

Minicurso de Criptografia - Dia 2

Dyckson Ternoski

Semana da Matemática 2020



O que veremos hoje?

- ① Números Primos
- ② Congruência Modular
- ③ Aritmética Modular
- ④ Divisão Modular
- ⑤ Potências
- ⑥ Função ϕ de Euler
- ⑦ Teoremas de Fermat e Euler

Números Primos

Definição: Número primo

Dizemos que um número p é primo se, e somente se, seus únicos divisores inteiros são 1, -1, p e $-p$.

Definição: Número primo

Dizemos que um número p é primo se, e somente se, seus únicos divisores inteiros são 1, -1, p e $-p$.

Definição: Números coprimos

Dois números são ditos coprimos se não possuem nenhum divisor em comum além de 1 e -1. Além disso, o *mdc* entre eles é 1.

Resultados importantes

Teorema Fundamental da Aritmética (TFA)

Todo número inteiro ou é primo ou é um produto de primos. Além disso, sua decomposição é única.

Resultados importantes

Teorema Fundamental da Aritmética (TFA)

Todo número inteiro ou é primo ou é um produto de primos. Além disso, sua decomposição é única.

Ideia: Seja p um número inteiro. Queremos mostrar que, se p não for primo, então ele pode ser escrito como

Teorema Fundamental da Aritmética (TFA)

Todo número inteiro ou é primo ou é um produto de primos. Além disso, sua decomposição é única.

Ideia: Seja p um número inteiro. Queremos mostrar que, se p não for primo, então ele pode ser escrito como

$$p = p_1 \cdot p_2 \cdot \dots \cdot p_n,$$

em que p_1, p_2, \dots, p_n são números primos não necessariamente distintos.

Resultados importantes

Teorema Fundamental da Aritmética (TFA)

Todo número inteiro ou é primo ou é um produto de primos. Além disso, sua decomposição é única.

Ideia: Seja p um número inteiro. Queremos mostrar que, se p não for primo, então ele pode ser escrito como

$$p = p_1 \cdot p_2 \cdot \dots \cdot p_n,$$

em que p_1, p_2, \dots, p_n são números primos não necessariamente distintos.

A demonstração disso segue pelo Princípio de Indução Forte.

Resultados importantes

Teorema Fundamental da Aritmética (TFA)

Todo número inteiro ou é primo ou é um produto de primos. Além disso, sua decomposição é única.

Ideia: Seja p um número inteiro. Queremos mostrar que, se p não for primo, então ele pode ser escrito como

$$p = p_1 \cdot p_2 \cdot \dots \cdot p_n,$$

em que p_1, p_2, \dots, p_n são números primos não necessariamente distintos.

A demonstração disso segue pelo Princípio de Indução Forte.

Unicidade: caso existam outros primos q_1, q_2, \dots, q_m que decompõem p , devemos ter $m = n$ e $q_i = p_i$, para todo i de 1 até n .

Resultados importantes

Teorema de Euclides

Existem infinitos números primos.

Resultados importantes

Teorema de Euclides

Existem infinitos números primos.

Demonstração: Suponha que exista uma lista finita de números primos, digamos $P = \{p_1, p_2, \dots, p_n\}$ e claro, todos distintos.

Resultados importantes

Teorema de Euclides

Existem infinitos números primos.

Demonstração: Suponha que exista uma lista finita de números primos, digamos $P = \{p_1, p_2, \dots, p_n\}$ e claro, todos distintos.

Note que $a = p_1 p_2 \dots p_n + 1$ é inteiro, mas não é múltiplo de p_1 . Tampouco de p_2 ou de qualquer outro primo pertencente a P .

Resultados importantes

Teorema de Euclides

Existem infinitos números primos.

Demonstração: Suponha que exista uma lista finita de números primos, digamos $P = \{p_1, p_2, \dots, p_n\}$ e claro, todos distintos.

Note que $a = p_1 p_2 \dots p_n + 1$ é inteiro, mas não é múltiplo de p_1 . Tampouco de p_2 ou de qualquer outro primo pertencente a P .

Mas pelo TFA, a é primo ou é produto de primos. Se a for primo, então temos a contradição. Se não for, sabemos que a é decomposto por primos que não pertencem a P .

Resultados importantes

Teorema de Euclides

Existem infinitos números primos.

Demonstração: Suponha que exista uma lista finita de números primos, digamos $P = \{p_1, p_2, \dots, p_n\}$ e claro, todos distintos.

Note que $a = p_1 p_2 \dots p_n + 1$ é inteiro, mas não é múltiplo de p_1 . Tampouco de p_2 ou de qualquer outro primo pertencente a P .

Mas pelo TFA, a é primo ou é produto de primos. Se a for primo, então temos a contradição. Se não for, sabemos que a é decomposto por primos que não pertencem a P .

Logo, não existem finitos números primos. Portanto, existem infinitos.

- Poincaré do Marcel

Resultados importantes

Postulado de Bertrand

Dado um número natural $n > 1$, existe ao menos um primo p tal que $n < p < 2n$.

Resultados importantes

Postulado de Bertrand

Dado um número natural $n > 1$, existe ao menos um primo p tal que $n < p < 2n$.

Demonstração: Por ser mais complicada, deixamos a cargo do leitor.

Resultados importantes

Postulado de Bertrand

Dado um número natural $n > 1$, existe ao menos um primo p tal que $n < p < 2n$.

Demonstração: Por ser mais complicada, deixamos a cargo do leitor.

Brincadeira, ela está disponível no link abaixo (basta clicar).

[Demonstração do Postulado de Bertrand](#)

Problemas em aberto

- Conjectura de Goldbach

Problemas em aberto

- Conjectura de Goldbach
- Infinitude dos Primos de Mersenne

Problemas em aberto

- Conjectura de Goldbach
- Infinitude dos Primos de Mersenne
- Conjectura dos Primos Gêmeos

Problemas em aberto

- Conjectura de Goldbach
- Infinitude dos Primos de Mersenne
- Conjectura dos Primos Gêmeos
- Conjectura de Legendre

Problemas em aberto

- Conjectura de Goldbach
- Infinitude dos Primos de Mersenne
- Conjectura dos Primos Gêmeos
- Conjectura de Legendre
- Infinitude dos primos da forma $n^2 + 1$

Problemas em aberto

- Conjectura de Goldbach
- Infinitude dos Primos de Mersenne
- Conjectura dos Primos Gêmeos
- Conjectura de Legendre
- Infinitude dos primos da forma $n^2 + 1$
- **Extra:** Hipótese de Lindelöf

Congruência Modular

Congruência Modular

O exemplo mais simples que temos é a contagem das horas dos dias.

Congruência Modular

O exemplo mais simples que temos é a contagem das horas dos dias.



Congruência Modular

O exemplo mais simples que temos é a contagem das horas dos dias.



Dizemos que dois momentos que diferem por 24 horas correspondem a horas equivalentes em dias diferentes.

Congruência Modular

O exemplo mais simples que temos é a contagem das horas dos dias.



Dizemos que dois momentos que diferem por 24 horas correspondem a horas equivalentes em dias diferentes.

Faremos algo semelhante, mas utilizando o conjunto dos números inteiros.

Congruência Modular

Para os números inteiros:

Congruência Modular

Para os números inteiros:

Definimos a congruência nos números inteiros da seguinte forma:

- ① Escolha um inteiro n
- ② Escolha um marco inicial
- ③ A partir dele, conte os números pulando de n em n .
- ④ Conte também de $-n$ em $-n$, isto é, no sentido inverso.

Congruência Modular

Para os números inteiros:

Definimos a congruência nos números inteiros da seguinte forma:

- ① Escolha um inteiro n
- ② Escolha um marco inicial
- ③ A partir dele, conte os números pulando de n em n .
- ④ Conte também de $-n$ em $-n$, isto é, no sentido inverso.

Resultado: os números contados são todos congruentes módulo n .

Congruência Modular

Para os números inteiros:

Definimos a congruência nos números inteiros da seguinte forma:

- ① Escolha um inteiro n
- ② Escolha um marco inicial
- ③ A partir dele, conte os números pulando de n em n .
- ④ Conte também de $-n$ em $-n$, isto é, no sentido inverso.

Resultado: os números contados são todos congruentes módulo n .

Exemplo: O conjunto dos números congruentes módulo n a partir do marco inicial 0 é:

$$\overline{0} = \{\dots, -4n, -3n, -2n, -n, 0, n, 2n, 3n, 4n, \dots\} = \overline{n} = \overline{-n} = \overline{2n} = \dots$$

Congruência Modular

Para os números inteiros:

Definimos a congruência nos números inteiros da seguinte forma:

- ① Escolha um inteiro n
- ② Escolha um marco inicial
- ③ A partir dele, conte os números pulando de n em n .
- ④ Conte também de $-n$ em $-n$, isto é, no sentido inverso.

