Lösningsförslag
Tenta 2004–01–10

Elementär Talteori
Sommaren 2003

Uppgift 1.

$$3^{2n+1} + 2^{n+2} = 3 \cdot (3^2)^n + 2^2 \cdot 2^n = 3 \cdot 9^n + 4 \cdot 2^n \equiv$$
$$3 \cdot 2^n + 4 \cdot 2^n = 7 \cdot 2^n \equiv 0 \pmod 7.$$

Uppgift 2. (a) Nej. För alla heltal x, y oxh z är vänsterledet delbart med 3, men högerledet är det ej.
(b) Nej. Om vi räknar modulo 13 så blir ekvationen $x^2 \equiv 6 \pmod{13}$, och 6 är ingen kvadratisk rest modulo 13 ty

$$\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = -\left(\frac{3}{13}\right) = -\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Uppgift 3. Genom att lösa var kongruensekvation för sig får vi det ekvivalenta systemet:

$$\begin{cases} x & \equiv -1 \pmod 9 \\ x & \equiv 6 \pmod{11} \\ x & \equiv 8 \pmod{25} \end{cases}$$

Med notation från kinesiska restsatsen blir den allmänna lösningen

$$x \equiv -N_1x_1 + 6N_2x_2 + 8N_3x_3 \pmod{9 \cdot 11 \cdot 25}$$

Där $N_1 = 11 \cdot 25$, $N_2 = 9 \cdot 25$ och $N_3 = 9 \cdot 11$. Vi hittar x_1, x_2 och x_3 genom att testa oss fram. Vi får $x_1 = 2$, $x_2 = -2$ och $x_3 = -1$ och den allmänna lösningen blir

$$x \equiv -11 \cdot 25 \cdot 2 + 6 \cdot 9 \cdot 25 \cdot (-2) + 8 \cdot 9 \cdot 11 \cdot (-1) = -4042 \equiv 908 \pmod{2475}$$

ty $9 \cdot 11 \cdot 25 = 2475$.

Uppgift 4. **(a)** 4 stycken. Enligt sats 8.12 i Burton är

$$x^k \equiv a \pmod{n},$$

där $\mathrm{SGD}(a,n)=1$, lösbar omm

$$a^{\phi(n)/\mathrm{SGD}(k,\phi(n))} \equiv 1 \pmod{n}$$

och antalet inkongruenta lösningar modulo 17 är, i så fall, $\mathrm{SGD}(k,\phi(n))$.

I vårt fall är ekvationen lösbar ty $\mathrm{SGD}(16,17)=1$ och

$$16^{\phi(17)/\mathrm{SGD}(12,\phi(17))} \equiv (-1)^{16/4} = 1 \pmod{17}.$$

Antalet inkongruenta lösningar modulo 17 är då $\mathrm{SGD}(12,\phi(17))=4$.

(b) Noll, ty

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$$

så 3 är ingen kvadratisk rest modulo 17 och om ekvationen hade haft en lösning, x_0, hade $(x_0^6)^2 \equiv 3 \pmod{17}$ dvs 3 hade varit en kvadratsik rest modulo 17.

Uppgift 5. Antag $a \equiv a' \pmod{n}$ och $b \equiv b' \pmod{n}$, då finns heltal k,l så att $a' = a+kn$ och $b' = b+ln$. Nu är

$$a+b = a'+b'+kn+ln = a'+b'+(k+l)n,$$

så $a+b \equiv a'+b' \pmod{n}$. Dessutom är

$$ab = (a'+kn)(b'+ln) = a'b'+a'ln+knb'+kln^2 = a'b'+(a'l+b'k+kln)$$

och alltså har vi att $ab \equiv a'b' \pmod{n}$.

Uppgift 6. Skriv alla bråk i vänsterledet på gemensamt bråkstreck. Då får vi

$$\frac{\frac{(p-1)!}{1}+\frac{(p-1)!}{2}+\frac{(p-1)!}{3}+\ldots+\frac{(p-1)!}{p-1}}{(p-1)!} = \frac{a}{b}.$$

Eftersom $p \nmid (p-1)!$ så räcker det att visa att p delar täljaren i vänsterledet, ty i så fall delar p heltalet vi får om vi multiplicerar vänsterledet med b, det vill säga a.

Enligt Wilsons sats är $(p-1)! \equiv -1 \pmod{p}$ och alltså, om $1 \le k \le p-1$, $(p-1)!/k \equiv -l \pmod{p}$ där $kl \equiv 1 \pmod{n}$, ty

$$\frac{(p-1)!}{k}\cdot kl = (p-1)!\cdot l \equiv -l \pmod{n}.$$

Inverserna till 1, 2, ..., $p-1$ är precis 1, 2, ..., $p-1$ i någon ordning, så

$$\frac{(p-1)!}{1}+\frac{(p-1)!}{2}+\ldots+\frac{(p-1)!}{p-1} \equiv -(1+2+\ldots+(p-1)) = -\frac{p-1}{2}p \equiv 0 \pmod{p}.$$

Uppgift 7. **(a)** Om inte så skulle $A = 4(p_2p_3 \ldots p_k) + 3 = q_1q_2 \ldots q_l$ där alla q_i var primtal på formen $4n + 1$ (observera att A är udda). Men produkten av två tal på formen $4n + 1$ är också på den formen så det skulle betyda att A var på formen $4n + 1$ vilket är en motsägelse.
(b) Låt p vara ett primtal på formen $4n + 3$ som delar A. Om $p = 3$ så har vi $3 \mid A - 3$ dvs $3 \mid 4(p_2p_3 \ldots p_k)$ och alltså att $3 \mid p_i$ för något i, vilket är en motsägelse mot att $p_i \neq 3$. Om $p \neq 3$ så måste $p = p_i$ för något $i \geq 2$ och då har vi att $p \mid A - 4(p_2p_3 \ldots p_k)$ dvs $p \mid 3$, vilket också är en motsägelse (ty $p \neq 3$).

Uppgift 8. Ja. Vi vill hitta två heltal a och b sådana att

$$\frac{a}{87} + \frac{b}{143} = \frac{7}{87 \cdot 143}$$

dvs sådana att $143a + 87b = 7$. Euklides algoritm på 143 och 87 ger

$$\begin{aligned}
143 &= 1 \cdot 87 + 56 \\
87 &= 1 \cdot 56 + 31 \\
56 &= 1 \cdot 31 + 25 \\
31 &= 1 \cdot 25 + 6 \\
25 &= 4 \cdot 6 + 1
\end{aligned}$$

Lindar vi nu upp detta "baklänges" får vi

$$\begin{aligned}
1 &= 25 - 4 \cdot 6 = 25 - 4 \cdot (31 - 25) = 5 \cdot 25 - 4 \cdot 31 = 5 \cdot (56 - 31) - 4 \cdot 31 = \\
&\quad 5 \cdot 56 - 9 \cdot 31 = 5 \cdot 56 - 9 \cdot (87 - 56) = 14 \cdot 56 - 9 \cdot 87 = 14 \cdot (143 - 87) - 9 \cdot 87 = \\
&\quad 14 \cdot 143 - 23 \cdot 87
\end{aligned}$$

så $7 = 7 \cdot 14 \cdot 143 + 7 \cdot (-23) \cdot 87$. Alltså är

$$\frac{98}{87} \quad \text{och} \quad -\frac{161}{143}$$

två sådana tal.

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