FUNDAMENTOS DE MATEMÁTICA PARA A COMPUTAÇÃO

17 de Abril, 2020

Prof. Sinai Robins

IME, USP

Hoje: Nos abordaremos alguns dos seguintes tópicos:

Coeficientes binomiais

Teorema Binomial

Aritmética modular

Teorema Binomial

Para todos os números reais a, b

e para todos os números inteiros não negativos n,

Teorema Binomial

Para todos os números reais a, b

e para todos os números inteiros não negativos n,

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + b^n$$

Teorema Binomial

Para todos os números reais a, b

e para todos os números inteiros não negativos n,

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + b^n$$

Em outras palavras, $$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$$

O coeficiente binomial é

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

para todos os números inteiros $n \geq k$.

O coeficiente binomial é

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

para todos os números inteiros $n \geq k$.

Esse também é o número de maneiras de escolher k elementos diferentes de um conjunto que possui n elementos.

Pergunta: $\binom{n}{k} = \binom{n}{n-k}$?

Pergunta: $\binom{n}{k} = \binom{n}{n-k}$?

Vamos ver:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Pergunta: $\binom{n}{k} = \binom{n}{n-k}$?

Vamos ver:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

e temos $\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!}$

Pergunta: $\binom{n}{k} = \binom{n}{n-k}$?

Vamos ver:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

e temos $\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!}$

Então sim!

Afirmação. $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$

Afirmação. $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$

Tarefas - não para entrega

Prove isso, usando Indução

Afirmação. $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$

Tarefas - não para entrega

Prove isso, usando Indução

Prove também a teorema binomial
usando indução em n

Vamos voltar para aritmética modular

Tínhamos:

Definição. $a \equiv b \mod m$

Vamos voltar para aritmética modular

Tínhamos:

Definição. $a \equiv b \mod m$

significa que $m \mid a - b$

Vamos voltar para aritmética modular

Tínhamos:

Definição. $a \equiv b \mod m$

significa que $m \mid a - b$

ou equivalente,

$a - b = qm$, para algum número inteiro q.

Exemplo. $99 \equiv 4 \mod 5$, porque

$$99 - 4 = 5 \cdot 19$$

Dizemos que “a é congruente com b mod m ”.
Um objetivo que temos é:

Dizemos que “a é congruente com b mod m ”.
Um objetivo que temos é:

Teorema. [O pequena teorema de Fermat]

Dizemos que “a é congruente com b mod m ”.
Um objetivo que temos é:

Teorema. [O pequena teorema de Fermat]

Seja p um número primo.

Então, para qualquer número inteiro a,
com $p \not| a$, nós temos

$$a^{p-1} \equiv 1 \mod p$$

Dizemos que “a é congruente com b mod m ”.
Um objetivo que temos é:

Teorema. [O pequena teorema de Fermat]

Seja p um número primo.

Então, para qualquer número inteiro a,
com $p \not| a$, nós temos

$$a^{p-1} \equiv 1 \mod p$$

Exemplo. Seja $a = 2$, $p = 1009$, um primo.

essa relação $a^{p-1} \equiv 1 \mod p$ se torna

Exemplo. Seja $a = 2$, $p = 1009$, um primo.

essa relação $a^{p-1} \equiv 1 \mod p$ se torna

$$2^{1008} \equiv 1 \mod 1009.$$

Exemplo. Seja $a = 2$, $p = 1009$, um primo.

essa relação $a^{p-1} \equiv 1 \mod p$ se torna

$$2^{1008} \equiv 1 \mod 1009.$$

Em outras palavras,

$$1009 \mid 2^{1008} - 1$$

Exemplo. Seja $a = 2$, $p = 1009$, um primo.

essa relação $a^{p-1} \equiv 1 \mod p$ se torna

$$2^{1008} \equiv 1 \mod 1009.$$

Em outras palavras,

$$1009 \mid 2^{1008} - 1$$

Uau!

Se $a \equiv b \mod m$,
e $b \equiv c \mod m$,
é verdade que que $a \equiv c \mod m$?

Se $a \equiv b \mod m$,
e $b \equiv c \mod m$,
é verdade que que $a \equiv c \mod m$?

Vamos ver: $a - b = km$,
$b - c = nm$,
implicar que $a - c = km + nm$

Se $a \equiv b \mod m$,
e $b \equiv c \mod m$,
é verdade que que $a \equiv c \mod m$?

Vamos ver: $a - b = km$,

$b - c = nm$,

implicar que $a - c = km + nm$

Entao: $a - c = (k + n)m$

Se $a \equiv b \mod m$,
e $b \equiv c \mod m$,
é verdade que que $a \equiv c \mod m$?

Vamos ver: $a - b = km$,

$b - c = nm$,

implicar que $a - c = km + nm$

Entao: $a - c = (k + n)m$

Portanto $a \equiv c \mod m$.

