Notas sobre teoria dos números (1)

Fonte: livros do L. Lóvasz e Kenneth Rosen (ref. completa na página)

Centro de Informática
Universidade Federal de Pernambuco

2007.1 / CIn-UFPE

Motivação

- Criptografia
- Segurança
- Complexidade de Algoritmos

Divisibilidade de inteiros

- Sejam a e b dois inteiros. Dizemos que *a divide b*, ou *a é um divisor de b*, ou *b é um múltiplo de a*, se existe um inteiro m tal que $b = am$.
- Notação: $a|b$
- Se a não é um divisor de b: $a \nmid b$

Divisibilidade de inteiros

- Sejam a e b dois inteiros. Dizemos que *a divide b*, ou *a é um divisor de b*, ou *b é um múltiplo de a*, se existe um inteiro m tal que $b = am$.
- Notação: $a|b$
- Se a não é um divisor de b: $a \nmid b$

Divisibilidade de inteiros

- Sejam a e b dois inteiros. Dizemos que *a divide b*, ou *a é um divisor de b*, ou *b é um múltiplo de a*, se existe um inteiro m tal que $b = am$.
- Notação: $a|b$
- Se a não é um divisor de b: $a \nmid b$

Divisibilidade de inteiros

Teorema (O algoritmo da divisão)

Sejam a um inteiro e d um inteiro positivo. Então existem inteiros únicos q e r, com $0 \leq r < d$, de forma que $a = dq + r$.

- d é chamado divisor;
- a é chamado dividendo;
- q é chamado quociente;
- e r é chamado de resto.

Exemplo

- Qual o quociente e o resto quando -11 é dividido por 3?
- Temos que $-11 = 3(-4) + 1$.
- Portanto, o quociente é -4 e o resto é 1.
- Poderíamos responder que o resto seria -2 e o quociente -3. Pois $-11 = 3(-3) - 2$. Mas, o resto não pode ser negativo. no exemplo, deve ser um inteiro entre 0 e 2.

Exemplo

- Qual o quociente e o resto quando -11 é dividido por 3?
- Temos que $-11 = 3(-4) + 1$.
- Portanto, o quociente é -4 e o resto é 1.
- Poderíamos responder que o resto seria -2 e o quociente -3. Pois $-11 = 3(-3) - 2$. Mas, o resto não pode ser negativo. no exemplo, deve ser um inteiro entre 0 e 2.

Exemplo

- Qual o quociente e o resto quando -11 é dividido por 3?
- Temos que $-11 = 3(-4) + 1$.
- Portanto, o quociente é -4 e o resto é 1.
- Poderíamos responder que o resto seria -2 e o quociente -3. Pois $-11 = 3(-3) - 2$. Mas, o resto não pode ser negativo. no exemplo, deve ser um inteiro entre 0 e 2.

Exemplo

- Qual o quociente e o resto quando -11 é dividido por 3?
- Temos que $-11 = 3(-4) + 1$.
- Portanto, o quociente é -4 e o resto é 1.
- Poderíamos responder que o resto seria -2 e o quociente -3. Pois $-11 = 3(-3) - 2$. Mas, o resto não pode ser negativo. no exemplo, deve ser um inteiro entre 0 e 2.

Exercícios

1 Prove que

a) se $a|b$ e $b|c$ então $a|c$;

b) se $a|b$ e $a|c$ então $a|b+c$ e $a|b-c$;

c) se $a, b > 0$ e $a|b$ então $a \leq b$;

d) se $a|b$ e $b|a$ então $a = b$ ou $a = -b$.

2 Seja r o resto da divisão $b : a$. Assuma que $c|a$ e $c|b$. Prove que $c|r$.

Definição

Um inteiro $p > 1$ é chamado um número primo se ele não é divisível por qualquer inteiro diferente de $1, -1, p$ e $-p$.

- Uma outra maneira de dizer isso é que um inteiro $p > 1$ é um primo se ele não pode ser escrito como o produto de dois inteiros positivos menores que ele.

Definição

Um inteiro $n > 1$ que não é um primo é chamado composto.

- E o número 1?
- É considerado nem primo, nem composto.
- Os primos podem ser considerados os átomos da matemática.
- Eles têm fascinado as pessoas desde os tempos antigos.