Resultado: os números contados são todos congruentes módulo n .

Exemplo: O conjunto dos números congruentes módulo n a partir do marco inicial 0 é:

$$\bar{0} = \{\dots, -4n, -3n, -2n, -n, 0, n, 2n, 3n, 4n, \dots\} = \bar{n} = \overline{-n} = \overline{2n} = \dots$$

e chamamos tal conjunto de "classe $\bar{0}$ de \mathbb{Z}_n ".

Congruência Modular

Já o conjunto dos números congruentes a 1 módulo n é:

$$\bar{1} = \{..., -2n + 1, -n + 1, 1, n + 1, 2n + 1, ...\}$$

Congruência Modular

Já o conjunto dos números congruentes a 1 módulo n é:

$$\bar{1} = \{ \dots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \dots \}$$

Assim, entendemos que se $n = 2$, teríamos:

$$\bar{0} = \text{Conjunto dos números pares}$$

Congruência Modular

Já o conjunto dos números congruentes a 1 módulo n é:

$$\bar{1} = \{ \dots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \dots \}$$

Assim, entendemos que se $n = 2$, teríamos:

$\bar{0}$ = Conjunto dos números pares

$\bar{1}$ = Conjunto dos números ímpares

Congruência Modular

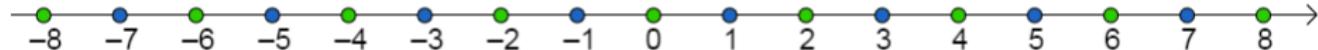
Já o conjunto dos números congruentes a 1 módulo n é:

$$\bar{1} = \{ \dots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \dots \}$$

Assim, entendemos que se $n = 2$, teríamos:

$\bar{0}$ = Conjunto dos números pares

$\bar{1}$ = Conjunto dos números ímpares



Congruência Modular

Já o conjunto dos números congruentes a 1 módulo n é:

$$\bar{1} = \{ \dots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \dots \}$$

Assim, entendemos que se $n = 2$, teríamos:

$\bar{0}$ = Conjunto dos números pares

$\bar{1}$ = Conjunto dos números ímpares



Dessa forma, $\bar{0} \cup \bar{1} = \mathbb{Z}$.

Congruência Modular

Definição: Congruência módulo n

Dizemos que a e b são congruentes módulo n se, e somente se, $a - b$ é múltiplo de n , e escrevemos

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

Congruência Modular

Definição: Congruência módulo n

Dizemos que a e b são congruentes módulo n se, e somente se, $a - b$ é múltiplo de n , e escrevemos

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

Exemplos:

Congruência Modular

Definição: Congruência módulo n

Dizemos que a e b são congruentes módulo n se, e somente se, $a - b$ é múltiplo de n , e escrevemos

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

Exemplos:

- $10 \equiv 0 \pmod{5}$, já que $10 - 0 = 10 = 5 \cdot 2$

Congruência Modular

Definição: Congruência módulo n

Dizemos que a e b são congruentes módulo n se, e somente se, $a - b$ é múltiplo de n , e escrevemos

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

Exemplos:

- $10 \equiv 0 \pmod{5}$, já que $10 - 0 = 10 = 5 \cdot 2$
- $14 \equiv 24 \pmod{5}$, já que $14 - 24 = -10 = 5 \cdot (-2)$

Congruência Modular

Definição: Congruência módulo n

Dizemos que a e b são congruentes módulo n se, e somente se, $a - b$ é múltiplo de n , e escrevemos

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

Exemplos:

- $10 \equiv 0 \pmod{5}$, já que $10 - 0 = 10 = 5 \cdot 2$
- $14 \equiv 24 \pmod{5}$, já que $14 - 24 = -10 = 5 \cdot (-2)$
- $29 \equiv 8 \pmod{7}$, já que $29 - 8 = 21 = 7 \cdot 3$

Propriedades de Congruência Modular

Vejamos propriedades importantes antes de seguirmos:

Propriedades de Congruência Modular

Vejamos propriedades importantes antes de seguirmos:

- Todo inteiro é congruente módulo n ao seu resto na divisão por n .

Propriedades de Congruência Modular

Vejamos propriedades importantes antes de seguirmos:

- Todo inteiro é congruente módulo n ao seu resto na divisão por n .

Demonstração: Seja a um inteiro. Ao efetuar a divisão por n , obtemos $a = n \cdot q + r$, em que q é um inteiro e r é o resto da divisão, $0 < r < n - 1$.

Propriedades de Congruência Modular

Vejamos propriedades importantes antes de seguirmos:

- Todo inteiro é congruente módulo n ao seu resto na divisão por n .

Demonstração: Seja a um inteiro. Ao efetuar a divisão por n , obtemos $a = n \cdot q + r$, em que q é um inteiro e r é o resto da divisão, $0 < r < n - 1$.

Logo, $a - r = n \cdot q$, e portanto, pela definição de congruência, $a \equiv r \pmod{n}$.

Propriedades de Congruência Modular

Vejamos propriedades importantes antes de seguirmos:

- Todo inteiro é congruente módulo n ao seu resto na divisão por n .

Demonstração: Seja a um inteiro. Ao efetuar a divisão por n , obtemos $a = n \cdot q + r$, em que q é um inteiro e r é o resto da divisão, $0 < r < n - 1$.

Logo, $a - r = n \cdot q$, e portanto, pela definição de congruência, $a \equiv r \pmod{n}$.

- $a \equiv b \pmod{n} \iff a$ e b têm o mesmo resto na divisão por n .

Inteiros Módulo n

Como todo inteiro é congruente ao seu resto, então existem apenas n diferentes classes para cada n inteiro.

Inteiros Módulo n

Como todo inteiro é congruente ao seu resto, então existem apenas n diferentes classes para cada n inteiro.

Definição:

Chamamos de Conjunto dos Inteiros módulo n o conjunto
 $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$.

Inteiros Módulo n

Como todo inteiro é congruente ao seu resto, então existem apenas n diferentes classes para cada n inteiro.

Definição:

Chamamos de Conjunto dos Inteiros módulo n o conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$.

Exemplo: Para $n = 5$, temos $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, em que

$$\overline{0} = \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}$$

$$\overline{1} = \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}$$

$$\overline{2} = \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\}$$

$$\overline{3} = \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\}$$

$$\overline{4} = \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}$$

Representação Geométrica

O conjunto \mathbb{Z} é representado por uma reta. Como representamos \mathbb{Z}_n ?

Aritmética Modular

Contas com os elementos de \mathbb{Z}_n

Soma:

Contas com os elementos de \mathbb{Z}_n

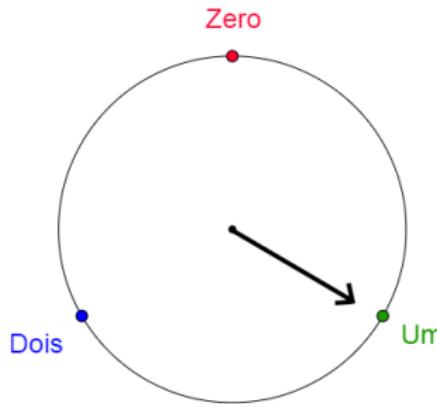
Soma:

Veremos primeiro o que nossa intuição diz:

Contas com os elementos de \mathbb{Z}_n

Soma:

Veremos primeiro o que nossa intuição diz:



Para $\bar{a} + \bar{b}$, posicione o ponteiro em a e mova b posições no sentido horário.

Soma em \mathbb{Z}_n

Definição: Soma

Definimos a soma em \mathbb{Z}_n como $\bar{a} + \bar{b} = \overline{a + b}$, para todas as classes $\bar{a}, \bar{b} \in \mathbb{Z}_n$.

Soma em \mathbb{Z}_n

Definição: Soma

Definimos a soma em \mathbb{Z}_n como $\bar{a} + \bar{b} = \overline{a + b}$, para todas as classes $\bar{a}, \bar{b} \in \mathbb{Z}_n$.

Interpretando corretamente: à esquerda, temos a soma de duas classes. Já à direita, temos a classe da soma de dois números inteiros.

Soma em \mathbb{Z}_n

Definição: Soma

Definimos a soma em \mathbb{Z}_n como $\bar{a} + \bar{b} = \overline{a + b}$, para todas as classes $\bar{a}, \bar{b} \in \mathbb{Z}_n$.

Interpretando corretamente: à esquerda, temos a soma de duas classes. Já à direita, temos a classe da soma de dois números inteiros.

Veja como isso corresponde com nossa expectativa:

$$\bar{1} + \bar{2} = \overline{1 + 2} = \bar{3} = \bar{0}$$

Soma em \mathbb{Z}_n

Vejamos o que ocorre com a soma quando utilizamos um n maior como módulo.

