Review.

Non-exhaustive list of topics. (See Course notes on Moodle and lecture notes)

Integers: CRT and Bezout's theorem, congruences, Euler's totient function.

Groups: Cyclic group, dihedral group, symmetric group

Subgroups, normal subgroups, orbit-stabilizer theorem, group homomorphisms, conjugacy classes, class equation, classification of finite abelian groups

Rings: Integral domais, ideals, principal ideals, principal ideal domain, zero divisors, units, fields, Euclidean domain, ring homomorphisms, quotient ring, characteristic of a ring, polynomial rings,

Chinese remainder theorem, congruences in polynomial rings, gcd of polynomials, irreducible elements, associates, finite fields, construction and classification of finite fields.

1. (a) Let $\mathbb{Q}$ be the field of rational numbers. Find a greatest common divisor $d(X)$ of the polynomials

$$f(X) = \frac{1}{2}X^3 - X^2 - X - \frac{3}{2} \qquad \text{and} \qquad g(X) = X^3 - 3X^2 + X - 3$$

in the ring $\mathbb{Q}[X]$. (Provide the details of your computation.)

(b) Find $r(X), s(X) \in \mathbb{Q}[X]$ such that $f(X)r(X) + g(X)s(X) = d(X)$.

(c) If $d(X)$ is not monic, find the unique monic greatest common divisor $t(X)$ of $f(X)$ and $g(X)$, and two polynomials $p(X), q(X) \in \mathbb{Q}[X]$ such that $f(X)p(X) + g(X)q(X) = t(X)$.

(a)

$$\overbrace{X^3 - 3X^2 + X - 3}^{g(x)} \;\Big|\; \tfrac{1}{2}X^3 - X^2 - X - \tfrac{3}{2}$$
$$X^3 - 2X^2 - 2X - 3 \qquad 2$$
$$-X^2 + 3X$$

$$\overbrace{\tfrac{1}{2}X^3 - X^2 - X - \tfrac{3}{2}}^{f(x)} \;\Big|\; -X^2 + 3X$$
$$\tfrac{1}{2}X^3 - \tfrac{3}{2}X^2 \qquad -\tfrac{1}{2}X - \tfrac{1}{2}$$
$$\tfrac{1}{2}X^2 - X - \tfrac{3}{2}$$
$$\tfrac{1}{2}X^2 - \tfrac{3}{2}X$$
$$\tfrac{1}{2}X - \tfrac{3}{2} = \gcd(f(x), g(x)) = d(x)$$

$$-X^2 + 3X \;\Big|\; \tfrac{1}{2}X - \tfrac{3}{2}$$
$$-X^2 + 3X \qquad -2X$$
$$0$$

(b) $$\frac{1}{2}x - \frac{3}{2} = f(x) - (-x^2 + 3x)\left(-\frac{1}{2}x - \frac{1}{2}\right) = f(x) - \left(-\frac{1}{2}x - \frac{1}{2}\right)\left(g(x) - 2f(x)\right) =$$

$$= \underbrace{\left(\frac{1}{2}x + \frac{1}{2}\right)}_{s(x)} g(x) + \underbrace{(-x)}_{r(x).} f(x)$$

(c) monic $\gcd(f(x), g(x)) = 2 \cdot d(x) = x-3 = t(x)$.

$$x-3 = \underbrace{(x+1)}_{q(x)} g(x) \underbrace{-2x}_{p(x)} f(x)$$

2. Let S_4 be the symmetric group of permutations of 4 elements. Let $A_4 \subset S_4$ be the alternating subgroup, the subgroup of all even permutations in S_4 (even permutations are products of an even number of transpositions, not necessarily disjoint).

   (a) List all elements in A_4.

   (b) Let G be a group of order 4. Show that G is abelian.

   (c) Find an abelian subgroup K of order 4 in A_4 and show that it is normal in A_4.
   Hint: Let $\rho, \pi \in S_n$ be two permutations. The disjoint cycle decomposition of $\pi\rho\pi^{-1}$ is obtained from that of ρ by replacing each integer i in the disjoint cycle decomposition of ρ by the integer $\pi(i)$.