Definição

Um inteiro $n > 1$ que não é um primo é chamado composto.

- E o número 1?
- É considerado nem primo, nem composto.
- Os primos podem ser considerados os átomos da matemática.
- Eles têm fascinado as pessoas desde os tempos antigos.

Definição

Um inteiro $n > 1$ que não é um primo é chamado composto.

- E o número 1?
- É considerado nem primo, nem composto.
- Os primos podem ser considerados os átomos da matemática.
- Eles têm fascinado as pessoas desde os tempos antigos.

Definição

Um inteiro $n > 1$ que não é um primo é chamado composto.

- E o número 1?
- É considerado nem primo, nem composto.
- Os primos podem ser considerados os átomos da matemática.
- Eles têm fascinado as pessoas desde os tempos antigos.

Algumas questões sobre os primos

- Será que existe uma quantidade infinita de tais números?
- Os gregos antigos provaram que sim.
- A seqüência de primos é razoavelmente suave, mas ela tem buracos e focos densos. Quão grande são tais buracos? Existe um número primo com um número dado qualquer de dígitos?
- Sim, isso foi respondido em meados do século XIX.

Algumas questões sobre os primos

- Será que existe uma quantidade infinita de tais números?
- Os gregos antigos provaram que sim.
- A seqüência de primos é razoavelmente suave, mas ela tem buracos e focos densos. Quão grande são tais buracos? Existe um número primo com um número dado qualquer de dígitos?
- Sim, isso foi respondido em meados do século XIX.

Algumas questões sobre os primos

- Será que existe uma quantidade infinita de tais números?
- Os gregos antigos provaram que sim.
- A seqüência de primos é razoavelmente suave, mas ela tem buracos e focos densos. Quão grande são tais buracos? Existe um número primo com um número dado qualquer de dígitos?
- Sim, isso foi respondido em meados do século XIX.

Algumas questões sobre os primos

- Será que existe uma quantidade infinita de tais números?
- Os gregos antigos provaram que sim.
- A seqüência de primos é razoavelmente suave, mas ela tem buracos e focos densos. Quão grande são tais buracos? Existe um número primo com um número dado qualquer de dígitos?
- Sim, isso foi respondido em meados do século XIX.

Teste de primalidade

- Como você decide sobre se um inteiro positivo n é primo?
- Faz apenas 20 anos que algoritmos muito mais eficientes existem para testar se um dado inteiro é um primo.

Teste de primalidade

- Como você decide sobre se um inteiro positivo n é primo?
- Faz apenas 20 anos que algoritmos muito mais eficientes existem para testar se um dado inteiro é um primo.

- Se um inteiro maior que 1 não é ele próprio um primo, então ele pode ser escrito como um produto de primos.
- podemos escrevê-lo como um produto de dois inteiros positivos menores que ele; se um desses não é um primo, escrevemo-lo como o produto de dois inteiros menores que ele etc.;
- isso termina somente com primos. Fato provado tem mais de 2000 anos pelos gregos e é conhecido pelo seguinte teorema:

Teorema (Teorema Fundamental da Aritmética)

Todo inteiro positivo pode ser escrito como o produto de primos, e essa fatoração é única a menos da ordem dos fatores primos.

- Se um inteiro maior que 1 não é ele próprio um primo, então ele pode ser escrito como um produto de primos.
- podemos escrevê-lo como um produto de dois inteiros positivos menores que ele; se um desses não é um primo, escrevemo-lo como o produto de dois inteiros menores que ele etc.;
- isso termina somente com primos. Fato provado tem mais de 2000 anos pelos gregos e é conhecido pelo seguinte teorema:

Teorema (Teorema Fundamental da Aritmética)

Todo inteiro positivo pode ser escrito como o produto de primos, e essa fatoração é única a menos da ordem dos fatores primos.

- Se um inteiro maior que 1 não é ele próprio um primo, então ele pode ser escrito como um produto de primos.
- podemos escrevê-lo como um produto de dois inteiros positivos menores que ele; se um desses não é um primo, escrevemo-lo como o produto de dois inteiros menores que ele etc.;
- isso termina somente com primos. Fato provado tem mais de 2000 anos pelos gregos e é conhecido pelo seguinte teorema:

Teorema (Teorema Fundamental da Aritmética)

Todo inteiro positivo pode ser escrito como o produto de primos, e essa fatoração é única a menos da ordem dos fatores primos.

