MAT3250 EXERCISES 2025

1. Week of 20 Jan - Fundamentals of Counting and Permutations

Warm-Ups.

(1) How many lists of length 4 without repetition can be formed from a set of size 6? What if repetitions are allowed?
(2) How many binary strings of length 5 are there containing at most three 0's?
(3) Draw the Young diagrams[1] for all of the integer partitions of $n = 6$, and then count them.
(4) How many ways are there of partitioning a set of size 6 into 3 subsets?
(5) Write the following permutations on 7 elements in alternate forms (as words, bijective functions, and cycle notation):
   (a) The permutation of the word $\pi = 5673214$.
   (b) The permutation given by the map $\pi(i) = i+1$ for $i < 7$ and $\pi(7) = 1$.
   (c) The permutation given in cycle notation $(1, 2)(4, 7)(5, 3)$.
(6) How many permutations on 6 elements are there of cycle type $1^3 3^1$?

Problems.

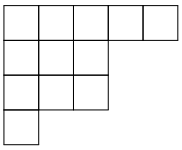
Problem 1.1. Show that the binomial coefficients satisfy the following chain of inequalities (this means that they are "unimodal"):

$$\binom{n}{0} < \binom{n}{1} < \binom{n}{2} < \cdots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \cdots > \binom{n}{n}.$$

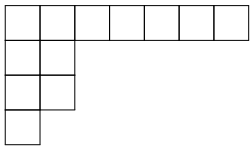
Problem 1.2. Let (n, m) be positive integers. A lattice path from $(0, 0)$ to (m, n) is a sequence of steps of length 1 either to the right or up (no steps down or left).

(1) How many distinct lattice paths are there from $(0, 0)$ to (m, n)? Hint: Write down the steps of a path in a word.
(2) Partition the set of lattice paths from $(0, 0)$ to (m, n) based on where they first meet the line $x = m$. Use this to derive a summation formula for the number of paths in Part (1).

[1] A **Young diagram** is a convenient graphical representation of an integer partition. It consists of rows of boxes, where the number of boxes in each row corresponds to the parts of the partition, arranged from the largest to the smallest. The following are Young diagrams for the partitions $5 + 3 + 3 + 1$ and $7 + 2 + 2 + 1$ of 12.



Partition $(5, 3, 3, 1)$



Partition $(7, 2, 2, 1)$

(3) Show that the number of lattice paths from $(0,0)$ to (n,m) which intersect the diagonal line from $(0,n)$ to $(n,0)$ at the point $(k,n-k)$ is equal to:

$$\binom{n}{k}\binom{m}{n-k}.$$

Use this to prove Vandermonde's identity:

$$\binom{m+n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{m}{n-k}.$$

Problem 1.3. The Bell number $\tilde{B}_n$ is the number of all set partitions of a set of size n (i.e., into any number of non-empty subsets). Write down the first four Bell numbers by listing all of the set partitions. Show that:

$$\tilde{B}_{n+1} = \sum_{k=0}^{n} \binom{n}{k} \tilde{B}_{n-k}.$$

Hint: Take the point of view of the set element $n+1$ and think about the size of the subset it ends up in.

Problem 1.4. Consider a permutation in word (one-line) notation given by $\pi = a_1 a_2 a_3 \dots a_n$. Let b_j denote the number of elements to the left of j in the word π which are strictly bigger than j. Prove that a permutation π is determined by its sequence $b_1, \dots, b_n$.

Hints: As an example, if $\pi = 1234\dots n$, then $b_j = 0$ for all j. Notice that $0 \leq b_j \leq n-j$ and that the number of sequences $b_1, \dots, b_n$ satisfying these inequalities is equal to $n!$.

Problem 1.5.
(1) Construct a map from the set of permutations of $\{1, \dots, n\}$ with k cycles to the set of set partitions of $\{1, \dots, n\}$ with k parts.
(2) Construct a map from the set of set partitions of $\{1, \dots, n\}$ with k parts to the set of integer partitions of n with k parts.
(3) Show that the maps from (1) and (2) are surjective and conclude that $P_{n,k} \leq S_{n,k} \leq \sigma_{n,k}$ for all n, k.
(4) Describe the composition of the two maps which sends the set of permutations of $\{1, \dots, n\}$ with k cycles to integer partitions of n with k parts. What does this have to do with the cycle type of a partition?

Problem 1.6. For the following formulas, give a proof using the rules of addition, multiplication and bijection.

(1) $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$
(2) $2^n = \sum_{k=0}^{n} \binom{n}{k}$
(3) $\binom{n}{k} = \binom{n}{n-k}$
(4) $\sum_{k=0}^{n} \binom{2n}{2k} = \sum_{k=0}^{n-1} \binom{2n}{2k+1}$
(5) $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$
(6) $s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$

2. Week of 27 Jan – Still fundamentals of counting and permutations

Problem 2.1. Let $n, h, l \geq 0$, and let $R_{n,h,l}$ be the number of partitions of n into at most l integers of size at most h. In other words, $R_{n,h,l}$ is the number of

partitions $n = a_1 + \cdots + a_r$ such that $r \leq l$ and such that $a_i \leq h$. For example, we get $R_{4,3,2} = 2$ by counting

$$2 + 2, 3 + 1,$$

In this count we have excluded partitions

$$4,$$

since $4 > h = 3$, and

$$2 + 1 + 1, 1 + 1 + 1 + 1,$$

since the number of summands should be at most 2.

(1) Prove that if $n > hl$, then
$$R_{n,h,l} = 0.$$
(2) What does the condition on the partitions counted by $R_{n,l,h}$ above say about the Young diagrams of the partition?
(3) Prove that for given h, l, we have
$$R_{n,h,l} = R_{n,l,h}$$
(4) Prove that for given h, l, we have
$$\sum_{n=0}^{hl} R_{n,h,l} = \binom{h+l}{h}.$$

Problem 2.2. Let $N = \{1, \ldots, n\}$.

(1) For each $i \in N$, count the number of 2-subsets $\{i, j\} \subseteq N$ such that $j \leq i$, and use this to prove
$$1 + 2 + \cdots + (n-1) = \binom{n}{2}.$$
(2) For $0 \leq k \leq n-1$, prove that
$$\binom{k}{k} + \binom{k+1}{k} + \cdots + \binom{n-1}{k} = \binom{n}{k+1}$$
(3) Find a suitable partition of $N \times N$ into subsets to prove that
$$1 + 3 + \cdots + (2n-1) = n^2.$$

Problem 2.3. Let a be the number of surjective functions from $\{1, \ldots, n\} \to \{1, 2\}$.