   (d) Is the subgroup K found in (c) normal in S_4?

   (e) Show that there is no subgroup of order 6 in A_4.
   Hint: What can be the order of an element in a group of order 6?

(a) $(ij)(kl)$ are even ; k-cycle is a product of $(k-1)$ transpositions

$A_4 = \{1, (12)(34), (13)(24), (14)(23), (123), (132), (134), (143), (234), (243), (124), (142)\}$

(b) $|G|=4 \Rightarrow G$ is abelian. (1) G has an elt of order 4 $\Rightarrow G \simeq C_4 = \{1, t, t^2, t^3\}$ abelian

(2) G does not have an elt of order 4 $\Rightarrow$ all nontrivial elts have order 2.

$\Rightarrow 1, s : s^2 = 1 \Rightarrow t ; t^2 = 1, \; st$: order 2 : $(st)^2 = stst = 1 \Rightarrow sts = t \Rightarrow st = ts$

$\Rightarrow \{1, s, t, ts = st\} \simeq C_2 \times C_2$ abelian

(c) $K = \{1, \underset{t}{(12)(34)}, \underset{s}{(13)(24)}, \underset{ts}{(14)(23)}\}$ By the hint, $\pi \rho \pi^{-1} \in K \; \forall \rho \in K \; \forall \pi \in A_4$.

$(12)(34)(13)(24) = (14)(23)$.

(d) Is $\pi\rho\pi^{-1} \in K$ $\forall \rho \in K$, $\forall \pi \in S_4$? Yes since the result of a conjugation in a symmetric group gives an elt of the same cycle type

$\Rightarrow$ here a product of two disjoint transpositions

K contains all such elements $\Rightarrow K \lhd S_4$.

(e) Let $H < A_4$, $|H| = 6$. $\Rightarrow \exists\, t \in H : t^3 = 1$ and $\exists\, s \in H : s^2 = 1$

$\Rightarrow$ at least one 3-cycle and at least one $(ij)(kl)$.

By direct computation $\Rightarrow$ they generate the whole A_4.

Ex: $(12)(34)\,(123)(12)(34) = (214)$, etc.

3. Let φ denote the Euler totient function.

(a) Compute $\varphi(16)$ and $\varphi(128)$.

(b) Describe all units (invertible elements) in the rings $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/128\mathbb{Z}$.

(c) Let p be a prime and $n \geq 1$. Derive a formula for $\sum_{k=0}^{n} \varphi(p^k)$ and prove it by induction (recall that by definition $\varphi(1) = 1$). The answer should depend on p and on n.

(d) Find all positive integers m such that $\varphi(m)$ is odd.

(a) $\varphi(2^4) = 2^4 - 2^3 = 8$; $\varphi(2^7) = 2^7 - 2^6 = 64$.

(b) $\left(\mathbb{Z}/16\mathbb{Z}\right)^* =$ all odd numbers $0 < \; < 16$; $\left(\mathbb{Z}/128\mathbb{Z}\right)^* = \{n : 0 < n < 128, n \text{ odd}\}$

(c) $\sum_{k=0}^{n} \varphi(p^k) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^n) = \cancel{1} + (\cancel{p} - \cancel{1}) + (\cancel{p^2} - \cancel{p}) + \cancel{\ldots} \; (p^n - \cancel{p^{n-1}}) = p^n$.

$\varphi(p^k) = p^k - p^{k-1}$

Induction: Base : $\varphi(p^0) = 1 = p^0$. $n = 0$ works.

Induction step: $\underline{\sum_{k=0}^{n+1} \varphi(p^k)} = \underbrace{\sum_{k=0}^{n} \varphi(p^k)} + \varphi(p^{n+1}) = p^n + p^{n+1} - p^n = \underline{p^{n+1}}$

"p^n" by induction hypothesis

$\Rightarrow$ by induction $\sum_{k=0}^{n} \varphi(p^k) = p^n$.

