, 6, 8, ...
- $[2(0) \equiv 0 \pmod{4}, 2(2) \equiv 0 \pmod{4}, 2(4) \equiv 0 \pmod{4}, \dots]$
- Só se apresentam as soluções 0 e 2 porque são as únicas entre 0 e 4-1
- Resultado: $x=0$ ou $x=2$ soluções múltiplas convenção



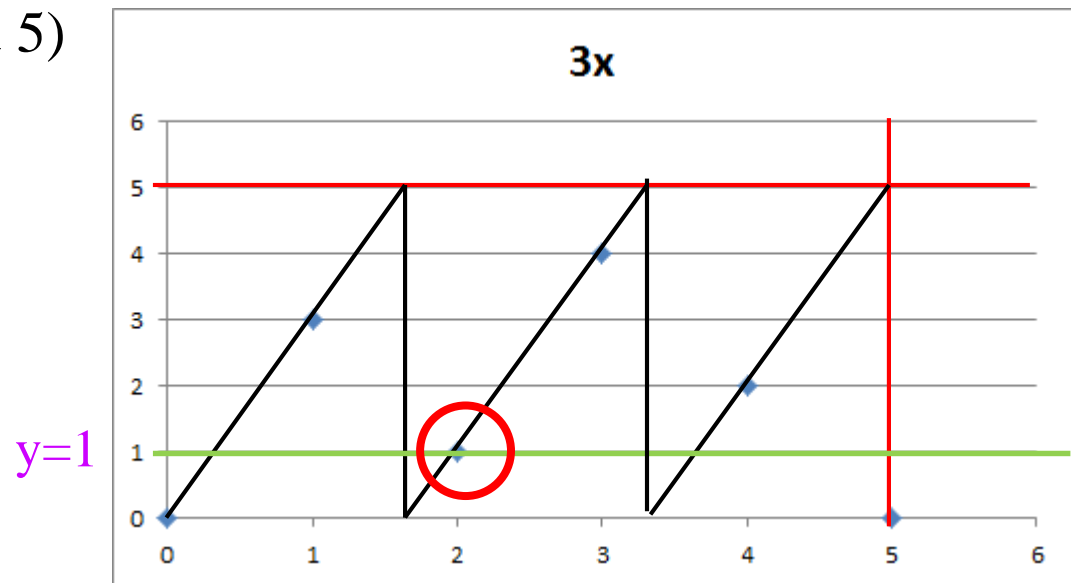
Equações

□ $3x \equiv 1 \pmod{5}$

- $x=0$ $3x=0 \equiv 0 \pmod{5}$
- $x=1$ $3x=3 \equiv 3 \pmod{5}$
- $x=2$ $3x=6 \equiv 1 \pmod{5}$
- $x=3$ $3x=9 \equiv 4 \pmod{5}$
- $x=4$ $3x=12 \equiv 2 \pmod{5}$
- Resultado: $x=2$

solução simples

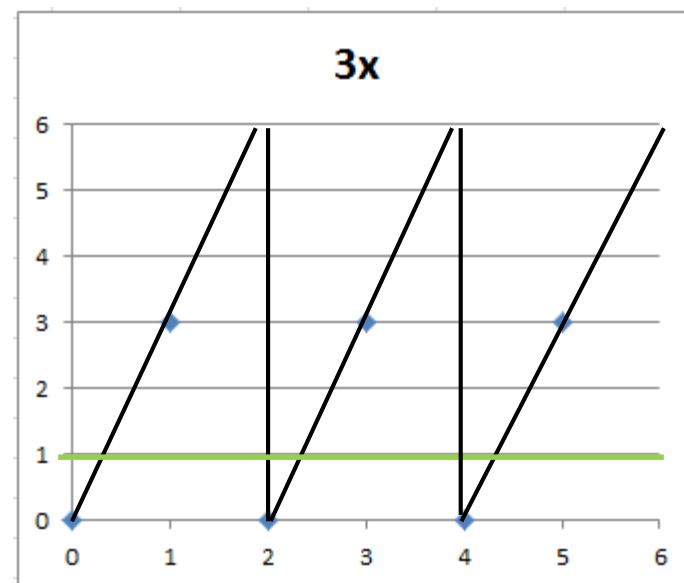
- De cada vez que a linha atinge o limite do módulo, dá a volta e recomeça em 0
- O cruzamento de linhas $3x \pmod{5}$ e $y \equiv 1 \pmod{5}$ só é solução se coincidir com um ponto



