LÖSNINGAR till

Tentamen i Elementär talteori, 5p 21 sept 2007 8.30 – 13.30

1. Bestäm alla heltal x sådana att $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 6 \\ x \equiv 3 \pmod 7 \end{cases}$ **(3p)**

Lösning: Med hjälp av kinesiska restsatsen får man att
$x = 2\cdot 42\cdot 3 + 1\cdot 5\cdot 35 + 3\cdot 30\cdot 4 = 787 \equiv 157 \pmod{210}$
Svar: $x = 157 + n210$

2. Visa att $2222^{5555} + 5555^{2222}$ är delbart med 7. **(3p)**

Lösning: Eftersom $a^6 \equiv 1 \pmod 7$ är $2222^{5555} + 5555^{2222} \equiv 3^5 + 4^2 \equiv 0 \pmod 7$

3. Låt (x, y, z) vara en primitiv pythagoreisk trippel, $x^2 + y^2 = z^2$.
Visa att z inte är $\equiv 0 \pmod 7$ **(3p)**

Lösning: Eftersom trippeln är primitiv kan inte två av talen vara delbara med 7 ty det skulle medföra att alla tre vore det. Så om z är delbart med 7 kan varken x eller y vara det. Men eftersom de kvadratiska resterna modulo 7 är respektive 1, 2 och 4 och det inte går att skriva 7 som en summa av två av dessa tal kan z inte vara delbart med 7.

4. Bestäm alla positiva heltal $x < 65$ sådana att $x^2 \equiv 49 \pmod{65}$ **(3p)**

Lösning: Eftersom $65 = 5\cdot 13$ löser vi dels $x^2 \equiv 49 \pmod 5$ som ger $x \equiv \pm 2 \pmod 5$, dels $x^2 \equiv 49 \pmod{13}$ som ger $x \equiv \pm 6 \pmod{13}$.
Lösningarna paras ihop till fyra par som vart och ett med hjälp av kinesiska restsatsen ger en lösning till den givna kongruensen:

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 6 \pmod{13} \end{cases} \Rightarrow x \equiv 32 \pmod{65}$$

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv -6 \pmod{13} \end{cases} \Rightarrow x \equiv 7 \pmod{65}$$

$$\begin{cases} x \equiv -2 \pmod 5 \\ x \equiv 6 \pmod{11} \end{cases} \Rightarrow \quad x \equiv 58 \pmod{65}$$

$$\begin{cases} x \equiv -2 \pmod 5 \\ x \equiv -6 \pmod{11} \end{cases} \Rightarrow \quad x \equiv 33 \pmod{65}$$

Svar: 7, 32, 33, 58

5. Betrakta implikationen

$x^2 \equiv y^2 \pmod n \quad \Rightarrow \quad x \equiv y \pmod n \quad$ *eller* $\quad x \equiv -y \pmod n$

Visa att implikationen är sann om *n* är ett primtal.
Ange ett sammansatt tal *n* sådant att implikationen är falsk.
Vad händer om man lägger till förutsättningen $(x,n)=(y,n)=1$? **(3p)**

Lösning: Om *n* är primtal gäller $n \mid x^2 - y^2 = (x-y)(x+y) \quad \Rightarrow \quad n \mid x-y$ eller $n \mid x+y$

Om däremot *n* är sammansatt gäller till exempel $1^2 \equiv 3^2 \pmod 8$

6. Bestäm alla positiva heltal *x* och *y* sådana att $\frac{1}{x} - \frac{1}{y} = \frac{1}{7}$. **(3p)**

Lösning: $\frac{1}{x} - \frac{1}{y} = \frac{1}{7} \quad \Rightarrow \quad 7y - 7x = xy$. Så antingen *x* eller *y* är delbara med 7. Antag att *x* är delbar med 7, $x = 7\tilde{x}$, så att
$7y - 49\tilde{x} = 7\tilde{x}y \quad \Rightarrow \quad y(1-\tilde{x}) = 7\tilde{x}$ som uppenbarligen saknar positiva heltalslösningar. Om å andra sidan *y* är delbar med 7, $y = 7\tilde{y}$, blir
$49\tilde{y} - 7x = 7x\tilde{y} \quad \Rightarrow \quad \tilde{y}(7-x) = x$. I denna ekvation prövar man de enda tänkbara värdena för *x*, alltså 1, 2, 3, 4, 5, 6. Man ser lätt att den enda möjligheten är $x = 6$ vilket ger $y = 42$.
Svar: $(x, y) = (6,42)$

7. Låt $y(n)$ vara antalet heltal *k* med $1 \le k \le n$ sådana att $(k,n) = (k+1,n) = 1$.

Visa att om *n* är en primtalspotens, $n = p^a$, är $y(n) = n\left(1 - \frac{2}{p}\right)$ **(3p)**

Lösning: Genom att räkna upp de positiva heltalen från 1 till p^a:
$1, 2, 3, \ldots, p, \ldots, 2p, \ldots, p^{a-1} \cdot p$ ser man att det finns p^{a-1} stycken *k* sådana

att $(k, p^a)=1$ och lika många sådana att $(k+1, p^a)=1$. Alltså är
$y(p^a)= p^a - 2p^{a-1} = p^a\left(1-\frac{2}{p}\right)$

8. Låt *n* vara ett positivt heltal och $p = 2^n + 1$ ett primtal. Visa att varje kvadratisk icke-rest modulo *p* är en primitiv rot modulo *p*.

Visa omvändningen, det vill säga att om alla kvadratiska icke-rester är primitiva rötter måste *p* kunna skrivas $p = 2^n + 1$ **(4p)**

Lösning: Antag att *a* är en kvadratisk icke-rest modulo *p* så att $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ och vidare att $a^m \equiv 1 \pmod{p}$ där *m* delar $p-1 = 2^n$. Om nu *m* är en äkta delare till $p-1 = 2^n$, det vill säga $m = 2^k$, $k < n$, blir $a^{2^{n-1}} \equiv 1 \pmod{p}$ vilket är en motsägelse, ty $\frac{p-1}{2} = 2^{n-1}$. Alltså är $p-1 = m$ och *a* är en primitiv rot.

Om å andra sidan alla kvadratiska icke-rester är primitiva rötter har vi $\Phi(p-1) \geq \frac{p-1}{2}$ ty enligt kända satser finns det $\Phi(p-1)$ primitiva rötter och $\frac{p-1}{2}$ kvadratiska icke-rester. Men $p-1$ är jämnt, så $p-1 = 2^r \prod_{q_i \mid p-1} q_i^{v_i}$ där $r > 0$ och q_i är primtal >2 och därför $\Phi(p-1) = (p-1)\frac{1}{2}\prod_{q_i \mid p-1}\left(1-\frac{1}{q_i}\right)$ som är $\leq \frac{p-1}{2}$. Alltså är $\Phi(p-1) = \frac{p-1}{2}$ och $p-1 = 2^n$