3 The fundamentals: Algorithms, the integers, and matrices

3.4 The integers and division

This section introduces the basics of number theory (number theory is the part of mathematics involving integers and their properties).

1. \(a|b\) if \(b = ak\), for some integer \(k\) (note that \(a|b\) is not the fraction \(b/a\), but it rather shows that \(a\) is a factor of \(b\))

2. \(a \not| b\) if \(a\) is not a factor of \(b\). Examples: \(3|18\) but \(3 \not| 20\).

3. properties of \(a|b\): (you should be able to prove them) Let \(a, b, c \in \mathbb{Z}\). Then:
   - \((a|b) \land a|c) \rightarrow a|(b + c)
   - \(a|b \rightarrow a|(bc), \forall c \in \mathbb{Z}
   - \((a|b) \land b|c) \rightarrow a|c
   - \((a|b) \land a|c) \rightarrow a|(mb + nc), \forall m, n \in \mathbb{Z}

4. Division algorithm: \(\forall a, d \in \mathbb{Z}\), with \(d > 0 \Rightarrow \exists! q, r \ (0 \leq r < d)\) such that \(a = dq + r\)

5. in the equation above, \(a\) is called the dividend, \(d\) is the divisor, \(q\) is the quotient, and \(r\) is the remainder. Note that \(a\) and \(d\) are the given integers, and \(q\) and \(r\) are the unique two integers that make the division algorithm work for the given \(a\) and \(d\). Example: Given 14 and 5, find the quotient and the remainder: \(14 = 5 \cdot 2 + 4\), so \(q = 2\) and \(r = 4\) and they are unique for the pair of numbers 14 and 5. We then have that \(2 = 14 \text{ div 5} \) and \(4 = 14 \text{ mod 5}\)

6. modular arithmetics: \(a \equiv b(\text{mod } m) \iff m|(a - b)\)

7. modular arithmetics: \(a \not\equiv b(\text{mod } m) \iff m \nmid (a - b)\)
   Example: \(14 \equiv 4(\text{mod 5})\) since \(5|(14 - 4)\), however \(14 \not\equiv 2(\text{mod 5})\) since \(5 \nmid (14 - 2)\)
8. **Theorem:** $a \equiv b \pmod{m}$ if and only if $a \mod m = b \mod m$ (note that if there is only one mod $m$ in the equation, then we use the symbol $\equiv$, but if we use the mod $m$ on each side of our equation, then we use the symbol $=$. Both equations mean that both $a$ and $b$ have the same remainder when they are divided by $m$)

9. **modular arithmetic operations:**

   - **addition:** $\left((a \mod m) + (b \mod m)\right) \mod m = (a + b) \mod m$
   
   - **subtraction:** $\left((a \mod m) - (b \mod m)\right) \mod m = (a - b) \mod m$
   
   - **multiplication:** $\left((a \mod m) \cdot (b \mod m)\right) \mod m = (a \cdot b) \mod m$

10. **not true for division** (division is not defined for modular arithmetic. We define cancelation, and one can only cancel if the number that one cancels by is relatively prime to $m$—see Section 3.7)

11. if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

   - $a + c \equiv b + d \pmod{m}$
   
   - $a - c \equiv b - d \pmod{m}$
   
   - $a \cdot c \equiv b \cdot d \pmod{m}$
   
   - $a \alpha \equiv b \alpha \pmod{m}$, for $\alpha > 0, m \geq 2, \alpha \in \mathbb{Z}$
   
   - $a \alpha \equiv b \alpha \pmod{m \alpha}$, for $\alpha > 0, m \geq 2, \alpha \in \mathbb{Z}$

12. **Applications:** hash functions, pseudo random numbers, code generating in cryptography