(1) Find a.
(2) Prove that $S_{n,2} = \frac{a}{2}$.

Problem 2.4. Let N be an n-set. For $k = 0, 1, 2, 3$, determine the number of permutations of N with exactly $n - k$ fix points.

Problem 2.5. Let π be a permutation of $\{1, 2, \ldots, n\}$, with $n \geq 2$. Define the permutation $F(\pi)$ by

$$F(\pi)(i) = \begin{cases} \pi(1) \text{ if } i = 2 \\ \pi(2) \text{ if } i = 1 \\ \pi(i) \text{ if } 3 \leq i \leq n. \end{cases}$$

(1) Prove that $F(\pi)$ is a permutation.
(2) Prove that $F(F(\pi)) = \pi$.

(3) Prove that if 1 and 2 are in different cycles of π, then the number of cycles of $F(\pi)$ is one less than that of π. E.g. if $\pi = (13)(24)$, we get $F(\pi) = (1423)$.
(4) Prove that if 1 and 2 are in the same cycle of π, then the number of cycles of $F(\pi)$ is one more than that of π.
(5) Prove that

$$\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} s_{n,2k} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} s_{n,2k+1}.$$

Problem 2.6. For $n \geq 0$, the n-th Catalan number C_n is defined by letting $C_0 = 1$, and letting C_n be the number of strings on two letters U, R, with

(1) R and U occurring n times, and
(2) for $0 \leq k \leq 2n$ the letter R appears at least as often as U among the first k letters.

So

- $C_1 = 1$, counting RU.
- $C_2 = 2$, counting $RRUU$ and $RURU$.
- $C_3 = 5$, counting $RRRUUU, RRURUU, RURURU, RURRUU, RRUURU$.

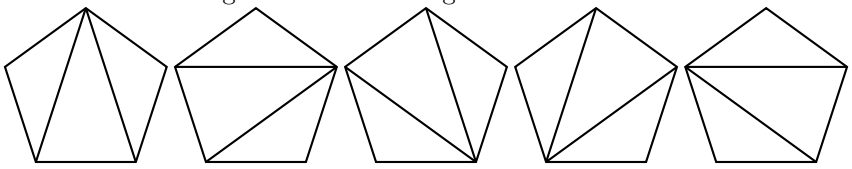
Problems:

(1) What do these strings correspond to in the lattice path picture of Problem 1.2?
(2) Prove that for $n \geq 1$,

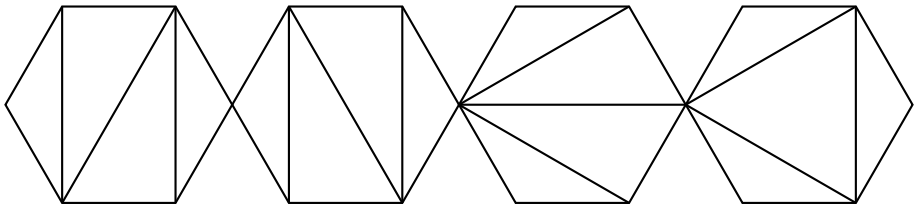
$$C_n = \sum_{i=0}^{n-1} C_i C_{n-1-i}.$$

Hint: For a valid string S, let $k(S) > 0$ be the smallest number such that the number of R equals the number of U among the first $k(S)$ letters. What is the number of valid strings with a fixed value of $k(S)$?

Problem 2.7. A **triangulation** of a polygon is way of dividing the polygon into triangles by adding straight lines between corners in such a way that no lines intersect. Let D_n be the number of triangulations of a polygon with $n \geq 3$ edges. The illustration below gives all 5 ways of dividing a pentagon, proving $D_5 = 5$, and shows some of the triangulations of a hexagon.

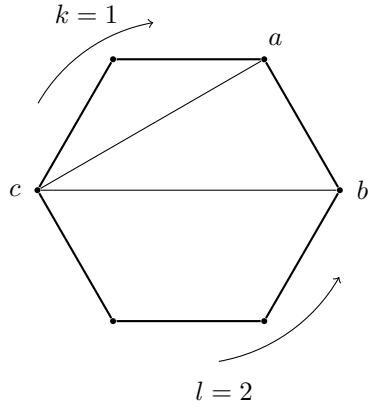


$n = 5$



$n = 6$

(1) Find D_3, D_4 and D_6.
(2) Let a and b be adjacent corners of the polygon, and let c be a third corner. Let k be the number of corners in between c and a, and let l be the number of corners in between c and b (see an example illustration below).



Prove that the number of triangulations of the n-gon which contain the triangle with corners a, b, c is $D_{k+2}D_{l+2}$.
(3) Prove that $D_n = 2D_{n-1} + \sum_{k=1}^{n-4} D_{k+2}D_{n-k-1}$.
(4) Prove that $D_n = C_{n-2}$, the Catalan number from Problem 2.6.

3. Week 3 – Recurrence relations and generating functions

Warm-ups.

(1) Expand out the rising factorial polynomials $x^{\bar{3}}$ and $x^{\bar{4}}$ and identify the coefficients as Stirling numbers of the first kind.
(2) Use the recurrence relation

$$\binom{x}{k} = \binom{x-1}{k} + \binom{x-1}{k-1}$$

for binomial coefficients to give a recurrence relation for falling factorials $x^{\underline{k}}$.
(3) Let (a_n), (b_n), and (c_n) be sequences indexed by $n \in \mathbb{N}$, and let $A(z)$, $B(z)$, and $C(z)$ be their respective generating functions. What are the generating functions for the following sequences in terms of $A(z)$, $B(z)$, $C(z)$, and some known generating functions? (Sums, differences, products, derivatives, and substitutions are all allowed!)
   (a) $(a_n + 10b_n - c_n)$
   (b) $(2^n a_n)$

(c) $(a_n + b_{n-1})$ (assume $b_{-1} = 0$)
(d) $(a_n + 1)$
(e) (na_n)

(4) Find the sequences given by the generating functions:
(a) $\frac{x}{1-2x}$
(b) $\frac{1}{(1-x)^2}$ *Hint: What is the derivative of* $\frac{1}{1-x}$*?*
(c) $\frac{1}{1-x-y}$ *Hint: The coefficient of* $x^k y^{n-k}$ *is one of the known counting coefficients.*

Problem 3.1. Prove the following recurrence formula for Stirling numbers of the second kind:

$$S_{n+1,k+1} = \sum_{i=k}^{n} \binom{n}{i} S_{i,k}.$$

Hint: Empathize with the element $n+1$ *and partition the set of all* $(k+1)$*-set partitions of* $\{1, \ldots, n+1\}$ *based on the size of the subset in the partition containing* $n+1$.

