Diskret Matematik – IT, TMV200, HT10, Laura Fainsilber

Veckoblad 5 :

(rättat tisdag 23 nov kl.15.30, med RSA!)

• 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 Φ-funktion, kryptering.

Kryssuppgifter

1. Beräkna $5^8 - 7^{25}$ modulo 15.

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 (och ta större primtal om du har ett program).

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. Även här är program välkomna, och då kan du ta t.ex. 3-siffriga tal.