Lösningsförslag till
tentan i elementär talteori 2003–09–20

Uppgift 1. Vi reducerar 91^{243} modulo 100. Eftersom $\mathrm{SGD}(91, 100) = 1$ kan vi använda Eulers sats. Vi har att $\phi(100) = \phi(2^2)\phi(5^2) = 2 \cdot 20 = 40$ så enligt Euler får vi

$$91^{243} \equiv 91^{40 \cdot 6 + 3} \equiv (91^{40})^6 \cdot 91^3 \equiv (-9)^3 \equiv -729 \equiv 71 \pmod{100}.$$

Entalssiffran i 91^{243} är alltså 1 och tiotalssiffran är 7.

Uppgift 2.

(a) Talen mellan 1 och 500 som delas av både 2 och 3 är precis följande multipler av sex: $6, 2 \cdot 6, 3 \cdot 6, \ldots, 83 \cdot 6$. Svaret är alltså 83.

(b) Som i (a)-uppgiften får man att mellan 1 och 500 finns det precis 250 tal som delas av 2 och 166 tal som delas av 3. Drar vi 250+166 ifrån 500 får vi antalet tal som inte delas av vare sig 2 eller 3 så när som på att vi har dragit ifrån antalet tal som delas av både 2 och 3 en gång för mycket, dvs. vi har dragit bort 83 för mycket. Alltså, antalet tal mellan 1 och 500 som inte delas av vare sig 2 eller 3 är: $500 - 250 - 166 + 83 = 167$.

Uppgift 3. Betrakta den diofantiska ekvationen

$$78x + 102y = 12. \tag{1}$$

En lösning till denna (om en sådan finns) hittas genom att utföra Euklides algoritm framlänges och baklänges:

$$\begin{aligned} 102 &= 78 + 24 \\ 78 &= 3 \cdot 24 + 6 \\ 24 &= 4 \cdot 6 + 0 \end{aligned}$$

så att

$$6 = 78 - 3 \cdot 24 = 78 - 3(102 - 78) = 4 \cdot 78 - 3 \cdot 102.$$

Alltså är $x = 8$ och $y = -6$ en lösning till (1). Studenten kan således lösa sin uppgift genom att först hälla i åtta 78dl-spänner i blandkaret och sedan ösa ur sex 102dl-spänner. Kvar i karet har han då precis 12dl.

Uppgift 4. Eftersom r uppfyller $er \equiv 1 \pmod{\phi(m)}$ gäller att $er = 1 + k\phi(m)$ för något heltal k. Enligt Eulers sats gäller då

$$a^r \equiv (x^e)^r \equiv x^{er} \equiv x^{1+k\phi(m)} \equiv x(x^{\phi(m)})^k \equiv x \pmod{m}.$$

Vidare, eftersom $0 \leq x < m$ och talen mellan 0 och m är inkongruenta modulo m (enl. divisionsalg.) är x det unika tal mellan 0 och m som är kongruent med a^r modulo m.

Uppgift 5. Funktionen f_1 är multiplikativ ty givet två godtyckliga heltal m och n (inte nödvändigtvis relativt prima) gäller

$$f_1(mn) = 1 = 1 \cdot 1 = f_1(m)f_1(n).$$

Funktionen f_2 är inte multiplikativ eftersom

$$f_2(mn) = 2 \neq 2 \cdot 2 = f_2(m)f_2(n).$$

Funktionen f_3 är multiplikativ enligt sats 6.4 eftersom funktionen $g(n) = n^3$ är det.
Funktionen f_4 är också multiplikativ. Detta följer inte direkt från satserna utan vi får argumentera som följer. Låt m och n vara relativt prima heltal. Om nu d är en delare till mn så kan d entydigt skrivas $d = d_1d_2$ där $d_1 \mid m$ och $d_2 \mid n$ och $\text{SGD}(d_1, d_2) = 1$, se lemma på sidan 107. Alltså får vi

$$\begin{aligned} f_4(mn) &= \sum_{d|mn} \mu(\frac{mn}{d})\phi(d) = \sum_{d_1|m, d_2|n} \mu(\frac{m}{d_1}\frac{n}{d_2})\phi(d_1d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} \mu(\frac{m}{d_1})\mu(\frac{n}{d_2})\phi(d_1)\phi(d_2) \\ &= \sum_{d_1|m} \mu(\frac{m}{d_1})\phi(d_1) \sum_{d_2|n} \mu(\frac{n}{d_2})\phi(d_2) \\ &= f_4(m)f_4(n). \end{aligned}$$

Uppgift 6.

