

## Veckoblad 5 :

- Bokens övningar, kap 7, **Heltalen** , alla övningar.

- Stoff att fundera på och hitta egna uppgifter om: Allt om heltalen: delbarhet, Euklides algoritm, största gemensamma delare, Bezouts relation, diofantiska ekvationer, primtal, aritmetikens fundamentalsats, kongruensräkning och ekvationslösning mod n, kinesiska restsatsen, Eulers  $\Phi$ -funktion, kryptering.

## Kryssuppgifter

1. Efter uppgifterna 7.6, 7.6, och 7.11 till 7.14 i boken

Kan du hitta alla lösningar till ekvationen

$$x^2 + y^2 = 0$$

i  $\mathbf{Z}_{11}$ , i  $\mathbf{Z}_{13}$ , i  $\mathbf{Z}_{17}$ ?

Kan du skriva 11, 13 eller 17 som summa av två kvadrater (i  $\mathbf{Z}$ )?

2. Konstruera din egen RSA-nyckel (med två tvåsiffriga primtal) och ge den till dina grupp-kamrater (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 grupp-kamrat (med hans/hennes offentlig nyckel) och avkoda en som en kamrat kodat åt dig.