Mais equações

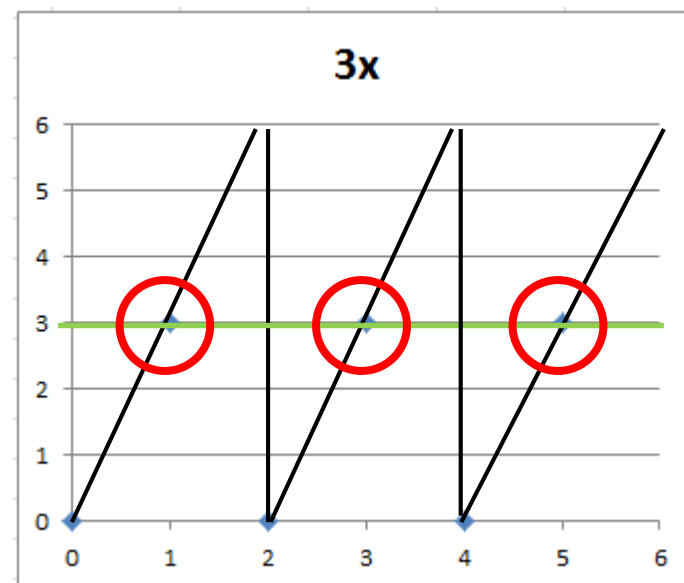
□ $3x \equiv 1 \pmod{6}$

- $3(0)=0$ $3(1)=3$
- $3(2)=6 \equiv 0$ $3(3)=9 \equiv 3$
- $3(4)=12 \equiv 0$ $3(5)=15 \equiv 3$
- Impossível
- Mudar o n muda a equação



□ $3x \equiv 3 \pmod{6}$

- R: $x=1, x=3, x=5$
- Múltipla



Aritmética modular

- ❑ **Proposição:** Se $a \equiv x \pmod{n}$ e $b \equiv y \pmod{n}$, então
 - $a+b \equiv x+y \pmod{n}$
 - $ab \equiv xy \pmod{n}$

- ❑ **Problema:** suponha que a e b são inteiros e que $3 \mid (a^2+b^2)$.
Mostre que $3 \mid a$ e $3 \mid b$.

- ❑ **R:** pretende-se mostrar que $a \equiv 0 \pmod{3}$ e $b \equiv 0 \pmod{3}$.
Prova por contradição: se afirmação falsa então $a \equiv 1$ ou $2 \pmod{3}$; daí que $a^2 \equiv 1$ ou $a^2 \equiv 4 \equiv 1 \pmod{3}$; da mesma forma $b^2 \equiv 1 \pmod{3}$; portanto $a^2+b^2 \equiv 1+1 \equiv 2 \pmod{3}$, o que contradiz o pressuposto.

Redução ao espaço modular

- ❑ $1017+2876 \pmod{7} = 3893 \equiv 1 \pmod{7}$
- ❑ $1017+2876 \equiv 2 + 6 \equiv 1 \pmod{7}$
- ❑ $(1017)(2876) \equiv (2)(6) = 12 \equiv 5 \pmod{7}$
- ❑ $(1017)^2 \equiv 2^2 = 4$
- ❑ $(1017)^3 = (1017)^2(1017) \equiv 4(2) \equiv 1$
- ❑ Simplificação das operações tirando partido da modularidade quer nos operandos quer nos resultados intermédios

Cuidado com divisão e multiplicação

- ❑ Dividir a congruência, verdadeira, $30 \equiv 12 \pmod{9}$ por 3 dá $10 \equiv 4 \pmod{9}$ o que é falso.
- ❑ **Proposição (divisão da congruência):** se $ac \equiv bc \pmod{n}$ e $\text{mdc}(c,n)=1$, então $a \equiv b \pmod{n}$.
 - Prova: dado que $\text{mdc}(c,n)=1$ existem inteiros x e y tais que $cx+ny=1$. A congruência significa que $ac-bc=kn$, para algum inteiro k . Portanto $(a-b)cx=kcx$ e $(a-b)(1-ny)=kcx$. De onde se conclui que $a-b=n(kx+y(a-b))$. Portanto $n|(a-b)$ e então $a \equiv b \pmod{n}$.
- ❑ No exemplo acima o problema está em $\text{mdc}(3,9)=3$.
- ❑ Dividir $28 \equiv 10 \pmod{3}$ por 2 não tem problema dado que $\text{mdc}(2,3)=1$. O resultado é $14 \equiv 5 \pmod{3}$
- ❑ **Exercício:** resolver $2x \equiv 1 \pmod{9}$ e $6x \equiv 3 \pmod{9}$
 - As congruências são equivalentes? As soluções são as mesmas?

