Lösningsförslag
Tenta 2003–08–16

Elementär Talteori
Sommaren 2003

Uppgift 1. Vi räknar kongruens modulo 135.

$$748^{217} \equiv 73^{217} \pmod{135}$$

$\phi(135) = \phi(3^3 \cdot 5) = \phi(3^3)\phi(5) = (3^3 - 3^2)(5-1) = 18 \cdot 4 = 72$ så

$$73^{217} = 73^{3\cdot 72+1} = 73^{3\cdot 72} \cdot 73 = (73^{72})^3 \cdot 73 \equiv 1^3 \cdot 73 = 73 \pmod{135}$$

ty $\mathrm{SGD}(73, 135) = 1$ (Eulers sats). Resten blir alltså 73.

Uppgift 2. En diofantisk ekvation $ax + by = c$ är lösbar omm $\mathrm{SGD}(a, b) \mid c$. I (a) har vi $\mathrm{SGD}(126, -165) = \mathrm{SGD}(2 \cdot 3^2 \cdot 7, 3 \cdot 5 \cdot 11) = 3$ vilket delar 231. Med Euklides algoritm hittar vi lösning till ekvationen $126x - 165y = 3$:

$$\begin{aligned} 165 &= 1 \cdot 126 + 39 \\ 126 &= 3 \cdot 39 + 9 \\ 39 &= 4 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

Lindar vi nu upp detta "baklänges" får vi

$3 = 39-4\cdot 9 = 39-4(126-3\cdot 39) = 13\cdot 39-4\cdot 126 = 13(165-126)-4\cdot 126 = 13\cdot 165-17\cdot 126.$

Multiplicera allt detta med $231/3 = 77$ så får vi sambandet

$$(13 \cdot 77) \cdot 165 - (17 \cdot 77) \cdot 126 = 231.$$

En specifik lösning blir alltså $x_0 = -17 \cdot 77, y_0 = -13 \cdot 77$. Den allmänna lösningen blir då

$$x = -17 \cdot 77 + \frac{-165}{3}k \quad y = -13 \cdot 77 - \frac{126}{3}k,$$

det vill säga

$$x = -1309 - 55k \quad y = -1001 - 42k,$$

I (b) har vi $\mathrm{SGD}(70, 75) = 5 \nmid 137$ så den har ej lösningar.

Uppgift 3. Översatt till matematiska undras det om följande system har en lösning och i så fall vilken den minsta positiva lösningar är:

$$\begin{cases} x & \equiv 0 \pmod 4 \\ x & \equiv 3 \pmod 5 \\ x & \equiv 4 \pmod 7 \end{cases}$$

Med notation från kinesiska restsatsen blir den allmänna lösningen

$$x \equiv 0N_1x_1 + 3N_2x_2 + 4N_3x_3 \pmod{4 \cdot 5 \cdot 7}$$

Där $N_2 = 4 \cdot 7 = 28$ och $N_3 = 4 \cdot 5 = 20$, vi hittar x_2 och x_3 genom att testa oss fram. Vi får $x_2 = 2$ och $x_3 = -1$ och den allmänna lösningen blir

$$x \equiv 3 \cdot 28 \cdot 2 + 4 \cdot 20 \cdot (-1) = 168 - 80 = 88 \pmod{140}.$$

Sekund 88 slår alltså alla tre klockorna samtidigt för första gången, dvs det $88/4+1 = 23$:e (glöm inte slaget på 0:te sekunden) slaget för den första klockan. (Svaret borde kanske vara 22 eftersom det frågas om hur många slag första klockan har slått *innan* alla slår tillsammans.)

Uppgift 4. a)

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$$

Detta betyder att alla tre Legendre symboler inte kan vara -1.

b) 1, 4, och 9 är kvadratiska rester för alla p så antingen är $1, 2$ eller $4, 5$ eller $9, 10$ två på varandra följande kvadratiska rester modulo p.

c)

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$$

Detta betyder att alla tre Legendre symboler ej kan vara -1, dvs en av 2, 3, eller 6 är en kvadratisk rest modulo p. Detta betyder att antingen $2, 4$ eller $1, 3$ eller $4, 6$ är kvadratiska rester.

Uppgift 5. Möbius inversionsformel ger att

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$$

så

$$g(12) = \sum_{d|12} \mu(d) f(\frac{12}{d}) = \mu(1)f(12) + \mu(2)f(6) + \mu(3)f(4) +$$
$$\mu(4)f(3) + \mu(6)f(2) + \mu(12)f(1) = f(12) - f(6) - f(4) + f(2).$$

Det vill säga

$$g(12) = f(12) - f(6) - f(4) + f(2).$$

Uppgift 6. Inget par av de 10 talen

$$1\cdot 3, 2\cdot 3, 3\cdot 3, 4\cdot 3, 5\cdot 3, 6\cdot 3, 7\cdot 3, 8\cdot 3, 9\cdot 3, 10\cdot 3$$

är kongruenta (modulo 11), och inget tal är kongruent (modulo 11) med noll. Detta betyder att talen måste vara kongruenta med $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ i någon ordning. Multiplicerar vi ihop dem får vi

$$(1\cdot 3)\cdot(2\cdot 3)\cdot(3\cdot 3)\cdot(4\cdot 3)\cdot(5\cdot 3)\cdot(6\cdot 3)\cdot(7\cdot 3)\cdot(8\cdot 3)\cdot(9\cdot 3)\cdot(10\cdot 3) \equiv 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10 \pmod{11}$$

Det vill säga

$$10!3^{10} \equiv 10! \pmod{11}$$

och eftersom $\mathrm{SGD}(10!, 11) = 1$ kan vi stryka $10!$ från båda sidorna och vi får

$$3^{10} \equiv 1 \pmod{11}.$$

Uppgift 7. a) $\mathrm{SGD}(a, b)$ är det största heltal d sådant att $d \mid a$ och $d \mid b$.
b)

$$\begin{aligned} 1872 &= 4\cdot 458 + 40 \\ 458 &= 11\cdot 40 + 18 \\ 40 &= 2\cdot 18 + 4 \\ 18 &= 4\cdot 4 + 2 \\ 4 &= 2\cdot 2 \end{aligned}$$

Så $\mathrm{SGD}(1872, 458) = 2$.
c) Vi vill visa att största talet som delar både a och b är samma som det största talet som både delar b och r. Det gör vi genom att visa att paren har exakt samma delare. Tag en delare d till a och b, dvs $d \mid a$ och $d \mid b$, då gäller att $d \mid bq$ och vi får att $d \mid (a - bq)$ dvs $d \mid r$. Om å andra sidan $d \mid b$ och $d \mid r$ så har vi att $d \mid bq$ och vi får att $d \mid (bq + r)$, dvs $d \mid a$.

Uppgift 8. Påståendet är falskt! En kvadrat är kongruent med 0, 1, eller 4 modulo 8, dvs $x^2 \equiv 0, 1, 4 \pmod{8}$ för alla heltal x. Ett tal som kan skrivas som produkten av tre kvadrater kan alltså inte vara kongruent med 7. Tag $a = 2^2 + 1^2 + 0^2 = 5$ och $b = 1^2 + 1^2 + 1^2 = 3$. Produkten $ab = 5\cdot 3 = 15$ är kongruent med 7 modulo 8, så den kan ej skrivas som summan av tre kvadrater.

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