4 Number Theory and Cryptography

4.1 Divisibility and Modular Arithmetic

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

1. For $a, b \in \mathbb{Z}, a \neq 0$ we say that a divides b, written as $a|b$, if $b = a\,k$, $\exists k \in \mathbb{Z}$ (note that $a|b$ is not the fraction a/b, 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 $a|b$: Let $a, b, c \in \mathbb{Z}, a \neq 0$. Then:

   - $(a|b \ \wedge \ a|c) \quad \rightarrow \quad a|(b+c)$

   - $a|b \quad \rightarrow \quad a|(bc), \quad \forall c \in \mathbb{Z}$

   - $(a|b \ \wedge \ b|c) \quad \rightarrow \quad a|c$

   - $(a|b \ \wedge \ a|c) \quad \rightarrow \quad a|(mb+nc), \quad \forall m, n \in \mathbb{Z}$, which generalizes all the bullets

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

   $$a = dq + r,$$

   where 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 $a = dq + r$ true for the given a and d.

   Example: Given 14 and 5, find the quotient q and the remainder r: $14 = 5 \cdot 2 + 4$, so $q = 2$ and $r = 4$, which are unique for the pair of numbers 14 and 5.

5. We define two functions on the set of integers:

   - $a \,\mathbf{mod}\, m$ gives the remainder of a divided by m
   - $a \,\mathbf{div}\, m$ gives the quotient of a divided by m

   Example: $14 \,\mathbf{mod}\, 12 = 2$, and $14 \,\mathbf{div}\ 12 = 1$, since $14 = 1 \cdot 12 + 2$
   $-14 \,\mathbf{mod}\, 12 = 10$, and $-14 \,\mathbf{div}\, 12 = -2$, since $-14 = -2 \cdot 12 + 10$
   (note: $-14 = -1 \cdot 12 - 2$ does not work since r must satisfy $a \leq r \leq d$)

6. **Theorem**: $a \equiv b \pmod{m}$ iff $a \,\mathbf{mod}\, m = b \,\mathbf{mod}\, m$

7. $a \equiv b \pmod{m} \quad \iff \quad a \,\mathbf{mod}\, m = b \,\mathbf{mod}\, m \quad \iff \quad m|(a-b) \iff \quad a = km+b$

8. Example: $14 \equiv 4(\text{mod} 5)$ since $14 \,\mathbf{mod}\, 5 = 4 \,\mathbf{mod}\, 5$ or since $5|(14-4)$.

9. Additionally, $14 \not\equiv 2 \pmod{5}$ since $14 \,\mathbf{mod}\, 5 \neq 2 \,\mathbf{mod}\, 5$ or since $5 \not| (14-2)$

10. <u>Modular arithmetic operations</u> (they help evaluate numbers modulo m):

    - addition: $(a+b) \,\mathbf{mod}\, m = \Big(a \,\mathbf{mod}\, m + b \,\mathbf{mod}\, m\Big) \,\mathbf{mod}\, m$

    - subtraction: $(a-b) \,\mathbf{mod}\, m = \Big(a \,\mathbf{mod}\, m - b \,\mathbf{mod}\, m\Big) \,\mathbf{mod}\, m$

    - multiplication: $(a \cdot b) \,\mathbf{mod}\, m = \Big(a \,\mathbf{mod}\, m \cdot b \,\mathbf{mod}\, m\Big) \,\mathbf{mod}\, m$

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 $\alpha > 0, m \geq 2, \alpha \in \mathbb{Z}$

12. This is not true for division (division is not defined for modular arithmetic. We will use cancellation with numbers that are relatively prime to m)

13. For each integer $m \geq 2$, we define $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. And then we have the following arithmetic modulo m:
    - $a +_m b = a + b \,\mathbf{mod}\, m$
    - $a \cdot_m b = a \cdot b \,\mathbf{mod}\, m$

    For example $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, and then we have the following:
    $3 +_5 4 = 2$ since $3 +_5 4 = 7 \,\mathbf{mod}\, 5 = 2$ and
    $3 \cdot_5 3 = 4$ since $3 \cdot_5 3 = 9 \,\mathbf{mod}\, 5 = 4$.