(SKETCHES OF) SOLUTIONS, NUMBER THEORY, TATA 54, 2013-03-14

(1) (a) $\operatorname{ord}_{37} 7$ divides $36 = 2^2 3^2$. $7^2 = 49 \equiv 12 \pmod{37}$, $7^3 = 7 \cdot 7^2 \equiv 7 \cdot 12 \equiv 84 \equiv 10 \pmod{37}$, $7^4 = 7 \cdot 7^3 \equiv 7 \cdot 10 \equiv 70 \equiv -4 \pmod{37}$, $7^6 = 7^2 \cdot 7^4 \equiv 12(-4) \equiv -48 \equiv -11 \pmod{37}$, $7^9 = 7^3 \cdot 7^6 \equiv 10(-11) \equiv -110 \equiv 1 \pmod{37}$. Hence $\operatorname{ord}_{37} 7 = 9$.

(b) $7^{1000} = 7^{999} \cdot 7 = (7^9)^{111} \cdot 7 \equiv 1^{111} \cdot 7 \equiv 7 \pmod{37}$.

ANSWER: (a): 9 (b): 7

(2) We can read off from the prime factorization of n if n can be written as the sum of two squares and the number of ways it can be done.

(a) $81000 = 2^3 3^4 5^3$. Yes and that in $4(3+1) = 16$ ways.

(b) Since $270 = 2 \cdot 3^3 \cdot 5$ and 3 occurs to an odd power, the number 270 cannot be written as the sum of two squares.

ANSWER: (a): Yes, in 16 ways. (b): No

(3) (a) $143 = 11 \cdot 13$, $(\frac{18}{143}) = (\frac{18}{11})(\frac{18}{13})$, $(\frac{18}{11}) = (\frac{3^2}{11})(\frac{2}{11}) = (\frac{2}{11}) = -1$. Where for the last computation we used that $11 \equiv 3 \pmod{8}$. Similarly we get $(\frac{18}{13}) = (\frac{2}{13}) = -1$, since $13 \equiv 5 \pmod{8}$. Hence $(\frac{18}{143}) = (-1)(-1) = 1$.

(b) No, since if x satisfies $x^2 \equiv 18 \pmod{143}$, then x also satisfies $x^2 \equiv 18 \pmod{11}$. But the last congruence has no solution, since the Legendre symbol $(\frac{18}{11}) = -1$.

ANSWER: (a): 1 (b): No

(4) We first find a primitive root modulo 11. Since $\operatorname{ord}_{11} 2 \mid \varphi(11) = 10$, the only thing we have to exhibit is $2^5 \equiv -1$, in order to conclude that $\operatorname{ord}_{11} 2 = 10$. Let $n = \operatorname{ord}_{121} 2$. Since $2^n \equiv 1 \pmod{11^2}$ implies that $2^n \equiv 1 \pmod{11}$, we get that $10 \mid n$. But n is also a divisor of $\varphi(11) = 11 \cdot 10$ Hence $n = 10$ or $n = 110$. But $2^{10} = 2^7 \cdot 2^3 = 128 \cdot 8 = 7 \cdot 8 = 56 \not\equiv 1 \pmod{121}$. Thus $n = 110$ and 2 is a primitive root modulo 121.

ANSWER: E.g. 2 is a primitive root modulo 121.

(5) We first compute the infinite simple continued fraction of $\alpha_0 = \sqrt{30}$.. Since $5^2 < 30 < 6^2$, $5 < \sqrt{30} < 6$ and $a_0 = [\sqrt{30}] = 5$. $\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{\sqrt{30}+5}{5}$. $2 = \frac{5+5}{5} < \alpha_1 < \frac{6+5}{5} < 3$. Hence $a_1 = 2$. $\alpha_2 = \frac{1}{\alpha_1 - a_1} = \sqrt{30} + 5$. $a_2 = 5 + 5 = 10$. We then get $\alpha_3 = \alpha_1$. Hence $\sqrt{30} = [5; \overline{2, 10}]$. The period length is even, namely 2.

Then the positive solutions of the diophantine equation $x^2 - 30y^2 = 1$ will be $(x_j, y_j) = (p_{2j-1}, q_{2j-1})$ for $j = 1, 2, 3, \ldots$. The least one is obtained from $\frac{p_1}{q_1} = [5; 2] = 5 + \frac{1}{2} = \frac{11}{2}$. The next one from $\frac{p_3}{q_3} = [5; 2, 10, 2] = \frac{241}{44}$, and therefore the two first solutions are $x = 11, y = 2$ and $x = 241, y = 44$.

Alternative solution:

There is no solution with $y = 1$. But it is easily seen that $x_1 = 11, y_1 = 2$ is a solution and thus the smallest one. The next solution (x_2, y_2) is computed using the formula $x_2 + y_2\sqrt{30} = (x_1 + y_1\sqrt{30})^2$.

ANSWER: The two smallest solutions are $(x, y) = (11, 2)$ and $(x, y) = (241, 44)$.

(6) Let $f(x) = x^3 + 2x - 7$. Then $f(x) \equiv 0 \pmod{100}$ is equivalent to that both $f(x) \equiv 0 \pmod 4$ and $f(x) \equiv 0 \pmod{25}$ hold. Computing $f(x)$ for $x = 0, 1, 2, 3$ we get $-7, -4, 5, 26$ resp. Hence the solutions of $f(x) \equiv 0 \pmod 4$ are $x \equiv 1 \pmod 4$. Then we find the solutions of $f(x) \equiv 0 \pmod 5$. Doing as above we get the solutions $x \equiv 2 \pmod 5$ and $x \equiv 4 \pmod 5$.

Since $f'(4) = 50 \equiv 0 \pmod 5$ and $f(4) = 65 \not\equiv 0 \pmod{5^2}$ there are no solutions of $f(x) \equiv 0 \pmod{5^2}$ with $x \equiv 4 \pmod 5$. Let us find the solutions of the form $x = 2+5t$. $f(2+5t) = (2+5t)^3+2(2+5t)-7 = 5+14\cdot 5t+5(6t^2)+5^3t^3 \equiv 5 + (15-1)5t \equiv 5(1-t) \pmod{5^2}$ Hence $f(x) \equiv 0 \pmod{5^2}$ is equivalent to $1 - t \equiv 0 \pmod 5$ i.e. $t = 1 + 5s$ Therefore these solutions are of the form $x = 2 + 5(1 + 5s) = 7 + 25s$ We find out when also $7 + 25s \equiv 1 \pmod 4$. We get $s \equiv 2 \pmod 4$. Hence the solutions of $f(x) \equiv 0 \pmod{100}$ are $x = 7+25(2+4n) = 57+100n$.
ANSWER: $x \equiv 57 \pmod{100}$.