Soma em \mathbb{Z}_n

Vejamos o que ocorre com a soma quando utilizamos um n maior como módulo.

Seja $n = 13$ nosso módulo.

Soma em \mathbb{Z}_n

Vejamos o que ocorre com a soma quando utilizamos um n maior como módulo.

Seja $n = 13$ nosso módulo.

$$\text{Então } \overline{81} + \overline{17} = \overline{81 + 17} = \overline{98}$$

Soma em \mathbb{Z}_n

Vejamos o que ocorre com a soma quando utilizamos um n maior como módulo.

Seja $n = 13$ nosso módulo.

$$\text{Então } \overline{81} + \overline{17} = \overline{81 + 17} = \overline{98}$$

Basta agora encontrar o resto de 98 na divisão por 13.

Soma em \mathbb{Z}_n

Vejamos o que ocorre com a soma quando utilizamos um n maior como módulo.

Seja $n = 13$ nosso módulo.

$$\text{Então } \overline{81} + \overline{17} = \overline{81 + 17} = \overline{98}$$

Basta agora encontrar o resto de 98 na divisão por 13.

$$\overline{98} = \overline{98 - 13 \cdot 7} = \overline{98 - 91} = \overline{7}$$

Soma em \mathbb{Z}_n

Vejamos o que ocorre com a soma quando utilizamos um n maior como módulo.

Seja $n = 13$ nosso módulo.

$$\text{Então } \overline{81} + \overline{17} = \overline{81 + 17} = \overline{98}$$

Basta agora encontrar o resto de 98 na divisão por 13.

$$\overline{98} = \overline{98 - 13 \cdot 7} = \overline{98 - 91} = \overline{7}$$

Também poderíamos fazer $\overline{81} = \overline{3}$ e $\overline{17} = \overline{4}$ para obter $\overline{3} + \overline{4} = \overline{7}$.

Produto em \mathbb{Z}_n

Definição: Produto

Para todas as classes $\bar{a}, \bar{b} \in \mathbb{Z}_n$, definimos $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Produto em \mathbb{Z}_n

Definição: Produto

Para todas as classes $\bar{a}, \bar{b} \in \mathbb{Z}_n$, definimos $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Exemplo em \mathbb{Z}_{13} :

$$\overline{81} \cdot \overline{17} = \overline{3} \cdot \overline{4} = \overline{3 \cdot 4} = \overline{12}$$

Oposto para a soma em \mathbb{Z}_n

Oposto para a soma

Toda classe $\bar{a} \in \mathbb{Z}_n$ tem um elemento simétrico para a soma, e ele é $\overline{-a} = \overline{n - a}$.

Oposto para a soma em \mathbb{Z}_n

Oposto para a soma

Toda classe $\bar{a} \in \mathbb{Z}_n$ tem um elemento simétrico para a soma, e ele é $\overline{-a} = \overline{n - a}$.

Exemplo em \mathbb{Z}_5 :

O oposto de $\bar{3}$ é $\overline{-3} = \overline{5 - 3} = \bar{2}$.

Oposto para a soma em \mathbb{Z}_n

Oposto para a soma

Toda classe $\bar{a} \in \mathbb{Z}_n$ tem um elemento simétrico para a soma, e ele é $\overline{-a} = \overline{n - a}$.

Exemplo em \mathbb{Z}_5 :

O oposto de $\bar{3}$ é $\overline{-3} = \overline{5 - 3} = \bar{2}$.

De fato, $\bar{3} + \bar{2} = \overline{3 + 2} = \bar{5} = \bar{0}$

Outras propriedades de \mathbb{Z}_n

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, vale:

Outras propriedades de \mathbb{Z}_n

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, vale:

- $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c});$

Outras propriedades de \mathbb{Z}_n

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, vale:

- $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$;
- $\bar{a} + \bar{b} = \bar{b} + \bar{a}$;

Outras propriedades de \mathbb{Z}_n

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, vale:

- $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$;
- $\bar{a} + \bar{b} = \bar{b} + \bar{a}$;
- $\bar{a} + \bar{0} = \bar{a}$;

Outras propriedades de \mathbb{Z}_n

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, vale:

- $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$;
- $\bar{a} + \bar{b} = \bar{b} + \bar{a}$;
- $\bar{a} + \bar{0} = \bar{a}$;
- $\bar{a} + \overline{-\bar{a}} = \bar{0}$;

Outras propriedades de \mathbb{Z}_n

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, vale:

- $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$;
- $\bar{a} + \bar{b} = \bar{b} + \bar{a}$;
- $\bar{a} + \bar{0} = \bar{a}$;
- $\bar{a} + \overline{-\bar{a}} = \bar{0}$;
- $(\bar{a}\bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b}\bar{c})$;

Outras propriedades de \mathbb{Z}_n

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, vale:

- $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$;
- $\bar{a} + \bar{b} = \bar{b} + \bar{a}$;
- $\bar{a} + \bar{0} = \bar{a}$;
- $\bar{a} + \overline{-\bar{a}} = \bar{0}$;
- $(\bar{a}\bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b}\bar{c})$;
- $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$;

Outras propriedades de \mathbb{Z}_n

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, vale:

- $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$;
- $\bar{a} + \bar{b} = \bar{b} + \bar{a}$;
- $\bar{a} + \bar{0} = \bar{a}$;
- $\bar{a} + \overline{-\bar{a}} = \bar{0}$;
- $(\bar{a}\bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b}\bar{c})$;
- $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$;
- $\bar{a} \cdot \bar{1} = \bar{a}$;

Outras propriedades de \mathbb{Z}_n

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, vale:

- $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$;
- $\bar{a} + \bar{b} = \bar{b} + \bar{a}$;
- $\bar{a} + \bar{0} = \bar{a}$;
- $\bar{a} + \overline{-\bar{a}} = \bar{0}$;
- $(\bar{a}\bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b}\bar{c})$;
- $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$;
- $\bar{a} \cdot \bar{1} = \bar{a}$;
- $\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} = \bar{a} \cdot \bar{c}$;

Duas propriedades importantes

São duas propriedades de congruência que utilizaremos muito:

Duas propriedades importantes

São duas propriedades de congruência que utilizaremos muito:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

Duas propriedades importantes

São duas propriedades de congruência que utilizaremos muito:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

- $a + a' \equiv b + b' \pmod{n}$;

Duas propriedades importantes

São duas propriedades de congruência que utilizaremos muito:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

- $a + a' \equiv b + b' \pmod{n}$;
- $aa' \equiv bb' \pmod{n}$.

Duas propriedades importantes

São duas propriedades de congruência que utilizaremos muito:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

- $a + a' \equiv b + b' \pmod{n}$;
- $aa' \equiv bb' \pmod{n}$.

Ambas propriedades podem ser demonstradas utilizando a definição de congruência módulo n (isto é, $x \equiv y \pmod{n} \Leftrightarrow x - y = n \cdot q, q \in \mathbb{Z}$).

Divisão Modular

Intuitivamente...

Em \mathbb{R} , realizamos a divisão $\frac{a}{b}$ ao multiplicar o elemento a pelo inverso de b , isto é:

$$\frac{a}{b} = a \cdot b^{-1}$$

Intuitivamente...

Em \mathbb{R} , realizamos a divisão $\frac{a}{b}$ ao multiplicar o elemento a pelo inverso de b , isto é:

$$\frac{a}{b} = a \cdot b^{-1}$$

Também, sabemos que $b \in \mathbb{R}$ tem inverso se, e somente se, $b \neq 0$.

Intuitivamente...

Em \mathbb{R} , realizamos a divisão $\frac{a}{b}$ ao multiplicar o elemento a pelo inverso de b , isto é:

$$\frac{a}{b} = a \cdot b^{-1}$$

Também, sabemos que $b \in \mathbb{R}$ tem inverso se, e somente se, $b \neq 0$.

Mas quando saímos de \mathbb{R} e vamos para \mathbb{Z}_n , a situação é um pouco diferente:

Intuitivamente...

Em \mathbb{R} , realizamos a divisão $\frac{a}{b}$ ao multiplicar o elemento a pelo inverso de b , isto é:

$$\frac{a}{b} = a \cdot b^{-1}$$

Também, sabemos que $b \in \mathbb{R}$ tem inverso se, e somente se, $b \neq 0$.

Mas quando saímos de \mathbb{R} e vamos para \mathbb{Z}_n , a situação é um pouco diferente:

$\bar{b} \neq \bar{0}$ é uma condição necessária, mas não suficiente. Vejamos o que mais é necessário para que \bar{b} tenha inverso.

Inverso em \mathbb{Z}_n

Definição: Inverso módulo n

Dizemos que $\bar{b} \in \mathbb{Z}_n$ é invertível se existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1} \in \mathbb{Z}_n$.

