Elementär talteori, våren 2013
Förslag till lösningar för övning 3

1. Bestäm talets 5 multiplikativa invers modulo 9, dvs. hitta ett x för vilket $5x \equiv 1 \pmod 9$.

Lösning. Genom att gissa eller genom att tillämpa Euklides algoritm på Diofantiska ekvationen $5x - 9y = 1$ hittar vi en lösning $x = 2$. Av kongruensen $5x \equiv 1 \pmod 9$ följer, att

$$x \equiv 10x = 2 \cdot 5x \equiv 2 \cdot 1 \equiv 2 \pmod 9,$$

alltså för alla lösningar x gäller $x \equiv 2 \pmod 9$. Å andra sidan om det för ett heltal x gäller att $x \equiv 2 \pmod 9$, så måste $5x \equiv 5 \cdot 2 \equiv 1 \pmod 9$.

2. Lös kongruensekvationen

$$5x + 3 \equiv 4 \pmod 7$$

Lösning. Vi kan som i förra uppgiften hitta en lösning $x = 3$ till ekvationen $5x \equiv 1 \pmod 7$ genom att pröva oss fram, eller genom att tillämpa Euklides algoritm på Diofantiska ekvationen $5x - 7y = 1$.

Om ett heltal x är en lösning för kongruensekvationen, så gäller

$$x \equiv 15x \equiv 3 \cdot 5x \equiv 3 \cdot 1 \equiv 3 \pmod 7,$$

alltså för varje lösning x gäller $x \equiv 3 \pmod 7$. Å andra sidan, om $x \equiv 3 \pmod 7$, så gäller $5x \equiv 5 \cdot 3 \equiv 15 \equiv 1 \pmod 7$.

3. Visa, att $17 \mid 11^{1600} - 1$.

Lösning. Talet 17 är ett primtal som inte delar talet 11, alltså gäller enligt Fermats lilla sats

$$11^{1600} = \left(11^{16}\right)^{100} \equiv 1^{100} \equiv 1 \pmod{17}.$$

4. Lös kongruensekvationssystemet

$$\begin{cases} x \equiv 3 \pmod 9 \\ x \equiv 7 \pmod 8. \end{cases}$$

Lösning. Antag att x är en lösning. Enligt den första kongruensekvationen gäller $x = 3 + 9k$ för något heltal k. Genom att placera detta i den andra kongruensekvationen får vi

$$3 + 9k \equiv 7 \pmod 8, \quad \text{dvs.} \quad k \equiv 4 \pmod 8.$$

Alltså måste $k = 4 + 8\ell$ för något heltal ℓ, och den ursprungliga lösningen x måste vara av formen

$$x = 3 + 9k = 3 + 9\,(4 + 8\ell) = 3 + 9 \cdot 4 + 9 \cdot 8\ell = 39 + 72\ell \equiv 39 \pmod{72}.$$

Å andra sidan, ifall $x \equiv 39 \pmod{72}$, så är $x = 39 + 72\ell$ för något heltal ℓ, och därmed gäller

$$x \equiv 39 + 72\ell \equiv 3 + 0 \equiv 3 \pmod 9 \quad \text{och} \quad x \equiv 39 + 72\ell \equiv 7 + 0 \equiv 7 \pmod 8.$$

5. I kompendiet definieras Eulers φ-funktion, och påstås att om $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (primtalsfaktoriseringen för talet n), så gäller

$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1} (p_j - 1) .$$

Bevisa påståendet. (Tips: Visa först påståendet för primtalspotenser, och gör sedan induktion över antalet olika primtalsfaktorer.)

