UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE MATEMÁTICA

25 JULHO 2016
www.professores.uff.br/nmedeiros

EXISTEM INFINITOS NÚMEROS PRIMOS

1. Considere a sequência:

$$a_0 := 2, a_1 := a_0! + 1, \ldots, a_{n+1} := a_n! + 1, \ldots$$

Então:

(a) Se $i < j$, então $a_i \mid a_j!$;

(b) Se $i \neq j$, então mdc(a_i, a_j)=1;

(c) Conclua, a partir de (b), que existem infinitos números primos (tome um fator primo de cada a_i).

2. Para cada $n = 0, 1, 2, \ldots$, o n-ésimo *número de Fermat* é definido como $F_n = 2^{2^n} + 1$. O objetivo deste exercício é mostrar que os números de Fermat são primos entre si, isto é, mdc$(F_i, F_j) = 1$ se $i \neq j$. Sejam m, n inteiros positivos.

(a) Defina $x = 2^{2^n} (= F_n - 1)$. Mostre que $x^{2^m} = F_{n+m} - 1$;

(b) Mostre que $x + 1$ divide $x^{2^m} - 1$ e portanto F_n divide $F_{n+m} - 2$;

(c) Conclua que mdc$(F_n, F_{n+m}) = 1$;

(d) Como no exercício anterior, conclua que existem infinitos números primos.

Quando F_n é primo, o chamamos de *primo de Fermat*. São conhecidos cinco deles:

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65537 \qquad .$$

Fermat afirmou, erroneamente, que F_n é primo para todo n; Euler mais tarde demonstrou que $641 \mid F_5 = 2^{32} + 1$. Acredita-se que os cinco números acima são os únicos primos de Fermat que existem.

3. Suponha, por contradição, que o conjunto dos números primos é finito, digamos $p_1, \ldots, p_k$. Seja n um número natural. Então podemos escrever qualquer número $m \leq n$ na forma $m = m_1^2 m_2$, onde $m_1^2 \leq n$ e

$$m_2 = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} \qquad \text{onde } a_k = 0 \text{ ou } 1 \text{ para cada } k.$$

Assim, considerando todas as possíveis maneiras de escrever os naturais $m \leq n$, temos: 2^k escolhas para m_2 e no máximo $[\sqrt{n}]$ escolhas para m_1 (aqui, $[x]$ é o maior inteiro $\leq x$). Ou seja, para todo n natural, vale que

$$n \leq 2^k \sqrt{n}$$

absurdo, pois esta desigualdade não vale para n suficientemente grande.

4. (Utilizando séries) O argumento do exercício anterior é útil para provar que a soma dos inversos dos números primos *diverge.*

Teorema (Euler)

$$\sum_{p \text{ primo}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots = \infty$$

isto é, essa soma fica arbitrariamente grande para p grande.

De fato, suponha que esta série converge. Então existe um índice k tal que

$$\frac{1}{p_{k+1}} + \frac{1}{p_{k+2}} + \frac{1}{p_{k+3}} + \cdots < \frac{1}{2}.$$

Seja $\pi_k(x)$ o número de naturais $n \leq x$ que são divisíveis *apenas* pelos primos $2, 3, \ldots, p_k$. Como o número de naturais $n \leq x$ que são divisíveis por p não ultrapassa x/p, temos

$$x - \pi_k(x) < \frac{x}{p_{k+1}} + \frac{x}{p_{k+2}} + \frac{x}{p_{k+3}} + \cdots < \frac{x}{2}.$$

Agora percebemos que no argumento da prova anterior foi mostrado que

$$\pi_k(x) \leq 2^k \sqrt{x}$$

e logo obtemos

$$\frac{x}{2} < 2^k \sqrt{x}$$

o que é uma contradição para x suficientemente grande.

5. Vamos mostrar que existem infinitos números primos da forma $4k + 3$. A ideia é adaptar a prova de Euclides, vista em sala.

(a) Se $a_1 \cdot a_2 \cdots a_n \equiv 3 \pmod 4$, então existe i tal que $a_i \equiv 3 \pmod 4$.

(b) Suponha que existe apenas um número finito de primos da forma $4k + 3$, digamos $p_1, p_2, \ldots, p_k$. Defina $N = 2(p_1 \cdots p_k) + 1$ e mostre que $N \equiv 3 \pmod 4$. Aqui, o Teorema Fundamental da Aritmética e o item (a) devem terminar o trabalho.

(c) É possível adaptar o método do Exercício 1?

6. (Série harmônica) Mostre que:

$$\sum_{n=1}^{\infty} \frac{1}{n} = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) = \infty.$$

De fato:

$$\begin{aligned}
\frac{1}{3} + \frac{1}{4} &> \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \\
\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} &> \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = \frac{1}{2} \\
\frac{1}{9} + \cdots + \frac{1}{16} &> \frac{1}{16} + \cdots + \frac{1}{16} = \frac{1}{2} \\
&\vdots
\end{aligned}$$

ou seja, a soma $1 + \frac{1}{2} + \cdots + \frac{1}{n}$ assume valores arbitrariamente grandes para n grande.

7. (Existem infinitos números primos: outra prova) Vamos mostrar que

$$P := \prod_{p \text{ primo}} \left(1 - \frac{1}{p}\right)^{-1} = \infty.$$

A partir daí concluímos que existem infinitos números primos.

Uma prova maravilhosa, devida a Euler: dado $n > 0$, seja q o maior primo que aparece na fatoração dos números $\{2, \ldots, n\}$. Daí, se e é um inteiro positivo:

$$\begin{aligned}
P &\geq \left(1 - \frac{1}{2}\right)^{-1} \left(1 - \frac{1}{3}\right)^{-1} \left(1 - \frac{1}{5}\right)^{-1} \cdots \left(1 - \frac{1}{q}\right)^{-1} \\
&= \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) \left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots\right) \cdots \left(1 + \frac{1}{q} + \frac{1}{q^2} + \cdots\right) \\
&\geq \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^e}\right) \left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots + \frac{1}{3^e}\right) \cdots \left(1 + \frac{1}{q} + \frac{1}{q^2} + \cdots + \frac{1}{q^e}\right)
\end{aligned}$$

e logo, para e suficientemente grande,

$$P \geq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Como a série harmônica diverge, temos $P = \infty$.