

Lärmål Kapitel 5, Inledande diskret matematik D, HT2015

Viktiga begrepp och resultat

- Begreppen delar och multipel.
- Delbarhet är en partiell ordning på de naturliga talen.
- Om a delar b och c , så delar det också $bm+cn$ för alla heltal m och n .
- Divisionsalgoritmen.
- Begreppen största gemensamma delaren och relativt prima.
- Euklides algoritmen för att beräkna största gemensamma delaren.
- Bezouts identitet.
- Begreppen primtal och sammansatt tal.
- Linjära diofantiska ekvationer.
- Om ett primtal delar en produkt så delar det minst en av faktorerna.
- Aritmetikens fundamentalsats.
- 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

- Avgöra om ett tal delar ett annat.
- Beräkna rest och kvot i divisionsalgoritmen.

- Beräkna största gemensamma delaren med både primtalsfaktorisering och Euklides algoritmen och kunna avgöra vilken metod som är bäst i givet läge.
- Använda Euklides utökade algoritmen för att bestämma talen i Bezouts identitet.
- Primtalsfaktorisera ett rimligt stort heltal.
- Avgöra om ett rimligt stort tal är primtal.
- Bestäm den allmänna lösningen till en linjär diofantisk ekvation.
- Beräkna den minsta positiva representanten för klassen av ett tal modulo n .
- Lös enkla ekvationer i $\mathbb{Z}_n$.
- Lös system av kongruenskvationer 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.