Matematiska Institutionen
KTH

Lösningar till några övningar inför lappskrivning nummer 2A på kursen Diskret matematik för D2 och F, SF1631 och SF1630, vt10.

1. Bestäm den största gemensamma delaren och den minsta gemensamma multipeln till de bägge talen 732 och 568.

   Lösning:

   $$\begin{array}{rcrcr} 732 & = & 568 & + & 164 \\ 568 & = & 3 \cdot 164 & + & 76 \\ 164 & = & 2 \cdot 76 & + & 12 \\ 76 & = & 6 \cdot 12 & + & 4 \\ 12 & = & 3 \cdot 4 & + & 0 \end{array}$$

   Den sista ickeförsvinnande resten i Euklides algoritm är den största gemensamma delaren. Ur sambandet

   $$mgm(a,b) = \frac{a \cdot b}{sgd(a,b)}$$

   får vi nu resten av svaret.

   Svar: $sgd(732, 568) = 4$ och $mgm(732, 568) = 103944$.

2. Bestäm en lösning till den diofantiska ekvationen $732x + 568y = 24$.

   Lösning: Bestämmer först en lösning till den diofantiska ekvationen $732x + 568y = 12$, eftersom 12 uppträder som en rest vid Euklides algoritm i uppgift 1. Använder räkningarna i algoritmen.

   $$12 = 164 - 2 \cdot 76 = 164 - 2 \cdot (568 - 3 \cdot 164) = 7 \cdot 164 - 2 \cdot 568 = 7 \cdot (732 - 568) - 2 \cdot 568 = 7 \cdot 732 - 9 \cdot 568.$$

   Alltså

   $$12 = 7 \cdot 732 - 9 \cdot 568,$$

   och därmed

   $$24 = 14 \cdot 732 - 18 \cdot 568.$$

   Svar: T ex $x = 14$ och $y = -18$.

3. Undersök om talet 197 är ett primtal.

   Lösning: Om 197 ej är ett primtal så finns ett primtal $p < \sqrt{197}$ som delar 197, se läroboken eller använd följande resonemang: Om 197 ej är ett primtal så finns primtal p_1, p_2, ..., p_k, $k \geq 2$, sådana att

   $$197 = p_1 \cdot p_2 \cdot ... \cdot p_k$$

   där vi kan förutsätta att

   $$p_1 \leq p_2 \leq ... \leq p_k.$$

   Då gäller säkert att

   $$p_1^2 \leq p_1 p_2 \leq 197 \qquad \Longrightarrow \qquad p_1 \leq \sqrt{197}.$$

   Roten ur 197 är mindre än 15 ty $15^2 = 225$ så det räcker att testa om något av primtalen, 2, 3, 5, 7, 11 eller 13 delar 197, vilket det är lätt att kontrollera att de inte gör.

4. Skriv talet 37512 som en produkt av primtal.

   Lösning:

   $$37512 = 2 \cdot 18756 = 2 \cdot 2 \cdot 9378 = 2^3 \cdot 4689 = 2^3 \cdot 3 \cdot 1563 = 2^3 \cdot 3^2 \cdot 521.$$

   Men 521 är ett primtal eftersom inget av primtalen 2, 3, 5, 7, 11, 13, 17, 19 delar talet, och nästa primtal 23 i kvadrat är större än 521.

   Svar: $37512 = 2^3 \cdot 3^2 \cdot 521$.

5. Visa att om x och y är hela tal sådana att $x^2 - y^2$ är ett jämnt tal så är detta tal också delbart med 4.

   Lösning: Eftersom $x^2 - y^2$ kan faktoriseras

   $$x^2 - y^2 = (x + y)(x - y),$$

   så måste primtalet 2 dela minst en av dessa faktorer eftersom talet 2 förutsattes dela vänstra ledet ovan. Men vi finner att

   $$x + y \equiv_2 x + y - 2y \equiv_2 x - y,$$

   så om $x + y$ är delbart med två så måste även $x + y$ vara det och vice versa. Vi har då

   $$x + y = 2k, \quad x - y = 2k' \qquad \Longrightarrow \qquad (x + y)(x - y) = 2k2k' = 4kk',$$

   och således att talet 4 delar $x^2 - y^2$.