Exemplo

Aplique o teorema fundamental da aritmética para provar que $\sqrt{2}$ é irracional.

Prova: por contradição.

1. Supomos que $\sqrt{2}$ é racional.
2. Logo, $\sqrt{2} = \frac{a}{b}$, onde a e b são dois inteiros.
3. Elevando ao quadrado ambos os lados e rearrumando, obtemos $2b^2 = a^2$.
4. Agora considere a fatoração prima de ambos os lados, suponha que 2 ocorra m vezes na fatoração prima de a e n vezes na fatoração prima de b.
5. Então ele ocorre $2m$ vezes na fatoração prima de a^2 e $2n$ vezes na fatoração prima de b^2.
6. Como $2b^2 = a^2$, e a fatoração prima é única, temos que ter $2n + 1 = 2m$. Uma contradição. Isso prova que $\sqrt{2}$ tem que ser irracional.

Exemplo

Aplique o teorema fundamental da aritmética para provar que $\sqrt{2}$ é irracional.

Prova: por contradição.

1. Supomos que $\sqrt{2}$ é racional.
2. Logo, $\sqrt{2} = \frac{a}{b}$, onde a e b são dois inteiros.
3. Elevando ao quadrado ambos os lados e rearrumando, obtemos $2b^2 = a^2$.
4. Agora considere a fatoração prima de ambos os lados, suponha que 2 ocorra m vezes na fatoração prima de a e n vezes na fatoração prima de b.
5. Então ele ocorre $2m$ vezes na fatoração prima de a^2 e $2n$ vezes na fatoração prima de b^2.
6. Como $2b^2 = a^2$, e a fatoração prima é única, temos que ter $2n + 1 = 2m$. Uma contradição. Isso prova que $\sqrt{2}$ tem que ser irracional.

Exemplo

Aplique o teorema fundamental da aritmética para provar que $\sqrt{2}$ é irracional.

Prova: por contradição.

1. Supomos que $\sqrt{2}$ é racional.
2. Logo, $\sqrt{2} = \frac{a}{b}$, onde a e b são dois inteiros.
3. Elevando ao quadrado ambos os lados e rearrumando, obtemos $2b^2 = a^2$.
4. Agora considere a fatoração prima de ambos os lados, suponha que 2 ocorra m vezes na fatoração prima de a e n vezes na fatoração prima de b.
5. Então ele ocorre $2m$ vezes na fatoração prima de a^2 e $2n$ vezes na fatoração prima de b^2.
6. Como $2b^2 = a^2$, e a fatoração prima é única, temos que ter $2n + 1 = 2m$. Uma contradição. Isso prova que $\sqrt{2}$ tem que ser irracional.

Exemplo

Aplique o teorema fundamental da aritmética para provar que $\sqrt{2}$ é irracional.

Prova: por contradição.

1. Supomos que $\sqrt{2}$ é racional.
2. Logo, $\sqrt{2} = \frac{a}{b}$, onde a e b são dois inteiros.
3. Elevando ao quadrado ambos os lados e rearrumando, obtemos $2b^2 = a^2$.
4. Agora considere a fatoração prima de ambos os lados, suponha que 2 ocorra m vezes na fatoração prima de a e n vezes na fatoração prima de b.
5. Então ele ocorre $2m$ vezes na fatoração prima de a^2 e $2n$ vezes na fatoração prima de b^2.
6. Como $2b^2 = a^2$, e a fatoração prima é única, temos que ter $2n + 1 = 2m$. Uma contradição. Isso prova que $\sqrt{2}$ tem que ser irracional.

Exemplo

Aplique o teorema fundamental da aritmética para provar que $\sqrt{2}$ é irracional.

Prova: por contradição.

1. Supomos que $\sqrt{2}$ é racional.
2. Logo, $\sqrt{2} = \frac{a}{b}$, onde a e b são dois inteiros.
3. Elevando ao quadrado ambos os lados e rearrumando, obtemos $2b^2 = a^2$.
4. Agora considere a fatoração prima de ambos os lados, suponha que 2 ocorra m vezes na fatoração prima de a e n vezes na fatoração prima de b.
5. Então ele ocorre $2m$ vezes na fatoração prima de a^2 e $2n$ vezes na fatoração prima de b^2.
6. Como $2b^2 = a^2$, e a fatoração prima é única, temos que ter $2n + 1 = 2m$. Uma contradição. Isso prova que $\sqrt{2}$ tem que ser irracional.

