1 Talteori[1]

Definition: The function f from X to Y is a **surjection** if every y in Y is a value $f(x)$ for *at least one* x in X. It is a **injection** if every y in Y is a value $f(x)$ for *at most one* x in X. It is a **bijection** if it is both a surjection and an injection, that is, if every y in Y is a value $f(x)$ for *exacly one* x in X.

Primtal-test:

1. Om talet t kan primtalsfaktoriseras är det inte ett primtal.
2. Om talet t inte är ett primtal måste talet ha en primtalsfaktor $p \leq \lfloor \sqrt{t} \rfloor$. Exempel: $p \leq \lfloor \sqrt{1019} \rfloor = 31$ (Testa att dela talet med [2...31], om inget av talen delar t är t ett primtal).

Definition: If $gcd(a, b) = 1$ then **coprime**.

Theorem 6.2.1 Let m be a natural number. Then the following statement is true for every natural number n: if there is an injection from $\mathbb{Z}_n$ to $\mathbb{Z}_m$, then $n \leq m$. ($\implies$ the **pigeonhole principle/brevlådeprincipen**)

A **relation** R on a set X is a set of ordered pairs of members of X. R is **reflexive** if xRx for every $x \in X$. R is **symmetric** if, whenever we have xRy, we also have yRx. R is **transitive** if, whenever we have both xRy and yRz, we also have xRz. R is a **equivalence relation** if its **reflexive**, **symmetric** and **transitive**.

En **multiplikativ invers** till ett tal A är det tal B som vid multiplikation ger 1, $AB = 1$. Den multiplikativa inversen till talet 2 är 0,5, ty $2 * 0,5 = 1$. Under congruence, t.ex. $\mathbb{Z}_{113}$ se 2.9.

1.1 Byta talbas

Exempel: $(109)_{10} = (1101101)_2$

$$109 = 2 \times 54 + 1$$
$$54 = 2 \times 27 + 0$$
$$27 = 2 \times 13 + 1$$
$$13 = 2 \times 6 + 1$$
$$6 = 2 \times 3 + 0$$
$$3 = 2 \times 1 + 1$$
$$1 = 2 \times \mathbf{0} + 1$$

1.2 Hitta $gcd(x, y)$ (Euclidean algorithm)

$gcd(2406, 654)$

$$2406 = 654 \times 3 + 444 \implies gcd(2406, 654) = gcd(654, 444)$$
$$654 = 444 \times 1 + 210 \implies gcd(2406, 654) = gcd(444, 210)$$
$$444 = 210 \times 2 + 24 \implies gcd(2406, 654) = gcd(210, 24)$$
$$210 = 24 \times 8 + 18 \implies gcd(2406, 654) = gcd(24, 18)$$
$$24 = 18 \times 1 + 6 \implies gcd(2406, 654) = gcd(16, 6)$$
$$18 = 6 \times 3 \implies gcd(2406, 654) = gcd(6, 0) = \mathbf{6}$$

Tillämpning: Antal 13-liter-hinkar x och 31-liter-hinkar y för att få 3 liter, $13x + 31y = 3$. Ges av att lösa $13x + 31y = 1$ utifrån resultatet från euklides och därefter multiplicera med 3. Euklides:

$$31 = 13 * 2 + 5 \to 13 = 5 * 2 + 3 \to 5 = 3 * 2 + 2 \to 3 = 1 * 2 + 1$$

[1]Compiled on 2019/05/05 at 14:37 GMT
`GitHub.com/SkruvdragarN/Diskret_matematik_formelblad.git`

Algebra utifrån euklides-resultat:
$1 = 3*2 = 3-(5-3) = (-1)*5+2*3 = (-1)*5+2*(13-2*5) =$
$= (-5) * 5 + 2 * 13 = (-5)(31 - 2 * 13) + 2 * 13 =$
$(-5) * 31 + 12 * 13 = 1$
Multiplicera med 3 $\to 13(3 * 13) + 31(-5 * 3) = 3$
$x = 36 \quad y = -16$

2 Enumerationsproblem

$$\sum_{k=1}^{n-1} k = \frac{n(n-1)}{2}$$

2.1 Kombinatorik

"Ur en mängd med storlek n välj ut r stycken."

2.1.1 Ordered | Without repetition

$$\frac{n!}{(n-r)!} = n(n-1)...(n-r+1)$$

Pallplaceringar (tävling). Antalet injektioner mellan mängder $f : N_r \to N_n$ med storlek r och n.

