26. Usando a fatorização de 507 e 1287 em fatores primos, determine o máximo divisor comum e o mínimo múltiplo comum entre esses inteiros.

507	3
169	13
13	13
1	

1287	3
429	3
143	11
13	13
1	

$507 = 3 \times 13^2$ $\qquad$ $1287 = 3^2 \times 11 \times 13$

$m.d.c\,(507, 1287) = 3 \times 13 = 39$

$m.m.c\,(507, 1287) = 3^2 \times 11 \times 13^2 = 16781$

27. Usando a fatorização de 525 e 2205 em fatores primos, determine o máximo divisor comum e o mínimo múltiplo comum entre esses inteiros. Indique todos os divisores positivos de 525.

$$\begin{array}{r|l} 525 & 3 \\ 175 & 5 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array} \qquad \begin{array}{r|l} 2205 & 3 \\ 735 & 3 \\ 245 & 5 \\ 49 & 7 \\ 7 & 7 \\ 1 & \end{array}$$

$525 = 3 \times 5^2 \times 7$ $\qquad$ $2205 = 3^2 \times 5 \times 7^2$

$m.d.c\,(525, 2205) = 3 \times 5 \times 7 = 105$

$m.m.c\,(525, 2205) = 3^2 \times 5^2 \times 7^2 = 11\,025$

Divisores positivos de 525: $1, 3, 5, 3 \times 5 = 15, 7, 3 \times 7 = 21, 5 \times 7 = 35$

$5^2 = 25, \quad 3 \times 5^2 = 75, \quad 7 \times 5^2 = 175, \quad 3 \times 7 \times 5 = 105$

$3 \times 5^2 \times 7 = 525$

28. Verifique se 701 é um número primo, testando todos os primos $p \leq \sqrt{701}$ como possíveis divisores.

Proposição: Se $n \in \mathbb{N}$ e n é um número composto então se p é primo e $p \mid n$ então $p \leq \sqrt{n}$

Corolário: Para testar se $n \in \mathbb{N}$ é primo então basta testar a divisibilidade pelos primos p com $p \leq \sqrt{n}$.

Temos $26^2 \leq 701 \leq 27^2 \Rightarrow \sqrt{701} = 26, \ldots$

Os números primos até 26 são: 2, 3, 5, 7, 11, 13, 17, 19, 23

É fácil verificar que $2 \nmid 701$, $3 \nmid 701$, $5 \nmid 701$, $7 \nmid 701$, $11 \nmid 701$, $13 \nmid 701$, $17 \nmid 701$, $19 \nmid 701$ e $23 \nmid 701$

Podemos então concluir que 701 é primo.

29. (a) Mostre que é condição necessária para que um inteiro $p \neq 2$ seja primo que satisfaça $p = 4n \pm 1$, $n \in \mathbb{N}$.

(b) Esta condição é também suficiente? Justifique.

(b) A condição não é suficiente.
Temos $9 = 4n+1$ com $n=2$ e 9 não é primo, $9 = 3 \times 3$.

(a) Queremos ver que se p é primo então p é da forma

$$p = 4n+1 \quad \text{ou} \quad p = 4n-1 = 4n-1+4-4 = 4(n-1)+3$$

ou seja, que o resto da divisão de p por 4 é 1 ou 3.
Pelo Teorema do algoritmo da divisão, dado um número $p \in \mathbb{N}$ existem $q \in \mathbb{N}_0$ e $r \in \{0,1,2,3\}$ tais que

$$p = 4q + r$$

Basta mostrar que $r \neq 0$ e $r \neq 2$.

- $R = 0$, se $p = 4q$ então p não é primo pois $4 \mid p$.

- $R = 2$, se $p = 4q + 2 = 2(2q+1)$ então p não é primo a não ser que $p = 2$, pois $2 \mid p$ e $\underbrace{2q+1}_{>1} \mid p$ e, por hipótese, $q \neq 0$ pois $p \neq 2$.

30. Prove que

(a) todo o primo da forma $3n+1$ é da forma $6m+1$ $(m, n \in \mathbb{N})$;

(b) o único primo da forma n^3-1 é o 7 $(n \in \mathbb{N})$; [Sugestão: $n^3-1=(n-1)(n^2+n+1)$]

(c) todo o inteiro da forma n^4-4, em que $n>1$, é composto.

(a) Basta mostrar que n é par.

Suponhamos, por redução ao absurdo, que existe um primo p da forma $3n+1$ com n ímpar.