Problem 3.2. Let $P_{n,k}$ be the number of integer partitions of n with k parts.

(1) Give a combinatorial proof of the following relation for integer partitions:

$$P_{n,k} = \sum_{i=1}^{k} P_{n-k,i}.$$

What initial conditions need to be fixed in order to make this a recurrence relation giving all numbers $P_{n,k}$?

Hint: Remove the first column from the Young diagram of a partition of n *with* k *parts and count what remains.*

(2) Use the fact that every positive integer can be uniquely expressed as a sum of distinct powers of two to prove the following identity:

$$\frac{1}{1-x} = \prod_{k=0}^{\infty} (1 + x^{2^k}).$$

Problem 3.3. Let a_n be the number of ways a $2 \times n$ rectangle can be covered by 1×2 dominoes. Give a recurrence relation[2] for the sequence (a_n). What does this tell you about $A(z) = \sum_{k=0}^{\infty} a_n z^n$?

Let b_n be the number of ways a $3 \times n$ rectangle can be covered by 1×3 dominoes. Determine a recurrence relation for (b_n) and explain what this means for $B(z) = \sum_{n=0}^{\infty} b_n z^n$.

Problem 3.4. Let $A(z) = \sum_{n=0}^{\infty} a_n z^n$. Show that:

$$\frac{1}{2}(A(z) + A(-z)) = \sum_{n=0}^{\infty} a_{2n} z^{2n} \quad \text{and} \quad \frac{1}{2}(A(z) - A(-z)) = \sum_{n=0}^{\infty} a_{2n+1} z^{2n+1}.$$

4. Week of 10 Feb – Generating functions continued

Warm-ups.

[2]This was done in lectures.

(1) Let the sequence a_n be defined by the recurrence $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ and $a_0 = 1$, $a_1 = 1$, $a_2 = 1$. Find an expression of the generating function for a_n as a rational function (do not find the partial fraction expansion).
(2) Suppose the generating function of a sequence a_n is given by
$$A(z) = \frac{1}{(1-z)^2} + \frac{2}{1-2z}.$$
Give a formula for a_n as in Theorem 3.1. of Aigner.
(3) Find the closed form for the exponential generating function for the sequence given by the number of permutations of a set of size n.

Problem 4.1. Give the partial fraction decomposition of
$$\frac{1}{1-3z+2z^2}$$
and use this to compute the a_n given by
$$\frac{1}{1-3z+2z^2} = \sum_{n=0}^{\infty} a_n z^n.$$
What is the recurrence relation satisfied by the sequence (a_n)? For which n is this relation valid?

Problem 4.2. Determine the recurrence relations, generating functions, and an explicit formula for the following sequences in n:

(1) The number of words of length n on an alphabet of size 5.
(2) The number of binary words of length n with no consecutive ones.
(3) The number of binary words of length n with an even number of zeros. *Hint: Let e_n and o_n be the number of words of length n with even and odd number of zeros, respectively. Give two relations between their generating functions $E(z)$ and $O(z)$.*

Problem 4.3. (1) From Problem 2.3, we know that $S_{n,2} = 2^{n-1} - 1$ for $n \geq 1$. Use this to express the generating function
$$S_2(z) = \sum_{n=0}^{\infty} S_{n,2} z^n$$
as a rational function.
(2) Use the recurrence relation $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$ and the formula found for $S_2(z)$ to show
$$S_3(z) = \frac{z^3}{(1-z)(1-2z)(1-3z)}.$$
(3) Use a partial fraction decomposition to find a closed formula for $S_{n,3}$.

Problem 4.4. Let F_n be the n-th Fibonacci number. Prove that
$$F_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-1-k}{k}.$$
Hint: Expand the generating function $F(z)$ as a sum over terms $z(z+z^2)^k$.

Problem 4.5. Let C_n be the Catalan numbers from Problem 2.6, and let $C(z)$ be their generating function.

(1) Prove that $C(z) = zC(z)^2 + 1$.
(2) Solve the quadratic equation to determine $C(z)$.
(3) Show that
$$C_n = 2 \cdot (-4)^n \binom{\frac{1}{2}}{n+1}.$$

Problem 4.6. (1) Consider the product
$$F(x, y, z) = (x + y + z)^n = \sum_{i,j,k} a_{i,j,k} x^i y^j z^k$$
Explain why $a_{i,j,k}$ is the number of words on the alphabet $\{0, 1, 2\}$ of length n with i 0s, j 1s and k 2s.
(2) Let b_n be the number of words of length n on the alphabet $\{0, 1, 2\}$ with an even number of 0s and and even number of 1s. Show that
$$b_n = \frac{F(1, 1, 1) + F(-1, 1, 1) + F(1, -1, 1) + F(-1, -1, 1)}{4}.$$
(3) Write the generating function of b_n as a rational function, and give a recurrence relation for the b_n.

Problem 4.7. Give formulas for the generating function and the exponential generating function for the sequence $a_n = 2^n + 5^n$.

Problem 4.8. Recall the Bell numbers from Problem 1.3. Using the recursive formula proven there for $\tilde{B}_{n+1}$, show that the exponential generating function $\hat{B}(z)$ for $\tilde{B}_n$ satisfies:
$$\frac{d\hat{B}(z)}{dz} = e^z \hat{B}(z).$$
Verify that $\hat{B}(z) = e^{e^z - 1}$ satisfies the above differential equation and that the first 3 terms of the series expansion of e^{e^z-1} give $\frac{\tilde{B}_i}{i!}$ for $i = 0, 1, 2$.

5. Week of 17 Feb – Inclusion-exclusion and asymptotic analysis

5.1. **Inclusion-exclusion, warm-ups.**

(1) In a class of 50 students, 25 of the students study English, 20 study French, and 15 study German. Furthermore, 10 students study both English and French, 8 study both English and German, 5 study both French and German, and 3 study all three languages. How many students do not study any of the three languages?
(2) In how many ways can you arrange the digits $1, 2, 3, 4, 5$ such that 1 is not directly to the left of 2 and 2 is not directly to the left of 3? E.g. 13245 is allowed, 3**12**54 and 514**23** is not.
(3) What is the number of permutations on the set $\{1, \ldots, 4\}$ with k fixed points for $k = 0, 1, 2, 3, 4$?
(4) Use inclusion-exclusion to find how many words on the alphabet $0, 1, 2$ of length 5 contain each number at least once.
(5) How many of the numbers from 1 to 18 are divisible by either 2 or 3? How many of the numbers from 1 to 42 are not divisible by either 2, 3 or 7?