2.1.2 Unordered | Without repetition

$$\binom{n}{r}$$

Hur många olika händer kan man få givna i poker?

2.1.3 Ordered | With repetition

$$n^r$$

Pinkoder. Binära tal med 13 siffror? (2^{12} inte börja med 0)

2.1.4 Unordered | With repetition

$$\binom{n-1+r}{r}$$

Antal sätt man kan slå 4 tärningar? Lösningar till $x+y+z+w = 45$ där $x, y, z, w \in \mathbb{N}$ ger $n = 4$ $r = 45$, dvs $\binom{4-1+45}{45}$.

2.2 Euler's phi-funktion $\phi(n)$

$\phi(n)$ is the number of non-negative integers less than n that are relatively prime (coprime) to n.

$$\phi(n) = \phi(p_1^{\varepsilon_1} * p_2^{\varepsilon_2} * ... * p_k^{\varepsilon_k})$$

där $p_n^{\varepsilon_n}$ är primtal i primtalsfaktoriseringen av n.

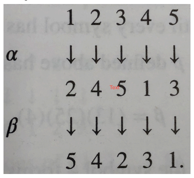
$$\phi(p) = p - 1 \qquad \phi(p^\varepsilon) = p^\varepsilon - p^{\varepsilon - 1}$$

Där p är ett primtal.

$$\phi(a * b) = \phi(a) * \phi(b) \quad om\ gcd(a, b) = 1$$

2.3 Permutations

Cyklisk notation: $\alpha = (124)(35)$ och $\beta = (13)(25)(4)$ ger:



Dvs $\beta\alpha = (15)(243)$. Först α sedan β. För att återfå samma permutation kan du blanda k gånger. Där k är den minsta gemensamma nämnare av cyklernas storlek. Minsta gemensamma nämnare till 2 och 8 är 8. Invers: $(\beta\alpha)^{-1} = (51)(342)$

2.4 Binomial numbers

Theorem 11.1.1 + 11.1.2

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r} = \frac{n!}{r!(n-r)!}$$

Pascals triangel

$n=0$					1				
$n=1$				1		1			
$n=2$			1		2		1		
$n=3$		1		3		3		1	
$n=4$	1		4		6		4		1

2.5 Binomial theorem

Theorem 11.3

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + ... + \binom{n}{n}b^n$$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k}(a^{n-k} * b^k)$$

2.6 The sieve principle (Sållningsprincipen)

Theorem 11.4
If $A_1, A_2, ..., A_n$ are finite sets then

$$|A_1 \cup A_2 \cup ... \cup A_n| = a_1 - a_2 + a_3 - ... + (-1)^{n-1} * a_n$$

where a_i is the sum of the cardinalities of the intersections of the sets taken i at a time $(1 \le i \le n)$.

Exempel:
Heltal $1 \le n \le 1000$ där n är delbar med minst en av $3, 5, 7$:
$|A_3 \cup A_5 \cup A_7| =$
$|A_3|+|A_5|+|A_7|-(|A_3 \cap A_5|+|A_3 \cap A_7|+|A_5 \cap A_7|)+(|A_3 \cap A_5 \cap A_7|)$
$\lfloor\frac{1000}{3}\rfloor+\lfloor\frac{1000}{5}\rfloor+\lfloor\frac{1000}{7}\rfloor-(\lfloor\frac{1000}{3*5}\rfloor+\lfloor\frac{1000}{3*7}\rfloor+\lfloor\frac{1000}{5*7}\rfloor)+\lfloor\frac{1000}{3*5*7}\rfloor = 544$

2.7 Partitions

Definition: A **partition** of a set X is a family $\{X_i | i \in I\}$ of non-empty subsets of X such that

- X is the union of the sets X_i $(i \in I)$,
- each pair X_i, X_j $(i \neq j)$ is disjoint

The subsets X_i are called the **parts** of the partition.

Theorem 12.1
Let $S(n,k)$ denote the number of partitions of an n-set X into k parts, where $1 \le k \le n$. Then

$$S(n,1) = 1, \quad S(n,n) = 1,$$
$$S(n,k) = S(n-1,k-1) + kS(n-1,k) \quad (2 \le k \le n-1)$$

The number $S(n,k)$ are sometimes called **Stirling numbers** (of the second kind). Can be tabulated as below.