Exemplo

Aplique o teorema fundamental da aritmética para provar que $\sqrt{2}$ é irracional.

Prova: por contradição.

1. Supomos que $\sqrt{2}$ é racional.
2. Logo, $\sqrt{2} = \frac{a}{b}$, onde a e b são dois inteiros.
3. Elevando ao quadrado ambos os lados e rearrumando, obtemos $2b^2 = a^2$.
4. Agora considere a fatoração prima de ambos os lados, suponha que 2 ocorra m vezes na fatoração prima de a e n vezes na fatoração prima de b.
5. Então ele ocorre $2m$ vezes na fatoração prima de a^2 e $2n$ vezes na fatoração prima de b^2.
6. Como $2b^2 = a^2$, e a fatoração prima é única, temos que ter $2n + 1 = 2m$. Uma contradição. Isso prova que $\sqrt{2}$ tem que ser irracional.

Exercícios

1. Prove que se p é um primo, a e b são inteiros, e $p|ab$, então $p|a$ ou $p|b$ (ou ambos).
2. Suponha que a e b sejam inteiros e $a|b$. Suponha também que p é um primo e $p|b$ mas $p \nmid a$. Prove que p é um divisor da fração b/a.
3. Prove que a fatoração prima de um número n contém no máximo $\log_2 n$ fatores.

Respostas

1) Prove que se p é um primo, a e b são inteiros, e $p|ab$, então $p|a$ ou $p|b$ (ou ambos).

Resp. p ocorre na fatoração prima de $a.b$, logo ele deve ocorrer na fatoração prima de a ou de b, ou de ambos.

2) Suponha que a e b sejam inteiros e $a|b$. Suponha também que p é um primo e $p|b$ mas $p \nmid a$. Prove que p é um divisor da fração b/a.

Resp. Como $b = a.(b/a)$, e $p|b$, então $p|a$ ou $p|(b/a)$, como $p \nmid a$, logo $p|(b/a)$.

Respostas

1) Prove que se p é um primo, a e b são inteiros, e $p|ab$, então $p|a$ ou $p|b$ (ou ambos).

Resp. p ocorre na fatoração prima de $a.b$, logo ele deve ocorrer na fatoração prima de a ou de b, ou de ambos.

2) Suponha que a e b sejam inteiros e $a|b$. Suponha também que p é um primo e $p|b$ mas $p \nmid a$. Prove que p é um divisor da fração b/a.

Resp. Como $b = a.(b/a)$, e $p|b$, então $p|a$ ou $p|(b/a)$, como $p \nmid a$, logo $p|(b/a)$.

Respostas

1) Prove que se p é um primo, a e b são inteiros, e $p|ab$, então $p|a$ ou $p|b$ (ou ambos).

Resp. p ocorre na fatoração prima de $a.b$, logo ele deve ocorrer na fatoração prima de a ou de b, ou de ambos.

2) Suponha que a e b sejam inteiros e $a|b$. Suponha também que p é um primo e $p|b$ mas $p \nmid a$. Prove que p é um divisor da fração b/a.

Resp. Como $b = a.(b/a)$, e $p|b$, então $p|a$ ou $p|(b/a)$, como $p \nmid a$, logo $p|(b/a)$.

Respostas

1) Prove que se p é um primo, a e b são inteiros, e $p|ab$, então $p|a$ ou $p|b$ (ou ambos).

Resp. p ocorre na fatoração prima de $a.b$, logo ele deve ocorrer na fatoração prima de a ou de b, ou de ambos.

2) Suponha que a e b sejam inteiros e $a|b$. Suponha também que p é um primo e $p|b$ mas $p \nmid a$. Prove que p é um divisor da fração b/a.

Resp. Como $b = a.(b/a)$, e $p|b$, então $p|a$ ou $p|(b/a)$, como $p \nmid a$, logo $p|(b/a)$.

3) Prove que a fatoração prima de um número n contém no máximo $\log_2 n$ fatores.