6. Visa att om p är ett primtal så gäller att om p delar a och p delar $a^2 + b^2$ så gäller det att p delar b.

   Lösning:

   $$\left\{ \begin{array}{lcl} p & | & a \\ p & | & a^2 + b^2 \end{array} \right. \quad \Rightarrow \quad p \mid (a^2 + b^2) - a \cdot a \quad \Rightarrow \quad p \mid b^2 \quad \Rightarrow \quad p \mid b \cdot b \quad \Rightarrow \quad p \mid b.$$

7. Lös i ringen Z_{43} ekvationen $34x + 7 = 42$.

   Lösning: Svaret ges av

   $$x = 34^{-1} \cdot (42 - 7) = 34^{-1} \cdot 35.$$

   Beräknar inversen till elementet 34 i ringen Z_{43} enligt standardmetoden med Euklides algoritm:

   $$\begin{array}{rcrcr} 43 & = & 34 & + & 9, \\ 34 & = & 4 \cdot 9 & - & 2 \\ 9 & = & 4 \cdot 2 & + & 1 \end{array}$$

   varur

   $$1 = 9 - 4 \cdot 2 = 9 - 4(4 \cdot 9 - 34) = 4 \cdot 34 - 15 \cdot 9 = 4 \cdot 34 - 15(43 - 34) = 19 \cdot 34 - 15 \cdot 43,$$

   varur

   $$1 \equiv_{43} 19 \cdot 34 - 15 \cdot 43 \equiv_{43} 19 \cdot 34 - 15 \cdot 0 \equiv_{43} 19 \cdot 34.$$

   Vi vet nu att $34^{-1} = 19$ och får då att

   $$x = 19 \cdot 35 = 19 \cdot (-8) = 38 \cdot (-4) = (-5)(-4) = 20.$$

8. Bestäm den minsta positiva rest som erhålles när talet 8^{553} delas med talet 21 respektive delas med talet 23.

   Lösning: Vi ser att
   $$8^2 = 64 = 3 \cdot 21 + 1,$$
   dvs att
   $$8^2 \equiv_{21} 1.$$
   Alltså får vi att
   $$8^{553} \equiv_{21} (8^2)^{276} \cdot 8 \equiv_{21} 1^{276} \cdot 8.$$
   Alltså är 8 en rest vid division med 21, och eftersom den är ickenegativ och mindre än 21 så är det den minsta positiva resten.

   När vi delar med 23 använder vi att 23 är ett primtal och att därmed Fermats lilla sats är tillämpbar. Den ger att
   $$8^{553} \equiv_{23} (8^{22})^{25} \cdot 8^3 \equiv 1^{25}64 \cdot 8 \equiv_{23} (-5) \cdot 8 \equiv_{23} -40 \equiv_{23} 6.$$

9. Bestäm samtliga hela tal x, sådana att
   $$\begin{aligned} x &\equiv 3 \pmod 7, \\ x &\equiv 4 \pmod 8, \\ x &\equiv 6 \pmod 9. \end{aligned}$$

   Lösning Tillämpar kinesiska restsatsen och ansätter
   $$x = A \cdot 8 \cdot 9 + B \cdot 7 \cdot 9 + C \cdot 7 \cdot 8 + n \cdot 7 \cdot 8 \cdot 9.$$
   Löser nu följande tre kongruensekvationer:
   $$A \cdot 8 \cdot 9 \equiv_7 3 \quad \Leftrightarrow \quad 2A \equiv_7 3 \quad \Leftrightarrow \quad A \equiv_7 5,$$
   $$B \cdot 7 \cdot 9 \equiv_8 4 \quad \Leftrightarrow \quad -B \equiv_8 4 \quad \Leftrightarrow \quad B \equiv_8 -4 \equiv_8 4,$$
   samt
   $$C \cdot 7 \cdot 8 \equiv_9 6 \quad \Leftrightarrow \quad -2C \equiv_9 6 \quad \Leftrightarrow \quad C \equiv_9 -3 \equiv_9 6.$$

   SVAR: $x = 5 \cdot 8 \cdot 9 + 4 \cdot 7 \cdot 9 + 6 \cdot 7 \cdot 8 + n \cdot 7 \cdot 8 \cdot 9$ där n är ett godtyckligt heltal.

10. Visa att ekvationen $x^2 = -1$ inte är lösbar i ringen Z_{990}, men att den ekvationen faktiskt är lösbar i ringen Z_{1105}.