Problem 5.1. Let E be the set of maps $\phi\colon \{1, \ldots, n\} \to \{1, \ldots, r\}$. For an $m \in \{1, \ldots, r\}$, let $E_m \subseteq E$ be the set of maps ϕ which do not hit m, i.e. of maps ϕ such that $\phi(k) \neq m$ for $k = 1, \ldots, n$.

(1) Show that a map ϕ is surjective if and only if it does not lie in E_m for any $m \in \{1, \ldots, r\}$.
(2) Prove that
$$|E_m| = (r-1)^n.$$
(3) If $m_1, m_2, \ldots, m_k \in \{1, \ldots, r\}$ are distinct, prove that
$$|E_{m_1} \cap E_{m_2} \cap \cdots \cap E_{m_k}| = (r-k)^n$$
(4) Prove using inclusion-exclusion that the number of surjective maps from $\{1, \ldots, n\}$ to the set $\{1, \ldots, r\}$ is
$$\sum_{k=0}^{r} (-1)^k \binom{r}{k} (r-k)^n.$$
(5) Deduce that[3]
$$S_{n,r} = \sum_{k=0}^{r} \frac{(-1)^k (r-k)^n}{k!(r-k)!}.$$

Problem 5.2. Let $\phi(n)$ denote the number of integers k such that $1 \leq k \leq n$ and k is relatively prime to n. Prove using inclusion-exclusion that
$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right),$$
where $n = p_1^{l_1} p_2^{l_2} \cdots p_t^{l_t}$ for distinct primes $p_1, \ldots, p_t$ and $l_i > 0$ for all $1 \leq i \leq t$.

Asymptotic analysis, warm-ups.

(1) Order the following functions by the relation $\prec$:
$$e^n, n^n, \log(2n), n, 2, 2^n, \log(n), n^2, n!$$
(2) Let $f_1(n) = n$, $f_2(n) = n^2$, $g_1(n) = n^3 + n$ and $g_2(n) = -n^3$. Show that
$$f_1(n) \prec g_1(n), \quad f_2(n) \prec g_2(n),$$
but that we do not have
$$f_1(n) + f_2(n) \prec g_1(n) + g_2(n).$$
(3) Find an example of two polynomials $f(n)$ and $g(n)$ such that $f(n) < g(n)$ for all n but such that we do not have
$$f(n) \prec g(n).$$
(4) If an algorithm for an input of length n executes n steps where the ith step requires 2 operations, what is the Big-O running time of the algorithm?
(5) If an algorithm for an input of length n executes n steps where the ith step requires n^2 operations, what is the Big-O running time of the algorithm?

Problem 5.3. (1) Show that

(A)
$$n^n \leq (n!)^2 \quad \text{for } n \geq 1.$$

Hint: First use
$$k(n+1-k) = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n+1}{2} - k\right)^2$$

[3]Recall from [Aigner, p. 13] that the number of surjections $\{1, \ldots, n\} \to \{1, \ldots, r\}$ is $r! S_{n,r}$.

to show that for $1 \leq k \leq n$, we have

$$k(n+1-k) \geq n$$

(2) Use Stirling's formula for the asymptotics of $n!$ to show that

(B) $$n^n \prec (n!)^2.$$

Explain why (A) does not imply (B).

Problem 5.4. Use Stirling's formula to show

$$\binom{2n}{n} \sim \frac{4^n}{\sqrt{\pi n}}.$$

Get a sense of the accuracy of this asymptotic estimate by computing

$$\frac{\binom{2n}{n}}{4^n/\sqrt{\pi n}}$$

as a decimal number for $n = 1, 10, 100, 1000$, and by plotting the graph of this expression as a function of n.

Problem 5.5. Let $f, g \colon \mathbb{N} \to \mathbb{R}$ be positive functions. Prove that if $h(n) \in O(f(n))$ and $j(n) \in O(g(n))$, then

(1) $h(n)j(n) \in O(f(n)g(n))$
(2) $h(n) + j(n) \in O(f(n) + g(n))$.

6. Week of 24 Feb - Graph theory

Warm ups.

(1) How many edges are in the complete graph on n vertices?
(2) Is there a 3-regular graph on 5 vertices?
(3) Write down the adjacency and incidence matrices for the complete graph on 4 vertices.
(4) Write down the adjacency and incidence matrices for a labelling of the circuit graph on 4 vertices.
(5) Write down the adjacency and incidence matrices for the hypercube graph Q_2.

Problem 6.1. Show that a graph with $n \geq 2$ vertices has at least two vertices of the same degree.
Hint: The degree $d(v)$ of a vertex v must satisfy $0 \leq d(v) \leq n-1$. If there is a vertex of degree $n-1$, can there be a vertex of degree 0?

Problem 6.2. Which of the graphs K_n, P_n, C_n, Q_n are bipartite? The answer may depend on n.

Problem 6.3. A k-colouring of a graph $G = (V, E)$ is an assignment $f : V \to C$ where $|C| = k$ and such that $uv \in E$ implies $f(u) \neq f(v)$ (imagine that C is considered a set of colours, and we ask for ways to colour the vertices so that adjacent vertices have different colours).

(1) Prove that G has a 1-colouring if and only if $E = \varnothing$.
(2) Prove that G has a 2-colouring if and only if G is bipartite.
(3) Show that the number of k-colourings of
    (a) the complete graph K_n is $k^{\underline{n}}$.

(b) the path graph P_n is $k(k-1)^{n-1}$.
(c) the circuit graph C_n is

$$\sum_{i=0}^{n-1}(-1)^i\binom{n}{i}k^{n-i}+(-1)^n k$$

Hint: Use the inclusion-exclusion principle on the set of colour functions $f\colon V \to C$ and, for each edge uv, the subset E_{uv} of functions where $f(u) = f(v)$.

Problem 6.4. A **cut edge** k of a graph $G = (V, E)$ is an edge such that the graph $(V, E \setminus \{k\})$ has more components than G.

(1) Which of the graphs K_n, C_n and P_n, and the Peterson graph have a cut edge?
(2) If k is the edge between vertices u and v, show that k is a cut edge if and only if there is no path connecting u and v which does not contain k.
(3) Show that k is a cut edge if and only if it is not contained in any circuit.

Problem 6.5. Let G be a graph, and let v be a vertex. Let $G - v$ be the graph obtained by deleting v and all edges incident to v. We say v is a **cut vertex** if $G - v$ has more connected components than G.