Resp. Seja a fatoração prima de n igual a $p_1.p_2 \ldots p_k$; temos que cada p_i é menor ou igual a 2, logo $n \geq 2^k$, então $\log_2 n \geq \log_2 2^k \rightarrow \log_2 n \geq k \rightarrow k \leq \log_2 n$, onde k é a quantidade de fatores de n.

3) Prove que a fatoração prima de um número n contém no máximo $\log_2 n$ fatores.

Resp. Seja a fatoração prima de n igual a $p_1.p_2 \ldots p_k$; temos que cada p_i é menor ou igual a 2, logo $n \geq 2^k$, então $\log_2 n \geq \log_2 2^k \rightarrow \log_2 n \geq k \rightarrow k \leq \log_2 n$, onde k é a quantidade de fatores de n.

Teorema

Se n é um número composto, então n possui um divisor primo menor ou igual a $\sqrt{n}$

1. Se n é composto, então ele possui um fator a, $1 < a < n$.
2. Logo, $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
3. Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$, pois senão teríamos $ab > \sqrt{n}.\sqrt{n}$.
4. Logo, n possui um divisor positivo que não é maior que $\sqrt{n}$.
5. Esse divisor ou é um primo ou pelo teorema fundamental da aritmética, posui um divisor primo. Em qualquer dos casos, n possui um divisor primo menor ou igual a $\sqrt{n}$

Teorema

Se n é um número composto, então n possui um divisor primo menor ou igual a $\sqrt{n}$

1. Se n é composto, então ele possui um fator a, $1 < a < n$.
2. Logo, $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
3. Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$, pois senão teríamos $ab > \sqrt{n}.\sqrt{n}$.
4. Logo, n possui um divisor positivo que não é maior que $\sqrt{n}$.
5. Esse divisor ou é um primo ou pelo teorema fundamental da aritmética, posui um divisor primo. Em qualquer dos casos, n possui um divisor primo menor ou igual a $\sqrt{n}$

Teorema

Se n é um número composto, então n possui um divisor primo menor ou igual a $\sqrt{n}$

1. Se n é composto, então ele possui um fator a, $1 < a < n$.
2. Logo, $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
3. Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$, pois senão teríamos $ab > \sqrt{n}.\sqrt{n}$.
4. Logo, n possui um divisor positivo que não é maior que $\sqrt{n}$.
5. Esse divisor ou é um primo ou pelo teorema fundamental da aritmética, posui um divisor primo. Em qualquer dos casos, n possui um divisor primo menor ou igual a $\sqrt{n}$

Teorema

Se n é um número composto, então n possui um divisor primo menor ou igual a $\sqrt{n}$

1. Se n é composto, então ele possui um fator a, $1 < a < n$.
2. Logo, $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
3. Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$, pois senão teríamos $ab > \sqrt{n}.\sqrt{n}$.
4. Logo, n possui um divisor positivo que não é maior que $\sqrt{n}$.
5. Esse divisor ou é um primo ou pelo teorema fundamental da aritmética, posui um divisor primo. Em qualquer dos casos, n possui um divisor primo menor ou igual a $\sqrt{n}$

Teorema

Se n é um número composto, então n possui um divisor primo menor ou igual a $\sqrt{n}$

1. Se n é composto, então ele possui um fator a, $1 < a < n$.
2. Logo, $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
3. Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$, pois senão teríamos $ab > \sqrt{n}.\sqrt{n}$.
4. Logo, n possui um divisor positivo que não é maior que $\sqrt{n}$.
5. Esse divisor ou é um primo ou pelo teorema fundamental da aritmética, posui um divisor primo. Em qualquer dos casos, n possui um divisor primo menor ou igual a $\sqrt{n}$

Exemplo

Mostre que 101 é primo.

- O únicos primos menores ou iguais a $\sqrt{101}$ são 2,3,5 e 7.
- Como 101 não é divisível por 2, 3, 5 e nem 7, logo 101 é primo

Exemplo

Mostre que 101 é primo.

- O únicos primos menores ou iguais a $\sqrt{101}$ são 2,3,5 e 7.
- Como 101 não é divisível por 2, 3, 5 e nem 7, logo 101 é primo

Teorema

Existe uma quantidade infinita de números primos.