Solução de uma congruência linear

- ❑ **Proposição (congruência linear):** Se $ax \equiv b \pmod{n}$ e $\text{mdc}(a,n)=d$, então a congruência tem d soluções sse $d|b$.
Seja x' a solução de $\frac{a}{d}x' \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. As soluções da primeira congruência são $x = x' + k\frac{n}{d}$, com $k=0, \dots, d-1$.
- ❑ Voltando ao exemplo $6x \equiv 3 \pmod{9}$
 - $d=\text{mdc}(6,9)=3$
 - $\frac{6}{3}x' \equiv \frac{3}{3} \pmod{\frac{9}{3}}$
 - $2x' \equiv 1 \pmod{3}$ tem exatamente uma solução $x'=2$, porque 2 e 3 são primos entre si
 - As soluções da congruência dada são assim
 - $x=2+0*3=2$
 - $x=2+1*3=5$
 - $x=2+2*3=8$

Solução gráfica

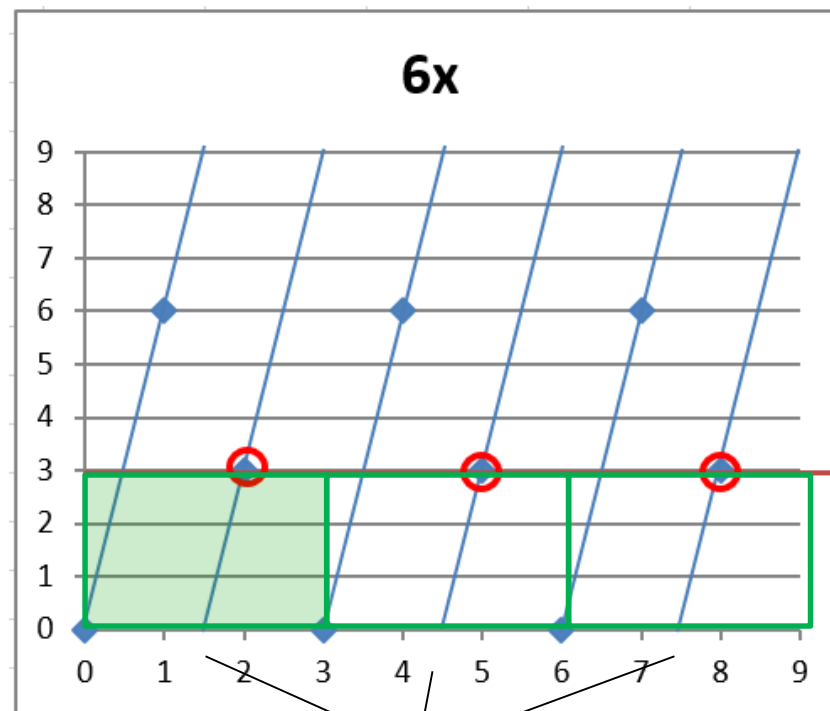
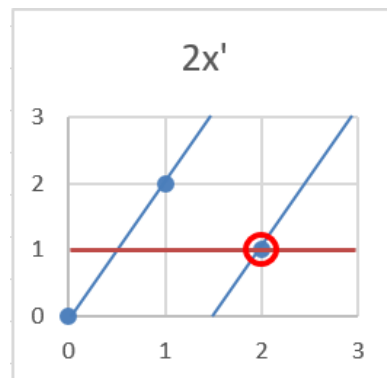
❑ $2x' \equiv 1 \pmod{3}$

❑ $x' = 2$

❑ $6x \equiv 3 \pmod{9}$

❑ $x=2, x=5, x=8$

Quando $\text{mdc}(a,n)=d > 1$, o espaço modular pode ser subdividido em d subespaços modulares no eixo dos xx e a solução é única no primeiro e repetida nos seguintes.



$3=\text{mdc}(6,9)$

Prova

- ❑ Se $ax \equiv b \pmod{n}$ então $ax = b + kn$ para algum inteiro k . Como $d = \text{mdc}(a, n)$, $b = ax - kn = a' dx - kn' d = (a' x - kn') d$ e, portanto, b é um múltiplo de d , $d | b$.
- ❑ Do algoritmo de Euclides, d é uma combinação linear de a e n , $d = ra + sn$. Se b for múltiplo de d , então $b = ax + ny$. Daqui conclui-se que $ax \equiv b \pmod{n}$ e portanto existe uma solução quando b é um múltiplo de d .

Prova (cont.)

- ❑ Supondo que $ax \equiv b \pmod{n}$ tem solução, então $d|b$ e $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ também tem solução. Seja x' essa solução. Então $\frac{a}{d}x' = \frac{b}{d} + k\frac{n}{d}$, para algum inteiro k , e $ax' = b + kn$.
- ❑ As soluções de $ax \equiv b \pmod{n}$ são da forma $x = x' + l\frac{n}{d}$, $l = 0, \dots, (d-1)$. Para isso, $ax - b = jn$, para algum inteiro j .
- ❑ $a(x' + l\frac{n}{d}) - b = jn$
- ❑ $ax' + al\frac{n}{d} - b = jn$
- ❑ $b + kn + al\frac{n}{d} - b = jn$
- ❑ $(k + a\frac{l}{d})n = jn$
- ❑ Como $d|a$, j é um inteiro para cada valor de l de 0 a $d-1$

Sistemas de equações

- ❑ Resolver os seguintes pares de congruências

$$\begin{cases} 2x + 3y \equiv 1 \pmod{6} \\ x + 3y \equiv 4 \pmod{6} \end{cases}$$