$n=1$							1						
$n=2$						1		1					
$n=3$					1		3		1				
$n=4$				1		7		6		1			
$n=5$			1		15		25		10		1		
$n=6$		1		31		90		65		15		1	
$n=7$	1		63		301		350		140		21		1

2.8 Distributions and multinomial numbers

Theorem 12.3.2
Given any positive integers $n, n_1, ..., n_k$ satisfying $n_1+n_2+...+n_k = n$, we have

$$\binom{n}{n_1, n_2, ..., n_k} = \frac{n!}{n_1!n_2!...n_k!}$$

Kallas ett *multinomial number*. Exempel: How many 11-letter words can be made from the letters of the word ABRACADABRA? Ger antal A $n_1 = 5$, antal B $n_2 = 2$, antal R $n_3 = 2$ etc.

Theorem 12.3.3
For any positive integers n and k

$$(x_1 + x_2 + ... + x_k)^n = \sum \binom{n}{n_1, n_2, ..., n_k} = x_1^{n_1}x_2^{n_2}...x_k^{n_k}$$

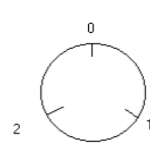
Notera att $\binom{n}{n_1,n_2,...,n_k}$ är det ett *multinomial number*, se ovan.

2.9 Concurrence $x_1 \equiv x_2$ $(mod\ m)$

Definition: Let x_1 and x_2 be integers, and m a positive integer. We say that x_1 is **congruent** to x_2 **modulo** m, and write $x_1 \equiv x_2$ $(mod\ m)$ whenever $x_1 - x_2$ is divisible by m.

Definition: The set of **integers modulo m**, written as $\mathbb{Z}_m$, is the set of distinct equivalence classes under the relation of congruence modulo m in $\mathbb{Z}$. Exempel: $\mathbb{Z}_3 = \{X_0 \cup X_1 \cup X_2\}$, where $X_0 = [0]_3 = \{..., -3, 0, 3, 6, ...\}$ $X_1 = [1]_3 = \{..., -2, 1, 4, 7, ...\}$ $X_2 = [2]_3 = \{..., -1, 2, 5, 8, ...\}$ $7+5 = 0$ $(i\ \mathbb{Z}_3) \iff [7]_3 \oplus [5]_3 = [0]_3$

Talen i $X_P = [P]_3$ har alla rest P vid division med 3.



Theorem 13.3.1
The element r in $\mathbb{Z}_m$ is invertible if and only if r and m are coprime in $\mathbb{Z}$. In particular, when p is a prime every element of $\mathbb{Z}_p$ except

0 is invertible.

Theorem 13.3.2
If y is invertible in $\mathbb{Z}_m$ then $y^{\phi(m)} = 1 \; in \; \mathbb{Z}_m$

Multiplikativ invers i t.ex. $\mathbb{Z}_{113}$. Använd euclides (1.2) och algebra-jonglera uttrycket till $32x + 113k = 1$ ($113k = 0$ och $32 * 53 = 1$ i $\mathbb{Z}_{113}$).

3 Grafteori och algoritmer

Binära metoden för exponentiering:
Beräkna 2^{50} med 7 multiplikationer istället för 49. Skriv exponenten som summa av 2-potenser $50 = 32 + 16 + 2 = 2^5 + 2^4 + 2^1$. Vi beräknar potenserna $2^1, 2^2, 2^4, 2^8, 2^{16}, 2^{32}$ genom att kvadrera föregående potens i listan (5 multiplikationer). Vi kan därefter beräkna $2^{50} = 2^{32+16+2} = 2^{32} * 2^{16} * 2^2$ (2 multiplikationer till).

Definition: A **graph** G consists of a finite set V, whose members are called **vertices**, and a set E of 2-subsets of V, whose members are called **edges**. We usually write $G = (V, E)$ and say that V is the **vertex set** and E is the **edge set**.

Definition: Two graphs G_1 and G_2 are said to b **isomorphic** when there is a bijection a from the vertex set of G_1 to the vertex set of G_2 such that $\{a(x), a(y)\}$ is an edge of G_2 if and only if $\{x, y\}$ is an edge of G_1. The bijection a is said to be an **isomorphism**.

Definition: The **degree** of a vertex v is a graph $G = (V, E)$ is the number of edges of G which contains v. Notation: $\delta(v)$.

Theorem 15.3
The sum of the values of degree $\delta(v)$, taken over all the vertices v of a graph $G = (V, E)$, is equal to twice the number of edges:

$$\sum_{v \in V} \delta(v) = 2|E|$$

Definition: A **walk** in a graph G is a sequence of vertices $v_1, v_2, ..., v_k$, such that v_i and v_{i+1} are adjacent ($1 \leq i \leq k-1$). If all its vertices are distinct, a walk is called a **path**.