Assume now that G is connected, that v is a cut vertex, and that $u \neq v$ is some other vertex.

(1) Prove that there exists a vertex w such that every path from u to w passes through v.
(2) Prove that for this w we have

$$d(u, w) = d(v, w) + d(v, u).$$

(3) Prove that $d(v, u) < D(G)$.
(4) Prove that G has at least two vertices which are not cut.

Problem 6.6. Assume a graph G has the property that every pair of edges are incident. Prove that then either

(1) There exists a vertex v so that every edge is incident to v, or
(2) There exist vertices u, v, w so that the edges of G are uv, vw, uw.

7. Week of 3 March - Trees

Warm-ups. The **Prüfer code** of a spanning tree of K_n is the sequence produced in the proof of Theorem 7.4.

(1) Draw the spanning tree of K_7 of the Prüfer code $(1, 1, 3, 2, 6)$.
(2) Find the Prüfer code of the path P_n labelled sequentially with $1, 2, \ldots, n$.
(3) How many edges must be removed from the hypercube graph to obtain a spanning tree?
(4) What trees do the breadth-first and depth-first searches return on K_n?
(5) What are the bases of the matroid of the circuit graph C_n?

Problem 7.1. Let $d_1, \ldots, d_n$ be natural numbers with $d_i \geq 1$ and

$$\sum_{i=1}^{n} d_i = 2n - 2.$$

Show that the number of spanning trees of K_n with vertex i having degree d_i is equal to

$$\frac{(n-2)!}{(d_1-1)!\cdots(d_n-1)!}.$$

Problem 7.2. Perform the depth-first search and breadth-first search algorithms on the hypercube graph Q_3 from starting vertex $(0,0,0)$ and describe the resulting trees.

Problem 7.3. Label the vertices of K_n with $\{1,\ldots,n\}$ and consider the weight function given by $w(ij) = i + j$. Construct a minimal spanning tree T for this weight function. Is this tree unique? What is $w(T)$?

Problem 7.4. In a matroid $M = (S, U)$, we say $B \subseteq S$ is a **circuit** if every strict subset $A \subsetneq B$ is independent.

(1) Show that if $G = (V, E)$ and $M = (E, W)$ is its associated matroid, then $B \subseteq E$ is a circuit if and only if B is the set of edges in some circuit of G.
(2) Let M be the matroid associated with a set of vectors in $\mathbb{R}^n$. Show that a set $B = \{v_1, \ldots, v_b\}$ is a circuit if and only if the following two conditions hold:
   - We can find $c_1, \ldots, c_b \in \mathbb{R}$, not all equal to 0, such that
   $$\sum_{i=1}^{b} c_i v_i = 0$$
   - For every choice of c_i such that the above equation holds, either all c_i are 0 or all c_i are non-0.

Problem 7.5. Choose real numbers $x_1, \ldots, x_n, y_1, \ldots, y_n$, and define the weight function w on K_n by $w(ij) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$.

We can think of K_n as drawn in the plane by putting vertex i at (x_i, y_i), in which case $w(ij)$ is the distance between vertices i and j in the plane. With this weight function, what does the spanning tree of K_n given by Dijkstra's algorithm look like?

8. Week of 10 March – Matchings, Eulerian and Hamiltonian circuits

Warm-ups.

(1) Can you remove 3 edges from $K_{4,4}$ so that there is no longer a matching with $|M| = 4$?
(2) For what values of n is K_n Eulerian?
(3) For what values of n and m is $K_{n,m}$ Eulerian?

Problem 8.1. Suppose a bipartite graph is k-regular for $k \geq 1$. Show that $|S| = |T|$ and that G contains a matching with $|M| = |S| = |T|$.

Problem 8.2. Use Algorithm 8.12 from the book to find a perfect matching of $K_{5,5}$ of minimal weight if the weight function on the edges is encoded by the matrix:

$$\begin{pmatrix} 8 & 7 & 5 & 11 & 4 \\ 9 & 7 & 6 & 11 & 3 \\ 12 & 9 & 4 & 8 & 2 \\ 1 & 2 & 3 & 5 & 6 \\ 11 & 4 & 2 & 8 & 2 \end{pmatrix}$$

9. Week of 17 March – More on matchings and the travelling salesman problem

Problem 9.1. (1) For what values of n is the hypercube graph Q_n Eulerian?
(2) For $n \geq 2$, describe a Hamiltonian circuit in the hypercube graph Q_n.

Problem 9.2. Give an example of a bipartite graph G and a matching M with $|M| < m(G)$ such that there is no matching M' with $M \subsetneq M'$.

Problem 9.3. Consider K_n with vertices $1, \ldots, n$ and the weight function where, for $i < j$, we have

$$w(ij) = \begin{cases} j - i \text{ if } j \leq i + n/2 \\ i + n - j \text{ if } j > i + n/2 \end{cases}.$$

Convince yourself that placing vertices $1, \ldots, n$ evenly on a circle of circumference n, then $w(ij)$ is the arc length distance between i and j. Find an optimal travelling salesman tour on K_n with this weight function.

Problem 9.4. Let $G = (V, E)$ be a connected graph. We use notation as in Theorem 8.27.

(1) Prove that if $C > 0$ is such that $w(k) \geq C$ for every $k \in E$, then
$$w(C_{MST}) \leq 2w(C_{opt}) - 2C.$$
(2) (A little harder:) Let
$$D = \max_{v \in V}(\min_{u \in N(v)} w(uv)),$$
and show that we always have
$$w(C_{MST}) \leq 2w(C_{opt}) - 2D.$$

10. Week of 24 March – Modular arithmetic and finite fields

Warm ups

(1) Determine the remainders when 3^{15} and 15^{83} are divided by 13.
(2) Is the polynomial $x^2 + x + 1$ irreducible over $\mathbb{Z}_2$? What about over $\mathbb{Z}_3$?
(3) If $f(x)$ is a degree 5 irreducible polynomial over $\mathbb{Z}_p$, how many elements are in the field $\mathbb{Z}_p[x]/\langle f(x)\rangle$?
(4) Show that the polynomial $x^2 + x + 2$ is irreducible over $\mathbb{Z}_3$. What is the product $[x][x^2 + 2]$ in $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$ (i.e. represent the product by a polynomial of degree at most one)? What is the multiplicative inverse of $x + 1$ in $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$?

Problems

Problem 10.1. Solve the set of equations

$$x + 2y = 4$$
$$4x + 3y = 4$$

in $\mathbb{Z}_7$ and $\mathbb{Z}_5$. It will be useful to first know the multiplicative inverses of 2 and 3 in both fields.