Idéia da prova: Vamos mostrar que para todo inteiro positivo n, existe um número primo maior que n. A prova será por contradição. Considere o número $n! + 1$, e qualquer divisor primo p dele. Mostraremos que $p > n$. A prova será por contradição.

1. Considere o número $n! + 1$, e qualquer divisor primo p dele.
2. Suponha que $p \leq n$, logo $p|n!$, pois ele é um dos inteiros cujo produto é $n!$.
3. De 1, temos que $p|n! + 1$.
4. Se $p|n!$ e $p|n! + 1$ então $p|(n! + 1) - n!$, isso significa que $p|1$, temos uma contradição. Consequentemente, p tem que ser maior que n.

Teorema

Existe uma quantidade infinita de números primos.

Idéia da prova: Vamos mostrar que para todo inteiro positivo n, existe um número primo maior que n. A prova será por contradição. Considere o número $n! + 1$, e qualquer divisor primo p dele. Mostraremos que $p > n$. A prova será por contradição.

1. Considere o número $n! + 1$, e qualquer divisor primo p dele.
2. Suponha que $p \leq n$, logo $p|n!$, pois ele é um dos inteiros cujo produto é $n!$.
3. De 1, temos que $p|n! + 1$.
4. Se $p|n!$ e $p|n! + 1$ então $p|(n! + 1) - n!$, isso significa que $p|1$, temos uma contradição. Consequentemente, p tem que ser maior que n.

Teorema

Existe uma quantidade infinita de números primos.

Idéia da prova: Vamos mostrar que para todo inteiro positivo n, existe um número primo maior que n. A prova será por contradição. Considere o número $n! + 1$, e qualquer divisor primo p dele. Mostraremos que $p > n$. A prova será por contradição.

1. Considere o número $n! + 1$, e qualquer divisor primo p dele.
2. Suponha que $p \leq n$, logo $p|n!$, pois ele é um dos inteiros cujo produto é $n!$.
3. De 1, temos que $p|n! + 1$.
4. Se $p|n!$ e $p|n! + 1$ então $p|(n! + 1) - n!$, isso significa que $p|1$, temos uma contradição. Consequentemente, p tem que ser maior que n.

Teorema

Existe uma quantidade infinita de números primos.

Idéia da prova: Vamos mostrar que para todo inteiro positivo n, existe um número primo maior que n. A prova será por contradição. Considere o número $n! + 1$, e qualquer divisor primo p dele. Mostraremos que $p > n$. A prova será por contradição.

1. Considere o número $n! + 1$, e qualquer divisor primo p dele.
2. Suponha que $p \leq n$, logo $p|n!$, pois ele é um dos inteiros cujo produto é $n!$.
3. De 1, temos que $p|n! + 1$.
4. Se $p|n!$ e $p|n! + 1$ então $p|(n! + 1) - n!$, isso significa que $p|1$, temos uma contradição. Consequentemente, p tem que ser maior que n.

- Vimos que a seqüência de primos aprsenta uma certa irregularidade. Vemos grandes “lacunas” e também primos que são muito próximos.
- Vamos provar que esas “lacunas” ficam cada vez maiores quando consideramos números cada vez maiores. Em algum lugar da seqüência existe uma cadeia de 100 números compostos consecutivos, em outro lugar existe uma cadeia de 1000 números compostos consecutivos, etc.

Teorema

Para todo inteiro positivo k , existem k inteiros compostos consecutivos.

- Vimos que a seqüência de primos aprsenta uma certa irregularidade. Vemos grandes “lacunas” e também primos que são muito próximos.
- Vamos provar que esas “lacunas” ficam cada vez maiores quando consideramos números cada vez maiores. Em algum lugar da seqüência existe uma cadeia de 100 números compostos consecutivos, em outro lugar existe uma cadeia de 1000 números compostos consecutivos, etc.

Teorema

Para todo inteiro positivo k , existem k inteiros compostos consecutivos.

Prova

- Seja $n = k + 1$ e considere os números $n! + 2,\ n! + 3,\ \ldots,\ n! + n$.
- Algum desses pode ser um primo?
- o primeiro número é par, pois $n!$ e 2 são ambos pares
- O segundo número é divisível por 3, pois $n!$ e 3 são ambos divisíveis por 3 (assumindo que $n > 2$).
- Em geral $n! + i$ é divisível por i, para todo $i = 2, 3, \ldots, n$.
- Daí esses números não podem ser primos, e portanto encontramos $n - 1 = k$ números compostos consecutivos.

