Veckoblad 3, Diskret matematik IT, HT2012

Viktiga begrepp och resultat under veckan

- 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 algoritm för att beräkna största gemensamma delaren.
- Bezouts identitet.
- Begreppen primtal och sammansatt tal.
- Om ett primtal delar en produkt så delar det minst en av faktorerna.
- Aritmetikens fundamentalsats.
- Linjära diofantiska ekvationer.

Grundläggande kunskapsmål under veckan

- Avgöra om ett tal delar ett annat.
- Beräkna rest och kvot i divisionsalgoritmen.
- Beräkna största gemensamma delaren med både primtalsfaktorisering och Euklides algoritm och kunna avgöra vilken metod som är bäst i givet läge.
- Använda Euklides utökade algoritm för att bestämma talen i Bezouts identitet.
- Primtalsfaktorisera ett rimligt stort heltal.
- Avgöra om ett rimligt stort tal är primtal.
- Bestämma den allmänna lösningen till en linjär diofantisk ekvation.

Gruppövningar

1. (a) Visa (med ett exempel) att förutsättningen att p är ett primtal är *nödvändig* i Sats 7.2.2.

   (b) Motivera att relationen given av att a är relaterat med b om och endast om $a \mid b$ är en partiell ordning på $\mathbb{N}$ men att den *inte* är det på $\mathbb{Z}$.

2. Diskutera (tills alla i gruppen förstår) varför Euklides algoritm fungerar; dels varför den garanterat tar slut och dels att det den ger verkligen är största gemensamma delaren.

3. Bestäm alla lösningar till följande Diofantiska ekvationer.

   (a) 323x+278y=7

   (b) 579x+921y=5

   Välj också ut den lösning i de båda fallen för vilken $|x| + |y|$ blir minimalt.

4. Motivera noggrant vilka av följande tal som är primtal: 577, 9177, 4039 och 1049. För de som inte är primtal ge också deras faktorisering i primtal.

5. Låt $F(n)$ vara det n:te Fibonacci-talet.

   (a) Visa att sgd$(F(n), F(n-1)) = 1$ för alla $n > 1$.

   (b) Visa att om man beräknar sgd$(F(n), F(n-1))$ med Euklides algoritm så krävs det alltid exakt $n - 3$ steg.

   (c) I själva verket är dessa par av efterföljande Fibonacci-tal de tal som kräver flest steg i förhållande till sin storlek. Kan ni motivera detta?