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

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 \(2 = 14 \div 5\) and \(4 = 14 \mod 5\)

6. \(a \mod m\) gives the remainder of \(a\) divided by \(m\) (book uses the notation \(a \text{ mod } m\)).
   - Example: \(14 \mod 12 = 2\), saying that \(14 : 00\) is the same as \(2 : 00\)pm.

7. **modular arithmetics:** \(a \equiv b \text{(mod } m)\) \iff \(m|(a - b)\)
   - Example: \(14 \equiv 4 \text{(mod } 5)\) since \(5|(14 - 4)\).
8. modular arithmetics: \( a \not\equiv b \pmod{m} \iff m \not| (a - b) \)
Example: \( 14 \not\equiv 2 \pmod{5} \) since \( 5 \not| (14 - 2) \)

9. **Theorem:** \( a \equiv b \pmod{m} \) iff \( a \mod m = b \mod m \)
(note that if there is only one \( \mod m \) in the equation, then we use the symbol \( \equiv \),
but if we use the \( \mod \) 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 \( m \))

10. \( a \equiv b \pmod{m} \iff a \mod m = b \mod m \iff m| (a - b) \iff a = km + b \)

11. **modular arithmetic operations** (they help evaluate numbers modulo \( m \)):

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

12. 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 \( m \))

13. if \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then
   - \( a + c = b + d \pmod{m} \)
   - \( a - c = b - d \pmod{m} \)
   - \( a \cdot c = b \cdot d \pmod{m} \)
   - \( a \alpha \equiv b \alpha \pmod{m} \), for \( \alpha > 0, m \geq 2, \alpha \in \mathbb{Z} \)
   - \( a \alpha \equiv b \alpha \pmod{ma} \), for \( \alpha > 0, m \geq 2, \alpha \in \mathbb{Z} \)

14. 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 \( m \):
   - \( a +_m c = b + d \mod m \) ( also \( a -_m c = b - d \mod m \) )
   - \( a \cdot_m c = b \cdot d \mod m \)

15. Applications: hash functions, pseudo random numbers, code generating in cryp-
tology