Problem 10.2. Let p be a prime number.

(1) Prove that for $1 \leq i \leq p-1$, we have

$$\binom{p}{i} \equiv 0 \pmod{p}.$$

(2) Use the binomial theorem to prove that for all $a, b \in \mathbb{Z}$, we have

$$(a+b)^p \equiv a^p + b^p \pmod{p}. \tag{1}$$

(3) One form of Fermat's little theorem says that for all $a \in \mathbb{Z}$, we have $a^p \equiv a \pmod{p}$. Give a proof of this statement using induction and equation (1).

Problem 10.3. Decompose $x^4 + 1 \in \mathbb{Z}_3[x]$ into irreducible factors.

Problem 10.4. Let $p > 2$ be a prime. We say an element a of a field F is a square if there is some $b \in F$ such that $b^2 = a$.

(1) Prove that for $a, b \in \mathbb{Z}_p$, we have $a^2 = b^2$ if and only if $a = b$ or $a = -b$. *Hint:* Factor $a^2 - b^2$.
(2) Prove that the set of squares in $\mathbb{Z}_p$ has $(p+1)/2$ elements.
(3) Prove that the polynomial $x^2 - a \in \mathbb{Z}_p$ is irreducible if and only if a is not a square in $\mathbb{Z}_p$.
(4) Prove that for $a \in \mathbb{Z}_p \setminus \{0\}$, we have $a = a^{-1}$ if and only if $a = 1$ or $a = p - 1$.
(5) Use the previous point to prove **Wilson's theorem**:

$$(p-1)! \equiv -1 \pmod{p}.$$

Hint: Show that all factors $2, 3, \ldots, p-2$ cancel out pairwise in the field $\mathbb{Z}_p$.
(6) Let $n \geq 1$. Prove that if $a, b \in GF(2^n)$ are such that $a^2 = b^2$, then $a = b$.
(7) Prove that every element of $GF(2^n)$ is a square.

11. Week of 31 March – Latin squares and designs

Warm ups

(1) How many mutually orthogonal Latin squares are there of order 5? Find a pair of them.
(2) Why is there at least one pair of orthogonal Latin squares of order 12?
(3) Write down the blocks $B_1, \ldots, B_7 \subset \{1, \ldots, 7\}$ for the 2-design from the Fano plane.
(4) How many lines and points are in a finite projective plane of order 3? How many points are on each line?

Problem 11.1. Let $L_1, L_2 \colon \{1, \ldots, n\} \times \{1, \ldots, n\} \to \{1, \ldots, n\}$ be orthogonal Latin squares, and let π be a permutation of $\{1, \ldots, n\}$.

(1) Let $L_1'(i,j) = L_1(\pi(i), j)$ and $L_2'(i,j) = L_2(\pi(i), j)$. Show that L_1' and L_2' are Latin squares and that they are orthogonal to one another.
(2) Let $L_2''(i,j) = \pi(L_2(i,j))$. Show that L_2'' is a Latin square and that L_1 and L_2'' are orthogonal to one another.

Problem 11.2. Construct a pair of orthogonal Latin squares of order 12.

Problem 11.3. Let $G = (V, E)$ be a graph. Show that E are the blocks of of a 1-design on V with $(v, k, \lambda) = (|V|, 2, \lambda)$ if and only if G is λ-regular.

Problem 11.4. Consider the set of squares on a chessboard $S = \{1, \dots, 8\} \times \{1, \dots, 8\}$. Say that squares are *related* if they lie in the same row or the same column. Is there a permutation $\pi \colon S \to S$ with the property that for every pair of related squares s_1, s_2, we have that $\pi(s_1)$ and $\pi(s_2)$ are not related? *Hint:* Write $\pi(i,j) = (\pi_1(i,j), \pi_2(i,j))$. What can you say about π_1 and π_2?

Problem 11.5. Let $D(v,k,\lambda)$ be a 2-design with b blocks $B_1, \dots, B_b$ on $\{1, \dots, v\}$ and $M = (m_{ij})$ the $v \times b$ matrix given by $m_{ij} = 1$ if $i \in B_j$ and $m_{ij} = 0$ if $i \notin B_j$. The goal of this problem is to show that if $k < v$, then $v \leq b$.

Let $A = MM^T$.

(1) Show that $A_{ij} = \lambda$ for $i \neq j$.
(2) Show that $A_{ii} = \lambda(v-1)/(k-1)$.
(3) Let $\vec{x}, \vec{y} \in \mathbb{R}^v$ be such that $\vec{y} = A\vec{x}$. Let $x = \sum_{i=1}^{v} x_i$. Prove that $y_i = \lambda(x + \frac{v-k}{k-1} x_i)$ for all i.
(4) Prove that if $k < v$, then $\vec{y} = 0 \Leftrightarrow \vec{x} = 0$.
(5) Assume $k < v$. Justify each of the (in-)equalities

$$v = rk(A) \leq rk(M) \leq b$$

to conclude that $v \leq b$.

12. Week of 7 April – Finite projective planes

Problem 12.1. Let

$$S = \{s_1, \dots, s_n\}$$

and let

$$\mathcal{B} = \{B_1, \dots, B_b\},$$

where the B_i are distinct subsets of S. The **incidence matrix** of $(S, \mathcal{B})$ is the $(n \times k)$-matrix M such that

$$M_{jk} = \begin{cases} 1 \text{ if } s_j \in B_k \\ 0 \text{ if } s_j \notin B_k \end{cases}$$

(1) Write down the 7×7 incidence matrix for the Fano plane.
(2) Let $(S, \mathcal{B})$ be a finite projective plane of order n, with incidence matrix M.
   (a) Show that dot product of two disctinct column vectors of M is 1, and that the dot product of two distinct row vectors of M is 1.
   (b) Show that
   $$M^T M = MM^T = nI + A,$$
   where I is the identity matrix and A is the matrix with entries only ones.

Problem 12.2. Let $(S, \mathcal{B})$ be a finite projective plane of order n, i.e. where S is the set of points and $\mathcal{B} \subseteq 2^S$ is the set of lines. We construct a new pair $(S', \mathcal{B}')$ as follows. Let $S' = \mathcal{B}$. For every $x \in S$, define $l_x \subseteq S'$ by

$$l_x = \{l \in \mathcal{B} \mid x \in l\},$$

and let $\mathcal{B}'$ be the set of all l_x. Prove that $(S', \mathcal{B}')$ is a projective plane.

