GÖTEBORGS UNIVERSITET
MATEMATIK 1, MMG200, HT2015
INLEDANDE ALGEBRA

Övningshäfte 4: Heltalen och delbarhet

Övning K

Syftet med övningen är att bekanta sig med delbarhetsegenskaper hos heltalen. De viktigaste begreppen är

- delbarhet och divisionsalgoritmen
- största gemensamma delare och Euklides algoritm
- primtal
- Aritmetikens fundamentalsats

I den sista uppgiften ska vi också titta på liknande frågeställningar för polynom.

1. Ni har förmodligen redan tidigare stött på det matematiska begreppet att ett heltal a *delar* ett heltal b. Vad betyder det?

   Diskutera och försök förklara innebörden. Försök att ge en definition utan att titta i boken. Titta nu på bokens definition. Är det samma definitionen? Om inte, hur skiljer de sig åt?

   (Delbarhet är en relation på $\mathbb{Z}$ och om man bara betraktar $\mathbb{Z}_+$ så är det i själva verket en så kallad *partiell ordning*, se avsnitt 3.8 i boken om du är intresserad.)

2. Avgör vilka av följande påståenden som är sanna: $4|1$, $1|4$, $4|0$, $0|1$, $7|102$ och $3|102$.

3. Avgör vilka av följande utsagor som är sanna och vilka som är falska. Ge ett bevis eller motexempel för att motivera. Om det går trögt så ta hjälp av bokens avsnitt 5.1.

   (a) $\forall a : a \mid a$, d v s '$|$' är reflexiv

   (b) $\forall a : 1 \mid a$

   (c) $\forall a : a \mid 1$

   (d) $\forall a : 0 \mid a$

   (e) $\forall a : a \mid 0$

   (f) $\forall a \forall b : a \mid b \Longrightarrow b \mid a$, d v s '$|$' är symmetrisk

   (g) $\forall a \forall b \forall c : a \mid b \wedge a \mid c \Longrightarrow a \mid (b + c)$

   (h) $\forall a \forall b \forall c : a \mid b \wedge b \mid c \Longrightarrow a \mid c$, d v s '$|$' är transitiv

(i) $\forall a \forall b : a \mid b \wedge b \mid a \Longrightarrow a = b \vee a = -b$

4. Betrakta det rationella talet $n = 1014/19$.

   (a) Någon gång för ganska länge sedan lärde ni er (förmodligen) att skriva rationella tal på "blandad form", d v s som ett heltal plus ett rationellt tal mindre än 1 med nämnaren 19. Gör detta för n.

   (b) Heltalet man får brukar kallas för *kvoten* (eller heltalskvoten) och talet i nämnaren av det rationella talet för *resten*. Hur stor kan resten högst bli?

   (c) Om vi betecknar kvoten med q och resten med r, så har vi alltså att

   $$\frac{1014}{19} = q + \frac{r}{19} \text{ eller } 1014 = 19q + r.$$

   Titta på Divisionsalgoritmen i boken (Sats 5.9). Vad har den med det ni just gjorde att göra? Vad säger satsen egentligen?

5. (a) Bestäm alla positiva heltal som delar 98. Hur många fann ni? (Om svaret på förra frågan inte var 6 så försök igen.) Gör samma sak för 105.

   (b) I båda fallen ovan så fann ni (förhoppningsvis) bara ett ändligt antal delare. Kan man alltid vara säker på att det bara blir ändligt många (positiva) delare till ett tal? Varför?

   (c) Formulera vad som menas med *största gemensamma delaren* till två tal.

   (d) Vad är $\text{sgd}(98, 105)$, d v s största gemensamma delaren till dessa tal? Försök med hjälp av första deluppgiften formulera en allmän metod att bestämma största gemensamma delaren till två tal. (OBS: Detta är ingen bra metod om talen är stora.)

6. Vi ska nu härleda en metod som är mycket effektiv för att bestämma största gemensamma delaren även av gigantiska tal. Alla tal i uppgiften förutsättes vara olika heltal.

   (a) Antag att ett tal d delar både a och b. Visa att i så fall delar d också $a + nb$ och b.

   (b) Antag omvänt att ett tal d delar både $a + nb$ och b. Visa att i så fall delar d också a och b.

   (c) Försök från de två första deluppgifterna dra någon slutsats om gemensamma delare till a och b samt $a + nb$ och b.

   (d) Utnyttja nu det du visat för att visa att $\text{sgd}(a, b) = \text{sgd}(a + nb, b)$.

   (e) Titta på Euklides algoritm i boken (Sats 5.15) och hur det du just bevisat ligger till grund för beviset av denna.

   (f) Beräkna $d = \text{sgd}(2331, 2037)$ med hjälp av Euklides algoritm. Bestäm heltal m och n sådana att $d = 2331m + 2037n$ med hjälp av *Euklides utökade algoritm* (se i boken avslutningen av avsnitt 5.1.)

   (g) Kan du hitta alla heltalslösningar till ekvationen $\text{sgd}(2331, 2037) = 2331m + 2037n$ i förra uppgiften? Tips: Börja med att förkorta med största gemensamma delaren. Om det fortfarande känns trögt så ta en titt på avsnitt 5.2 i boken.

   (h) Extrauppgift till den hågade: Visa att om $a = F_{n+1}$ och $b = F_n$ är två på varandra följande Fibonacci-tal så tar Euklides algoritm för att beräkna största gemensamma delaren av dem $n - 1$ steg. (Detta är "värsta tänkbara" givet storleken hos talen.)