Definition: We say that a graph T is a **tree** if T is connected and there are no cycles in T.

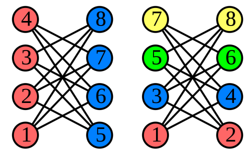
Ett **rotat träd** är träd där man valt ut en nod i trädet, och kallar den för en rot, som utgör basen för trädet. Två rotade träd anser lika endast om det finns en isomorfi från den ena till den andra som avbildar roten från den första till roten av den andra. En **komplett graf** är en graf där varje par av distinkta hörn har en kant mellan sig.

3.1 Vertex colouring

Definition: A **vertex colouring** of a graph $G = (V, E)$ is a function $c : V \to \mathbb{N}$ with the property that

$$c(x) \neq c(y) \quad whenever \quad \{x, y\} \in E$$

Definition: The **chromatic number** (**hörnkromatiska talet**) of G, written $\chi(G)$, is defined to be the least integer k for which there is vertex colouring c which is a function from V to $\mathbb{N}_k$, and k is the least integer with this property.



3.2 Spanning trees

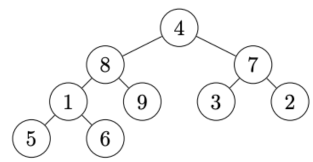
Suppose that $G = (V, E)$ is a connected graph, and T is a subset of E such that: **1.** Every vertex of G belongs to an edge in T; **2.** the edges in T form a tree. In this case, we say that T is a **spanning tree** for G.

3.3 Sortering

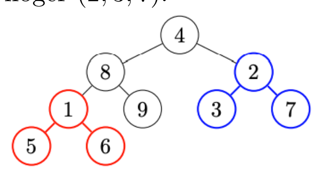
3.3.1 Heap sort

Sorterar listan $4, 8, 7, 1, 9, 3, 2, 5, 6$. Först fylls noderna i ett binärt träd med elementen i listan.

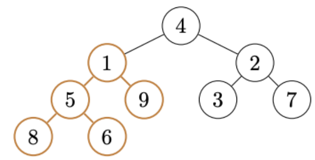
1. Först fylls noderna i ett binärt träd med elementen i listan.



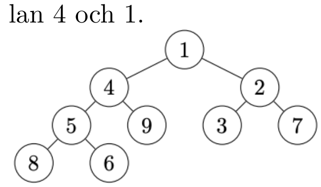
2. Nu ska trädet omvandlas till en heap genom att byta plats på element så att alla fäder innehåller ett lägre värde än sina söner. Vi börjar med delträdet till vänster $(1, 5, 6)$ och sedan delträdet till höger $(2, 3, 7)$.



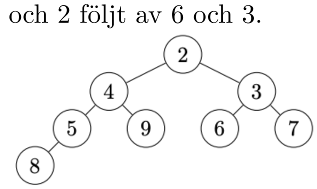
3. Vi fortsätter sedan med det vänstra delträdet $(1, 5, 9, 8, 6)$ nedan och byter plats på 8 och 1 följt av 8 och 5.



4. Avslutningsvis behandlas hela trädet med bytet mellan 4 och 1.



5. Trädet är nu en heap och det minsta elementet finns i roten. Vi tar bort detta element och ersätter det men det element som ligger längst ner till höger, d.v.s. elementet 6. Vi uppdaterar därefter trädet genom att byta plats på 6 och 2 följt av 6 och 3.



Antal jämförelser: $O(n*log(n))$.
Antal byten: $O(n * log(n))$.

3.3.2 Bubble sort

Sortering av listan $X = \{x_1, x_2, ..., x_n\}$ ger:
for $j := 1$ *to* $n - 1$ *do*
for $i := 1$ *to* $n - j$ *do*
if $x_i > x_{i+1}$ *then switch* x_i *and* x_{i+1}

Jämförelser (efter $j$te genomgången): $n - j$.
Antal jämförelser: $O(n^2)$. Antal byten: $O(n^2)$.

