(SKETCHES OF) SOLUTIONS, NUMBER THEORY, TATA 54, 2015-03-19

(1) $\varphi(25) = \varphi(5^2) = 5 \cdot 4 = 20$. Euler's theorem says that $7^{20} \equiv 1 \pmod{25}$. Therefore $7^{8253} = (7^{20})^{412} 7^{13} \equiv 7^{13} \equiv (7^2)^6 7 \equiv (49)^6 7 \equiv (-1)^6 7 \equiv 7 \pmod{25}$
ANSWER: 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) $1845 = 9 \cdot 205 = 3^2 \cdot 5 \cdot 41$. Since no prime of the form $4k+3$ occurs with an odd power in 1845, the number 1845 can be written as the sum of two squares of integers.
  (b) Since $3510 = 10 \cdot 351 = 2 \cdot 5 \cdot 3 \cdot 117 = 2 \cdot 3^3 \cdot 5 \cdot 13$, where 3 occurs to an odd power, the number 3510 cannot be written as the sum of two squares.
  (c) Since $n = 11\,700\,000 = 117 \cdot 10^5 = 2^5 \cdot 5^5 \cdot 3^2 \cdot 13$, the searched number of ordered pairs is $4(5+1)(1+1) = 48$
ANSWER: (a): Yes (b): No (c): In 48 ways.

(3) $77 = 7 \cdot 11$, so the congruence $x^2 \equiv 17 \pmod{77}$ is solvable if and only if the congruences $x \equiv 17 \pmod{7}$ and $x^2 \equiv 17 \pmod{11}$ are both solvable. Computing the Legendre symbol $(\frac{17}{7}) = (\frac{3}{7}) = -(\frac{7}{3}) = -(\frac{1}{3}) = -1$, where the quadratic reciprocity law is used. shows that the first congruence is not solvable. (The second congruence is not solvable either.) Note that the Jacobi symbol $(\frac{17}{77}) = 1$. but this gives us no information about the solvability of the congruence $x^2 \equiv 17 \pmod{77}$.
ANSWER: No, the congruence has no solutions.

(4) (a) Since $8^2 < 80 < 9^2$, $8 < \sqrt{80} < 9$ and $a_0 = [\sqrt{80}] = 8$. $\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{80}-8} = \frac{\sqrt{80}+8}{16}$. $1 = \frac{8+8}{16} < \alpha_1 < \frac{9+8}{16} < 2$. Hence $a_1 = 2$. $\alpha_2 = \frac{1}{\alpha_1 - a_1} = \sqrt{80} + 8$. $a_2 = [\sqrt{80} + 8] = [\sqrt{80}] + 8 = 16$. We then get $\alpha_3 = \alpha_1$. Hence $\sqrt{80} = [8; \overline{1, 16}]$. The period length is even, namely 2.
  (b) The positive solutions of the diophantine equation $x^2 - 80y^2 = 1$ are given by $(x_j, y_j) = (p_{2j-1}, q_{2j-1})$ for $j = 1, 2, 3, \ldots$. The least one is obtained from $\frac{p_1}{q_1} = [8; 1] = 8 + \frac{1}{1} = \frac{9}{1}$. The next solution we get from $\frac{p_3}{q_3} = [8; 1, 16, 1] =$

$\frac{161}{18}$, and therefore the two smallest solutions are $x = 9, y = 1$ and $x = 161, y = 18$. If you have found the first solution $x_1 = 9, y_1 = 1$, which you can also find by inspection, then the next solution (x_2, y_2) can also be computed by using the formula $x_2 + y_2\sqrt{80} = (x_1 + y_1\sqrt{80})^2 = (9 + \sqrt{80})^2 = 161 + 18\sqrt{80}$.

ANSWER: (a): $[8; \overline{1, 16}]$ (b): The two smallest solutions are $(x, y) = (9, 1)$ and $(x, y) = (161, 18)$.

(5) (a) $\operatorname{ord}_{41} 6 \mid \varphi(41) = 40$. $6^2 = 36 \equiv -5 \pmod{41}$, $6^4 \equiv 25 \equiv -16 \pmod{41}$, $6^5 \equiv -96 \equiv -14 \pmod{41}$, $6^8 \equiv (-16)^2 \equiv 256 \equiv 10 \pmod{41}$, $6^{10} = (6^5)^2 \equiv 196 \equiv -9 \pmod{41}$, $6^{20} \equiv (-9)^2 \equiv 81 \equiv -1 \pmod{41}$ Hence $\operatorname{ord}_{41} 6 = 40$ and 6 is a primitive root modulo 41.

(b) $82 = 2 \cdot 41$ and 6 is a primitive root modulo 41. Since 6 is an even number we get that $6 + 41 = 47$ is a primitive root modulo 82.

ANSWER: (b): E.g. 47 is a primitive root modulo 82.

(6) (a) The largest possible order of an integer modulo 77 equals $\lambda(77)$ computed as the least common multiple of the numbers $\lambda(7) = 6$ and $\lambda(11) = 10$, since $77 = 7 \cdot 11$. Hence $\lambda(77) = 30$.

(b) In order to find an integer whose order modulo 77 is 30, we first find integers a_1 and a_2, such that $\operatorname{ord}_7 a_1 = 6$ and $\operatorname{ord}_{11} a_2 = 10$. Let us take $a_1 = 3$

and $a_2 = 2$. Then if $a \cong 3 \pmod 7$, then $a^k \equiv 1 \pmod{77}$ if and only if $a^k \equiv 1 \pmod 7$ and $\pmod{11}$ if and only if k is divisible by both 6 and 10 i.e divisible by 30. Hence $\operatorname{ord} a = 30$. Using the chinese remainder theorem we can take $a = 23$.

ANSWER: (a): 30 (b): E.g. 24.