Inverso em \mathbb{Z}_n

Definição: Inverso módulo n

Dizemos que $\bar{b} \in \mathbb{Z}_n$ é invertível se existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1} \in \mathbb{Z}_n$.

Exemplo: Para $\bar{2} \in \mathbb{Z}_5$ e $\bar{3} \in \mathbb{Z}_5$, temos

$$\bar{2} \cdot \bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{1}$$

Condições de existência do inverso em \mathbb{Z}_n

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $mdc(b, n) = 1$.

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $\text{mdc}(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$.

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $\text{mdc}(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $\text{mdc}(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

$$b \cdot \beta \equiv 1 \pmod{n}$$

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $\text{mdc}(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

$$b \cdot \beta \equiv 1 \pmod{n} \Rightarrow b \cdot \beta - 1 = n \cdot q, q \in \mathbb{Z}$$

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $\text{mdc}(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

$$b \cdot \beta \equiv 1 \pmod{n} \Rightarrow b \cdot \beta - 1 = n \cdot q, q \in \mathbb{Z} \Rightarrow b\beta + n(-q) = 1$$

Condições de existência do inverso em \mathbb{Z}_n

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $mdc(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

$$b \cdot \beta \equiv 1 \pmod{n} \Rightarrow b \cdot \beta - 1 = n \cdot q, q \in \mathbb{Z} \Rightarrow b\beta + n(-q) = 1$$

Como $d = mdc(b, n)$ é divisor de b e de n , então existem $k, r \in \mathbb{Z}$ tais que $b = d \cdot k$ e $n = d \cdot r$.

Condições de existência do inverso em \mathbb{Z}_n

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $mdc(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

$$b \cdot \beta \equiv 1 \pmod{n} \Rightarrow b \cdot \beta - 1 = n \cdot q, q \in \mathbb{Z} \Rightarrow b\beta + n(-q) = 1$$

Como $d = mdc(b, n)$ é divisor de b e de n , então existem $k, r \in \mathbb{Z}$ tais que $b = d \cdot k$ e $n = d \cdot r$.

$$\Rightarrow dk\beta + dr(-q) = 1$$

Condições de existência do inverso em \mathbb{Z}_n

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $mdc(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

$$b \cdot \beta \equiv 1 \pmod{n} \Rightarrow b \cdot \beta - 1 = n \cdot q, q \in \mathbb{Z} \Rightarrow b\beta + n(-q) = 1$$

Como $d = mdc(b, n)$ é divisor de b e de n , então existem $k, r \in \mathbb{Z}$ tais que $b = d \cdot k$ e $n = d \cdot r$.

$$\Rightarrow dk\beta + dr(-q) = 1 \Rightarrow d(k\beta + r(-q)) = 1$$

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $mdc(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

$$b \cdot \beta \equiv 1 \pmod{n} \Rightarrow b \cdot \beta - 1 = n \cdot q, q \in \mathbb{Z} \Rightarrow b\beta + n(-q) = 1$$

Como $d = mdc(b, n)$ é divisor de b e de n , então existem $k, r \in \mathbb{Z}$ tais que $b = d \cdot k$ e $n = d \cdot r$.

$$\Rightarrow dk\beta + dr(-q) = 1 \Rightarrow d(k\beta + r(-q)) = 1 \Rightarrow 1 \text{ é múltiplo de } d.$$

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $mdc(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

$$b \cdot \beta \equiv 1 \pmod{n} \Rightarrow b \cdot \beta - 1 = n \cdot q, q \in \mathbb{Z} \Rightarrow b\beta + n(-q) = 1$$

Como $d = mdc(b, n)$ é divisor de b e de n , então existem $k, r \in \mathbb{Z}$ tais que $b = d \cdot k$ e $n = d \cdot r$.

$$\Rightarrow dk\beta + dr(-q) = 1 \Rightarrow d(k\beta + r(-q)) = 1 \Rightarrow 1 \text{ é múltiplo de } d.$$

Note que se tivéssemos $d > 1$ isso não seria possível. Logo, $d = 1$.

Condições de existência do inverso em \mathbb{Z}_n

Proposição

\bar{b} possui inverso em \mathbb{Z}_n se, e somente se, $mdc(b, n) = 1$.

Demonstração: (\Rightarrow) Se \bar{b} possui inverso em \mathbb{Z}_n , então existe $\bar{\beta} \in \mathbb{Z}_n$ tal que $\bar{b} \cdot \bar{\beta} = \bar{1}$. Isto é, $b \cdot \beta$ possui resto 1 na divisão por n . Então:

$$b \cdot \beta \equiv 1 \pmod{n} \Rightarrow b \cdot \beta - 1 = n \cdot q, q \in \mathbb{Z} \Rightarrow b\beta + n(-q) = 1$$

Como $d = mdc(b, n)$ é divisor de b e de n , então existem $k, r \in \mathbb{Z}$ tais que $b = d \cdot k$ e $n = d \cdot r$.

$$\Rightarrow dk\beta + dr(-q) = 1 \Rightarrow d(k\beta + r(-q)) = 1 \Rightarrow 1 \text{ é múltiplo de } d.$$

Note que se tivéssemos $d > 1$ isso não seria possível. Logo, $d = 1$.

(\Leftarrow) Segue diretamente pelo Teorema de Bezout.

Encontrando o inverso de uma classe

Vamos calcular o inverso de $\bar{3}$ em \mathbb{Z}_{32} . Sabemos que ele existe, já que $mdc(3, 32) = 1$.

Encontrando o inverso de uma classe

Vamos calcular o inverso de $\bar{3}$ em \mathbb{Z}_{32} . Sabemos que ele existe, já que $mdc(3, 32) = 1$. Dividindo 32 por 3, obtemos:

$$32 = 10 \cdot 3 + 2$$

Encontrando o inverso de uma classe

Vamos calcular o inverso de $\bar{3}$ em \mathbb{Z}_{32} . Sabemos que ele existe, já que $mdc(3, 32) = 1$. Dividindo 32 por 3, obtemos:

$$32 = 10 \cdot 3 + 2$$

Agora, dividindo 3 por 2:

$$3 = 2 \cdot 1 + 1$$

Encontrando o inverso de uma classe

Vamos calcular o inverso de $\bar{3}$ em \mathbb{Z}_{32} . Sabemos que ele existe, já que $mdc(3, 32) = 1$. Dividindo 32 por 3, obtemos:

$$32 = 10 \cdot 3 + 2$$

Agora, dividindo 3 por 2:

$$3 = 2 \cdot 1 + 1$$

$\Rightarrow 2 = 3 - 1$. Substituindo acima:

Encontrando o inverso de uma classe

Vamos calcular o inverso de $\bar{3}$ em \mathbb{Z}_{32} . Sabemos que ele existe, já que $mdc(3, 32) = 1$. Dividindo 32 por 3, obtemos:

$$32 = 10 \cdot 3 + 2$$

Agora, dividindo 3 por 2:

$$3 = 2 \cdot 1 + 1$$

$\Rightarrow 2 = 3 - 1$. Substituindo acima:

$$\Rightarrow 32 = 10 \cdot 3 + (3 - 1)$$

Encontrando o inverso de uma classe

Vamos calcular o inverso de $\bar{3}$ em \mathbb{Z}_{32} . Sabemos que ele existe, já que $mdc(3, 32) = 1$. Dividindo 32 por 3, obtemos:

$$32 = 10 \cdot 3 + 2$$

Agora, dividindo 3 por 2:

$$3 = 2 \cdot 1 + 1$$

$\Rightarrow 2 = 3 - 1$. Substituindo acima:

$$\Rightarrow 32 = 10 \cdot 3 + (3 - 1)$$

$$\Rightarrow 32 = 11 \cdot 3 - 1$$

Encontrando o inverso de uma classe

Vamos calcular o inverso de $\bar{3}$ em \mathbb{Z}_{32} . Sabemos que ele existe, já que $mdc(3, 32) = 1$. Dividindo 32 por 3, obtemos:

$$32 = 10 \cdot 3 + 2$$

Agora, dividindo 3 por 2:

$$3 = 2 \cdot 1 + 1$$

$\Rightarrow 2 = 3 - 1$. Substituindo acima:

$$\Rightarrow 32 = 10 \cdot 3 + (3 - 1)$$

$$\Rightarrow 32 = 11 \cdot 3 - 1$$

$\Rightarrow 11 \cdot 3 \equiv 1 \pmod{32}$. Logo, $\bar{11}$ é o inverso multiplicativo de $\bar{3}$ em \mathbb{Z}_{32} .

Conjunto $U(n)$

Definição: Conjunto $U(n)$

É o conjunto dos elementos de \mathbb{Z}_n que possuem inverso, isto é:
 $U(n) \doteq \{\bar{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$

Conjunto $U(n)$

Definição: Conjunto $U(n)$

É o conjunto dos elementos de \mathbb{Z}_n que possuem inverso, isto é:
 $U(n) \doteq \{\bar{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$

Perceba que se p é um número primo, podemos facilmente determinar $U(p)$.

