1. Reading: K. Rosen *Discrete Mathematics and Its Applications*, 2.3

2. The main message of this lecture:

Similar to addition, multiplication, and subtraction of integers, division by a nonzero integer is also always defined, one only has to take a remainder into account. Such related notions as primes, prime factors, modular arithmetic, etc., play pivotal role in mathematics and have striking applications in Computer Science.

Within this lecture the variables range over the set of integers \( \mathbb{Z} = \{ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \} \). Every \( a \) can be divided by any nonzero \( d \) with a remainder. For example,

- If \( a = 12 \) and \( d = 4 \) the quotient is \( q = 12 / 4 = 3 \) and the remainder \( r = 0 \),
- If \( a = 13 \) and \( d = 4 \) then \( q = 13 / 4 = 3 \), \( r = a - dq = 13 - 3 \cdot 4 = 13 - 12 = 1 \),
- If \( a = 14 \) and \( d = 4 \) then \( q = 14 / 4 = 3 \), \( r = a - dq = 14 - 3 \cdot 4 = 14 - 12 = 2 \),
- If \( a = 15 \) and \( d = 4 \) then \( q = 15 / 4 = 3 \), \( r = a - dq = 15 - 3 \cdot 4 = 15 - 12 = 3 \),
- If \( a = 16 \) and \( d = 4 \) then \( q = 16 / 4 = 4 \), \( r = a - dq = 16 - 4 \cdot 4 = 16 - 16 = 0 \),
- If \( a = 0 \) and \( d = 4 \) then \( q = 0 / 4 = 0 \), \( r = a - dq = 0 - 0 \cdot 4 = 0 - 0 = 0 \),
- If \( a = -1 \) and \( d = 4 \) then \( q = -1 / 4 = -1 \), \( r = a - dq = -1 + (1) \cdot 4 = 1 + 4 = 5 \),
- If \( a = -2 \) and \( d = 4 \) then \( q = -2 / 4 = -1 \), \( r = a - dq = -2 + (1) \cdot 4 = 2 \),
- If \( a = -3 \) and \( d = 4 \) then \( q = -3 / 4 = -1 \), \( r = a - dq = -3 + (1) \cdot 4 = 1 \),
- If \( a = -4 \) and \( d = 4 \) then \( q = -4 / 4 = -1 \), \( r = a - dq = -4 + (1) \cdot 4 = 0 \).

**Theorem 8.1.** For any \( a \) (dividend) and \( d \neq 0 \) (divisor) there exist unique \( q \) (quotient) and \( r \) (remainder) such that \( a = dq + r \) and \( 0 \leq r < d \).

**Proof.** Existence of \( q \) and \( r \). Given \( a \) find the largest \( q \) such that \( d \cdot q \leq a \) and put \( d = a - dq \). Both requirements \( a = dq + r \) and \( 0 \leq r < d \) are then met. Note that this instruction covers all the possible cases: \( a > 0 \), \( a < 0 \) and \( a = 0 \).

Uniqueness. Suppose \( a = dq_1 + r_1 = dq_2 + r_2 \) and both \( 0 \leq r_1, r_2 < d \). Subtract both representation of \( a \) from each other: \( 0 = (a - a) = (dq_1 + r_1) - (dq_2 + r_2) = d(q_1 - q_2) + (r_1 - r_2) \).

Therefore, \( d(q_2 - q_1) = r_1 - r_2 \) and \( |d(q_2 - q_1)| = |r_1 - r_2| \). If \( q_2 \neq q_1 \) then \( |q_2 - q_1| \geq 1 \) and \( |d(q_2 - q_1)| \geq d \). On the other hand, \( |r_1 - r_2| < d \), which makes the assumption that \( q_2 \neq q_1 \) impossible. Therefore, \( q_2 = q_1 \) and thus \( r_1 = r_2 \).

**Definition 8.2.** \( a \neq 0 \) divides \( b \) (notation \( a \mid b \)) if \( \exists c (ac = b) \). We say that \( a \) is a factor of \( b \), and \( b \) is a multiple of \( a \). Examples: \( 4 \mid 12, 1 \mid 1, 101 \mid 101, 1 \mid 0 \).

Some easy properties of \( \mid \) :

\[ a \mid b \land a \mid c \implies a \mid (b + c) \quad \text{(Proof: } ax = b \land ay = c \implies ax + ay = b + c \implies a(x + y) = b + c) \]

\[ a \mid b \implies a \mid bc \quad \text{(Proof: } ax = b \implies axc = bc) \]

\[ a \mid b \land b \mid c \implies a \mid c \quad \text{(Proof: } ax = b \land by = c \implies axy = by = c) \]

**Definition 8.3.** \( p \) is a prime, if \( p > 1 \) and \( p \) has no factors other then 1 and itself. Examples: \( 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots \) are primes. \( n \) is a composite integer, if \( n > 1 \) and \( n \) is not a prime. It is clear that every composite integer is a product (not necessarily unique) of two strictly less integers: \( 30 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6 \).
**Theorem 8.4.** (The Fundamental Theorem of Arithmetic.)

Any \( n > 1 \) is a unique product of primes.

**Proof (sketch).** Finding all prime factors: given \( n \) keep dividing until all the factors are prime. For example, \( 60 = 2 \cdot 30 = 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5 \). Proving uniqueness needs some more work, we will do it later.