(d) $\varphi(m) = \varphi(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) =$

prime factorization of m

$= p_1^{k_1-1}(p_1-1)p^{k_2-1}(p_2-1)\cdots p_r^{k_r-1}(p_r-1)$ is odd $\Rightarrow$ the only $p = p_1 = 2$

$\Rightarrow 2^{k_1-1}(2-1) \Rightarrow k_1 = 1 \Rightarrow \underline{\varphi(2) = 1 \text{ odd}}.$

$\underline{\varphi(1) \overset{def}{=} 1}. \Rightarrow \underline{m = 1 \text{ or } 2}.$

4. (a) How many different (non-isomorphic) abelian groups of order 32 are there? $32 = 2^5$

(b) Let p be a prime. How many different (non-isomorphic) abelian groups of order p^5 are there? List these groups without repetition. (You can use the notation C_m to denote the cyclic group of order m.)

(c) List all abelian groups of order p^5 that contain an element of order p^3. Justify your answer.

(d) Let $p_1, p_2, \ldots p_r$ be r distinct primes. How many different abelian groups of order $n = p_1 p_2 \ldots p_r$ are there? Justify your answer.

(b) $|G| = p^5$ abelian $\Rightarrow$ $G = C_{p_1^{k_1}} \times \times C_{p_\ell^{k_\ell}}$, where p_i are primes, not nec. distinct.

$\Rightarrow$ # of different abelian gps of order p^5 is equal to # of partitions of 5.

Partitions of 5: (5), $(4,1)$, $(3,2)$, $(3,1,1)$, $(2,2,1)$, $(2,1,1,1)$, $(1,1,1,1,1)$

$\Rightarrow$ 7 different groups:

C_{p^5}, $C_{p^4} \times C_p$, $C_{p^3} \times C_{p^2}$, $C_{p^3} \times C_p \times C_p$, $C_{p^2} \times C_{p^2} \times C_p$, $C_{p^2} \times C_p \times C_p \times C_p$

$C_p \times C_p \times C_p \times C_p \times C_p$

(a) is a particular case of (b) with $p=2$.

(c) Containing an elt of order p^3: C_{p^5}, $C_{p^4} \times C_p$, $C_{p^3} \times C_{p^2}$, $C_{p^3} \times C_p \times C_p$.

(d) $|G| = p_1 p_2 \dots p_r$, distinct primes.

$C_{p_1} \times C_{p_2} \times \dots \times C_{p_r}$ there is only one abelian group of order $p_1 p_2 \dots p_r$ up to isomorphism

5. Let $\mathbb{F}_2$ be the field of 2 elements. Let $I = \langle X^3 \rangle$ be the ideal in the ring $\mathbb{F}_2[X]$, generated by the polynomial X^3, and let

$$A = \mathbb{F}_2[X]/I.$$

(a) Show that the ring A is not a field (cite a theorem). How many elements does it have? List all elements in A as classes modulo I.

(b) Which of the elements in A are zero divisors?

(c) Find the inverse of the element $[X^2+1]_I$ and the inverse of the element $[X^2+X+1]_I$ in A.

(d) Show that A is not isomorphic to either of the rings $B = \mathbb{Z}/8\mathbb{Z}$, $C = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Hint:* compute the characteristic of each ring.

(e) Let $D = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Are the rings A and D isomorphic? *Hint:* consider the number of invertible elements in A and D.

(a) A is not a field : $\mathbb{F}_2[X]/\langle f(x) \rangle$ is a field $\Leftrightarrow$ $f(x)$ is irreducible.

$f(x) = X^3 = X \cdot X \cdot X$ is not irreducible $\Rightarrow$ A is not a field.

2^3 elements in A : $\{[0], [1]_I, [X], [X+1], [X^2], [X^2+X], [X^2+1], [X^2+X+1]\}$.