Isso é chamado de “ relação transitiva ”

Mais sobre essas relações outra vez .....

Se $a \equiv b \mod m$

e também $c \equiv d \mod m$,

é verdade que

$$ac \equiv bd \mod m \ ?$$

Prova. Por hipótese, , $a = b + q_1 m, \quad c = d + q_2 m.$

Prova. Por hipótese, , $a = b + q_1 m, \quad c = d + q_2 m.$

Então, multiplicando as duas equações,

Prova. Por hipótese, , $a = b + q_1 m, \quad c = d + q_2 m.$

Então, multiplicando as duas equações,

$ac = (b + q_1 m)(d + q_2 m) =$

Prova. Por hipótese, , $a = b + q_1 m, \quad c = d + q_2 m.$

Então, multiplicando as duas equações,

$$ac = (b + q_1 m)(d + q_2 m) =$$

$$= bd + (q_1 dm + q_2 bm + q_1 q_2 m^2)$$

Prova. Por hipótese, , $a = b + q_1 m, \quad c = d + q_2 m.$

Então, multiplicando as duas equações,

$$ac = (b + q_1 m)(d + q_2 m) =$$

$$= bd + (q_1 dm + q_2 bm + q_1 q_2 m^2)$$

$$= bd + (q_1 d + q_2 b + q_1 q_2 m)m.$$

Lembrar:

Definição. $x \equiv y \mod m$

significa que $m \mid x - y$

ou equivalente,

$x - y = qm$, para algum numero inteiro q.

Prova. Por hipótese, , $a = b + q_1 m, \quad c = d + q_2 m.$

Então, multiplicando as duas equações,

$$ac = (b + q_1 m)(d + q_2 m) =$$

$$= bd + (q_1 dm + q_2 bm + q_1 q_2 m^2)$$

$$= bd + (q_1 d + q_2 b + q_1 q_2 m)m.$$

Prova. Por hipótese, , $a = b + q_1 m, \quad c = d + q_2 m.$

Então, multiplicando as duas equações,

$$ac = (b + q_1 m)(d + q_2 m) =$$

$$= bd + (q_1 dm + q_2 bm + q_1 q_2 m^2)$$

$$= bd + (q_1 d + q_2 b + q_1 q_2 m)m.$$

$ac - bd = (q_3)m$, onde $q_3 := q_1 d + q_2 b + q_1 q_2 m.$

$$ac - bd = (q_3)m, \text{ onde } q_3 := q_1 d + q_2 b + q_1 q_2 m.$$

$ac - bd = (q_3)m$, onde $q_3 := q_1 d + q_2 b + q_1 q_2 m$.

Então, por definição,

$$ac \equiv bd \mod m.$$

□

$ac - bd = (q_3)m$, onde $q_3 := q_1 d + q_2 b + q_1 q_2 m$.

Então, por definição,

$$ac \equiv bd \mod m.$$

□

Próxima,

Também podemos dividir uma congruência?

Próxima,

Também podemos dividir uma congruência?

Próxima,

Também podemos dividir uma congruência?

Exemplo.

É verdade que - se tivermos

$$5a \equiv 5b \mod 10,$$

Próxima,

Também podemos dividir uma congruência?

Exemplo.

É verdade que - se tivermos

$$5a \equiv 5b \mod 10,$$

então

$$a \equiv b \mod 10?$$

Se $a = 1, b = 2$, temos:

$$5 \cdot 1 \equiv 5 \cdot 2 \mod 10$$

Se $a = 1, b = 2$, temos:

$$5 \cdot 1 \equiv 5 \cdot 2 \mod 10$$

$$\text{mas } 5 \cdot 2 \equiv 0 \mod 10$$

Se $a = 1, b = 2$, temos:

$$5 \cdot 1 \equiv 5 \cdot 2 \mod 10$$

$$\text{mas } 5 \cdot 2 \equiv 0 \mod 10$$

Então $5 \equiv 0 \mod 10$, uma contradição.

Se $a = 1, b = 2$, temos:

$$5 \cdot 1 \equiv 5 \cdot 2 \mod 10$$

$$\text{mas } 5 \cdot 2 \equiv 0 \mod 10$$

Então $5 \equiv 0 \mod 10$, uma contradição.

Então, em geral, não podemos dividir!

Se $a = 1, b = 2$, temos:

$$5 \cdot 1 \equiv 5 \cdot 2 \mod 10$$

$$\text{mas } 5 \cdot 2 \equiv 0 \mod 10$$

Então $5 \equiv 0 \mod 10$, uma contradição.

Então, em geral, não podemos dividir!

Mas se trabalharmos mod a prime p?

Pensar sobre números inteiros mod p, um primo.

Tentar exemplos pequenos.....

até próxima!