**MATEMATIK**
**Göteborgs Universitet**
**Lösningar till**
**Tentamen i Matematik 1 (MMG200), Inledande algebra.**
**Datum: 2016-01-04.**

1. (a) Se boken sidan 231.
   (b) Man kan t ex ta heltalen med (vanlig) addition och multiplikation, alternativt $\mathbb{Z}_n$ där $n > 1$ *inte* är ett primtal med addition och multiplikation modulo $n$.

2. Se boken sidorna 136-137.

3. Definitionerna finns på sidan 61 i boken.

   Exempel på funktion $f : \mathbb{Z} \to \mathbb{Z}$ som är

   - injektiv och surjektiv: $f(x) = x$
   - injektiv men inte surjektiv: $f(x) = x^3$
   - inte injektiv men surjektiv: $f(x) = x$ om $x < 0$, $f(x) = x-1$ om $x \geq 0$
   - varken injektiv eller surjektiv: $f(x) = x^2$

4. (a) Vi använder Euklides algoritm:

$$\begin{aligned} 1254 &= 1 \cdot 789 + 465 \\ 789 &= 1 \cdot 465 + 324 \\ 465 &= 1 \cdot 324 + 141 \\ 324 &= 2 \cdot 141 + 42 \\ 141 &= 3 \cdot 42 + 15 \\ 42 &= 2 \cdot 15 + 12 \\ 15 &= 1 \cdot 12 + 3 \\ 12 &= 4 \cdot 3. \end{aligned}$$

   Från detta drar vi slutsatsen att $\mathrm{SGD}(1254, 789) = 3$.

   (b) Eftersom 3 delar både 1254 och 789 så kommer 3 att dela $1254x+789y$ för alla $x, y \in \mathbb{Z}$. Därför kommer aldrig $1254x + 789y = 7$ om $x, y \in \mathbb{Z}$ och alltså saknas det sådana lösningar.

5. (a) Det finns 9 bokstäver och av dessa finns det två dubbla (K och L) och en trippel (A). Det betyder att det totala antalet möjliga ord är

$$\frac{9!}{2!2!3!} = \frac{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{2 \cdot 2 \cdot 6} = 9 \cdot 8 \cdot 7 \cdot 5 \cdot 3 \cdot 2 = 72 \cdot 210 = 15120.$$

   (b) Det är enklare att räkna ut antalet som innehåller tre A i rad och subtrahera detta från det totala antalet. Antalet möjliga ord med de övriga sex bokstäverna är $6!/(2!)^2$. Man kan sedan placera in A:na på sju olika ställen. Det ger att antalet utan tre A i rad är

$$15120 - 7 \cdot \frac{6!}{2!2!} = 15120 - \frac{7!}{4} = 15120 - 1260 = 13860.$$

6. Definiera först

$$f(n) = \sum_{k=1}^{2n} (-1)^{k+1} \frac{1}{k} \text{ och } g(n) = \sum_{k=n+1}^{2n} \frac{1}{k}.$$

Vi ska då visa att $f(n) = g(n)$ för alla heltal $n \geq 1$. Vi gör ett induktionsbevis.

Basfall: Om $n = 1$ så får vi

$$f(1) = \sum_{k=1}^{2} (-1)^{k+1} \frac{1}{k} = 1 - \frac{1}{2} = \frac{1}{2},$$

$$g(1) = \sum_{k=2}^{2} \frac{1}{k} = \frac{1}{2}.$$

Alltså stämmer det för $n = 1$.

Induktionssteg: Antag att $f(p) = g(p)$ för något $p \geq 1$. Visa att i så fall är $f(p+1) = g(p+1)$. Vi startar med $f(p+1)$ och får om vi i fjärde steget utnyttjar induktionsantagandet att

$$\begin{aligned}
f(p+1) = &\sum_{k=1}^{2(p+1)} (-1)^{k+1} \frac{1}{k} = \sum_{k=1}^{2p} (-1)^{k+1} \frac{1}{k} + \frac{1}{2p+1} - \frac{1}{2p+2} \\
&= f(p) + \frac{1}{2p+1} - \frac{1}{2p+2} = g(p) + \frac{1}{2p+1} - \frac{1}{2p+2} \\
&= \sum_{k=p+1}^{2p} \frac{1}{k} + \frac{1}{2p+1} - \frac{1}{2p+2} \\
&= \sum_{k=(p+1)+1}^{2(p+1)} \frac{1}{k} + \frac{1}{p+1} - \frac{1}{2p+1} - \frac{1}{2p+2} + \frac{1}{2p+1} - \frac{1}{2p+2} \\
&= g(p+1) + \frac{1}{p+1} - 2\frac{1}{2p+2} = g(p+1).
\end{aligned}$$

Enligt indukionsprinipen gäller därmed, med stöd av basfall och induktionssteg, att $f(n) = g(n)$ för alla heltal $n \geq 1$.

7. (a) Funktionen är inte injektiv eftersom $\varphi(p, q) = \varphi(q, p)$ per definition.
   (b) Funktionen är inte surjektiv eftersom vi bara får polynom med reella nollställen så att t.ex. $(0, 1)$ som svarar mot $x^2 + 1$ träffas inte av $\varphi$.
   (c) Polynomet som har $p$ och $q$ som nollställen är

$$(x - p)(x - q) = x^2 - (p + q)x + pq$$

så $\varphi(p, q) = (-(p + q), pq)$. Vi får alltså ekvationssystemet

$$\begin{aligned}
p &= -p - q \\
q &= pq.
\end{aligned}$$

Om $q \neq 0$ så ger den andra ekvationen $p = 1$ vilket ger $q = -2p = -2$ enligt den första. Andra möjligheten är $q = 0$ vilket ger $p = 0$. Vi har alltså två lösningspar: $(0, 0)$ och $(1, -2)$

8. Alla kongruenser är modulo $p$.

   Det finns totalt $p-1$ tal $x$ sådana att $0 < x < p$ så totalt (för alla möjliga tal $b$) finns det $p-1$ lösningar till $x^2 \equiv b$. Dessa förekommer i par eftersom $x^2 = (-x)^2 \equiv (p-x)^2$ och $x \not\equiv -x$ eftersom $p$ är udda primtal. Återstår alltså att visa alla dessa par av lösningar är olika, d v s att det finns $(p-1)/2$ olika lösningar.

   Men vi fick reda på att det fanns $a$ sådant att $a, a^2, \ldots, a^{p-1}$ alla är olika. Därmed är $a^2, (a^2)^2, \ldots (a^{(p-1)/2})^2$ alla olika. Därmed finns det $(p-1)/2$ olika kvadrater och därmed finns det så många olika lösningar till $x^2 \equiv b$. Detta var precis vad som återstod att visa.