Prova

- Seja $n = k + 1$ e considere os números $n! + 2,\ n! + 3,\ \ldots,\ n! + n$.
- Algum desses pode ser um primo?
- o primeiro número é par, pois $n!$ e 2 são ambos pares
- O segundo número é divisível por 3, pois $n!$ e 3 são ambos divisíveis por 3 (assumindo que $n > 2$).
- Em geral $n! + i$ é divisível por i, para todo $i = 2, 3, \ldots, n$.
- Daí esses números não podem ser primos, e portanto encontramos $n - 1 = k$ números compostos consecutivos.

Prova

- Seja $n = k + 1$ e considere os números $n! + 2,\ n! + 3,\ \ldots,\ n! + n$.
- Algum desses pode ser um primo?
- o primeiro número é par, pois $n!$ e 2 são ambos pares
- O segundo número é divisível por 3, pois $n!$ e 3 são ambos divisíveis por 3 (assumindo que $n > 2$).
- Em geral $n! + i$ é divisível por i, para todo $i = 2, 3, \ldots, n$.
- Daí esses números não podem ser primos, e portanto encontramos $n - 1 = k$ números compostos consecutivos.

Prova

- Seja $n = k + 1$ e considere os números $n! + 2,\ n! + 3,\ \ldots,\ n! + n$.
- Algum desses pode ser um primo?
- o primeiro número é par, pois $n!$ e 2 são ambos pares
- O segundo número é divisível por 3, pois $n!$ e 3 são ambos divisíveis por 3 (assumindo que $n > 2$).
- Em geral $n! + i$ é divisível por i, para todo $i = 2, 3, \ldots, n$.
- Daí esses números não podem ser primos, e portanto encontramos $n - 1 = k$ números compostos consecutivos.

Prova

- Seja $n = k + 1$ e considere os números $n! + 2,\ n! + 3,\ \ldots,\ n! + n$.
- Algum desses pode ser um primo?
- o primeiro número é par, pois $n!$ e 2 são ambos pares
- O segundo número é divisível por 3, pois $n!$ e 3 são ambos divisíveis por 3 (assumindo que $n > 2$).
- Em geral $n! + i$ é divisível por i, para todo $i = 2, 3, \ldots, n$.
- Daí esses números não podem ser primos, e portanto encontramos $n - 1 = k$ números compostos consecutivos.

Prova

- Seja $n = k + 1$ e considere os números $n! + 2,\ n! + 3,\ \ldots,\ n! + n$.
- Algum desses pode ser um primo?
- o primeiro número é par, pois $n!$ e 2 são ambos pares
- O segundo número é divisível por 3, pois $n!$ e 3 são ambos divisíveis por 3 (assumindo que $n > 2$).
- Em geral $n! + i$ é divisível por i, para todo $i = 2, 3, \ldots, n$.
- Daí esses números não podem ser primos, e portanto encontramos $n - 1 = k$ números compostos consecutivos.

E a questão de encontrar primos muito próximos?

Definição (primos gêmeos)

Dois primos cuja a diferença é dois são chamados de números primos gêmeos.

Exemplo

$(3, 5),\ (5, 7),\ (11, 13)$

- Será que existe uma quantidade infinita de primos gêmeos?
- Questão em aberto.

E a questão de encontrar primos muito próximos?

Definição (primos gêmeos)

Dois primos cuja a diferença é dois são chamados de números primos gêmeos.

Exemplo

$(3, 5),\ (5, 7),\ (11, 13)$

- Será que existe uma quantidade infinita de primos gêmeos?
- Questão em aberto.

- Uma das questões mais importantes sobre primos é: quantos primos existem até um dado número n?
- Se representarmos o número de primos até n por $\pi(n)$, o seguinte teorema responde essa questão.

Teorema (O teorema do número primo)

Suponha que $\pi(n)$ represente a quantidade de primos entre $1 \ldots n$. Então $\pi(n)$ é aproximadamente igual a $n/\ln n$.

- Em 1896, esse teorema foi provado por dois matemáticos, Hadamard e de la Vallée Poussin.