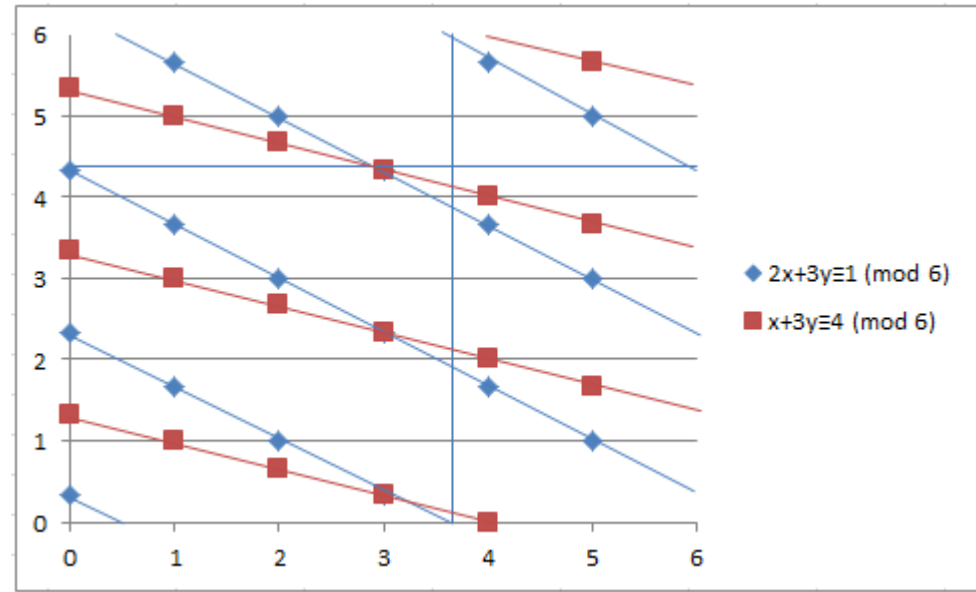
- Somar as duas equações dá $3x + 6y \equiv 5 \pmod{6}$
- Como $6y \equiv 0 \pmod{6}$, fica $3x \equiv 5 \pmod{6}$; esta equação não tem solução

$$\begin{cases} 2x + 3y \equiv 1 \pmod{6} \\ x + 3y \equiv 5 \pmod{6} \end{cases}$$

- Neste caso somar as equações dá $3x \equiv 0 \pmod{6}$ que tem como soluções $x \equiv 0, x \equiv 2, x \equiv 4 \pmod{6}$
- Se $x \equiv 0$ a segunda equação fica $3y \equiv 5 \pmod{6}$ sem solução
- Se $x \equiv 2$ fica $2 + 3y \equiv 5$ ou $3y \equiv 3$ com solução $y \equiv 1, y \equiv 3, y \equiv 5$
- Se $x \equiv 4$ tem-se $4 + 3y \equiv 5$, sem solução
- Resultado: há três pares de soluções: $x \equiv 2$ e $y \equiv 1, y \equiv 3, y \equiv 5$

Resolução gráfica

- Azul: $2x+3y \equiv 1 \pmod{6}$
 - $y = -(2/3)x + (1/3) \pmod{6}$
 - $x=2 \quad y=5,1,3$
 - $x=5 \quad y=3,5,1$
- Castanho: $x+3y \equiv 4 \pmod{6}$
 - $y = -(1/3)x + (4/3) \pmod{6}$
 - $x=1 \quad y=1,3,5$
 - $x=4 \quad y=0,2,4$
- Não há nenhum ponto de ambas as coordenadas inteiras comum às duas retas, logo não há solução



Só interessam os pontos de ambas as coordenadas inteiras

Resolução gráfica (cont.)