Conjunto $U(n)$

Definição: Conjunto $U(n)$

É o conjunto dos elementos de \mathbb{Z}_n que possuem inverso, isto é:
 $U(n) \doteq \{\bar{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$

Perceba que se p é um número primo, podemos facilmente determinar $U(p)$. De fato, se $mdc(a, p) \neq 1$, então a é múltiplo de p .

Conjunto $U(n)$

Definição: Conjunto $U(n)$

É o conjunto dos elementos de \mathbb{Z}_n que possuem inverso, isto é:
 $U(n) \doteq \{\bar{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$

Perceba que se p é um número primo, podemos facilmente determinar $U(p)$. De fato, se $mdc(a, p) \neq 1$, então a é múltiplo de p .

Logo, $a \equiv 0 \pmod{p}$, e portanto, $\bar{a} = \bar{0}$.

Conjunto $U(n)$

Definição: Conjunto $U(n)$

É o conjunto dos elementos de \mathbb{Z}_n que possuem inverso, isto é:
 $U(n) \doteq \{\bar{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$

Perceba que se p é um número primo, podemos facilmente determinar $U(p)$. De fato, se $mdc(a, p) \neq 1$, então a é múltiplo de p .

Logo, $a \equiv 0 \pmod{p}$, e portanto, $\bar{a} = \bar{0}$.

Como temos $mdc(a, p) \neq 1$ apenas quando $\bar{a} = \bar{0}$, então $U(p) = \mathbb{Z}_p - \{\bar{0}\}$.

Conjunto $U(n)$

Definição: Conjunto $U(n)$

É o conjunto dos elementos de \mathbb{Z}_n que possuem inverso, isto é:
 $U(n) \doteq \{\bar{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$

Perceba que se p é um número primo, podemos facilmente determinar $U(p)$. De fato, se $mdc(a, p) \neq 1$, então a é múltiplo de p .

Logo, $a \equiv 0 \pmod{p}$, e portanto, $\bar{a} = \bar{0}$.

Como temos $mdc(a, p) \neq 1$ apenas quando $\bar{a} = \bar{0}$, então $U(p) = \mathbb{Z}_p - \{\bar{0}\}$.

Exemplo de $U(n)$ com n composto: Para $n = 12$, temos que $mdc(a, 12) = 1$ apenas para $a = 1, 5, 7$ e 11 .

Conjunto $U(n)$

Definição: Conjunto $U(n)$

É o conjunto dos elementos de \mathbb{Z}_n que possuem inverso, isto é:
 $U(n) \doteq \{\bar{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$

Perceba que se p é um número primo, podemos facilmente determinar $U(p)$. De fato, se $mdc(a, p) \neq 1$, então a é múltiplo de p .

Logo, $a \equiv 0 \pmod{p}$, e portanto, $\bar{a} = \bar{0}$.

Como temos $mdc(a, p) \neq 1$ apenas quando $\bar{a} = \bar{0}$, então $U(p) = \mathbb{Z}_p - \{\bar{0}\}$.

Exemplo de $U(n)$ com n composto: Para $n = 12$, temos que $mdc(a, 12) = 1$ apenas para $a = 1, 5, 7$ e 11 .

Logo, $U(12) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$.

Potências

Potências

Realizaremos várias operações com potências na Criptografia RSA.

Para isso, utilizaremos as duas propriedades importantes que vimos anteriormente:

Potências

Realizaremos várias operações com potências na Criptografia RSA.

Para isso, utilizaremos as duas propriedades importantes que vimos anteriormente:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

- $a + a' \equiv b + b' \pmod{n}$;
- $aa' \equiv bb' \pmod{n}$.

Potências

Realizaremos várias operações com potências na Criptografia RSA.

Para isso, utilizaremos as duas propriedades importantes que vimos anteriormente:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

- $a + a' \equiv b + b' \pmod{n}$;
- $aa' \equiv bb' \pmod{n}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Potências

Realizaremos várias operações com potências na Criptografia RSA.

Para isso, utilizaremos as duas propriedades importantes que vimos anteriormente:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

- $a + a' \equiv b + b' \pmod{n}$;
- $aa' \equiv bb' \pmod{n}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Primeiro, vamos escolher um representante mais simples para as contas:

Potências

Realizaremos várias operações com potências na Criptografia RSA.

Para isso, utilizaremos as duas propriedades importantes que vimos anteriormente:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

- $a + a' \equiv b + b' \pmod{n}$;
- $aa' \equiv bb' \pmod{n}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Primeiro, vamos escolher um representante mais simples para as contas:

$$\begin{cases} 10 \equiv 3 \pmod{7} \\ 10 \equiv 3 \pmod{7} \end{cases}$$

Potências

Realizaremos várias operações com potências na Criptografia RSA.

Para isso, utilizaremos as duas propriedades importantes que vimos anteriormente:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

- $a + a' \equiv b + b' \pmod{n}$;
- $aa' \equiv bb' \pmod{n}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Primeiro, vamos escolher um representante mais simples para as contas:

$$\begin{cases} 10 \equiv 3 \pmod{7} \\ 10 \equiv 3 \pmod{7} \end{cases} \Rightarrow 10^2 \equiv 3^2 \pmod{7}$$

Potências

Realizaremos várias operações com potências na Criptografia RSA.

Para isso, utilizaremos as duas propriedades importantes que vimos anteriormente:

Se $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$, então:

- $a + a' \equiv b + b' \pmod{n}$;
- $aa' \equiv bb' \pmod{n}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Primeiro, vamos escolher um representante mais simples para as contas:

$$\begin{cases} 10 \equiv 3 \pmod{7} \\ 10 \equiv 3 \pmod{7} \end{cases} \Rightarrow 10^2 \equiv 3^2 \pmod{7} \Rightarrow \dots \Rightarrow 10^{135} \equiv 3^{135} \pmod{7}$$

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Note que, a partir da sexta potência, os restos se repetirão ciclicamente.

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Note que, a partir da sexta potência, os restos se repetirão ciclicamente.
Mas o que nos importa aqui é a sexta potência:

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Note que, a partir da sexta potência, os restos se repetirão ciclicamente.
Mas o que nos importa aqui é a sexta potência:

Como $135 = 22 \cdot 6 + 3$, então:

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Note que, a partir da sexta potência, os restos se repetirão ciclicamente.
Mas o que nos importa aqui é a sexta potência:

Como $135 = 22 \cdot 6 + 3$, então:

$$3^{135}$$

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Note que, a partir da sexta potência, os restos se repetirão ciclicamente.
Mas o que nos importa aqui é a sexta potência:

Como $135 = 22 \cdot 6 + 3$, então:

$$3^{135} \equiv 3^{22 \cdot 6 + 3}$$

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Note que, a partir da sexta potência, os restos se repetirão ciclicamente.
Mas o que nos importa aqui é a sexta potência:

Como $135 = 22 \cdot 6 + 3$, então:

$$3^{135} \equiv 3^{22 \cdot 6 + 3} \equiv (3^6)^{22} \cdot 3^3$$

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Note que, a partir da sexta potência, os restos se repetirão ciclicamente.
Mas o que nos importa aqui é a sexta potência:

Como $135 = 22 \cdot 6 + 3$, então:

$$3^{135} \equiv 3^{22 \cdot 6 + 3} \equiv (3^6)^{22} \cdot 3^3 \equiv 1^{22} \cdot (-1)^3$$

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Note que, a partir da sexta potência, os restos se repetirão ciclicamente.
Mas o que nos importa aqui é a sexta potência:

Como $135 = 22 \cdot 6 + 3$, então:

$$3^{135} \equiv 3^{22 \cdot 6 + 3} \equiv (3^6)^{22} \cdot 3^3 \equiv 1^{22} \cdot (-1)^3 \equiv (-1)$$

Potências

Perceba que:

$$3^2 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$$

$$3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod{7}$$

$$3^4 \equiv 3 \cdot (-1) \equiv -3 \equiv 4 \pmod{7}$$

$$3^5 \equiv 3 \cdot 4 \equiv 5 \pmod{7}$$

$$3^6 \equiv 3 \cdot 5 \equiv 1 \pmod{7}.$$

Note que, a partir da sexta potência, os restos se repetirão ciclicamente.
Mas o que nos importa aqui é a sexta potência:

Como $135 = 22 \cdot 6 + 3$, então:

$$3^{135} \equiv 3^{22 \cdot 6 + 3} \equiv (3^6)^{22} \cdot 3^3 \equiv 1^{22} \cdot (-1)^3 \equiv (-1) \equiv 6 \pmod{7}$$

Portanto, o resto de 10^{135} na divisão por 7 é 6.

Potências

Como isso aparecerá bastante, vamos fazer outro exemplo:

Calcule o resto da divisão de 3^{64} por 31.