    Lösning: Eftersom $990 = 9 \cdot 11 \cdot 2 \cdot 5$ så vet vi att
    $$Z_{990} \approx Z_2 \times Z_5 \times Z_9 \times Z_{11}$$
    varvid elementet x i ringen Z_{990} svarar mot nedanstående element
    $$x \quad \longleftrightarrow \quad (x \pmod 2, x \pmod 5, x \pmod 9, x \pmod{11}),$$
    och elementet x^2 mot elementet
    $$x^2 \quad \longleftrightarrow \quad (x^2 \pmod 2, x^2 \pmod 5, x^2 \pmod 9, x^2 \pmod{11}),$$
    Då uppenbarligen -1 svarar mot elementet $(-1, -1, -1, -1)$ så måste vi finna tal i samtliga dessa ringar vars kvadrater blir lika med -1. Men i ringen Z_{11} är de ”jämna” kvadraterna
    $$\mathcal{Q}_{11} = \{1^2 = (-1)^2 = 1, 2^2 = (-2)^2 = 4, 3^2 = (-3)^2 = 9, 4^2 = (-4)^2 = 5, 5^2 = (-5)^2 = 3\}.$$
    Ingen jämn kvadrat blir $-1 = 10$ i ringen Z_{11}. En lösning saknas alltså.

Däremot gäller att $1105 = 5 \cdot 221 = 5 \cdot 13 \cdot 17$ och vid närmare kontroll finner man att

$$2^2 \equiv_5 -1, \qquad 8^2 \equiv_{13} -1, \qquad 4^2 \equiv_{17} -1,$$

och allstå finns (a, b, c) i $Z_5 \times Z_{13} \times Z_{17}$ vars kvadrat är $(-1, -1, -1)$, t ex

$$(2, 8, 4)^2 = (-1, -1, -1).$$

En lösning x till ekvationen $x^2 = -1$ ges alltså t ex av den "kinesiska restsatslösning" till kongruenserna

$$x \equiv_5 2, \qquad x \equiv_{13} 8, \qquad x \equiv_{17} 4,$$

som ligger i intervallet $0 \leq x < 1105$.

11. Bestäm samtliga hel tal x sådana att

$$(x - 7)(x - 12) \equiv 0 \pmod{91}.$$

Łösning: Vi finner att $91 = 7 \cdot 13$ och allså skall det gälla att

$$7 \cdot 13 \mid (x - 7)(x - 12).$$

Detta ger fyra möjligheter:

$$7 \cdot 13 \mid (x - 7) \qquad \Longleftrightarrow \qquad x = 7 + k \cdot 91,$$

eller

$$7 \cdot 13 \mid (x - 12) \qquad \Longleftrightarrow \qquad x = 12 + k \cdot 91,$$

eller

$$x \equiv_7 7, \quad \text{och} \quad x \equiv_{13} 12,$$

varur vi lätt ser lösningen m hj av kinesiska restsatsen

$$x = -14 + k \cdot 91.$$

Eller till slut att

$$x \equiv_{12} 7, \quad \text{och} \quad x \equiv_7 12,$$

som vi raskt löser enligt formeln för kinesiska restsatsen till

$$x = 19 + k \cdot 91.$$

12. Bestäm ringar Z_n respektive Z_m, där $n \geq 10$ och $m \geq 10$, sådana att ekvationen $x^2+x+1 = 0$ är lösbar i Z_n men inte i Z_m.

Lösning En kvadratkomplettering ger

$$0 = x^2 + x + 1 = (x + 2^{-1})^2 - (2^{-1})^2 + 1, \qquad \Longleftrightarrow \qquad (x^2 + 2^{-1})^2 = (2^{-1})^2 - 1.$$

Nödvändigt och tillräckligt för lösbarhet är allså att uttrycket $(2^{-1})^2 - 1$ är en jämn kvadrat.

Lite trial and error ger att i ringen Z_{11} så är $(2^{-1})^2 - 1 = 6^2 - 1 = 2 - 1 = 1$, som ju är en jämn kvadrat. Ekvationen är alltså lösbar i ringen Z_{11}.

Om ekvationen skulle vara lösbar i ringen Z_{12} skulle det finnas tal x sådana att talet 12 skulle dela $x^2 + x + 1$ dvs

$$x^2 + x + 1 = n \cdot 12 = n \cdot 6 \cdot 2 = k \cdot 2$$

varur

$$x^2 + x + 1 \equiv_2 0 \qquad \Longleftrightarrow \qquad x(x + 1) \equiv_2 1,$$

dvs $x(x + 1)$ skulle vara ett udda tal.

Men talen x och $x + 1$ följer på varandra och det ena är då jämnt eftersom vartannat tal är jämnt. Då måste produkten $x(x + 1)$ vara ett jämnt tal.

Det finns inga tal som både är udda och jämna, så ekvationen kan inte vara lösbar i ringen Z_{12}.