Problem 12.3. Let $(S, \mathcal{B})$ be the projective plane of order 5 constructed from the field of three elements $\mathbb{Z}_5$. For a vector $(x, y, z) \in \mathbb{Z}_5^3 \setminus \{\vec{0}\}$, we let $[x : y : z] \in S$ be the subspace spanned by (x, y, z), that is

$$[x : y : z] = \mathbb{Z}_5(x, y, z) = \{(\alpha x, \alpha y, \alpha z) \mid \alpha \in \mathbb{Z}_5\}.$$

(1) How many points are contained in a line in this projective plane?
(2) Let l be the line containing points $[2 : 3 : 1]$ and $[1 : 2 : 3]$. List the points of l in the form $[x : y : z]$.
(3) Let $W = \{(x, y, z) \in \mathbb{Z}_5^3 \mid x+y+z = 0\} \subseteq \mathbb{Z}_5^3$, and let l' be the corresponding line in the projective plane. List the points of l' in the form $[x : y : z]$.
(4) Find $l \cap l'$.

Problem 12.4 (Inspired by the card game SET)**.** Let $n \geq 1$, and let $S = \mathbb{Z}_3^n$. Define a SET in S to be a $B = \{v_1, v_2, v_3\} \subseteq S$ with the v_i all distinct, such that $v_1 + v_2 + v_3 = 0$. Let $\mathcal{B}_n$ be the set of all SETs.

(1) Prove that $(S, \mathcal{B})$ forms a Steiner system, and determine $|\mathcal{B}|$.
(2) A **cap set** is a subset $T \subseteq S$, such that T contains no SET. Find the maximal possible size of a cap set when $n = 1$ and when $n = 2$.

Problem 12.5. Let $A = \{0, 1\}$.

(1) Determine which of the codes $C = \{0, 10, 11\}, D = \{1, 10, 11\}$ and $E = \{0, 01, 11\}$ are prefix codes.
(2) Let $X = \{\alpha, \beta, \gamma\}$, and suppose we encode messages written in the alphabet X using the above codes. Determine for which of the alphabets C, D and E a message can always be decoded uniquely.

Problem 12.6. Let $A = \{0, 1\}$, and let $C \subseteq A^*$ be a code. The **length sequence** of C is the lengths of the code words in C listed in ascending order, i.e. the code $\{0, 1, 100, 0100\}$ has length sequence $1, 1, 3, 4$.

(1) Prove that there is no prefix code C with length sequence

$$1, 2, 2, 2$$

(2) Prove that for $n \geq 3$, there is no prefix code C with length sequence

$$1, 2, \ldots, n-1, n, n, n.$$

13. Week of 21 April – Hamming distance and error correcting codes

13.1. **Warmups.**

(1) What is the Hamming distance between 0010 and 0100?
(2) What is the maximal Hamming distance between two code words in $\{0, 1\}^n$?
(3) For which t is the code $\{0000, 0011, 1100\}$ t-error detecting? For which t is it t-error correcting?
(4) What is the Hamming bound for the size of a code $C \subseteq \{0, 1, 2\}^4$ with $d(C) \geq 3$?

Problem 13.1. (1) Let $A = \{0, 1\}$, $n \geq 0$. Elements of A^n are identified with the vertices of the hypercube graph Q_n. Show that for words $w_1, w_2 \in A^n$, the Hamming distance $\Delta(w_1, w_2)$ equals the path-length distance $d(w_1, w_2)$ in Q_n.

(2) Let $A = \{0, 1, \ldots, k\}$, $n \geq 0$. Show that there is a graph G with vertex set A^n such that for $w_1, w_2 \in A^n$, we have $\Delta(w_1, w_2) = d_G(w_1, w_2)$. Draw this graph when $k = n = 2$.

Problem 13.2. Let $A = \{0, 1\}, n \geq 1$.

(1) Recall the **parity code** $C \subseteq A^n$, consisting of all words with an even number of 1s.
   (a) Prove that if $n = 1$, then C is 1-perfect.
   (b) Prove that if $n \geq 2$, then C is not t-perfect for any t.

(2) Let $n = 3k$, and recall the **double repetition code** $C \subseteq A^n$, consisting of all length k words repeated twice, that is

$$C = \{www \mid w \in A^k\}.$$

   (a) Prove that if $k = 1$, then C is 1-perfect.
   (b) Prove that if $k \geq 2$, then C is not t-perfect for any t.

14. Week of 28 April – Linear codes (and a little more on general codes)

Warm ups

(1) Consider the code

$$C = \{0000, 0101, 1010, 1111\} \subseteq GF(2)^4.$$

Explain why C is linear, and write down a generator matrix G and a parity check matrix H for it.

(2) Can a code $C \subseteq \{0, 1\}^n$ with $|C| = 9$ be linear, where $\{0, 1\} = \mathrm{GF}(2)$?

Problems

Problem 14.1.
(1) Show that if $C \subseteq GF(2)^8$ is a 2-error correcting linear code, then $|C| \leq 4$.
(2) Describe a linear code C with $|C| = 4$ which is 2-error correcting.
(3) (Harder, optional): Show that if $C \subseteq GF(2)^8$ is any 2-error correcting code (not necessarily linear), then $|C| \leq 4$.[4]

Problem 14.2. Let $A = GF(11)$, and consider the linear code $C \subseteq A^{11}$ determined by the parity checksum matrix

$$H = \begin{pmatrix} 3 & 7 & 6 & 1 & 8 & 9 & 4 & 5 & 2 & 1 & 0 \\ 5 & 4 & 3 & 2 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

A Norwegian personal identity number is a string of 11 digits $a_1 a_2 \ldots a_{11}$ which must satisfy $(a_1, \ldots, a_{11}) \in C$.

(1) Find the dimension of C, the cardinality $|C|$, and $d(C)$. Determine for what t the code C is t-error correcting and t-error detecting.
(2) Find two elements $\vec{a}, \vec{b} \in C$ such that $\Delta(\vec{a}, \vec{b}) = d(C)$.

[4] *Hint:* Given a 5 word code $C = \{w_1, \ldots w_5\} \subseteq GF(2)^8$ with $w_i = (w_{i1}, \ldots, w_{i8})$, let N be the number of triples (i_1, i_2, j) with $1 \leq i_1 < i_2 \leq 5$, $1 \leq j \leq 8$ such that $w_{i_1 j} = w_{i_2 j}$. Show that $32 \leq N \leq 10(8 - d(C))$.

