1. a) \(d = \text{g.c.d.}(a, b)\), Lectures 1, p. 4
   b) Euclid’s lemma, Lectures 1, p. 5
   c) Fundamental Theorem of Arithmetic, Lectures 1, p. 4, Lectures 2, pp. 5-6

Examples
   a) \(1 = \text{g.c.d.}(3, 5)\)
   b) \(2|8\), \(2|8\)
   c) \(24 = 3 \times 8 = 3 \times 2^3\) and this factorization is unique

2. a) \(A, B\) finite sets with same number of elements \(|A| = \#\text{elts of } A\)
   \(f: A \rightarrow B\)
   \(1-1 \Leftrightarrow f\ \text{onto}\)
   \(f\ \text{1-1} \Rightarrow |A| = |f(A)|\) and \(f(A) \subseteq B\) with \(|B| = |A| = |f(A)|\)
   \(\Rightarrow |f(A)| = |B|\) otherwise there would be an element of \(B\) not in \(f(A)\) and then \(|B| > |f(A)| = |A|\) contradicting \(|A| = |B|\). So \(f(A) = B\) and \(f\) is onto
   \(\Leftrightarrow f\ \text{onto} \Leftrightarrow |f(A)| = |B|\)
   If \(f\) were not 1-1 we could leave out a subset \(S\) of elements of \(A\) and make \(f\) 1-1 on \(A-S\).
   Thus \(f\) is 1-1.

b) \(f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p, f(x) = ax\) where \(p \nmid a\).
   \(ax = ay \pmod{p} \Rightarrow p|ax-ay = a(x-y)\)
   \(p\) prime \(\Rightarrow p|a(x-y) \Rightarrow p|a\)
   \(\Rightarrow x = y \pmod{p}\)
   So \(f\) is 1-1 and thus onto

c) Since the function in part b) is onto
   \(\exists x\ \text{st. } ax = 1 \pmod{p}\) if \(a \not\equiv 0 \pmod{p}\)
   Thus \(\mathbb{Z}_p\) is a field.
   It is commutative with identity for multiplication \(([1] \pmod{p})\) and every non-zero element has an inverse for multiplication.
3) a) See Lectures 4, p. 1, for ring. Example: \( \mathbb{Z}_5 \) or \( \mathbb{Z}_6 \)  
   See Lectures 5, p. 1, for integral domain Example \( \mathbb{Z} \) integers  
   See Lectures 5', p. 2, for field Example \( \mathbb{Q} \) rationals

b) \( \mathbb{Z}_6 \) a ring not an integral domain.  
   \( \mathbb{Z} \) an integral domain, not a field  
   \( \mathbb{Z}_p, p \text{ prime} \) is a field as is \( \mathbb{R} = \text{real } \# s \)

4) a) \( S \subseteq R, S \neq \emptyset \) is a subring if it is a ring under the same operations as \( R \)  
   \( \mathbb{Z} \) is a subring of \( \mathbb{R} \)

b) Lectures 4, p. 2

c) "

5) a) Lectures 4, p. 2

b) Homework 2, #1

b) Lectures 5, pp. 11-12

c) (See Lectures 5, p. 13)  
   \[ x, y \in \mathbb{Z}_3 \implies (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 \equiv x^3 + y^3 \pmod{3} \]

   \[ x, y \in \mathbb{Z}_4 \implies \text{the analogous result is false} \]
   \[ (x+y)^4 \equiv x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \]

   \[ 0 = 2^4 = (1+1)^4 = 1 + 2 + 1 = 4 \pmod{4} \]
   \[ 1^4 + 1^4 = 1 + 1 = 2 \neq 0 \pmod{4} \]
7a) Lectures 4, p. 4
b) \( U(\mathbb{Z}_{10}) = \{-1, 1\} \)

8a) \((1+i)^2 = 1 + 2i + i^2 = 2i = -1\)
\((1+i)^3 = -(1+i) = -i - 1 = -i - 2\)
\((1+i)^4 = (1+i)(1-i) = 1 - i^2 = 2 = -1\)
\((1+i)^5 = -(1+i) = -i - 2\)
\((1+i)^6 = (-1)(1+i)^2 = i\)
\((1+i)^7 = -(1)(1+i)^3 = -1 + i\)
\((1+i)^8 = (-1)(1+i)^4 = 1\)

So \(\langle 1+i \rangle = \mathbb{Z}_8[i] \cong \mathbb{Z}_2 \times \mathbb{Z}_4\) = cyclic group of order 8 under multiplication.

b) No since \(\mathbb{Z}_8[i]\) has order 8, the non-zero elements have order 8.

c) char \(\mathbb{Z}_8[i] = 3\) = additive order of 1

9a) \(\mathbb{Z}_{12}\)

b) \(M_2(\mathbb{Z}_2)\)

10a) Lectures 6, p. 15
b) Lectures 6, p. 21

c) Homework 4 #1

11a) \(\mathbb{Z}\) is not a field \(\frac{1}{2} \notin \mathbb{Z}\)

b) \(\mathbb{F}\) \(3 \cdot 3 \equiv 0\) (mod 9) but \(3 \equiv 0\) (mod 9)

c) \(T\) is a ring, commutative, with 1, no zero divisors, \(f(x) \cdot g(x) = 0\) polynomial

\(\Rightarrow\) either \(f(x)\) or \(g(x) = 0\).

d) \(T\) \(10n = 2(5n) \in <2>\)
11) (continued)

e) \( F \langle x^2+1 \rangle \) is not maximal ideal
\[ \Rightarrow \mathbb{Z}_2[x]/\langle x^2+1 \rangle \neq \text{field} \]
\[ x^2+1 = (x+1)^2 \Rightarrow \]
\[ \langle x^2+1 \rangle \nsubseteq \langle x+1 \rangle \]

f) \( F \mathbb{Z}_2 \cup 3\mathbb{Z} \) is not closed under +
\[ a + 3 \notin \mathbb{Z}_2 \cup 3\mathbb{Z} \]

\( g) T \quad x, y \in A \cap B \Rightarrow x - y \in A \cap B \]
\( x, y \in A \cap B \]

h) \( T \quad \text{so } 0 \in A = \text{ideal of } F \]
\[ a + b \in A \Rightarrow \exists b', b \in A, b - 1 \in A \]
\[ \Rightarrow \forall x \in F, x, 1 \in A \Rightarrow F_{CA} = A = F \]

12) a) \( \overline{a + b} = \overline{a} + \overline{b} \)
\[ \overline{a \cdot b} = \overline{ab} \]
well defined as \( \overline{a} = \overline{a'}, \overline{b} = \overline{b'} \Rightarrow \)
\[ \overline{a' + b'} = \overline{a + b} \]

since \( a' + b' = (a + b) = (a' - a) + (b' - b) \in I \)
\[ \overline{a' \cdot b'} = \overline{a \cdot b} \]

since \( a' \cdot b' - ab = a' \cdot b' - a' \cdot b + ab - ab \)
\[ = a' \cdot (b' - b) + (a' - a) \cdot b \in I \]

Here we use \( I \) is an additive subgp
s.t. \( RIC = I \)

b) Lectures 6, pp. 22-23