Como isso aparecerá bastante, vamos fazer outro exemplo:

Calcule o resto da divisão de 3^{64} por 31.

Já percebemos algo logo de cara: se encontrarmos alguma potência de 3 congruente a 32, nosso trabalho estaria quase feito, pois $32 \equiv 1 \pmod{31}$.

Como isso aparecerá bastante, vamos fazer outro exemplo:

Calcule o resto da divisão de 3^{64} por 31.

Já percebemos algo logo de cara: se encontrarmos alguma potência de 3 congruente a 32, nosso trabalho estaria quase feito, pois $32 \equiv 1 \pmod{31}$.

Mas a princípio, não sabemos qual é essa potência, afinal, existem muitas opções e por inspeção isso seria bem demorado.

Como isso aparecerá bastante, vamos fazer outro exemplo:

Calcule o resto da divisão de 3^{64} por 31.

Já percebemos algo logo de cara: se encontrarmos alguma potência de 3 congruente a 32, nosso trabalho estaria quase feito, pois $32 \equiv 1 \pmod{31}$.

Mas a princípio, não sabemos qual é essa potência, afinal, existem muitas opções e por inspeção isso seria bem demorado.

Vamos então apenas escolher uma potência que facilite nosso trabalho.

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1}$$

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3$$

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3$$

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv (-1)^{21} \cdot (2^2)^{21} \cdot 3 \pmod{31}$$

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv (-1)^{21} \cdot (2^2)^{21} \cdot 3 \pmod{31}$$

Por que fizemos $4 = 2^2$ na última congruência? Bem, lembre-se do nosso objetivo inicial: conseguir mostrar algo congruente a 32, e $32 = 2^5$.

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv (-1)^{21} \cdot (2^2)^{21} \cdot 3 \pmod{31}$$

Por que fizemos $4 = 2^2$ na última congruência? Bem, lembre-se do nosso objetivo inicial: conseguir mostrar algo congruente a 32, e $32 = 2^5$.

Portanto, já vamos realizar a divisão de 42 por 5: $42 = 5 \cdot 8 + 2$. Logo:

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv (-1)^{21} \cdot (2^2)^{21} \cdot 3 \pmod{31}$$

Por que fizemos $4 = 2^2$ na última congruência? Bem, lembre-se do nosso objetivo inicial: conseguir mostrar algo congruente a 32, e $32 = 2^5$.

Portanto, já vamos realizar a divisão de 42 por 5: $42 = 5 \cdot 8 + 2$. Logo:

$$(-1)^{21} \cdot 2^{5 \cdot 8 + 2} \cdot 3$$

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv (-1)^{21} \cdot (2^2)^{21} \cdot 3 \pmod{31}$$

Por que fizemos $4 = 2^2$ na última congruência? Bem, lembre-se do nosso objetivo inicial: conseguir mostrar algo congruente a 32, e $32 = 2^5$.

Portanto, já vamos realizar a divisão de 42 por 5: $42 = 5 \cdot 8 + 2$. Logo:

$$(-1)^{21} \cdot 2^{5 \cdot 8 + 2} \cdot 3 \equiv (-3) \cdot (2^5)^8 \cdot 2^2$$

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv (-1)^{21} \cdot (2^2)^{21} \cdot 3 \pmod{31}$$

Por que fizemos $4 = 2^2$ na última congruência? Bem, lembre-se do nosso objetivo inicial: conseguir mostrar algo congruente a 32, e $32 = 2^5$.

Portanto, já vamos realizar a divisão de 42 por 5: $42 = 5 \cdot 8 + 2$. Logo:

$$(-1)^{21} \cdot 2^{5 \cdot 8 + 2} \cdot 3 \equiv (-3) \cdot (2^5)^8 \cdot 2^2 \equiv (-3) \cdot 1^8 \cdot 4$$

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv (-1)^{21} \cdot (2^2)^{21} \cdot 3 \pmod{31}$$

Por que fizemos $4 = 2^2$ na última congruência? Bem, lembre-se do nosso objetivo inicial: conseguir mostrar algo congruente a 32, e $32 = 2^5$.

Portanto, já vamos realizar a divisão de 42 por 5: $42 = 5 \cdot 8 + 2$. Logo:

$$(-1)^{21} \cdot 2^{5 \cdot 8 + 2} \cdot 3 \equiv (-3) \cdot (2^5)^8 \cdot 2^2 \equiv (-3) \cdot 1^8 \cdot 4 \equiv -12$$

Potências

Sem grande esforço, verificamos que $3^3 \equiv -4 \pmod{31}$.

Vejamos então que $64 = 3 \cdot 21 + 1$. Substituindo, obtemos:

$$3^{64} \equiv 3^{3 \cdot 21 + 1} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv (-1)^{21} \cdot (2^2)^{21} \cdot 3 \pmod{31}$$

Por que fizemos $4 = 2^2$ na última congruência? Bem, lembre-se do nosso objetivo inicial: conseguir mostrar algo congruente a 32, e $32 = 2^5$.

Portanto, já vamos realizar a divisão de 42 por 5: $42 = 5 \cdot 8 + 2$. Logo:

$$(-1)^{21} \cdot 2^{5 \cdot 8 + 2} \cdot 3 \equiv (-3) \cdot (2^5)^8 \cdot 2^2 \equiv (-3) \cdot 1^8 \cdot 4 \equiv -12 \equiv 19 \pmod{31}$$

Conclusão: o resto da divisão de 3^{64} por 31 é 19.

Função ϕ de Euler

Função ϕ de Euler

Definição:

$$\phi : \mathbb{Z}_+ \longrightarrow \mathbb{Z}_+$$

$n \longmapsto \phi(n)$, em que $\phi(n) = \#U(n)$, isto é, a quantidade de elementos de $U(n)$.

Função ϕ de Euler

Definição:

$\phi : \mathbb{Z}_+ \longrightarrow \mathbb{Z}_+$
 $n \longmapsto \phi(n)$, em que $\phi(n) = \#U(n)$, isto é, a quantidade de elementos de $U(n)$.

Lembre-se que $U(n) = \{\bar{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$.

Também, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$.

Função ϕ de Euler

Definição:

$\phi : \mathbb{Z}_+ \longrightarrow \mathbb{Z}_+$
 $n \longmapsto \phi(n)$, em que $\phi(n) = \#U(n)$, isto é, a quantidade de elementos de $U(n)$.

Lembre-se que $U(n) = \{\bar{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$.

Também, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$.

Por isso, podemos definir $\phi(n)$ como a quantidade de números inteiros positivos menores ou iguais que n que são coprimos com n .

Função ϕ de Euler

Definição:

$\phi : \mathbb{Z}_+ \longrightarrow \mathbb{Z}_+$
 $n \longmapsto \phi(n)$, em que $\phi(n) = \#U(n)$, isto é, a quantidade de elementos de $U(n)$.

Lembre-se que $U(n) = \{\bar{a} \in \mathbb{Z}_n; \text{mdc}(a, n) = 1\}$.

Também, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$.

Por isso, podemos definir $\phi(n)$ como a quantidade de números inteiros positivos menores ou iguais que n que são coprimos com n .

Exemplo: Havíamos visto que $U(12) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. Logo, $\phi(12) = 4$

Propriedades de ϕ

- Se p é primo, então $\phi(p) = p - 1$.

Essa propriedade segue diretamente de $U(p) = \mathbb{Z}_p - \{\bar{0}\}$.

Propriedades de ϕ

- Se p é primo, então $\phi(p) = p - 1$.

Essa propriedade segue diretamente de $U(p) = \mathbb{Z}_p - \{\bar{0}\}$.

- Se $mdc(m, n) = 1$, então $\phi(m) \cdot \phi(n) = \phi(m \cdot n)$

A demonstração desse resultado se encontra na Apostila de Criptografia.

Propriedades de ϕ

- Se p é primo e k é um inteiro positivo, então $\phi(p^k) = p^k - p^{k-1}$.

Demonstração:

Propriedades de ϕ

- Se p é primo e k é um inteiro positivo, então $\phi(p^k) = p^k - p^{k-1}$.

Demonstração: Queremos saber quantos são os números $n \in \mathbb{Z}$ tais que $1 \leq n \leq p^k$ e $\text{mdc}(n, p^k) = 1$.

Propriedades de ϕ

- Se p é primo e k é um inteiro positivo, então $\phi(p^k) = p^k - p^{k-1}$.

Demonstração: Queremos saber quantos são os números $n \in \mathbb{Z}$ tais que $1 \leq n \leq p^k$ e $\text{mdc}(n, p^k) = 1$.

