(SKETCHES OF) SOLUTIONS, NUMBER THEORY, TATA 54, 2012–03–08

(1) $126 = 2 \cdot 63 = 2 \cdot 3^2 \cdot 7$
- $n^8 \equiv n^2 \pmod 2$ for all n.
- Since $\varphi(3^2) = 3 \cdot 2 = 6$, Eulers theorem implies that $n^6 \equiv 1 \pmod 9$ when $(n, 9) = 1$, i.e. when $3 \nmid n$. Hence $n^8 \equiv n^2 \pmod 9$ when $3 \nmid n$. When $3 \mid n$, then n^2 and n^8 are both divisible by 9. It follows that $n^8 \equiv n^2 \pmod 9$ for every integer n.
- $n^7 \equiv n \pmod 7$ for all n.(Fermat)
  Hence $n^8 \equiv n^2 \pmod 7$ for all n.
  It follows that $n^8 - n^2$ is divisible by 126 for all $n \in \mathbb{Z}$

(2) (a) $\varphi(25) = 5 \cdot 4 = 20$, $\operatorname{ord}_{25} 2 \mid 20$, $2^4 \equiv 16 \pmod{25}$, $2^5 = 32 \equiv 7 \pmod{25}$, $2^{10} = (2^5)^2 \equiv 7^2 \equiv 49 \equiv -1 \pmod{25}$. Hence $\operatorname{ord}_{25} 2 = 20$, so 2 is a primitive root of 25.

(b) Computing with indices with respect to the primitive root 2 of 25, the nonlinear congruence $x^7 \equiv 7 \pmod{25}$ will be turned into the linear congruence $7 \operatorname{ind} x \equiv \operatorname{ind} 7 \pmod{20}$.
Now $2^5 \equiv 7 \pmod{25}$, so $\operatorname{ind} 7 = 5$. Multiplying both sides with 3, which is an inverse of 7 modular 20, we obtain $\operatorname{ind} x \equiv 15 \pmod{20}$.
Since $2^{15} = 2^{10} \cdot 2^5 \equiv (-1)7 \equiv -7 \equiv 18 \pmod{25}$ the solutions are given by $x \equiv 18 \pmod{25}$

ANSWER:
(a) E.g. 2 is a primitive root modulo 25
(b) $x \equiv 18 \pmod{25}$

(3) (a) The prime number 7 is congruent to 3 modulo 4 and it occurs with an odd power in the prime factorization $1729 = 7 \cdot 13 \cdot 19$. Therfore the number 1729 cannot be written as the sum of two squares of integers.

(b) Every positive integer can be written as the sum of four squares.

(c) One possibilty to write 1729 as the sum of three squares is $1729 = 1000 + 729 = 30^2 + 10^2 + 27^2$, another one is $1729 = 289 + 1440 = 17^2 + 12^2 \cdot 10 = 17^2 + 12^2(3^2 + 1^2) = 17^2 + 36^2 + 12^2$. (Can you find more possibilities?)

ANSWER:
(a) No
(b) Yes
(c) Yes

(4) $121 = 11^2$ is composite and we must also show that

$$3^{\frac{121-1}{2}} \equiv \left(\frac{3}{121}\right) \pmod{121}$$

$3^{60} \equiv (3^5)^{12} \equiv (243)^{12} \equiv 1^{12} \equiv 1 \pmod{121}$

By the definition of the Jacobi symbol: $\left(\frac{3}{121}\right) = \left(\frac{3}{(11)^2}\right) = \left(\frac{3}{11}\right)^2 = 1$

(5) (a) We use the recursion formula

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k},$$

where $a_k = [\alpha_k]$ and $\alpha_0 = \sqrt{95}$.
$9^2 < 95 < 10^2$, $9 < \sqrt{95} < 10$, $a_0 = [\sqrt{95}] = 9$.
$\alpha_1 = \frac{1}{\sqrt{95}-9} = \frac{\sqrt{95}+9}{14}$, $1 < \frac{9+9}{14} < \alpha_1 < \frac{10+9}{14} < 2$, $a_1 = 1$.
$\alpha_2 = \frac{\sqrt{95}+5}{5}$, $2 < \frac{9+5}{5} < \alpha_2 < \frac{10+5}{5} = 3$, $a_2 = 2$.
$\alpha_3 = \frac{\sqrt{95}+5}{14}$, $1 = \frac{9+5}{14} < \alpha_3 < \frac{10+5}{14} < 2$, $a_3 = 1$.
$\alpha_4 = \sqrt{95} + 9$, $a_4 = [\sqrt{95} + 9] = [\sqrt{95}] + 9 = 9 + 9 = 18$.
$\alpha_5 = \frac{1}{\sqrt{95}-9} = \alpha_1$.
Hence $\sqrt{95} = [9; \overline{1, 2, 1, 18}]$

(b) The continued fraction expansion of $\sqrt{79}$ is periodic with period 4, which is even.
The positive solutions of the Pell equation $x^2 - 95y^2 = 1$ are given by $x_j = p_{4j-1}$, $y_j = q_{4j-1}$, $j = 1, 2, 3 \ldots$.

$$\frac{p_3}{q_3} = [9; 1, 2, 1] = 9 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1}}} = \frac{39}{4}$$

ANSWER
(a) $\sqrt{95} = [9; \overline{1, 2, 1, 18}]$
(b) $x = 39$, $y = 4$

(6) $637 = 7 \cdot 91 = 7^2 \cdot 13$
$63700 = 637 \cdot 100 = 2^2 \cdot 5^2 \cdot 7^2 \cdot 13$
$5 \equiv 13 \equiv 1 \pmod 4$, $7 \equiv 3 \pmod 4$.
Hence there are $4(2 + 1)(1 + 1) = 24$ pairs of integers (x, y), such that $x^2 + y^2 = 63700$.
ANSWER: 24