Diskret matematik IT ht 2004: Kryssuppgifter vecka 6

1. Låt p och q vara två olika primtal. Visa att $\Phi(pq) = (p-1)(q-1)$.

2. Axel har skaffat sig en RSA-nyckel med alldeles för små primtal; hans öppna nyckel är $pq = 8989$ och $a = 13$. 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. $\Phi(pq)$ är antalet heltal i $\{1, 2, \ldots, pq-1\}$ som är relativt prima pq. Totalt finns det $pq-1$ tal i den aktuella mängden och för att få $\Phi(pq)$ ska vi alltså subtrahera antalet tal i den aktuella mängden som delas av antingen p eller q. Det finns $q-1$ stycken tal som delas av p, nämligen $p, 2p, 3p, \ldots, (q-1)p$. På samma sätt finns det $p-1$ stycken tal som delas av q, nämligen $q, 2q, 3q, \ldots, (p-1)q$. Kan något tal finnas med i båda dessa uppräkningar? Nej, ty om det för två heltal x och y gäller att $xp = yq$ får vi för x och y den diofantiska ekvationen $px - qy = 0$ som har den allmänna lösningen $(x, y) = (nq, np), n \in \mathbf{Z}$, och inget av dessa tal finns representerat i våra uppräkningar.

   Vi får alltså $\Phi(pq) = pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1)$.

2. Man ser väldigt snabbt att Axels hemliga primtal måste vara $p = 89$ och $q = 101$. Axels hemliga invers b är alltså inversen till 13 modulo $\Phi(pq) = 88 \cdot 100 = 8800$. Med hjälp av Euklides utökade algoritm beräknas denna snabbt till $b = 677$. För att dekryptera ska vi alltså beräkna $1772^{677} \bmod 8989$, vilket man med datorhjälp beräknar till 50. Det riktiga meddelandet var alltså 50.

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.