Examples of prime factorizations: \( 2 = 2, 3 = 3, 4 = 2 \cdot 2, 5 = 5, 6 = 2 \cdot 3, 7 = 7, 8 = 2 \cdot 2 \cdot 2, 9 = 3 \cdot 3, 10 = 2 \cdot 5, 30 = 2 \cdot 3 \cdot 5, 100 = 2 \cdot 2 \cdot 5 \cdot 5, \) etc.

**Theorem 8.5.** (An easy primality test) A composite \( n \) has a prime divisor less or equal to \( \sqrt{n} \). Therefore, if none of the primes \( p \leq \sqrt{n} \) divides \( n \), then \( n \) is itself a prime.

**Proof.** Given a composite \( n \) find \( a \leq b < n \) such that \( n = ab \). Obviously, \( a \leq \sqrt{n} \), since otherwise both \( a, b > \sqrt{n} \) and thus \( a \cdot b > \sqrt{n} \sqrt{n} = n \). By 8.4, \( a \) has a prime divisor \( p \leq a \leq \sqrt{n} \), which is a divisor of \( n \).

Examples: \( \sqrt{143} = 11.95826 \ldots < 12 \), therefore either 143 has a prime divisor \( \leq 11 \) or it is a prime. In fact 11|143, and thus 143 is a composite number. To check that 103 is a prime it suffices to verify that none of the primes \( \sqrt{103} = 10.148891 \) (i.e. \( 2, 3, 5, 7 \)) divides 103.

Comment: factoring and primality testing for large \( n \)'s remain very hard and time consuming problems. We will discuss this later when talking about RSA cryptosystem.

**Definition 8.6.** The greatest common divisor of \( a, b \) (not both zero) is the largest \( d \) which is a divisor of both \( a \) and \( b \) (notation \( d = gcd(a, b) \)). We say that \( a \) and \( b \) are relatively prime if \( gcd(a, b) = 1 \). Examples: \( gcd(36, 48) = 12 \) \( gcd(15, 28) = 1 \) – relatively prime.

Knowing prime factorizations of \( a, b \) helps finding \( gcd(a, b) \). Example: \( gcd(2^3 \cdot 3, 2 \cdot 3^2 \cdot 7) = 2^{\min(3, 1)} \cdot 3^{\min(1, 2)} \cdot 7^{\min(0, 1)} = 2 \cdot 3 \cdot 7 = 42 \).

**Definition 8.7.** The least common multiple of \( a, b \) \( > 0 \) is the smallest \( l \) which is a multiple of both \( a \) and \( b \) (notation: \( l = lcm(a, b) \)). Examples: \( lcm(36, 48) = 144 \), \( lcm(20, 21) = 20 \cdot 21 = 420 \), \( lcm(2^3 \cdot 3 \cdot 7^2, 2 \cdot 3^2 \cdot 5 \cdot 7) = 2^{\max(3, 1)} \cdot 3^{\max(1, 2)} \cdot 5^{\max(0, 1)} \cdot 7^{\max(2, 1)} = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^2 = 17640 \).

Exercise: show that \( a \cdot b = gcd(a, b) \cdot lcm(a, b) \) (i.e. \( 6 \cdot 8 = 48 = 2 \cdot 24 = gcd(6, 8) \cdot lcm(6, 8) \)).

**Definition 8.8.** Let \( m > 0 \). By \( a \mod m \) we understand the remainder when \( a \) is divided by \( m \). Integers \( a \) and \( b \) are congruent modulo \( m \) if \( a \mod m = b \mod m \) (or, equivalently, if \( m \) divides \( a - b \), or, equivalently, if \( a = b + km \) for some \( k \)). Another notation for \( a \) is congruent to \( b \) modulo \( m \) is \( a \equiv b \mod m \).

Examples: \( 0 \equiv 5 \equiv 10 \equiv 15 \equiv -5 \equiv 10 \equiv -15 \mod 5 \)
\( 1 \equiv 6 \equiv 11 \equiv 16 \equiv -4 \equiv -9 \equiv -14 \mod 5 \)
\( 2 \equiv 7 \equiv 12 \equiv 17 \equiv -3 \equiv -8 \equiv -13 \mod 5 \), etc.

**Theorem 8.9.** (Addition and multiplication of congruent numbers) If \( a \equiv b \mod m \) and \( c \equiv d \mod m \), then \( (a + c) \equiv (b + d) \mod m \) and \( (a \cdot c) \equiv (b \cdot d) \mod m \).

Examples: \( 7 \equiv 2 \mod 5 \), \( 8 \equiv 3 \mod 5 \) \( \Rightarrow (7 + 8) = 15 \equiv 0 \equiv (2 + 3) \mod 5 \), \( 7 \equiv 2 \mod 5 \), \( (-1) \equiv 4 \mod 5 \) \( \Rightarrow (7 \cdot (-1)) = -7 \equiv 3 \equiv 8 \equiv (2 \cdot 4) \mod 5 \).

Applications: hashing functions, pseudorandom numbers, encryption – see textbook and slides.

**Homework assignments.** (due Friday 02/16. Mind a new numeration of problems).

8A:Rosen2.3-8ef; 8B:Rosen2.3-10ef; 8C:Rosen2.3-28ab; 8D:Rosen2.3-46c.