❑ $2x+3y \equiv 1 \pmod{6}$

– $y = -(2/3)x + (1/3) \pmod{6}$

– $x=2 \quad y=5,1,3$

– $x=5 \quad y=3,5,1$

❑ $x+3y \equiv 5 \pmod{6}$

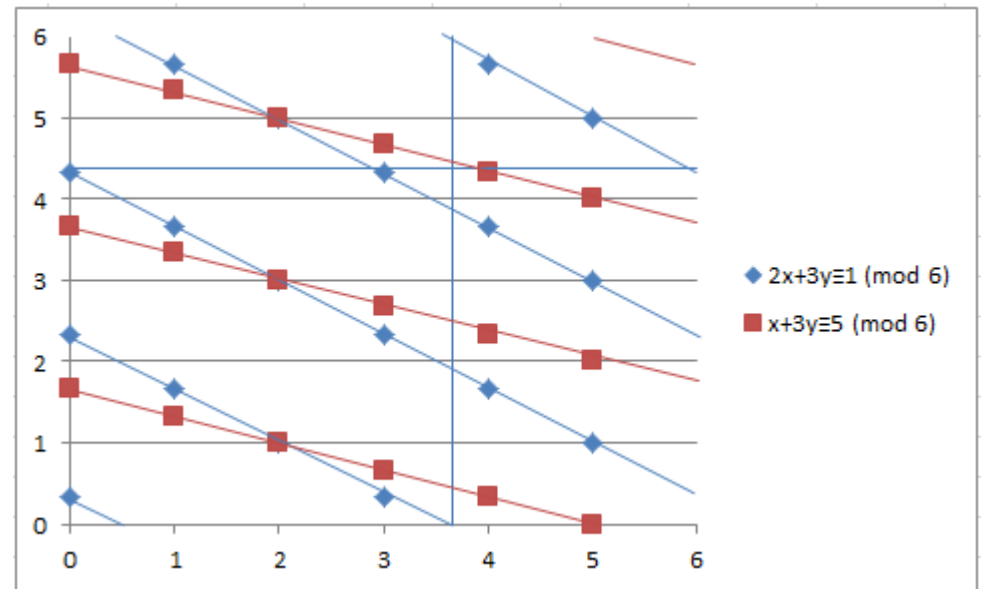
– $y = -(1/3)x + (5/3) \pmod{6}$

– $x=2 \quad y=1,3,5$

– $x=5 \quad y=0,2,4$

❑ Aqui já há coincidência em $x=2, y=1,3,5$

❑ Três soluções $(2,1), (2,3), (2,5)$



Solução única

- ❑ Todos os inteiros têm um **simétrico** módulo n
 - Isto é, existe sempre um x tal que $a+x \equiv 0 \pmod{n}$, eg. $x=n-a$
 - Então todas as congruências da forma $a+x \equiv b \pmod{n}$ têm solução
- ❑ Nem todas as congruências da forma $ax \equiv b \pmod{n}$ têm solução (o inverso módulo n nem sempre existe)
- ❑ **Proposição:** seja $n>1$ um número natural e a um inteiro tal que $\text{mdc}(a,n)=1$
 - Existe um inteiro s tal que $sa \equiv 1 \pmod{n}$, a que se chama **inverso** de $a \pmod{n}$.
 - Para qualquer inteiro b , a congruência $ax \equiv b \pmod{n}$ tem solução.
 - A solução de $ax \equiv b \pmod{n}$ é **única** mod n , no sentido de que $ax_1 \equiv b \pmod{n}$ e $ax_2 \equiv b \pmod{n}$ implica $x_1 \equiv x_2 \pmod{n}$

Determinação do inverso mod n

- ❑ O resultado anterior permite resolver uma congruência

$$ax \equiv b \pmod{n}$$

como se fosse uma equação fazendo $x \equiv a^{-1}b \pmod{n}$

- ❑ Para determinar o inverso note-se que, sendo a e n primos entre si, $\gcd(a,n) = 1$

- Já sabemos que existem s e t tais que $sa+tn=1$
- Então $sa \equiv 1 \pmod{n}$, dado que $tn \equiv 0 \pmod{n}$
- Conclui-se que $s=a^{-1}$

- ❑ Exemplo: resolva a congruência $20x \equiv 101 \pmod{637}$

- Do algoritmo de Euclides, $-7(637)+223(20)=1$
- $223(20) \equiv 1 \pmod{637}$ e portanto $223 = 20^{-1} \pmod{637}$
- Multiplicando ambos os lados por 223,

$$x \equiv 223(101) = 22523 \equiv 228 \pmod{637}$$

Ainda o Fermat

❑ **Pequeno Teorema de Fermat:** se p é um primo e p não divide c , então $c^{p-1} \equiv 1 \pmod{p}$

- Prova: como c e p são primos entre si, pela proposição da divisão de uma congruência por uma constante, pode concluir-se que nenhum par dentre os números $c, 2c, \dots, (p-1)c$ são congruentes mod p
 - em qualquer potencial congruência, a proposição permite simplificar o c e fica-se com dois números de classes de congruência mod p diferentes
- Também nenhum desses números é congruente com $0 \pmod{p}$, pela mesma razão
- Então, módulo p , os $p-1$ inteiros $c, 2c, \dots, (p-1)c$ têm que ser exatamente $1, 2, \dots, p-1$ por uma ordem qualquer. Portanto
$$c \cdot 2c \cdot 3c \cdot \dots \cdot (p-1)c \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$$
$$(p-1)! c^{p-1} \equiv (p-1)! \pmod{p}$$

$$c^{p-1} \equiv 1 \pmod{p} \text{ porque } \text{mdc}(p, (p-1)!) = 1$$

Aplicação

- ❑ O pequeno teorema de Fermat permite concluir que
 - $2^2 \equiv 1 \pmod{3}$
 - $4^6 \equiv 1 \pmod{7}$
 - $9^{10} \equiv 1 \pmod{11}$
 - $4^{13331} \equiv 4 \pmod{13331}$
 - $20^{40} \equiv 20^{4+3 \cdot 12} \equiv 20^4(20^{12})^3 \equiv 7^4(1)^3 \equiv 49^2 \equiv 10^2 \equiv 9 \pmod{13}$
 - No Excel não é possível calcular diretamente o resultado mas pode-se fazer a operação de multiplicar módulo 13 por 20, 40 vezes

