Lösningsförslag
Inlämningsuppgifter, omgång II

Elementär Talteori
Sommaren 2003

Uppgift 1. För enkelhets skull skriver vi om ekvationen till

$$x^2 \equiv 49 \pmod{300}.$$

Eftersom $300 = 2^2 \cdot 3 \cdot 5^2$ är ekvationen ekvivalent med systemet

$$\begin{cases} x^2 \equiv 49 \pmod 4 \\ x^2 \equiv 49 \pmod 3 \\ x^2 \equiv 49 \pmod{25} \end{cases}$$

Dessa löser vi var för sig. Den första är ekvivalent med

$$x^2 \equiv 1 \pmod 4$$

Vilket har lösningarna $x \equiv 1, 3 \pmod 4$, vilket kollas lätt genom testning. På samma sätt ser vi att den andra är ekvivalent med $x \equiv 1, 2 \pmod 3$. Enligt sats på övningen den 7:e augusti har den tredje ekvationen som mest två lösningar (modulo 25), det är enkelt att se att $x \equiv 7, -7 \pmod{25}$ eller $x \equiv 7, 18 \pmod{25}$. För att sammanfatta, den ursprungliga ekvationen är ekvivalent med att någon av följande åtta ekvationssystem är uppfyllt:

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 3 \\ x \equiv 7 \pmod{25} \end{cases} \quad \begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 3 \\ x \equiv 18 \pmod{25} \end{cases} \quad \begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 7 \pmod{25} \end{cases}$$

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 18 \pmod{25} \end{cases} \quad \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 3 \\ x \equiv 7 \pmod{25} \end{cases} \quad \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 3 \\ x \equiv 18 \pmod{25} \end{cases}$$

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 7 \pmod{25} \end{cases} \quad \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 18 \pmod{25} \end{cases}$$

Dessa åtta system löser vi antingen genom att gissa eller med tekniken från kinesiska restsatsen (kinesiska restsatsen säger också att varje system har en unik lösning modulo 300).

Med beteckningar från kinesiska restsatsen är $n_1 = 4$, $n_2 = 3$, $n_3 = 25$, $N = 300$, $N_1 = 75$, $N_2 = 100$ och $N_3 = 12$. Vi hittar inverser x_i till N_i modulo n_i genom att gissa eller med Euklides algoritm: $x_1 = -1$, $x_2 = 1$ och $x_3 = -2$. Lösningen till systemet

$$\begin{cases} x & \equiv a_1 \pmod 4 \\ x & \equiv a_2 \pmod 3 \\ x & \equiv a_3 \pmod{25} \end{cases}$$

är nu $x \equiv a_1 \cdot 75 \cdot (-1) + a_2 \cdot 100 \cdot 1 + a_3 \cdot 12 \cdot (-2) \equiv -75a_1 + 100a_2 - 24a_3 \pmod{300}$. Alltså ger våra 8 system i tur och ordning att

$$x \equiv -143, -407, -43, -307, -293, -557, -193, -457 \pmod{300}.$$

På enklare form blir svaret

$$x \equiv 157, 193, 257, 293, 7, 43, 107, 143 \pmod{300}.$$

Uppgift 2. Lår r vara en primitiv rot till p (sådan finns enligt sats 8.6). Enligt sats 8.4 är $1, r, r^2, r^3, \ldots, r^{p-2}$ kongruneta med $1, 2, 3, \ldots, p-1$ i någon ordning modulo p. Alltså är

$$1^n + 2^n + 3^n + \ldots + (p-1)^n \equiv 1^n + (r^1)^n + (r^2)^n + \ldots + (r^{p-2})^n \pmod p$$

Antag nu att $(p-1) \not| n$, så att $r^n \not\equiv 1 \pmod p$ så $(r^n - 1)x \equiv 1 \pmod p$ är lösbar (följer av att $\mathrm{ord}_p(r) = p-1$). Med formeln för en geometrisk summa är högerledet lika med

$$\frac{r^{(p-1)n} - 1}{r^n - 1}.$$

Eftersom $r^{p-1} \equiv 1 \pmod p$ så har vi

$$\frac{r^{(p-1)n} - 1}{r^n - 1} = \frac{(r^{p-1})^n - 1}{r^n - 1} \equiv \frac{1^n - 1}{r^n - 1} = 0 \pmod p.$$

Om istället $(p-1)|n$ så är $n = (p-1)k$ för något tal och alltså är $r^n = r^{(p-1)k} = (r^{p-1})^k \equiv 1^k = 1 \pmod p$, dvs

$$1^n + 2^n + 3^n + \ldots + (p-1)^n \equiv 1 + 1 + \ldots + 1 = (p-1) \equiv -1 \pmod p$$

precis som vi ville ha.

