Veckoblad 5, Diskret matematik IT, HT2014

Viktiga begrepp och resultat under veckan

- Principen för kryptering med öppen nyckel.
- Idén bakom RSA-kryptering.
- Multiplikationsprincipen för oberoende operationer.
- Formel för antalet permutationer av k element bland n.
- Formel för antalet kombinationer av k element bland n.

Grundläggande kunskapsmål under veckan

- Avgöra om ett givet kombinatoriskt problem består av permutationer eller kombinationer eller en blandning av dessa.
- Beräkna antalet möjliga kombinationer av k element bland n.
- Beräkna antalet möjliga permutationer av k element bland n.

Gruppövningar

1. Konstruera en kryptering (med meddelande $x \to y = x^a$ modulo pq, dvs med öppna nykeln $a = a_m$, $pq = p_m q_m$, och sgd$(a, (p-1)(q-1)) = 1$ hos mottagaren.) (Hoppa över Hash-signatur.) Du får gärna använda en dator till hjälp i beräkningarna (och ta större primtal om du har ett program).

   Skapa din egen RSA-nyckel (med två tvåsiffriga primtal, p, q) och ge den till en gruppkamrat (den offentliga delen, dvs a, pq). Låt kamraten kryptera ett meddelande x (t ex ett tvåsiffrigt tal) med din öppna nyckel. Du ska sedan avkoda detta. Byt sedan roll.

2. (a) Diskutera i gruppen (tills alla förstår) hur formeln för antalet permutationer av k element bland n kan härledas från multiplikationsprincipen.

   (b) Diskutera i gruppen (tills alla förstår) hur formeln för antalet kombinationer av k element bland n kan härledas från formeln fär antalet permutationer.

   (c) Hitta på två egna exempel på kombinatoriska problem där det handlar om permutationer respektive kombinationer (ett exempel för varje).

3. Stämman för AB Modern Styrning ska välja ny styrelse för bolaget. Det finns 13 kvinnliga kandidater och 9 manliga. Man ska utse en styrelse med 7 personer. Bolagsreglerna säger att det måste vara minst tre kvinnliga och minst tre manliga kandidater i styrelsen. Hur många olika styrelser är möjliga?

4. (a) Hur många olika "ord" (d v s bokstavspermutationer) med nio bokstäver kan man bilda av bokstäverna i MATEMATIK.

   (b) Hur många av dessa ord innehåller *inte* två A i rad?

   (c) Hur många av dessa har vokaler på de fyra första platserna?

   (d) Hur många av dessa har vokaler på de fem sista platserna?

5. (a) Hur många sexsiffriga tal, d v s heltal n som uppfyller $10^5 \leq n < 10^6$, finns det som innehåller exakt 2 ettor, exakt 1 trea och exakt 2 åttor?

   (b) Hur många av dessa är udda?