Aplicação: ISBN

- ❑ Muitos números de identificação incluem um ou mais dígitos de verificação: ISBN (International Standard Book Number), cartão de cidadão, referência Multibanco, etc.
- ❑ ISBN-10 é um código de 10 dígitos de identificação dos livros (em vigor até 2007)
- ❑ O livro do Goodaire tem o código ISBN 0-13-167995-3
 - O primeiro grupo identifica o país ou o grupo linguístico
 - O segundo grupo identifica a editora
 - O terceiro grupo identifica o título
 - O quarto grupo é um dígito de verificação

Dígito de verificação (no ISBN)

- Estando os primeiros 9 determinados, o 10º é calculado de forma a que

$$a_1 + 2a_2 + 3a_3 + \dots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}$$

- **Verificação:** tendo o número, calcula-se se a soma pesada pela posição do dígito é congruente com 0 (mod 11)
- **Geração:** tendo os primeiros 9 dígitos, resolve-se a equação acima para a variável a_{10}
 - Se a_{10} for 10, então representa-se por X

Exercício

❑ Verificação ISBN 0-13-167995-3:

- $1(0)+2(1)+3(3)+4(1)+5(6)+6(7)+7(9)+8(9)+9(5)+10(3) \equiv 0 \pmod{11}$
- Qualquer erro de transcrição de um dos dígitos faz com que a congruência não seja 0; o software de verificação emite um alerta
- Erros em mais do que um dígito podem cancelar os efeitos, embora seja pouco provável

❑ Geração:

- Determine o dígito de verificação para o ISBN 0-914894-36-?
- $1(0)+2(9)+3(1)+4(4)+5(8)+6(9)+7(4)+8(3)+9(6)+10a_{10} \equiv 0 \pmod{11}$
- $6 + 10a_{10} \equiv 0 \pmod{11}$
- $a_{10} \equiv 6 \pmod{11}$

Interesse da soma pesada

- ❑ A soma é pesada pela posição do dígito para detetar um erro comum na transcrição que é a troca de dois dígitos
 - Se a soma não fosse pesada, só interessava quais os dígitos, independentemente da ordem
- ❑ ISBN-13
 - Fazer a soma pesada dos 12 primeiros dígitos, usando o coeficiente 1 para os ímpares e 3 para os pares, módulo 10

Congruências com módulos diferentes

❑ Exercício

- Qual é o número entre 100 e 500 que quando dividido por 12 dá resto 4 e quando dividido por 25 dá resto 15?

❑ Resposta

- A questão colocada é determinar os números que satisfazem o sistema de congruências
 - $x \equiv 4 \pmod{12}$
 - $x \equiv 15 \pmod{25}$
- Força bruta: $x = 4 + 12k = 15 + 25j$ k, j inteiros
- Outra solução
 - Uma vez que 12 e 25 são primos entre si, existem s e t tais que
 - $12s + 25t = 1$ (usar o algoritmo de Euclides)
 - $12(-2) + 25(1) = 1$
 - $x \equiv 15(12)(-2) + 4(25)(1) \pmod{12 \cdot 25} = -260, 40, \mathbf{340}, 640, \dots$

Notar que este sistema
tem módulos diferentes

Teorema Chinês dos Restos

- ❑ Suponha que m e n são números primos entre si.

Então, para quaisquer inteiros a e b , o par de congruências

- $x \equiv a \pmod{m}$
- $x \equiv b \pmod{n}$

tem uma solução única módulo mn .

❑ Prova:

- ❑ $sm + tn = 1$ (algoritmo de Euclides) (*)