Lösning. Låt först p vara ett primtal och låt $\alpha \in \mathbb{Z}_+$. Ett heltal n har ingen (icke-trivial) gemensam delare med p^α om och endast om n inte är delbart med primtalet p. Av talen 1, 2, ..., p^α är talen p, $2p$, ..., $p^{\alpha-1} \cdot p$ delbara med p, och deras antal är $p^{\alpha-1}$. Resten av talen har alltså ingen gemensam delare med p^α, och därmed gäller

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1} (p - 1) .$$

För tal bestående av flera primtalspotenser kan vi bevisa formeln med induktion genom att använda nedanstående lemma: Om vi antar att formeln gäller för något $k \in \mathbb{Z}_+$, och vi granskar ett tal med primtalsfaktoriseringen $p_1^{\alpha_1} \cdots p_{k+1}^{\alpha_{k+1}}$, där p_1, ..., p_{k+1} är olika primtal och α_1, ..., α_{k+1} är heltal, så gäller enligt lemmat och induktionsantagandet

$$\begin{aligned} \varphi\big(p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot p_{k+1}^{\alpha_{k+1}}\big) &= \varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k})\, \varphi\big(p_{k+1}^{\alpha_{k+1}}\big) \\ &= \prod_{j=1}^{k} p_j^{\alpha_j - 1} (p_j - 1) \cdot p_{k+1}^{\alpha_{k+1}-1} (p_{k+1} - 1) = \prod_{j=1}^{k+1} p_j^{\alpha_j - 1} (p_j - 1) , \end{aligned}$$

vilket skulle bevisas.

Lemma. *Om sgd(m,n) = 1, så gäller*

$$\varphi(mn) = \varphi(m)\, \varphi(n) .$$

Vi bevisar lemmat genom att skriva talen 1, 2, ..., mn i en tabell på följande sätt:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \cdots & 3n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (m-1)\,n+1 & (m-1)\,n+2 & (m-1)\,n+3 & \cdots & mn \end{array}$$

I denna tabell finns enligt definitionen på funktionen $\varphi(\cdot)$ exakt $\varphi(mn)$ tal, som inte har någon (icke-trivial) gemensam delare med mn. Å andra sidan, eftersom ett tal inte har någon gemensam delare med mn om och endast om det inte har någon gemensam delare med varken m eller n, kan vi räkna de eftersökta $\varphi(mn)$ talen på ett annat sätt.

Eftersom alla tal i en kolumn i tabellen är kongruenta modulo n, bildar de tal som inte har gemensamma delare med n exakt $\varphi(n)$ stycken hela kolumner, alltså måste de ovannämnda $\varphi(mn)$ talen finnas i dessa kolumner.

Vi undersöker till näst en av dessa $\varphi(n)$ kolumer. Eftersom sgd(m,n) = 1, finns det i kolumnen m stycken tal som inte är kongurenta med varandra modulo m (jämför t.ex. med beviset av sats 22 i kompendiet). Alltså har exakt $\varphi(m)$ stycken av kolumnens tal ingen gemensam delare med varken n eller m, och därmed är beviset klart.

6. Slutför beviset för den kineniska restklassatsen: Låt $M = m_1 m_2 \cdots m_k$, för vilka sgd(m_i,m_j) = 1 alltid då $i \neq j$. Vi definierar $M_j = \frac{M}{m_j}$ och betecnar med y_j inversen för talet M_k modulo m_j, alltså gäller $M_j y_j \equiv 1 \pmod{m_j}$. Visa, att

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_k M_k y_k \pmod{M}$$

löser ekvationssystemet

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Lösning. Låt $j \in \{1, 2, \dots, k\}$. Talet m_j är en faktor i talet

$$a_\ell M_\ell y_\ell = a_\ell m_1 m_2 \cdots m_{\ell-1} m_{\ell+1} \cdots m_k y_\ell,$$

då $\ell \in \{1, 2, \dots, k\}$ och $\ell \neq j$, alltså måste $a_\ell M_\ell y_\ell \equiv 0 \pmod{m_j}$. Dessutom gäller $a_j M_j y_j \equiv a_j \cdot 1 \equiv a_j \pmod{m_j}$, och därmed får vi

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + \ldots + a_{j-1} M_{j-1} y_{j-1} + a_j M_j y_j + a_{j+1} M_{j+1} y_{j+1} + \ldots + a_k M_k y_k \\ &\equiv 0 + \ldots + 0 + a_j + 0 + \ldots + 0 \equiv a_j \pmod{m_j}. \end{aligned}$$