Note que para todo número $n \in \mathbb{Z}$, temos que $\text{mdc}(n, p^k) = 1$ ou $\text{mdc}(n, p^k) > 1$, sem que ambos ocorram simultaneamente. Defina então:

Propriedades de ϕ

- Se p é primo e k é um inteiro positivo, então $\phi(p^k) = p^k - p^{k-1}$.

Demonstração: Queremos saber quantos são os números $n \in \mathbb{Z}$ tais que $1 \leq n \leq p^k$ e $\text{mdc}(n, p^k) = 1$.

Note que para todo número $n \in \mathbb{Z}$, temos que $\text{mdc}(n, p^k) = 1$ ou $\text{mdc}(n, p^k) > 1$, sem que ambos ocorram simultaneamente. Defina então:

$$A = \{a \in \mathbb{Z}; 1 \leq a \leq p^k \text{ e } \text{mdc}(a, p^k) > 1\}.$$

Propriedades de ϕ

- Se p é primo e k é um inteiro positivo, então $\phi(p^k) = p^k - p^{k-1}$.

Demonstração: Queremos saber quantos são os números $n \in \mathbb{Z}$ tais que $1 \leq n \leq p^k$ e $\text{mdc}(n, p^k) = 1$.

Note que para todo número $n \in \mathbb{Z}$, temos que $\text{mdc}(n, p^k) = 1$ ou $\text{mdc}(n, p^k) > 1$, sem que ambos ocorram simultaneamente. Defina então:

$$A = \{a \in \mathbb{Z}; 1 \leq a \leq p^k \text{ e } \text{mdc}(a, p^k) > 1\}.$$

Portanto, teremos que $\phi(p^k) = p^k - \#A$.

Nosso problema agora se resume a encontrar a quantidade de elementos de A . Vejamos quem são eles:

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Pergunta: Quem é $mdc(a, p)$?

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Pergunta: Quem é $mdc(a, p)$?

Bem, seja $mdc(a, p) = d$.

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Pergunta: Quem é $mdc(a, p)$?

Bem, seja $mdc(a, p) = d$. Logo, d divide p .

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Pergunta: Quem é $mdc(a, p)$?

Bem, seja $mdc(a, p) = d$. Logo, d divide p . Como p é primo, então possui apenas dois divisores positivos: 1 e p .

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Pergunta: Quem é $mdc(a, p)$?

Bem, seja $mdc(a, p) = d$. Logo, d divide p . Como p é primo, então possui apenas dois divisores positivos: 1 e p . Se tivéssemos $mdc(a, p) = 1$, teríamos também $mdc(a, p^k) = 1$.

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Pergunta: Quem é $mdc(a, p)$?

Bem, seja $mdc(a, p) = d$. Logo, d divide p . Como p é primo, então possui apenas dois divisores positivos: 1 e p . Se tivéssemos $mdc(a, p) = 1$, teríamos também $mdc(a, p^k) = 1$.

Portanto, $mdc(a, p) = p$, e por isso, p divide a .

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Pergunta: Quem é $mdc(a, p)$?

Bem, seja $mdc(a, p) = d$. Logo, d divide p . Como p é primo, então possui apenas dois divisores positivos: 1 e p . Se tivéssemos $mdc(a, p) = 1$, teríamos também $mdc(a, p^k) = 1$.

Portanto, $mdc(a, p) = p$, e por isso, p divide a . Então $a = pa'$, $a' \in \mathbb{Z}$.

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Pergunta: Quem é $mdc(a, p)$?

Bem, seja $mdc(a, p) = d$. Logo, d divide p . Como p é primo, então possui apenas dois divisores positivos: 1 e p . Se tivéssemos $mdc(a, p) = 1$, teríamos também $mdc(a, p^k) = 1$.

Portanto, $mdc(a, p) = p$, e por isso, p divide a . Então $a = pa'$, $a' \in \mathbb{Z}$.

Conclusão parcial: Todos os elementos de A são múltiplos de p .

Propriedades de ϕ

Se $a \in A \Rightarrow mdc(a, p^k) > 1$.

Pergunta: Quem é $mdc(a, p)$?

Bem, seja $mdc(a, p) = d$. Logo, d divide p . Como p é primo, então possui apenas dois divisores positivos: 1 e p . Se tivéssemos $mdc(a, p) = 1$, teríamos também $mdc(a, p^k) = 1$.

Portanto, $mdc(a, p) = p$, e por isso, p divide a . Então $a = pa'$, $a' \in \mathbb{Z}$.

Conclusão parcial: Todos os elementos de A são múltiplos de p .

Resta saber quantos são os múltiplos de p compreendidos entre 1 e p^k .

Propriedades de ϕ

Isto é, queremos todos os números da forma pa' tal que $1 \leq pa' \leq p^k$.

Propriedades de ϕ

Isto é, queremos todos os números da forma pa' tal que $1 \leq pa' \leq p^k$.

Note que $a' \geq 1$

Propriedades de ϕ

Isto é, queremos todos os números da forma pa' tal que $1 \leq pa' \leq p^k$.

Note que $a' \geq 1 \Rightarrow pa' \geq p$.

Propriedades de ϕ

Isto é, queremos todos os números da forma pa' tal que $1 \leq pa' \leq p^k$.

Note que $a' \geq 1 \Rightarrow pa' \geq p$. Também, $pa' \leq p^k$. Logo:

Propriedades de ϕ

Isto é, queremos todos os números da forma pa' tal que $1 \leq pa' \leq p^k$.

Note que $a' \geq 1 \Rightarrow pa' \geq p$. Também, $pa' \leq p^k$. Logo:

$$p \leq pa' \leq p^k$$

Dividindo por p , obtemos

$$1 \leq a' \leq p^{k-1}$$

Propriedades de ϕ

Isto é, queremos todos os números da forma pa' tal que $1 \leq pa' \leq p^k$.

Note que $a' \geq 1 \Rightarrow pa' \geq p$. Também, $pa' \leq p^k$. Logo:

$$p \leq pa' \leq p^k$$

Dividindo por p , obtemos

$$1 \leq a' \leq p^{k-1}$$

Portanto, existem p^{k-1} a' 's que geram múltiplos de p dentro do intervalo $[1, p^k]$.

Propriedades de ϕ

Isto é, queremos todos os números da forma pa' tal que $1 \leq pa' \leq p^k$.

Note que $a' \geq 1 \Rightarrow pa' \geq p$. Também, $pa' \leq p^k$. Logo:

$$p \leq pa' \leq p^k$$

Dividindo por p , obtemos

$$1 \leq a' \leq p^{k-1}$$

Portanto, existem p^{k-1} a' 's que geram múltiplos de p dentro do intervalo $[1, p^k]$. Isto é: existem p^{k-1} múltiplos de p neste intervalo.

Propriedades de ϕ

Isto é, queremos todos os números da forma pa' tal que $1 \leq pa' \leq p^k$.

Note que $a' \geq 1 \Rightarrow pa' \geq p$. Também, $pa' \leq p^k$. Logo:

$$p \leq pa' \leq p^k$$

Dividindo por p , obtemos

$$1 \leq a' \leq p^{k-1}$$

Portanto, existem p^{k-1} a' 's que geram múltiplos de p dentro do intervalo $[1, p^k]$. Isto é: existem p^{k-1} múltiplos de p neste intervalo.

Assim respondemos nossa pergunta. $\#A = p^{k-1}$.

Portanto, $\phi(p^k) = p^k - p^{k-1}$.

Teoremas de Fermat e Euler

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Nesse exercício, anteriormente fizemos $10^{135} \equiv 3^{135} \pmod{7}$ e percorremos as potências de 3 até encontrar aquela congruente a 1.

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Nesse exercício, anteriormente fizemos $10^{135} \equiv 3^{135} \pmod{7}$ e percorremos as potências de 3 até encontrar aquela congruente a 1.

Note, entretanto, que como 7 é primo e não divide 10, então, pelo Teorema de Fermat, $10^6 \equiv 1 \pmod{7}$. Assim, é fácil ver que

Teorema de Fermat

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Nesse exercício, anteriormente fizemos $10^{135} \equiv 3^{135} \pmod{7}$ e percorremos as potências de 3 até encontrar aquela congruente a 1.

Note, entretanto, que como 7 é primo e não divide 10, então, pelo Teorema de Fermat, $10^6 \equiv 1 \pmod{7}$. Assim, é fácil ver que

$$10^{135}$$

Teorema de Fermat

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Nesse exercício, anteriormente fizemos $10^{135} \equiv 3^{135} \pmod{7}$ e percorremos as potências de 3 até encontrar aquela congruente a 1.

Note, entretanto, que como 7 é primo e não divide 10, então, pelo Teorema de Fermat, $10^6 \equiv 1 \pmod{7}$. Assim, é fácil ver que

$$10^{135} \equiv 10^{6 \cdot 22 + 3}$$

Teorema de Fermat

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Nesse exercício, anteriormente fizemos $10^{135} \equiv 3^{135} \pmod{7}$ e percorremos as potências de 3 até encontrar aquela congruente a 1.