7. (a) Vad är ett primtal? Vad är definitionen?

   (b) Gör en lista på de 15 minsta primtalen. (Den kommer att sluta på talet 47.)

   (c) Titta på Aritmetikens fundamentalsats (Sats 5.33) i boken. Den består av två delar: en *existensdel* och en *entydighetsdel*. Vad säger de två olika delarna?

   (d) Om n inte är ett primtal, så har n en primtalsdelare p som uppfyller $p \leq \sqrt{n}$. Varför det? Hur kan man utnyttja detta när man undersöker om ett tal är ett primtal eller inte? Motivera att 349 är ett primtal genom att kontrollera att inga primtal mindre än $\sqrt{349} \approx 18.7$ delar 349.

   (e) Bestäm primtalsfaktoriseringen av 2331 och 2037.

8. Låt $n \geq 2$ vara ett fixt positivt heltal. Man säger att två heltal a och b är kongruenta modulo n om $n \mid a - b$.

   (a) Visa att kongruens modulo n är en ekvivalensrelation på $\mathbb{Z}$.

   (b) Tag $n = 3$. Vad är ekvivalensklassen av 0, 1, 2, 3 och 4? Hur många olika ekvivalensklasser finns det?

   (c) Samma som förra uppgiften fast för godtyckligt n.

   (d) Motivera att två tal är kongruenta modulo n om och endast om de ger samma rest vid division med n.

   (e) Man kan definiera en summa och produkt för ekvivalensklasserna på följande sätt:

   $$[a] + [b] = [a + b] \text{ och } [a] \cdot [b] = [a \cdot b].$$

   Det är inte självklart att detta är korrekta definitioner. Varför inte? (Tänk på att en ekvivalensklass har (oändligt) många olika representanter.)

   (f) Har additionen respektive multiplikationen modulo n någon identitet?

   (g) Gör en multiplikationstabell för multiplikation modulo 5 och modulo 6.

   (h) Kolla i tabellen modulo 6 vad $[2] \cdot [3]$ och $[4] \cdot [3]$ blev. Några kommentarer?

   (i) Kolla i tabellerna vilka klasser som har (multiplikativ) invers. Försök att ge en hypotes för det allmänna fallet vilka klasser som har invers. (Observera att en invers till $[a]$ är en klass $[b]$ sådan att $[a] \cdot [b] = [1]$, d v s $ab + kn = 1$ för något $k \in \mathbb{Z}$.)

9. Det finns en divisionsalgoritm också för *polynom*, d v s funktioner som ges av något på formen

   $$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

   som påminner mycket om motsvarande för heltal. Den säger att om f och $g \neq 0$ är polynom så finns det unika polynom q och r sådana att

   $$f = q \cdot g + r,$$

   med $r = 0$ eller graden av r lägre än graden av g. (Graden av ett polynom är den högsta potens som den innehåller.) Skillnaden är alltså att här är resten av lägre grad istället för att vara "mindre" som saknar tolkning här.

(a) För att beräkna kvoten q och resten r så kan man ställa upp (en stol, trappa eller vad ni fick lära er i grundskolan) på samma sätt som för heltal. I varje steg gäller det här istället att lägga till en term så att termen med högst potens av x försvinner. Om man t ex ska beräkna kvoten av $f(x) = 5x^3 - x^2 + 4x - 5$ och $g(x) = 3x - 2$ så blir det i första steget $k(x) = \frac{5}{3}x^2$ eftersom $\frac{5}{3}x^2 \cdot 3x = 5x^3$. Därefter subtraherar man $k(x) \cdot g(x)$ från $f(x)$ och fortsätter sedan tills graden av det som är kvar är lägre än graden av g.

Beräkna kvoten och resten vid division av $f = 5x^3 - x^2 + 4x - 5$ med $g = 3x - 2$.

(b) Vad händer i specialfallet av divisionsalgoritmen med $g(x) = x - a$ ett förstagradspolynom? Vad blir det för grad på resten?

(c) Motivera att om a är ett nollställe till polynomet f så blir resten vid division med $x - a$ lika med 0, d v s

$$f(x) = (x - a) \cdot q(x).$$

Tips: Skriv ned det ni fick i förra deluppgiften och sätt in $x = a$.

(d) Tredjegradspolynomet $f(x)$ har nollställena 1, 2 och 3 och koefficienten framför x^3 är 1. Motivera varför det måste vara så att $f(x) = (x - 1)(x - 2)(x - 3)$.

(e) Betrakta polynomet

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

där koefficienterna $a_0, a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Antag att polynomet har ett rationellt nollställe $\alpha = p/q$, där p och q är relativt prima heltal (d v s $\text{sgd}(p, q) = 1$). Visa att då måste $p \mid a_0$ och $q \mid a_n$.

(f) Gör en lista över alla tänkbara rationella rötter till ekvationen

$$15x^3 + 10x^2 + 21x + 14 = 0.$$

(Det finns totalt 32 stycken.) Kontrollera att $x = -2/3$ är en lösning. Hur kan man utnyttja detta för att hitta övriga lösningar?

Uppgifter ur boken som rekommenderas för självstudier:

Kapitel 5: 1, 2, 9, 13, 19, 21, 22, 26 (ignorera Eulers Φ-funktion)