Diskret matematik IT ht 2005: Kryssuppgifter vecka 6

1. Vad blir $13^{37} + 33^{36} + 11^{35} + 38^{40}$ i $\mathbb{Z}_{76}$?

2. Axel har skaffat sig en RSA-nyckel med alldeles för små primtal; hans öppna nyckel är $pq = 9167$ och $a = 61$. En av Axels kompisar skickar ett krypterat meddelande som du snappar upp. Det krypterade meddelandet är 1772. Vad är det riktiga meddelandet? (Använd gärna datorhjälp till beräkningarna.)

3. Låt a och b vara två positiva heltal. Visa att det antingen gäller att $sgd(a + b, a - b) = sgd(a, b)$ eller $sgd(a + b, a - b) = 2sgd(a, b)$.

Lösningar

1. Eftersom $\Phi(76) = 2 \cdot 18 = 36$ följer det av Eulers sats att $a^{36} = 1$ modulo 76 då a och 76 är relativt prima. Därför är $13^{37} = 14$, $33^{36} = 1$ och $11^{35} = 11^{-1} = 7$, medan 38^{40} får behandlas separat. Men $38^2 = 1444 = 0$ så $38^{40} = 0$. Den sökta summan är alltså $14 + 1 + 7 = 22$.

2. Man ser väldigt snabbt att Axels hemliga primtal måste vara $p = 89$ och $q = 103$. Axels hemliga invers b är alltså inversen till 61 modulo $\Phi(pq) = 88 \cdot 102 = 8976$. Med hjälp av Euklides utökade algoritm beräknas denna snabbt till $b = 3973$. För att dekryptera ska vi alltså beräkna 1772^{3973} mod 9167, vilket man med datorhjälp beräknar till 4208. Det riktiga meddelandet var alltså 4208.

3. Skriv $d = sgd(a, b)$ och $c = sgd(a - b, a + b)$. Eftersom c är en gemensam delare till $a + b$ och $a - b$ gäller dels att $c|(a + b) + (a - b)$, dvs $c|2a$, dels att $c|(a + b) - (a - b)$, dvs $c|2b$. Därför gäller att $c|sgd(2a, 2b)$, dvs $c|2d$.

   Å andra sidan gäller ju att eftersom $d|a$ och $d|b$ så följer att $d|a + b$ och $d|a - b$ så att $d|c$.

   Vi har alltså att $d|c$ och $c|2d$ ur vilket det följer att $c = d$ eller $c = 2d$ som vi ville.