(a) Om m är ett heltal större än 2 gäller att $m = 2^k$ där $k \geq 2$ eller $m = p^l n$ där p är ett udda primtal som inte delar n. I första fallet får vi

$$\phi(m) = \phi(2^k) = 2^{k-1}$$

som är jämnt eftersom $k \geq 2$ och i andra fallet får vi

$$\phi(m) = \phi(p^l)\phi(n) = (p^l - p^{l-1})\phi(n)$$

som också är jämnt eftersom $p^l - p^{l-1}$ är jämnt (differansen mellan två udda tal).

(b) Enligt uppgift (a) har vi att $2 \mid \phi(m)$ och $2 \mid \phi(n)$ och eftersom

$$\text{SGD}(a, mn) = 1$$

har vi att $\text{SGD}(a, m) = \text{SGD}(a, n) = 1$ så enligt Eulers sats får vi

$$a^{\frac{\phi(m)\phi(n)}{2}} \equiv (a^{\phi(m)})^{\frac{\phi(n)}{2}} \equiv 1 \pmod{m}$$

och

$$a^{\frac{\phi(m)\phi(n)}{2}} \equiv (a^{\phi(n)})^{\frac{\phi(m)}{2}} \equiv 1 \pmod{n}.$$

Alltså delas $a^{\frac{\phi(m)\phi(n)}{2}} - 1$ av både m och n. Då m och n är relativt prima måste därför $a^{\frac{\phi(m)\phi(n)}{2}} - 1$ delas av mn, dvs

$$a^{\frac{\phi(m)\phi(n)}{2}} \equiv 1 \pmod{mn}.$$

Detta visar att mn saknar primitiva rötter eftersom $\phi(m)\phi(n)/2 < \phi(m)\phi(n) = \phi(mn)$.

Uppgift 7. Eftersom $2201 = 31 \cdot 71$ är kongruensekvationen ekvivalent med

$$\begin{cases} x^2 \equiv 671 \pmod{31} \\ x^2 \equiv 671 \pmod{71} \end{cases}$$

Vi evaluerar Legendresymboler för att se om detta är lösbart.

$$\left(\frac{671}{31}\right) = \left(\frac{20}{31}\right) = \left(\frac{2^2}{31}\right)\left(\frac{5}{31}\right) = \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$$\left(\frac{671}{71}\right) = \left(\frac{32}{71}\right) = \left(\frac{2 \cdot 4^2}{71}\right) = \left(\frac{2}{71}\right) = 1$$

eftersom $71 \equiv 7 \pmod{8}$. Alltså finns precis 2 lösningar $a_1, -a_1$ (modulo 31) till den första ekvationen och precis 2 lösningar $a_2, -a_2$ (modulo 71) till den

andra. Alltså är x en lösning till ekvationssystemet ovan omm x är en lösning till något av följande fyra linjära ekvationssystem.

$$\begin{cases} x \equiv a_1 \pmod{31} \\ x \equiv a_2 \pmod{71} \end{cases} \qquad \begin{cases} x \equiv a_1 \pmod{31} \\ x \equiv -a_2 \pmod{71} \end{cases}$$
$$\begin{cases} x \equiv -a_1 \pmod{31} \\ x \equiv a_2 \pmod{71} \end{cases} \qquad \begin{cases} x \equiv -a_1 \pmod{31} \\ x \equiv -a_2 \pmod{71} \end{cases}$$

Kinesiska restsatsen producerar en entydig lösning modulo 2201 till vart och ett av dessa. Vidare kan kan inga två av dessa vara kongruenta modulo 2201 ty om x_0 och x_1 vore lösningar till, säg översta radens ekvationssystem, och $x_0 \equiv x_1 \pmod{2201}$ så skulle $a_2 \equiv x_0 \equiv x_1 \equiv -a_2 \pmod{71}$, vilket är omöjligt. Alltså finns precis fyra lösningar till ursprungsekvationen.

Uppgift 8. Vad vi skall visa är att $7 \,|\, \sum_{i=0}^{r} a_i 10^i$ omm $7 \,|\, \sum_{i=1}^{r} a_i 10^{i-1} - 2a_0$. Men

$$\sum_{i=1}^{r} a_i 10^{i-1} - 2a_0 \equiv 0 \pmod{7}$$

gäller omm

$$10(\sum_{i=1}^{r} a_i 10^{i-1} - 2a_0) \equiv 0 \pmod{7}$$

dvs omm

$$\sum_{i=1}^{r} a_i 10^i - 20a_0 \equiv a_0 + \sum_{i=1}^{r} a_i 10^i \equiv 0 \pmod{7}$$

och vi är klara.