Teoria dos Números: Máximo divisor comum e algoritmo Euclidiano (1.4)

Prof. Rafael Alves Bonfim de Queiroz
rafael.queiroz@ufop.edu.br

Conteúdo programático

- 1.4) Máximo divisor comum e algoritmo Euclidiano

Máximo Divisor Comum (MDC)

- Suponha que a e b são inteiros, não ambos 0. Um inteiro d é chamado de divisor comum de a e b se d dividir tanto a quanto b, isto é, se $d|a$ e $d|b$.
- Observe que 1 é um divisor comum positivo de a e b, e que qualquer divisor de a e b não pode ser maior que $|a|$ ou $|b|$
- Assim existe um máximo divisor comum de a e b; isso é denotado por $mdc(a, b)$ e é chamado de máximo divisor comum de a e b
- Exemplo: Os divisores comuns de 12 e 18 são ±1, ±2, ±3, ±6. Assim mdc(12, 18) $=$ 6. Da mesma forma: mdc(12, -18) $=$ 6, mdc(12, -16) $=$ 4, mdc(29, 15) $=$ 1, mdc(14, 49) $=$ 7

- Para qualquer inteiro a, temos $mdc(1, a) = 1$.
- Para qualquer primo p, temos $mdc(p, a) = p$ ou $mdc(p, a) = 1$ conforme p divide ou não a.
- Suponha que a seja positivo. Então $a|b$ se e somente se $mdc(a, b) = a$.

MDC

- **Teorema**: Seja d o menor inteiro positivo da forma $ax + by$. Então $d = mdc(a, b)$.
- **Corolário**: Suponha $d = mdc(a, b)$. Então existem inteiros x e y tais que $d = ax + by$.
- **Teorema**: Um inteiro positivo $d = mdc(a, b)$ se e somente se d tiver as duas propriedades a seguir:
  - (1) d divide a e b.
  - (2) Se c divide a e b, então $c|d$.

As propriedades simples do máximo divisor comum são:

- (a) $mdc(a, b) = mdc(b, a)$.
- (b) Se $x > 0$, então $mdc(ax, bx) = xmdc(a, b)$.
- (c) Se $d = mdc(a, b)$, então $mdc(a/d, b/d) = 1$.
- (d) Para qualquer inteiro x, $mdc(a, b) = mdc(a, b + ax)$

Algoritmo para encontrar o mdc(a, b)

- Sejam a e b inteiros e $d = mdc(a, b)$.
- Sempre se pode encontrar d listando todos os divisores de a e em seguida, todos os divisores de b e, em seguida, escolhendo o maior divisor comum.
- A complexidade de tal algoritmo é $f(n) = O(\sqrt{n})$ onde $n = |a| + |b|$.
- Além disso, não fornecemos nenhum método para encontrar os inteiros x e y tais que $d = ax + by$

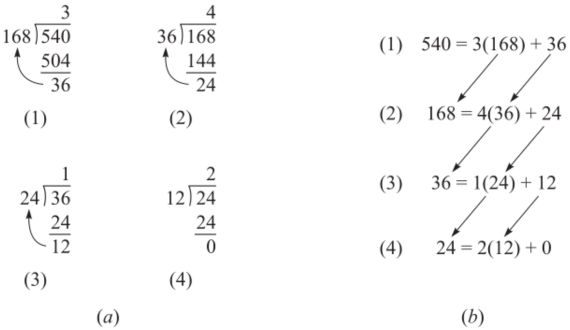
Algoritmo Euclidiano

- Um algoritmo muito eficiente, chamado algoritmo euclidiano, com complexidade $f(n) = O(logn)$, para encontrar $d = mdc(a, b)$ aplicando o algoritmo de divisão a a e b e depois aplicando-o repetidamente a cada novo quociente e resto até obter um resto diferente de zero. O último diferente de zero resto é $d = mdc(a, b)$.
- Então damos um algoritmo de "desvendar" que inverte os passos do algoritmo euclidiano para encontrar inteiros x e y tais que $d = xa + yb$.

Exemplo: a $=$ 540 and b $=$ 168 - algoritmo Euclideano

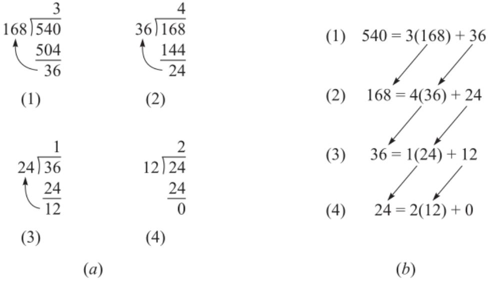
- Calcular o $d = \text{mdc}(549{,}168)$
- Determinar os inteiros x e y tais que $d = xa + yb$

Exemplo: a = 540 and b = 168 - algoritmo Euclideano



- mdc(540, 168) = mdc(168, 36) = mdc(36, 24) = mdc(24, 12) = 12

$d = \mathrm{mdc}(540, 168) = 12 = x\ (540) + y\ (168)$



- (1) 36 = 540 - 3(168),
- (2) 24 = 168 - 4(36),
- (3) 12 = 36 - 1(24)
- (i) 12 = 36 - 1[168 - 4(36)] = 36 - 1(168) + 4(36) = 5(36) - 1(168)
- (ii) 12 = 5[540 - 3(168)] - 1(168) = 5(540) - 15(168) - 1(168) = 5(540) - 16(168)
- x = 5 and y = -16.

Mínimo Múltiplo Comum (MMC)

- Suponha que a e b sejam inteiros diferentes de zero.
- Observe que $|ab|$ é a múltiplo comum positivo de a e b.
- Assim há um menor múltiplo comum positivo de a e b; é denotado por $mmc(a, b)$ e é chamado de mínimo múltiplo comum de a e b.

Exemplos - MMC

- (a) mmc(2, 3) $=$ 6; mmc(4, 6) $=$ 12; mmc(9, 10) $=$ 90.
- (b) Para qualquer inteiro positivo a, temos $mmc(1, a) = a$.
- (c) Para qualquer primo p e qualquer inteiro positivo a, $mmc(p, a) = a$ ou $mmc(p, a) = ap$ conforme p divide ou não a.
- (d) Suponha que a e b sejam inteiros positivos. Então $a|b$ se e somente se $mmc(a, b) = b$.

Teorema MMC + MDC

- **Teorema**: Suponha que a e b sejam inteiros diferentes de zero. Então

$$mmc(a, b) = \frac{|ab|}{mdc(a, b)}$$