3.3.3 Insertion sort

The basic idea of insertion sorting is to begin with the list $L = (x_1)$ and insert x_i in its correct place in the list for $i = 2, 3, ..., n$. For example, if $x_1, x_2, ..., x_8$ are the integers $47, 73, 21, 45, 28, 69, 19, 23$, the list is built up as shown below:

Table 14.8.2

47							
47	73						
21	47	73					
21	45	47	73				
21	28	45	47	73			
21	28	45	47	69	73		
19	21	28	45	47	69	73	
19	21	23	28	45	47	69	73

Antal jämförelser: $O(n * log(n))$. Antal byten: $O(n * log(n))$. Om man använder *bisection* metoden, dvs veta vilken halva av listan som x ska placeras i.

3.4 Greedy vertex colouring algorithm

Greedy vertex colouring algorithm

```
assign colour 1 to v_1;
for  i:=2 to n  do
  begin
  let  S be the empty set of colours;
  for  j:=1 to i-1  do
    if v_j is adjacent to v_i
      then  add the colour of v_j to S;
  k:=1;
  while  colour k is in S  do  k:=k+1;
  assign colour k to v_i
  end
```

Färgningen av kanter får ske i godtycklig ordning.

3.5 Minimum spanning tree problem (MST)

At each stage we add the *cheapest* edge joining a new vertex to the partial tree (If several edges with the same weight are available we can select any of them).

3.6 Depth-first search (DFS)

```
let stack = (v);
while   stack is not empty   do
   begin
   x := top (stack);
   if   x is adjacent to a new vertex y
     then  add y at the top of the stack
     else  remove x from the stack
   end
```

Table 16.4.1

Stack	Added	Removed
a	*a*	—
ab	*b*	—
abc	*c*	—
abcd	*d*	—
abc	—	*d*
abce	*e*	—
abc	—	*e*
ab	—	*c*
a	—	*b*
∅	—	*a*

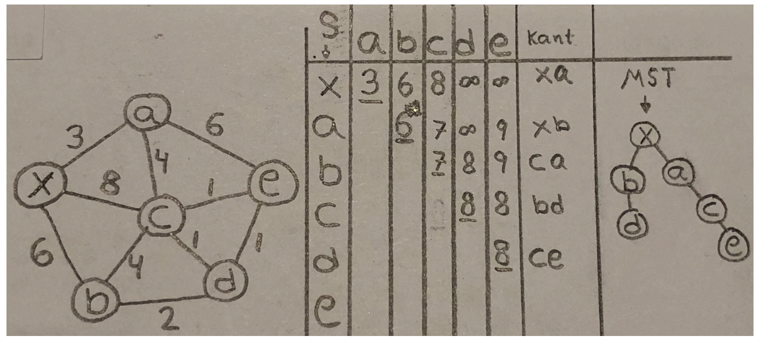
3.7 Breadth-first search (BFS)

```
let queue = (v);
while  queue is not empty  do
  begin
  x := front (queue);
  if   x is adjacent to new vertex y
    then  add y at the tail of the queue
    else  remove x from the queue
  end
```

Table 16.5.1

Queue	Added	Removed
a	*a*	—
ab	*b*	—
abc	*c*	—
abce	*e*	—
bce	—	*a*
bced	*d*	—
ced	—	*b*
ed	—	*c*
d	—	*e*
∅	—	*d*

3.8 Shortest path problem (Dijkstras algoritm)



Förklaring: S är mängden av alla besökta kanter. (*) 6:an i bilden (ab) ges av $min(L(b), L(a) + w(ab)) = min(6, 3 + \infty) = 6$, där $L(b)$ är den tidigare vägen till b och $w(ab)$ är vikten på kanten ab vilket inte existerar och därmed är ∞. Till höger i bild är det minimalt uppspännande trädet som erhålls från kant-kolumnen. **På en tenta** blir våra kära matematiker mycket glada om du bifogar det minimalt uppspännande trädet.

3.9 Bipartite & Matchings

Theorem 15.7.2
A graph is **bipartite** if and only if it contains no cycles with odd length. Alternativt: Om $\chi(G) = 2$, minsta antal färgningar är 2.

Definition: A **matching** in a bipartite graph $G = (U \cup Y, E)$ is a subset M of E with the property that no two edges in M have a common vertex. Mängd av kanter som inte har hörn gemensamt (parvis).

Definition: We shall say that a matching M is a **maximum matching** for $G = (U \cup Y, E)$ if no other matching has a greater cardinality.

Definition: If $|M| = |X|$ then we say that M is a **complete matching** (**komplett/perfekt matchning**).

Theorem 17.4
The bipartite graph $G = (U \cup Y, E)$ has a complete matching if and only if Hall's condition is satisfied, that is

$$|J(A)| \geq |A| \quad \text{for all} \quad A \subseteq X.$$