Mais questões em aberto

- *Conjectura de Goldbach*: todo inteiro par maior que 2 pode ser escrito como a soma de dois primos.
- Outra conjectura de Goldbach, que foi "essencialmente" provada, pois a prova somente funciona para números que são muito grandes, é a seguinte: todo inteiro ímpar maior que 5 pode ser escrito como a soma de três primos. (essencialmente provada por Vinogradov na década de 1930).

Mais questões em aberto

- *Conjectura de Goldbach*: todo inteiro par maior que 2 pode ser escrito como a soma de dois primos.
- Outra conjectura de Goldbach, que foi "essencialmente" provada, pois a prova somente funciona para números que são muito grandes, é a seguinte: todo inteiro ímpar maior que 5 pode ser escrito como a soma de três primos. (essencialmente provada por Vinogradov na década de 1930).

Mais questões

- Suponha que temos um inteiro n e queremos saber quão breve após n podemos ter certeza de encontrar um primo.
- Vimos na prova da infinitude de primos que para todo n, existe um primo entre n e $n! + 1$.
- Esse é um enunciado muito fraco; ele diz, por exemplo, que existe um primo entre 10 e $10! + 1 = 3628801$. Enquanto que o próximo primo é 11.
- Chebychev provou no século XIX que existe sempre um primo entre n e $2n$.

Mais questões

- Suponha que temos um inteiro n e queremos saber quão breve após n podemos ter certeza de encontrar um primo.
- Vimos na prova da infinitude de primos que para todo n, existe um primo entre n e $n! + 1$.
- Esse é um enunciado muito fraco; ele diz, por exemplo, que existe um primo entre 10 e $10! + 1 = 3628801$. Enquanto que o próximo primo é 11.
- Chebychev provou no século XIX que existe sempre um primo entre n e $2n$.

Mais questões

- Suponha que temos um inteiro n e queremos saber quão breve após n podemos ter certeza de encontrar um primo.
- Vimos na prova da infinitude de primos que para todo n, existe um primo entre n e $n! + 1$.
- Esse é um enunciado muito fraco; ele diz, por exemplo, que existe um primo entre 10 e $10! + 1 = 3628801$. Enquanto que o próximo primo é 11.
- Chebychev provou no século XIX que existe sempre um primo entre n e $2n$.

Mais questões

- Suponha que temos um inteiro n e queremos saber quão breve após n podemos ter certeza de encontrar um primo.
- Vimos na prova da infinitude de primos que para todo n, existe um primo entre n e $n! + 1$.
- Esse é um enunciado muito fraco; ele diz, por exemplo, que existe um primo entre 10 e $10! + 1 = 3628801$. Enquanto que o próximo primo é 11.
- Chebychev provou no século XIX que existe sempre um primo entre n e $2n$.

- Também se tem uma prova de que existe sempre um primo entre dois cubos consecutivos. Exemplo entre $27 = 3^3$ e $64 = 4^3$.

Aberto Existe sempre um primo entre dois quadrados consecutivos?

- Por exemplo entre $100 = 10^2$ e $121 = 11^2$ encontramos 101, 103, 107, 109, 113.

- Também se tem uma prova de que existe sempre um primo entre dois cubos consecutivos. Exemplo entre $27 = 3^3$ e $64 = 4^3$.

Aberto Existe sempre um primo entre dois quadrados consecutivos?

- Por exemplo entre $100 = 10^2$ e $121 = 11^2$ encontramos 101, 103, 107, 109, 113.

- Também se tem uma prova de que existe sempre um primo entre dois cubos consecutivos. Exemplo entre $27 = 3^3$ e $64 = 4^3$.

Aberto Existe sempre um primo entre dois quadrados consecutivos?

- Por exemplo entre $100 = 10^2$ e $121 = 11^2$ encontramos 101, 103, 107, 109, 113.

- Mais tarde, volteremos a falar sobre primos, pseudoprimos, o pequeno teorema de Fermat, teste de primalidade, etc. Mas, antes vamos estudar:
- Aritmética modular: algoritmo de Euclides, teorema chinês do resto, etc.

- Mais tarde, volteremos a falar sobre primos, pseudoprimos, o pequeno teorema de Fermat, teste de primalidade, etc. Mas, antes vamos estudar:
- Aritmética modular: algoritmo de Euclides, teorema chinês do resto, etc.