- ❑ $x = a(tn) + b(sm)$ é uma solução das congruências

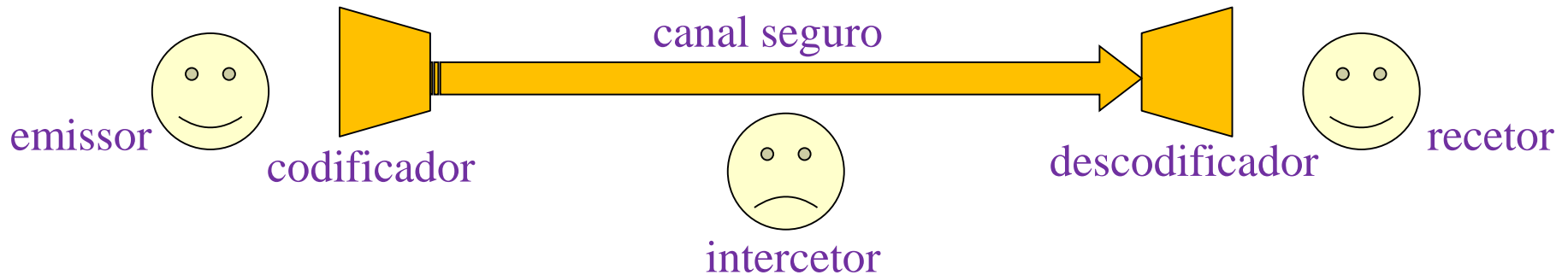
- $x \pmod{m} \equiv a(tn) \pmod{m}$ dado que $b(sm) \equiv 0 \pmod{m}$
- $\equiv a \pmod{m}$ dado que $tn \equiv 1 \pmod{m}$ ver (*)
- $x \pmod{n} \equiv b(sm) \pmod{n}$ dado que $a(tn) \equiv 0 \pmod{n}$
- $\equiv b \pmod{n}$ dado que $sm \equiv 1 \pmod{n}$ ver (*)

Representação de números grandes

- ❑ O resultado anterior pode ser generalizado para t congruências, desde que m_1, \dots, m_t sejam primos par a par
 - $x \equiv a_1 \pmod{m_1}$
 - $x \equiv a_2 \pmod{m_2}$
 - ...
 - $x \equiv a_t \pmod{m_t}$tem solução única módulo $m_1 m_2 \dots m_t$.
- ❑ Escolhendo $m_i = p_i^{\alpha_i}$ em que cada p_i é um primo, consegue-se representar de forma única um número grande à custa de t restos
- ❑ Se a e b forem representados por a_1, \dots, a_t e b_1, \dots, b_t então o **produto** ab é congruente com a representação $a_1 b_1, \dots, a_t b_t$
 - Determinar a escala por estimativa

Criptografia

- ❑ É o estudo das formas de encriptação (codificação) das mensagens entre um emissor e um recetor de forma a impedir que terceiros tenham acesso ao seu conteúdo



Problemas do método da tabela

- ❑ Há muitas técnicas de codificação

- Exemplo: estabelecer uma tabela de conversão dos caracteres

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	H	E	Q	U	I	C	K	B	R	O	W	N	F	X	J	M	P	S	V	L	A	Z	Y	D	G

- Mensagem: FCP GANHOU
 - Encriptada: IEJZCTFKXV

- Problema: enviar antes a tabela ao recetor

- Usar uma frase de um livro comum para fazer a conversão

- ❑ As línguas naturais têm uma distribuição de caracteres própria e construções de vocabulário e sintáticas específicas

- Com texto suficiente, consegue-se reconstruir a tabela de conversão, usando a comparação de frequências

- ❑ Estes métodos baseiam-se na confidencialidade da chave, conhecida pelos dois interlocutores

Codificação numérica

- ❑ A correspondência pode ser para números

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- ❑ Código de César: $E = f(M) = M+3 \pmod{26}$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- ❑ Generalizando: $E = f(M) = M+k \pmod{n}$

– $f(M)$ é o algoritmo, k é a chave, n o comprimento do alfabeto

Quantas chaves?

- ❑ Transformação afim: $E = f(M) = aM+b \pmod{n}$

– Aqui a chave é o par (a,b)

Ex: ~~(4,7)~~ (3,7) $\text{mdc}(a,n)=1$

Quantas chaves?

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E

Cifra de Hill

- ❑ Em vez de encriptar símbolo a símbolo, encriptar segmentos de texto de comprimento l , com transformação linear $A_{l \times l}$
 - Evita a correspondência biunívoca entre símbolo e sua encriptação
 - A transformação linear deve ser feita com aritmética modular, limitada ao comprimento do alfabeto n
- ❑ Encriptação: $E_k = AM_k \pmod{n}$
 - $E_{kl+1..(k+1)l} = A_{l \times l} M_{kl+1..(k+1)l}$
- ❑ Desencriptação: $M_k = A^{-1}E_k \pmod{n}$
- ❑ Condição a respeitar para garantir unicidade
 - $\text{mdc}(|A|, n) = 1$
- ❑ Evita a criptanálise baseada em frequências de ocorrência
- ❑ Fácil de quebrar se for conhecido um par (mensagem em claro, mensagem cifrada)

Exemplo de cifra de Hill

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	?	.
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

□ $M = \text{"EUCLID"}$ $M = \begin{bmatrix} 4 & 20 & 2 \\ 11 & 8 & 3 \end{bmatrix}$

□ $A = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 1 & 8 \\ 1 & 3 & 2 \end{bmatrix}$ $M_0 = \begin{bmatrix} 4 \\ 20 \\ 2 \end{bmatrix}$ $M_1 = \begin{bmatrix} 11 \\ 8 \\ 3 \end{bmatrix}$

□ **Enciptar** $E_0 = AM_0 = \begin{bmatrix} 34 \\ 52 \\ 68 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 23 \\ 10 \end{bmatrix} \pmod{29}$

