Diskret Matematik – IT, TMV200, HT08

Veckoblad 5 :

- Vi avslutar avsnittet om heltalen med att gå igenom RSA-kryptering.
- Det tredje temat inleds med kombinatorik. Vi går igenom multiplikationsprincipen, kombinationer och permutationer.
- När det gäller övningar så rekommenderas de uppgifter i kapitel 7 som ni ännu inte gjort bland 7.5–7.24.

Kryssuppgifter

1. Efter uppgifterna 7.6, 7.7 och 7.11 – 7.14 i boken.

   Kan du hitta alla lösningar till ekvationen

   $$x^2 + y^2 = p$$

   i $\mathbb{Z}_p$ för $p = 11, 13$ och 17?

   Kan du skriva $11, 13$ eller 17 som summa av två kvadrater i $\mathbb{Z}$, dvs har ekvationen

   $$x^2 + y^2 = p$$

   för $p = 11, 13$ och 17 någon lösning i $\mathbb{Z}$?

2. Konstruera din egen RSA-nyckel (med två tvåsiffriga primtal) och ge den till dina gruppkamrater (den offentliga delen!). Du får gärna använda en dator till hjälp i beräkningarna.

3. Koda in ett kort meddelande (t.ex ett tvåsiffrigt tal) för en gruppkamrat (med hans/hennes offentlig nyckel) och avkoda en som en kamrat kodat åt dig.