Lösningar till Övningstenta 3

1. Vi har $5^{60} = 1(61)$ således måste ordningen n vara en divisor av 60, med möjligheterna $n = 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$. V har $5^1 = 5, 5^2 = 25, 5^3 = 3, 5^4 = 15, 5^5 = 14, 5^6 = 9$ Ur detta följer $5^{10} = 5^4 \cdot 5^6 = 13, 5^{12} = 9 \cdot 9 = 20, 5^{15} = 14 \cdot 13 = -1$ således följer $n = 30$.

2. Vi kan antaga att $p \neq 2$ ty polynomet är altid 1 i detta fall. Vi har via kvadratkomplettering $x^2 + x + 1 = (x + \frac{1}{2})^2 + (1 - \frac{1}{4})$ vilket antyder att vi borde förlänga med 4. Detta ger $4(x^2 + x + 1) = (2x + 1)^2 + 3$ Denna ekvation har två lösningar precis när -3 är en kvadrat.

Vi har $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p})$ och eftersom $3 = 3(4)$ kan vi skriva $(\frac{3}{p})(\frac{p}{3}) = (\frac{-1}{p})$. Ur detta sluter vi $(\frac{-3}{p}) = (\frac{p}{3})$

Alternativ lösning. Avbildningen $x \to x^3$ är surjektiv om $(3, p - 1) = 1$. I detta fall har $x^3 - 1 = (x - 1)(x^2 + x + 1) = 0$ endast en lösning $x = 1$. Om $3|p - 1$ har den tre lösningar vilket betyder att $x^2 + x + 1$ har två lösningar.

3. $(\frac{55}{79}) = (\frac{5}{79})(\frac{11}{79})$. Vidare ger kvadratisk reciprocitet $(\frac{5}{79}) = (\frac{79}{5}) = (\frac{4}{5}) = 1$ och $(\frac{11}{79}) = -(\frac{79}{11}) = -(\frac{2}{11}) = 1$ eftersom $11 = 8n + 3$. Således är 55 en kvadrat modulo 79

4. De sista siffrorna i potenserna av två följer mönstret $2, 4, 8, 6, \ldots$ med period 4. För att finna andra siffran noterar vi att multiplication med $16 = 2^4$ med start vid 8 ger samtliga potenser som slutar med 8. Således 28, $16 \cdot 28 = 48, 16 \cdot 48 = 68, 16 \cdot 68 = 88, 16 \cdot 88 = 08$ och slutligen $16 \cdot 08 = 28$ d.v.s. efter $5 \cdot 4 = 20$ steg. Nästa två-potens som slutar på 28 blir således 2^{27}.

5. Om $p = ab$ med $a, b > 1$ följer att $3^a - 1, 3^b - 1$ delar $3^{ab} - 1$.

6. 24 kan skrivas som en produkt med faktorer > 1 på ett otal sätt. Om $n = p_1^{n_1} p_2^{n_2} \ldots$ är antalet divisorer $(n_1+1)(n_2+1)\ldots$. Vi kan göra en systematisk tabell.

24	2^{23}	–
$12 \cdot 2$	$2^{11} \cdot 3^3$	–
$8 \cdot 3$	$2^7 \cdot 3^2$	
$6 \cdot 4$	$2^5 3^4$	–
$6 \cdot 2 \cdot 2$	$2^5 \cdot 3 \cdot 5$	480
	$2^5 \cdot 3 \cdot 7$	672
$4 \cdot 3 \cdot 2$	$2^3 \cdot 3^2 \cdot 5$	360
	$2^3 \cdot 3^2 \cdot 7$	504
	$2^3 \cdot 3^2 \cdot 11$	792
	$2^3 \cdot 3^2 \cdot 13$	936
	$3^3 \cdot 2^2 \cdot 5$	540
	$3^3 \cdot 2^2 \cdot 7$	756
$3 \cdot 2 \cdot 2 \cdot 2$	$2^2 \cdot 3 \cdot 5 \cdot 7$	420
	$2^2 \cdot 3 \cdot 5 \cdot 11$	660
	$2^2 \cdot 3 \cdot 5 \cdot 13$	780
	$2^2 \cdot 3 \cdot 7 \cdot 11$	924
	$3^2 \cdot 2 \cdot 5 \cdot 7$	630
	$3^2 \cdot 2 \cdot 5 \cdot 11$	990

7. Betrakta primtalen p som är innehållna i a och primtalen q som är innehållna i b (de kan givetvis överlappa). Eftersom $c = ab$ kommer varje primtal r av typ 3(4)ha jämn exponent i c. Om det förekommer i a har det även jämn exponent i a och därmed även i b. Därmed fullfyller b kriteriet för att vara en summa av två kvadrater.