□ $E_1 = AM_1 = \begin{bmatrix} 39 \\ 76 \\ 41 \end{bmatrix} \equiv \begin{bmatrix} 10 \\ 18 \\ 12 \end{bmatrix} \pmod{29}$

□ $E = \text{"FXKKSM"}$

Matriz inversa em aritmética modular

- $\square A^{-1} = \frac{1}{|A|} \text{adj}(A) \equiv |A|^{-1} \text{adj}(A) \pmod{n}$
- $\square |A| = -11 \equiv 18 \pmod{29}$
- $\square |A|^{-1} \equiv 18^{-1} \equiv -8 \equiv 21$
- $\square A^{-1} \equiv 21 \begin{bmatrix} -22 & 7 & 5 \\ 0 & 1 & -4 \\ 11 & -5 & -2 \end{bmatrix} \equiv \begin{bmatrix} 2 & 2 & 18 \\ 0 & 21 & 3 \\ 28 & 11 & 16 \end{bmatrix} \pmod{29}$
- $\square \text{Desencriptar } M_0 = A^{-1}E_0 = A^{-1} \begin{bmatrix} 5 \\ 23 \\ 10 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 20 \\ 2 \end{bmatrix} \pmod{29}$
- $\square M_1 = A^{-1}E_1 = A^{-1} \begin{bmatrix} 10 \\ 18 \\ 12 \end{bmatrix} \equiv \begin{bmatrix} 11 \\ 8 \\ 3 \end{bmatrix} \pmod{29}$
- $\square M = \text{“EUCLID”}$

$$\text{Em } \mathbb{R} \begin{bmatrix} 2 & -\frac{7}{11} & -\frac{5}{11} \\ 0 & -\frac{1}{11} & \frac{4}{11} \\ -1 & \frac{5}{11} & \frac{2}{11} \end{bmatrix} = -\frac{1}{11} \begin{bmatrix} -22 & 7 & 5 \\ 0 & 1 & -4 \\ 11 & -5 & -2 \end{bmatrix}$$

Sistema RSA de chave pública

- ❑ Ideia na base dos sistemas usados para encriptar as comunicações na Internet e os dados nos computadores
 - Rivest, Shamir e Adleman (1977)
- ❑ Este sistema baseia-se na existência de pares de chaves para cada interlocutor
 - Chave pública de A, disponível num servidor de chaves público, serve para qualquer pessoa encriptar a mensagem M para A
 - Chave privada de A, só conhecida por A, serve para desencriptar M

Processo

❑ Preparação:

- Escolher dois números primos diferentes p e q e um número natural s primo com $(p-1)$ e com $(q-1)$; calcular $r=pq$
- Calcular a e b pelo algoritmo de Euclides, dado que $\text{mdc}(s,p-1)=1$, $\text{mdc}(s,q-1)=1$
 - $as + x(p-1) = 1$
 - $bs + y(q-1) = 1$
- Publicitar r e s

❑ Encriptação:

- Calcular $E \equiv M^s \pmod{r}$ e enviar E

❑ Desencriptação

- $M \equiv E^a \pmod{p}$ e $M \equiv E^b \pmod{q}$
- Calcular M pelo Teorema Chinês dos Restos

Exemplo

❑ Preparação: $p=17$, $q=59$, $r=1003$, $s=3$

- $as+x(p-1) = a(3)+x(16) = 1$ $11(3)+(-2)(16)=1$ $a=11$
- $bs+y(q-1) = b(3)+y(58) = 1$ $39(3)+(-2)(58)=1$ $b=39$

❑ Encriptação

- Mensagem: GO $M=715$ $E \equiv M^s \equiv 715^3 \equiv 579 \pmod{1003}$
- Transmite E

❑ Desencriptação

- $E^a = 579^{11} \equiv 1^{11} \equiv 1 \pmod{17}$
- $E^b = 579^{39} \equiv 7 \pmod{59}$
- $17n+59m=1$ $17(7)+59(-2)=1$
- $M = 7(17)(7) + (1)(59)(-2) = 715$

Justificação

- ❑ Como $E \equiv M^s \pmod{r}$ temos que $E \equiv M^s \pmod{p}$ e $E \equiv M^s \pmod{q}$
- ❑ Como $as+x(p-1)=1$
 - $M = M^{as+x(p-1)} = (M^s)^a(M^{p-1})^x \equiv E^a \pmod{p}$ pelo Pequeno Teorema de Fermat
 - $M = M^{bs+x(q-1)} = (M^s)^b(M^{q-1})^x \equiv E^b \pmod{q}$ idem
- ❑ Então, pelo Teorema Chinês dos Restos, M é determinado unicamente módulo r
- ❑ Isto só é verdade para mensagens $M < r$
- ❑ Para mensagens maiores, segmenta-se a mensagem em blocos que correspondam a um inteiro menor que $r=pq$