Uppgift 3. Wilsons sats säger att $70! \equiv -1 \pmod{71}$, resten r som vi söker måste alltså uppfylla att $18r \equiv -1 \pmod{71}$. Inversen till 18 modulo 71 hittar vi med Euklides algoritm:

$$\begin{aligned} 71 &= 3 \cdot 18 + 17 \\ 18 &= 1 \cdot 17 + 1 \\ 17 &= 17 \cdot 1 + 0 \end{aligned}$$

Baklänges ger nu detta

$$1 = 18 - 17 = 18 - (71 - 3 \cdot 18) = 4 \cdot 18 - 71$$

det vill säga

$$4 \cdot 18 \equiv 1 \pmod{71}.$$

Multiplicera med 4 på båda sidor:

$$4 \cdot 18r \equiv -4 \pmod{71}$$

eller

$$r \equiv -4 \equiv 67 \pmod{71}.$$

Resten blir alltså 67.

Uppgift 4. a) Vi har att $\text{ord}_7 2 = 3$, så vi kollar tre fall, nämligen när n är kongruent med 0, 1 eller 2 modulo 3. Om $n \equiv 0 \pmod 3$ så finns k så att $2^n + 1 = 2^{3k} + 1 = 8^k + 1 \equiv 1^k + 1 = 2 \not\equiv 0 \pmod 7$. Om $n \equiv 1 \pmod 3$ så finns k så att $2^n + 1 = 2^{3k+1} + 1 = 2 \cdot 8^k + 1 \equiv 2 \cdot 1^k + 1 \equiv 1 \not\equiv 0 \pmod 7$. Slutligen, om $n \equiv 2 \pmod 3$ så finns k så att $2^n + 1 = 2^{3k+2} + 1 = 4 \cdot 8^k + 1 \equiv 4 \cdot 1^k + 1 \equiv 2 \not\equiv 0 \pmod 7$. Det vill säga $2^n + 1 \not\equiv 0 \pmod 7$ för alla $n \geq 0$.
b) Om $n = 6k + 4$ får vi

$$10^n + 3 \equiv 3^{6k+4} + 3 = 3^4(3^6)^k + 3 \equiv 4 \cdot 1 + 3 = 7 \equiv 0 \pmod 7,$$

så 7 delar alla tal på formen $10^{6k+4} + 3$, vilket det finns oändligt många av (ett för varje val av k).

Uppgift 5. Att 97 delar $n^2 - 85$ är ekvivalent med att $n^2 \equiv 85 \pmod{97}$. Att det finns ett sådant n är samma sak som att säga att 85 är en kvadratisk rest, dvs om Legendre symbolen $(85/97) = 1$.

$$\begin{aligned}\left(\frac{85}{97}\right) = \left(\frac{17}{97}\right)\left(\frac{5}{97}\right) = \left(\frac{97}{17}\right)\left(\frac{97}{5}\right) = \left(\frac{12}{17}\right)\left(\frac{2}{5}\right) = -\left(\frac{12}{17}\right) \\ = -\left(\frac{4}{17}\right)\left(\frac{3}{17}\right) = -\left(\frac{17}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1.\end{aligned}$$

Svaret på frågan är alltså ja.

Uppgift 6. Kinesiska restsatsen! Översatt till matematiska blir uppgifterna (där x är antalet bananer) att hitta minsta positiva lösningen till systemet

$$\begin{cases} x \equiv 0 \pmod{17} \\ x \equiv 6 \pmod{11} \\ x \equiv 0 \pmod{16} \end{cases}$$

I notation från kinesiska restsatsen har vi alla lösningar till systemet givet av

$$x \equiv 0 \cdot N_1 \cdot x_1 + 6 \cdot N_2 \cdot x_2 + 0 \cdot N_3 \cdot x_3 \equiv 6 \cdot N_2 \cdot x_2 \pmod{11 \cdot 16 \cdot 17}$$

Vi har $N_2 = 17 \cdot 16 = 272$, och x_2 är invers till N_2 modulo 11, som vi hittar med Euklides algoritm: $x_2 = -4$. Vilket ger lösningarna

$$x \equiv 6 \cdot 272 \cdot (-4) \equiv -6528 \pmod{2992}.$$

Det minsta talet x som satisfierar detta är alltså $-6528 + 3 \cdot 2992 = 2448$. Antalet bananer är allltså 2448.

Fredrik Engström, email: `engstrom@math.chalmers.se`