Problem 14.3. Let $(S, \mathcal{B})$ be a t-design with $S = \{1, \dots, v\}$, $|B| = k$ for all $B \in \mathcal{B}$, and $\lambda = 1$. Define a code

$$C = \{c_B \mid B \in \mathcal{B}\} \subseteq \{0,1\}^v,$$

where c_B is the vector of zeros and ones with i-th coordinate equal to 1 if $i \in B$ and 0 otherwise.

(1) What is $|C|$?
(2) Show that for $B_1, B_2 \in \mathcal{B}$,
$$\Delta(c_{B_1}, c_{B_2}) = |B_1 \setminus B_2| + |B_2 \setminus B_1|.$$
(3) Show that $d(C) \geq 2(k - t + 1)$.

Problem 14.4. Prove that the Hamming distance satisfies the triangle inequality, namely

$$\Delta(a, c) \leq \Delta(a, b) + \Delta(b, c)$$

for all $a, b, c \in A^n$.

Problem 14.5. Consider the vectors $c = (0, 1, 1, 2)$ and $c' = (1, 0, 1, 1)$ in GF(3). The linear code $C \subseteq \mathrm{GF}(3)^4$ generated by c and c' consists of all linear combinations over GF(3) of c and c'.

(1) Write down the list of code words in C and verify that $d(C) = 3$.
(2) Show that C is 1-perfect.

15. Week of 5 May – More linear codes and cyclic codes

Warm ups

(1) Write down the polynomial for the code word $(1, 2, 0, 1, 2) \in \mathrm{GF}(3)$.
(2) Is the binary code $\{0000, 1100, 0110, 0011\}$ cyclic?
(3) What is the dimension of the cyclic code $C \subseteq GF(q)^n$ with generating polynomial $g(x) = x - 1$?
(4) Is there a cyclic code $C \subset \mathrm{GF}(3)^5$ with generating polynomial $g(x) = x+1$?

Problem 15.1. Consider the linear code $C \subseteq \mathrm{GF}(3)^5$ given by the check matrix

$$H = \begin{pmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

- Find a generating matrix of C.
- Show that C is 1-error correcting.
- Suppose the message 21012 was received over a channel with at most one error. Find the syndrome and correct the error.

Problem 15.2. Show that in a linear code C over $GF(2)$, either all codewords have even weight or half have even weight and half odd weight.

Problem 15.3. Let $C \subseteq \mathrm{GF}(2)^7$ be the cyclic code generated by $g(x) = x^3 + x^2 + 1$.

(1) Find a generating matrix and a parity check matrix of C.
(2) Is the word $c = (1, 1, 1, 0, 1, 0, 1)$ in C?
(3) Find the syndrome of c with respect to the parity check matrix.

Problem 15.4. Show that the dual code of a cyclic code is cyclic.

Problem 15.5. Let C_1 and C_2 be two cyclic codes over GF(q) with generator polynomials $g_1(x)$ and $g_2(x)$, respectively. Show that $C_1 \subseteq C_2$ if and only if $g_2(x)$ divides $g_1(x)$.

Problem 15.6. Let $f(x), g(x)$ be polynomials over $GF(q)$ of degree less than n, and let $\vec{f}, \vec{g} \in GF(q)^n$ be the associated code words. Prove that if

$$f(x^{-1})g(x) = \sum_{i=-n+1}^{n-1} c_l x^l \qquad c_l \in GF(q)$$

then

$$\vec{f} \cdot \vec{g} = c_0.$$

Problem 15.7. Let $K = GF(q)$, and say that a vector $\vec{a} \in K^m$ is **normalised** if $\vec{a} \neq \vec{0}$ and the first non-zero component of $\vec{a}$ is 1, i.e. we have

$$\vec{a} = (\overbrace{0, \ldots, 0}^{i-1}, 1, a_{i+1}, \ldots, a_m).$$

(1) Prove that if $\vec{a} \neq \vec{b}$ and both $\vec{a}$ and $\vec{b}$ are normalised, then $\vec{a}$ and $\vec{b}$ are linearly independent.
(2) Find the number of normalised vectors in K^m.
(3) Let H be a matrix whose columns are all the normalised vectors of K^m. Explain why the code C with parity check matrix H is a Hamming code.

16. Week of 12 May – Cryptography

Warm Ups

(1) Show that 2 is a primitive root mod 5.
(2) Compute $2^{103} \mod 5$ using Fermat's little theorem.
(3) Compute $3^7 \mod 11$ and $3^8 \mod 11$ using the successive square method.[5]

Problem 16.1. Solve the discrete logarithm problem

$$3 \equiv 7^x \mod 11$$

for $x \in \{0, 1, \ldots, 10\}$.

Problem 16.2. Let a be a primitive root mod p, let $b = a^k \pmod p$, and let $d = \gcd k, p-1$.

(1) With $m \geq 0$, show that $a^m \equiv 1 \pmod p$ if and only if $p-1$ divides m.
(2) Show that $b^{\frac{p-1}{d}} \equiv 1 \pmod p$.
(3) Show that b is a primitive root mod p if and only if $d = 1$.
(4) Find the number of primitive roots mod 13.

Problem 16.3. In a Diffie-Hellman key exchange Alice and Bob share the public key $p = 11$ and $a = 2$.

(1) Alice sends $A = 10$ to Bob and Bob sends $B = 6$ to Alice. What is their shared secret key K?

[5]The "successive square method" computes $a^b \pmod n$ by (1) writing b as a sum of powers of 2, $b = \sum_{i=1}^k 2^{e_i}$, then (2) computing each $a^{2^{e_i}}$ by squaring a e_i times, and finally (3) computing the product $\prod_{i=1}^k a^{2^{e_i}}$.

(2) The ElGamal protocol encrypts a text T to a cipher

$$C \equiv KT \mod p.$$

Using the ElGamal protocol with their public keys and shared secret, Bob sends the number $C = 6$ to Alice. What was the original number T?

Problem 16.4. (From Final Exam Spring 2020 at-home exam)

(1) Alice publishes the public key $n = 91$ and $k = 5$ hoping to receive secret messages via the RSA protocol. Use the fact that n is not very large combined with the Euclidean algorithm in reverse to crack Alice's secret key.

(2) Decode the following message that was sent from Bob to Alice using a (modular) calculator:

$$63 \quad 71 \quad 23 \quad 0 \quad 80 \quad 71 \quad 13 \quad 13 \quad 31 \quad 44.$$

Each block represents the encryption of a single letter via: space = 0, A = 1, B = 2, C = 3, D = 4, ... and then encrypted using RSA with Alice's public key. Explain the computation used to decode.