(b) $[X]\cdot[X^2] = [0]$ Zero divisors in A are multiples of $[X]$:

$\{[0], [X], [X^2], [X^2+X]\}$

(c) $[X^2+1][X^2+1] = [X^4 + \underbrace{2}_{\equiv 0} X^2 + 1] = [1] \bmod I$ $\Rightarrow$ $[X^2+1]^{-1} = [X^2+1]$

$$[X^2+X+1][X+1] = [X^3+\underset{0}{\underset{\shortparallel}{2}}X^2+\underset{0}{\underset{\shortparallel}{2}}X+1] = [1] \bmod I \Rightarrow [X^2+X+1]^{-1} = [X+1].$$

(d) $B = \mathbb{Z}/8\mathbb{Z}$, $C = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$$\tau(A) = \tau\left(\mathbb{F}_2[X]/I\right) = 2 \;;\; \tau(B) = 8 \;;\; \tau(C) = \operatorname{lcm}(4,2) = 4.$$

$$\tau(\mathbb{Z}/m\mathbb{Z}) = m$$

$\Rightarrow$ A is not isomorphic to B or C.

(e) $D = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\qquad \tau(D) = 2$

$$D = \{\underbrace{(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,1,0)(1,0,1),(0,1,1)}_{\text{zero divisors}},(1,1,1)\}$$

the only invertible elt.

But A has 4 invertible elts $\Rightarrow$ they are not isomorphic.

6. (a) Show that the system of congruences

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv -6 \pmod{22} \\ x \equiv 0 \pmod 7. \end{cases}$$

has infinitely many solutions in $\mathbb{Z}$.

(b) Find the smallest positive integer that solves the system in (a).

(a) $3, 22, 7$ are pairwise coprime $\Rightarrow$ The Chinese remainder thm
$\exists$ a solution x satisfying the congruences;
If x is a solution $\Rightarrow$ $\{x + 3\cdot 22\cdot 7k\}_{k\in\mathbb{Z}}$ is also a solution
set of all solutions.

$$\begin{cases} x \equiv 0 \pmod 7 \\ x \equiv 2 \pmod 3 \end{cases} \quad 7t = 3s+2 = x \Rightarrow \begin{cases} x \equiv 14 \pmod{21} \\ x \equiv -6 \pmod{22} \end{cases}$$

$$21p + 14 = 22q - 6$$
$$21p - 22q = -20$$

$\Rightarrow p=-2,\ q=-1 \Rightarrow x = -28 \pmod{\underset{462}{3\cdot 22\cdot 7}} \Rightarrow \{-28+462k\}_{k\in\mathbb{Z}}$

(b) the smallest positive solution is $= -28+462 = 434.$

7. Let S_6 denote the symmetric group of permutations of 6 elements.

   (a) Let $a = (12) \in S_6$, and $b = (234) \in S_6$. Write the element bab^{-1} in terms of disjoint cycles.

   (b) Write the elements b^2 and b^2ab^{-2} in terms of disjoint cycles.

   (c) Express every transposition of the form (ij) for $1 \le i < j \le 4$ as a product of elements a, b and their inverses. What can you conclude about the subgroup $H \subset S_6$ generated by a and b?

   (d) Find the orbit of 1 under the action of the group H. Find the stabilizer subgroup of 1 in H, $\mathrm{Stab}_H(1) \subset H$ and check explicitly that the orbit-stabilizer theorem holds for this action.

(a) $a = (12)$, $b = (234)$. $\Rightarrow$ $bab^{-1} = (234)(12)(243) = (13)$

$\pi(i_1 \dots i_k)\pi^{-1} = (\pi(i_1) \dots \pi(i_k))$.

(b) $b^2 = (234)(234) = (243)$ $\Rightarrow$ $b^2ab^{-2} = (243)(12)(234) = (14)$.

(c) Already have: $(12) = a$, $(13) = bab^{-1}$, $(14) = b^2ab^{-2}$

$(23) = (13)(12)(13) = bab^{-1}abab^{-1}$ $\qquad$ $(34) = (24)(23)(24)$

$(24) = (12)(14)(12) = ab^2ab^{-2}a$

$H \subset S_6$ generated by a, b $\Rightarrow$ $H = S_4$ because we can get all transpositions in S_4 permuting $\{1,2,3,4\}$.

