Diskret Matematik/TMV200/HT11, Genkai Zhang **Veckoblad 5**

Rek. upp.

• 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.

Demo-uppgifter

• 7.19(a).

• Bestäm inversen 33 modolo $200 = 2^3 \cdot 5^2$. (Se också avsnittet RSA-krypto)

Kryssuppgifter

1. Beräkna 11^8 och 2^{16} modulo 15.

2. 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$(a, pq) = 1$ hos mottagaren.) (Hoppar över Hash-signatur.) Du får gärna använda en dator till hjälp i beräkningarna (och ta större primtal om du har ett program).

   (a) Skapa din egen RSA-nyckel (med två tvåsiffriga primtal, p, q) och ge den till dina gruppkamrater (den offentliga delen, dvs a, pq). Koda in ett meddelande x (t.ex ett tvåsiffrigt tal) som y och ge den till en gruppkamrat.

   (b) Låt gruppkamraten avkoda detta, och vice versa.