MAN 060 – Elementär talteori
Sommaren 2007

Ibland synnerligen kortfattade och därför inte helt föredömliga lösningar till andra övningstentamen 2007

1. Ange den sista siffran i decimalutvecklingen av 7^{3943}

Lösning:
Eftersom $7^{\Phi(10)} = 7^4 \equiv 1 \pmod{10}$ *och* $3943 \equiv 3 \pmod{4}$ *blir* $7^{3943} \equiv 7^3 \equiv 3 \pmod{10}$

2. Avgör huruvida 111 är en kvadratisk rest modulo 991
(991 är ett primtal).

Lösning:

$$\left(\frac{111}{991}\right) = \left(\frac{3}{991}\right)\cdot\left(\frac{37}{991}\right) = (-1)(-1) = 1$$

3. Låt *p* vara ett primtal. Visa att produkten av samtliga primitiva rötter modulo *p* är $\equiv 1 \pmod{p}$.

Lösning:

Låt r vara en primitiv rot. Enligt sats kan då samtliga primitiva rötter skrivas r^a *där a genomlöper alla tal sådana att* $(a, \Phi(p)) = (a, p-1) = 1$. *Den efterfrågade produkten kan alltså skrivas* $r^{\sum_{(a_i, p-1)=1} a_i}$. *Nu gäller generellt att* $(a,n) = 1 \Leftrightarrow (a, n-a) = 1$ *varför de tal som är relativt prima mot p-1 kan samlas i par vars summa är* $= p-1$. *Alltså är exponenten i* $r^{\sum_{(a_i, p-1)=1} a_i}$ *delbar med p-1 och påståendet följer.*

4. Bestäm alla positiva heltal $x < 77$ sådana att $x^2 \equiv 64 \pmod{77}$

Lösning:

Vi använder tekniken från "slantsingling" och löser därför kongruenserna $x^2 \equiv 64 \pmod 7$ *och* $x^2 \equiv 64 \pmod{11}$ (*ty* $77 = 7 \cdot 11$) *och får* $x \equiv \pm 1 \pmod 7$ *respektive* $x \equiv \pm 3 \pmod{11}$. *Dessa lösningar paras ihop i fyra par och genererar med hjälp av kinesiska restsatsen fyra kongruenser modulo 77.*

Enligt kinesiska restsatsen har systemet $\begin{cases} x \equiv a \pmod 7 \\ x \equiv b \pmod{11} \end{cases}$ *lösningen* $x \equiv 11 \cdot 2 \cdot a + 7 \cdot 8 \cdot b$ *och modulo 77 blir lösningarna* $x \equiv 8, 36, 41, 69$

5. Lös kappsäcksproblemet $\sum_{i=1}^{6} x_i a_i = 108$ om följden $\{a_i\}_{i=1}^{6}$ är $= 6, 11, 21, 41, 81, 151$

Beskriv vad som menas med att en följd är superväxande.

Visa att om $\{a_i\}_{i=1}^{n}$ är en superväxande följd är $a_j \geq 2^{j-1}$ för $j = 1, 2, 3\ldots, n-1$

Lösning:

$108 = 81 + 21 + 6$

$\{a_i\}_{i=1}^{n}$ *är superväxande om* $a_j > \sum_{k=1}^{j-1} a_k$

Induktion: om påståendet gäller för alla $j \leq m$ *är* $a_{m+1} > \sum_{k=1}^{m} a_k \geq \sum_{k=1}^{m} 2^{k-1} = 2^m - 1$

så $a_{m+1} \geq 2^m$

6. Förklara tabellen

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	
5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	

Lös kongruensen $3x^{14} \equiv 2 \pmod{23}$

Lös kongruensen $x^x \equiv x \pmod{23}$

Lösning:

Tabellen visar potenser av 5 som är primitiv rot modulo 23.

Genom att bilda index av bägge led får man den linjära kongruensen $14 ind_5 x \equiv 8 \pmod{22}$ *som har de inkongruenta lösningarna* $ind_5 x = 10$ *respektive* $= 21$. *Ur tabellen får man* $x = 9$ *samt* $x = 14$ *– om vi förutsätter att* $x < 23$.

På samma sätt övergår den andra kongruensen i villkoret att $(x-1)\cdot ind_5 x$ *är delbart med 22. Vi skiljer mellan fyra fall:*
I. *x-1 delbart med 22. Då blir* $x = 22k+1$
II. $ind_5 x$ *delbart med 22. Då blir* $x = 23k+1$
III. *x-1 delbart med 2 och* $ind_5 x$ *delbart med 11. Då blir* $x = 22+(2k+1)23$
IV. *x-1 delbart med 11 och* $ind_5 x$ *delbart med 2. Då blir* $x = 11k+1$ *samtidigt som* $x = 2,3,4,6,8,9,12,13,16,18+23n$.
Dessutom har vi naturligtvis lösning så snart x är delbart med 23.
Svar: $x = 0,1,12,23,24,45,46,47,67,69,70\ldots$ *(modulo 506)*

7. Bestäm alla positiva heltal *x* och *y* sådana att $\frac{1}{x}+\frac{1}{y}=\frac{1}{p}$ där *p* är ett primtal.

Lösning:

$\frac{1}{x}+\frac{1}{y}=\frac{1}{p} \quad \Leftrightarrow \quad py+px=xy$ *varav följer att åtminstone en av x och y måste vara delbar med p. Eftersom uttrycket är symmetriskt kan vi utan inskränkning säga att p delar x,* $x = p\tilde{x}$. Alltså är
$py+p^2\tilde{x}=p\tilde{x}y \quad \Leftrightarrow \quad y+p\tilde{x}=\tilde{x}y \quad \Leftrightarrow \quad p\tilde{x}=y(\tilde{x}-1)$ *Så antingen y eller* $\tilde{x}-1$ *är delbart med p. Om y är delbart med p,* $y = p\tilde{y}$ *, blir den sista ekvationen* $p\tilde{x}=p\tilde{y}(\tilde{x}-1)\Leftrightarrow \tilde{x}=\tilde{y}(\tilde{x}-1)$ *med enda lösningen* $\tilde{x}=\tilde{y}=2$ *. Om* $\tilde{x}-1$ *är delbart med p,* $\tilde{x}-1=p\hat{x}$ *, blir samma ekvation i stället* $p\tilde{x}=yp\hat{x}\Leftrightarrow p\hat{x}+1=y\hat{x}$
$\Leftrightarrow \quad (y-p)\hat{x}=1$ *med enda lösningen* $y = p+1, \hat{x}=1$
Svar: antingen $x = y = 2p$ *eller* $x = p^2+p, \quad y = p+1$

8. Visa att $(a,b)=1 \quad \Rightarrow \quad a^{\Phi(b)}+b^{\Phi(a)}\equiv 1 \pmod{ab}$

Lösning:

Eftersom $(a,b)=1$ *räcker det att visa den givna kongruensen för a och b separat. Det gäller ju att* $b^{\Phi(a)}\equiv 1 \pmod{a}$ *enligt Eulers sats, och* $a^{\Phi(b)}$ *är naturligtvis* $\equiv 0 \pmod{a}$, *så* $a^{\Phi(b)}+b^{\Phi(a)}\equiv 0+1=1 \pmod{a}$. *Man resonerar analogt modulo b och påståendet följer.*