3 The fundamentals: Algorithms, the integers, and matrices

3.4 The integers and division

1. \(a \mid b\) if \(b = a \cdot k\), for some integer \(k\) (note that \(a \mid b\) is not the fraction \(b/a\))

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

3. Modular arithmetics: \(a \equiv b\) (mod \(m\)) \(\iff\) \(m\mid(a - b)\)

4. Addition: \((a \mod m) + (b \mod m)\) (mod \(m\)) = \((a + b)\) (mod \(m\))

5. Subtraction: \((a \mod m) - (b \mod m)\) (mod \(m\)) = \((a - b)\) (mod \(m\))

6. Multiplication: \((a \mod m) \cdot (b \mod m)\) (mod \(m\)) = \((a \cdot b)\) (mod \(m\))

7. Multiplication by a constant: for example if \(x \equiv 3\) (mod \(m\)), then \(2x\) (mod \(m\)) \(\equiv\) \(6\) (mod \(m\))

8. Not true for division (true for cancellation if the number you are canceling by is relatively prime to \(m\)—see Section 3.7)

9. If \(a \equiv b\) (mod \(m\)) and \(c \equiv d\) (mod \(m\)), then
   \(a + c \equiv b + d\) (mod \(m\))
   \(a \cdot c \equiv b \cdot d\) (mod \(m\))
   \(a^\alpha \equiv b^\alpha\) (mod \(ma\)), for \(\alpha > 0, m \geq 2\)

10. \(a \equiv b\) (mod \(m\)) iff \(a\) (mod \(m\)) = \(b\) (mod \(m\))

3.5 Primes and greatest common divisors

1. A prime \(p\) is an integer whose only positive factors are 1 and \(p\)

2. If \(n\) is a composite integer, then \(n\) has prime divisors less than or equal to \(\sqrt{n}\)
3. Fundamental Theorem of Arithmetic: every positive integer can be uniquely written as product of primes (where the factors are in a nondecreasing order) i.e.: \( n = p_1 \cdot p_2 \cdot \ldots \cdot p_\alpha \), where \( p_i \leq p_{i+1} \) for \( 1 \leq i \leq \alpha - 1 \)

4. there are infinitely many primes (know the construction in the proof)

5. gcd of two numbers = greatest common divisor

6. lcm of two numbers = least common multiple

7. relatively prime (or also called coprimes)

8. pairwise relatively prime

9. \( ab = \gcd (a, b) \cdot \lcm(a, b) \)

3.6 Integers and algorithms

1. Base b expansions of \( n \): \( n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0 \)

2. Binary (base 2) expansions are used by computers to represent and do arithmetic with integers

3. Hexadecimal expansion also used by computer. It uses 0, 1, \ldots, 9, A, B, C, D, E, F

4. Bytes are bit strings of length 8

5. Base conversion (expressing \( n \) base \( b \)):
   - \( n = bq_0 + a_0 (0 \leq a_0 < b) \) and \( a_0 \) is the rightmost digit of \( n \) base \( b \)
   - \( q_0 = bq_1 + a_1 (0 \leq a_1 < b) \) and \( a_1 \) is the 2nd digit from the right of \( n \) base \( b \)
   - repeat to find \( a_2, a_3, \ldots \) until \( q_i = 0 \) for some \( i \)

6. converting from binary to hexadecimal: each hexadecimal digit corresponds to a block of 4 digits

7. binary addition: let \( a = (a_{n-1}a_{n-2} \ldots a_1a_0) \) and \( b = (b_{n-1}b_{n-2} \ldots b_1b_0) \). Then
   - \( a + b \) is found using the usual method of adding two numbers modulo 2
   - \( ab = a(\sum_{i=0}^{n-1} 2^i) = \sum_{i=0}^{n-1} a2^i \), where multiplying \( a \) by \( 2^i \) is adding \( i \) zeros at the end of \( a \) (i.e. \( 101 \times 2^3 = 101000 \))

8. computing div and mod: for \( a = 72 \) and \( d = 10 \), we have that \( 2 = 72 \mod 10 \) and \( 7 = 72 \div 10 \)
3.7 Applications of number theory

1. writing the gcd\((a, b) = d\) as a linear combination \(d = \alpha a + \beta b\), for some \(\alpha, \beta \in \mathbb{Z}\)
2. if \(a\) and \(b\) are relatively prime, then \(1 = \alpha a + \beta b\), for some \(\alpha, \beta \in \mathbb{Z}\)
3. if \(p\) is a prime such that \(p|(a_1 \cdot a_2 \cdots \cdot a_n)\), then \(p|a_i\) for some \(i\) \((1 \leq i \leq n)\)
4. simplifications: if \(a, b, c, m \in \mathbb{Z}\) \((m > 0)\) and \(\gcd(c, m) = 1\), then
   \[ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}\]
5. however, if \(\gcd(c, m) \neq 1\), the above result doesn’t hold (see Example 2 page 234)
6. linear congruence: \(ax \equiv b \pmod{m}\) (where \(a, b, m \in \mathbb{Z}\) \((m > 0)\) and \(x\) is the variable)
7. \(\bar{a}\) (or \(a^{-1}\)) is the inverse of \(a\) modulo \(m\) if \(\bar{a}a \equiv 1 \pmod{m}\)
8. Chinese Remainder Thm (solving systems of linear congruences): for relatively prime numbers \(m_i\), the system
   \[
x = a_1 \mod m_1
   
x = a_2 \mod m_2
   
   \vdots
   
x = a_n \mod m_n
\]
   has unique solution modulo \(m = \prod_{i=1}^{n} m_i\), namely
   \[x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n,\]
   where \(M_i = \frac{m}{m_i}\), and \(y_i\) is the inverse of \(M_i\) modulo \(m_i\)
9. Fermat’s Little Thm: If \(p\) is a prime, and \(p \nmid a\), then \(a^{p-1} \equiv 1 \pmod{p}\)
   (or for any prime \(p\), \(a^p \equiv a \pmod{p}\))
10. the converse of Fermat’s Little Thm doesn’t hold since there are some composite primes in the form \(a^{p-1} \equiv 1 \pmod{p}\), for example 341