Então n é da forma $2k+1$ com $k \in \mathbb{N}_0$

Logo $p = 3(2k+1)+1 = 6k+4 = 2(\underbrace{3k+2}_{\geqslant 2})$

e $2 \mid p$ e $3k+2 \mid p$ logo p não é primo.

O absurdo resultou de supormos que n é ímpar.

Portanto n é par e $p = 6m+1$ para algum $m \in \mathbb{N}$.

(b) $p = n^3 - 1 = (n-1)(n^2+n+1)$

Se p é primo então ou $n-1 = 1$ ou $n^2+n+1 = 1$

Se $n-1 = 1$ então $n = 2$ e $p = 7$

Se $n^2+n+1 = 1$ então $n^2+n = 0 \iff n(n+1) = 0$

$\iff n = 0 \vee n = -1$

$p = -1 \vee p = -2$ não são primos

Logo o único primo da forma $n^3 - 1$ é $p = 7$.

(c) Temos que $n^4 - 4 = (n^2+2)(n^2-2)$

Como $n > 1$ então $n^2 + 2 > 1$ e $n^2 - 2 > 1$

Como $n^4 - 4$ é o produto de dois naturais diferentes de 1 então é um número composto.

(Alínea extra)

(d) Se $p \geq 5$ é um número primo então p^2+2 é um número composto.
[Sugestão: mostrar que p é da forma $6k+1$ ou $6k+5$]

Começamos por mostrar que p é da forma $6k+1$ ou $6k+5$

Pelo Teorema do Algoritmo da Divisão dado $p \in \mathbb{N}$ existem

$q \in \mathbb{N}_0$ e $r \in \{0, 1, 2, 3, 4, 5\}$ tais que

$$p = 6q + r$$

Basta mostrar que $r \neq 0$, $r \neq 2$, $r \neq 3$ e $r \neq 4$

- se $r=0$, $\quad p = 6q \quad$ e $\quad 6 \mid p \quad 6 = 2 \times 3$

logo p não é primo

- se $r=2$, $\quad p = 6q+2 = 2(3q+1)$

$2 \mid p$ e $3q+1 \mid p$

logo p não é primo a não ser que $p=2$

— se $r=3$, $p = 6q+3 = 3(2q+1)$

$3 \mid p$ e $2q+1 \mid p$

logo p não é primo a não ser que $p=3$

— se $r=4$, $p = 6q+4 = 2(3q+2)$

$2 \mid p$ e $3q+2 \mid p$ logo não é primo

Podemos então concluir que se p é primo e $p \geq 5$ então o resto da divisão por 6 ou é 1 ou é 5.

Vamos agora mostrar que p^2+2, com $p \geq 5$, é um número composto.

Se $p = 6k+1$ então $p^2+2 = (6k+1)^2 + 2 =$

$= 36k^2 + 12k + 1 + 2 = 3(12k^2+4k+1)$ e temos que

$3 \mid p^2+2$ e $12k^2+4k+1 \mid p^2+2$ e $12k^2+4k+1 > 1$

logo p^2+2 é composto.

Se $p = 6k+5$ então $p^2+2 = (6k+5)^2+2 =$

$= 36k^2 + 60k + 25 + 2 = 3(12k^2+20k+9)$ e temos que

$3 \mid p^2+2$ e $12k^2+20k+9 \mid p^2+2$ e $12k^2+20k+9 > 1$

logo p^2+2 é composto.

31. Prove que $\sqrt{p}$ é irracional para todo o primo p.

Suponhamos, por redução ao absurdo, que $\sqrt{p}$ é racional.

Então $\sqrt{p} = \frac{a}{b}$ com $a, b \in \mathbb{N}$ e podemos admitir que a fração é irredutível, ou seja, m.d.c $(a,b) = 1$.

Temos $\sqrt{p} = \frac{a}{b} \Rightarrow p = \frac{a^2}{b^2}$ e temos $a^2 = p\,b^2$

Assim $p \mid a^2$. Como p é primo e $p \mid a^2$ então $p \mid a$

Logo $a = pc$ para algum $c \in \mathbb{N}$.

De $a^2 = p\,b^2$ resulta que $p^2c^2 = p\,b^2$ logo $b^2 = p\,c^2$

Portanto $p \mid b^2$ e como p é primo então $p \mid b$.

Como $p \mid a$ e $p \mid b$ então m.d.c $(a,b) \neq 1$, o que é absurdo. Logo $\sqrt{p}$ é necessariamente irracional.