(d) Orbit of 1 under the action of H: $O_1 = \{1, 2, 3, 4\}$.

$\mathrm{Stab}_H(1)$ = all permutations of $\{2,3,4\} \simeq S_3$

Orbit-stabilizer thm:

$$|\mathrm{Orb}_1| \cdot |\mathrm{Stab}_H(1)| = |H| = 4!$$

$$4 \cdot 3! = 4!$$

8. Let A be a commutative ring. Recall that an element $c \in A$ is irreducible if $c \neq 0$, c is not a unit, and if $c = ab$ for $a, b \in A$, then either a or b is a unit.

(a) Find all irreducible elements in the ring of integers $\mathbb{Z}$.

(b) Are there any irreducible elements in the ring $\mathbb{Z}/4\mathbb{Z}$? Find them or prove that they don't exist.

(c) Is there an irreducible polynomial of degree 10 in $\mathbb{Q}[X]$? If so, provide an example and an explanation.

(a) Irreducible elts in $\mathbb{Z}$ units: $\{\pm 1\}$

$k = a \cdot b \Rightarrow$ either a or b is a unit $\Rightarrow$ irreducibles $= \{\pm p\}_{p \text{ prime}}$

(b) $\mathbb{Z}/4\mathbb{Z}$

multiplication table

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

1 and 3 are units in $\mathbb{Z}/4\mathbb{Z}$

$3 \cdot 3 = 1 \bmod 4$

2 is the only candidate for an irreducible

$2 = a \cdot b = 2 \cdot \underbrace{1} = \underbrace{1} \cdot 2 = \underbrace{3} \cdot 2 = 2 \cdot \underbrace{3}$

units

$\Rightarrow$ 2 is irreducible by def.

$\Rightarrow \exists$ exactly one irreducible elt in $\mathbb{Z}/4\mathbb{Z}$.

(c) In $\mathbb{Q}[X]$ The Eisenstein criterion:

$f(X) = a_n X^n + \dots + a_1 X + a_0$ s.t. $a_i \in \mathbb{Z}$, no common divisor,

$\exists$ prime p: $p \mid a_i$, $i = 0 \dots n-1$

$p \nmid a_n$ $\Rightarrow$ $f(X)$ is irreducible in $\mathbb{Q}[X]$.

$p^2 \nmid a_0$

$f(X) = X^{10} + p$, p a prime is irreducible

$X^{10} + 3$ is irreducible in $\mathbb{Q}[X]$.

9. (True/False) The dihedral group $D_4 = \langle r, s \mid r^4 = 1, s^2 = 1, srs = r^{-1} \rangle$ is isomorphic to the direct product of cyclic groups $C_4 \times C_2$.

abelian

not abelian $sr \neq rs$

10. (True/False) The ring $\mathbb{F}_5[X]/\langle X^3 - X^2 + 2 \rangle$ is a field.

$X^3 - X^2 + 2$; $X = -2 \Rightarrow -8 - 4 + 2 = -10 \equiv 0$ mod 5

not irreducible

11. (True/False) The number $13^{33} - 13$ is divisible by 20.

Euler's thm: $\gcd(a,n) = 1 \Rightarrow (a^{\varphi(n)} - 1)$ div. by n ; here $a = 13$, $n = 20$, $\varphi(n) = 8$.

12. (True/False) Let p, q be two distinct primes. Then $\mathbb{Z}/(pq)\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ is a ring isomorphism.

$\Rightarrow$ $(13^8 - 1)$ divisible by 20

$(13^{33} - 13) = 13(13^{32} - 1) = 13(13^{16} - 1)(13^{16} + 1) =$

$13\underbrace{(13^8 - 1)}_{\text{div. by } 20}(13^8 + 1)(13^{16} + 1)$ is divisible by 20.

12. CRT for integers: $\gcd(m,n) = 1 \Rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/(mn)\mathbb{Z}$

This holds because $\gcd(p,q) = 1$.