Note, entretanto, que como 7 é primo e não divide 10, então, pelo Teorema de Fermat, $10^6 \equiv 1 \pmod{7}$. Assim, é fácil ver que

$$10^{135} \equiv 10^{6 \cdot 22 + 3} \equiv (10^6)^{22} \cdot 10^3$$

Teorema de Fermat

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Nesse exercício, anteriormente fizemos $10^{135} \equiv 3^{135} \pmod{7}$ e percorremos as potências de 3 até encontrar aquela congruente a 1.

Note, entretanto, que como 7 é primo e não divide 10, então, pelo Teorema de Fermat, $10^6 \equiv 1 \pmod{7}$. Assim, é fácil ver que

$$10^{135} \equiv 10^{6 \cdot 22 + 3} \equiv (10^6)^{22} \cdot 10^3 \equiv 1^{22} \cdot 1000$$

Teorema de Fermat

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Nesse exercício, anteriormente fizemos $10^{135} \equiv 3^{135} \pmod{7}$ e percorremos as potências de 3 até encontrar aquela congruente a 1.

Note, entretanto, que como 7 é primo e não divide 10, então, pelo Teorema de Fermat, $10^6 \equiv 1 \pmod{7}$. Assim, é fácil ver que

$$10^{135} \equiv 10^{6 \cdot 22 + 3} \equiv (10^6)^{22} \cdot 10^3 \equiv 1^{22} \cdot 1000 \equiv 7 \cdot 144 + 6$$

Teorema de Fermat

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z}$.

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo: Qual o resto de 10^{135} na divisão por 7?

Nesse exercício, anteriormente fizemos $10^{135} \equiv 3^{135} \pmod{7}$ e percorremos as potências de 3 até encontrar aquela congruente a 1.

Note, entretanto, que como 7 é primo e não divide 10, então, pelo Teorema de Fermat, $10^6 \equiv 1 \pmod{7}$. Assim, é fácil ver que

$$10^{135} \equiv 10^{6 \cdot 22 + 3} \equiv (10^6)^{22} \cdot 10^3 \equiv 1^{22} \cdot 1000 \equiv 7 \cdot 144 + 6 \equiv 6 \pmod{7}.$$

E portanto, 6 é o resto da divisão.

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500}$$

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500} \equiv (a^4)^{500}$$

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500} \equiv (a^4)^{500} \equiv 1^{500}$$

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500} \equiv (a^4)^{500} \equiv 1^{500} \equiv 1 \pmod{5}.$$

Corolário

Seja p um primo qualquer e a um inteiro qualquer. Então:

$$a^p \equiv a \pmod{p}$$

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500} \equiv (a^4)^{500} \equiv 1^{500} \equiv 1 \pmod{5}.$$

Corolário

Seja p um primo qualquer e a um inteiro qualquer. Então:

$$a^p \equiv a \pmod{p}$$

Demonstração: Vamos dividir em dois casos:

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500} \equiv (a^4)^{500} \equiv 1^{500} \equiv 1 \pmod{5}.$$

Corolário

Seja p um primo qualquer e a um inteiro qualquer. Então:

$$a^p \equiv a \pmod{p}$$

Demonstração: Vamos dividir em dois casos:

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500} \equiv (a^4)^{500} \equiv 1^{500} \equiv 1 \pmod{5}.$$

Corolário

Seja p um primo qualquer e a um inteiro qualquer. Então:

$$a^p \equiv a \pmod{p}$$

Demonstração: Vamos dividir em dois casos:

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$. Logo, $a^p \equiv a \pmod{p}$.

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500} \equiv (a^4)^{500} \equiv 1^{500} \equiv 1 \pmod{5}.$$

Corolário

Seja p um primo qualquer e a um inteiro qualquer. Então:

$$a^p \equiv a \pmod{p}$$

Demonstração: Vamos dividir em dois casos:

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$. Logo, $a^p \equiv a \pmod{p}$.

Se p divide $a \Rightarrow a = pa'$, $a' \in \mathbb{Z}$

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500} \equiv (a^4)^{500} \equiv 1^{500} \equiv 1 \pmod{5}.$$

Corolário

Seja p um primo qualquer e a um inteiro qualquer. Então:

$$a^p \equiv a \pmod{p}$$

Demonstração: Vamos dividir em dois casos:

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$. Logo, $a^p \equiv a \pmod{p}$.

Se p divide $a \Rightarrow a = pa'$, $a' \in \mathbb{Z} \Rightarrow a \equiv 0 \pmod{p}$.

Teorema de Fermat

Exemplo 2: Sabendo que 5 não divide a , prove que $a^{2000} \equiv 1 \pmod{5}$.

Pelo Teorema de Fermat, $a^4 \equiv 1 \pmod{5}$.

Como $2000 = 4 \cdot 500$, então:

$$a^{2000} \equiv a^{4 \cdot 500} \equiv (a^4)^{500} \equiv 1^{500} \equiv 1 \pmod{5}.$$

Corolário

Seja p um primo qualquer e a um inteiro qualquer. Então:

$$a^p \equiv a \pmod{p}$$

Demonstração: Vamos dividir em dois casos:

Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$. Logo, $a^p \equiv a \pmod{p}$.

Se p divide $a \Rightarrow a = pa'$, $a' \in \mathbb{Z} \Rightarrow a \equiv 0 \pmod{p}$. Logo, $a^p \equiv a \pmod{p}$.

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

$$\phi(24) =$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

$$\phi(24) = \phi(8 \cdot 3)$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

$$\phi(24) = \phi(8 \cdot 3) = \phi(2^3 \cdot 3)$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

$$\phi(24) = \phi(8 \cdot 3) = \phi(2^3 \cdot 3) = \phi(2^3) \cdot \phi(3)$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

$$\phi(24) = \phi(8 \cdot 3) = \phi(2^3 \cdot 3) = \phi(2^3) \cdot \phi(3) = (2^3 - 2^{3-1}) \cdot (3 - 1)$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

$$\phi(24) = \phi(8 \cdot 3) = \phi(2^3 \cdot 3) = \phi(2^3) \cdot \phi(3) = (2^3 - 2^{3-1}) \cdot (3 - 1) = 4 \cdot 2 = 8.$$

Logo, $7^8 \equiv 1 \pmod{24}$.

$$\Rightarrow 7^{777} \equiv 7^{8 \cdot 97 + 1}$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

$$\phi(24) = \phi(8 \cdot 3) = \phi(2^3 \cdot 3) = \phi(2^3) \cdot \phi(3) = (2^3 - 2^{3-1}) \cdot (3 - 1) = 4 \cdot 2 = 8.$$

Logo, $7^8 \equiv 1 \pmod{24}$.

$$\Rightarrow 7^{777} \equiv 7^{8 \cdot 97 + 1} \equiv (7^8)^{97} \cdot 7$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

$$\phi(24) = \phi(8 \cdot 3) = \phi(2^3 \cdot 3) = \phi(2^3) \cdot \phi(3) = (2^3 - 2^{3-1}) \cdot (3 - 1) = 4 \cdot 2 = 8.$$

Logo, $7^8 \equiv 1 \pmod{24}$.

$$\Rightarrow 7^{777} \equiv 7^{8 \cdot 97 + 1} \equiv (7^8)^{97} \cdot 7 \equiv 1^{22} \cdot 7$$

Teorema de Euler

O Teorema de Fermat é muito útil mas vale apenas para módulos primos.

Teorema de Euler

Sejam $a, n \in \mathbb{Z}$ com $n > 1$ e $\text{mdc}(a, n) = 1$. Então:

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

Exemplo: Calcule o resto da divisão de 7^{777} por 24.

Como $\text{mdc}(7, 24) = 1$, então vale o Teorema de Fermat. Logo:

$$7^{\phi(24)} \equiv 1 \pmod{24}.$$

$$\phi(24) = \phi(8 \cdot 3) = \phi(2^3 \cdot 3) = \phi(2^3) \cdot \phi(3) = (2^3 - 2^{3-1}) \cdot (3 - 1) = 4 \cdot 2 = 8.$$

$$\text{Logo, } 7^8 \equiv 1 \pmod{24}.$$

$$\Rightarrow 7^{777} \equiv 7^{8 \cdot 97 + 1} \equiv (7^8)^{97} \cdot 7 \equiv 1^{22} \cdot 7 \equiv 7 \pmod{24}. \text{ O resto é 7.}$$

Referências



Severino Collier Coutinho

Números Inteiros e Criptografia RSA 2^a ed.
Rio de Janeiro, IMPA, 2014.



César Polcino Millies, Sônia Pitta Coelho

Números: Uma Introdução à Matemática 3^a ed.
São Paulo, Edusp, 2001.

Obrigado!

Espero vê-los amanhã para aprender RSA!