Veckoblad 4, Diskret matematik IT, HT2013

Viktiga begrepp och resultat under veckan

- Begreppet kongruens som ger partition av heltalen.
- Heltalen modulo ett heltal n med addition och multiplikation (modulo n).
- Ett heltal b har (multiplikativ) invers modulo n om och endast om $\text{sgd}(b, n) = 1$.
- Kinesiska restsatsen.
- Eulers Φ-funktion och beräkningsreglerna för denna.
- Eulers sats och specialfallet Fermats lilla sats.
- Principen för kryptering med öppen nyckel.
- Idén bakom RSA-kryptering.

Grundläggande kunskapsmål under veckan

- Beräkna den minsta positiva representanten för klassen av ett tal modulo n.
- Lösa enkla ekvationer i $\mathbb{Z}_n$.
- Lösa system av konruensekvationer med Kinesiska restsatsen.
- Beräkna Eulers Φ-funktion givet primtalsfaktoriseringen av ett tal.
- Beräkna den minsta positiva representanten för klassen av potensen av ett tal modulo n med Eulers sats.

Gruppövningar

1. (a) Ge alla klasser som har additiv invers modulo 26.
   (b) Ge den additiva inversen för alla klasser i förra deluppgiften modulo 26.
   (c) Ge alla klasser som har multiplikativ invers modulo 26.
   (d) Bestäm (multiplikativa) inversen modulo 26 för alla klasserna i förra deluppgiften.
2. Beräkna Φ av följande tal: 577, 9177, 4039 och 1049.
3. Bestäm det minsta positiva talet m som är sådant att det ger resten 3 vid division med 5, resten 5 vid division med 7 och resten 7 vid division med 13. (Ni ska använda en "generell" metod som är effektiv oavsett storleken på talen.)

4. Bestäm minsta positiva talet m sådant att $m \equiv 2013^{2013} \pmod{13}$.

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

   Skapa din egen RSA-nyckel (med två tvåsiffriga primtal, p, q) och ge den till en gruppkamrat (den offentliga delen, dvs a, pq). Låt kamraten kryptera ett meddelande x (t ex ett tvåsiffrigt tal) med din öppna nyckel. Du ska sedan avkoda detta. Byt sedan roll.