(SKETCHES OF) SOLUTIONS, NUMBER THEORY, TATA 54, 2016-08-27

(1) Since $75 = 3 \cdot 5^2$, $\varphi(75) = 2 \cdot 5 \cdot 4 = 40$. By Euler's theorem $7^{40} \equiv 1 \pmod{75}$, observing that $1242 = 31 \cdot 40 + 2$, we get $7^{1242} = (7^{40})^{31} \cdot 7^2 \equiv 7^2 \equiv 49 \pmod{75}$ **ANSWER:** 49.

(2) We use the law of quadratic reciprocity and the formula for the values at 2 of the Legendre symbol. First factorise into primes: $437 = 19 \cdot 23$.

$(\frac{6}{19}) = (\frac{2}{19})(\frac{3}{19}) = (-1)(\frac{3}{19}) = (\frac{19}{3}) = (\frac{1}{3}) = 1$.

$(\frac{6}{23}) = (\frac{2}{23})(\frac{3}{23}) = 1 \cdot (\frac{3}{23}) = -(\frac{23}{3}) = -(\frac{2}{3}) = -(-1) = 1$.

Since the Legendre symbols $(\frac{6}{19})$ and $(\frac{6}{23})$ have the value 1, the congruences $x^2 \equiv 6 \pmod{19}$ and $x^2 \equiv 6 \pmod{23}$ are both solvable. Hence also $x^2 \equiv 6 \pmod{19 \cdot 23}$ is solvable.

ANSWER: Yes

(3) Since each solution of the congruence $f(x) \equiv 0 \pmod{7^2}$ is also a solution of the congruence $f(x) \equiv 0 \pmod 7$, we first solve that congruence. This is done by computing $f(x)$ for $x = 0, \pm1, \pm2, \pm3$. We find that the solutions are $x \equiv 2 \pmod 7$. Hence the solutions of $f(x) \equiv 0 \pmod{7^2}$ must be of the form $x = 2 + 7t$ for some $t \in \mathbb{Z}$. Next we want to determine those t, which actually yield solutions. By the binomial theorem $f(2+7t) = (2+7t)^4+(2+7t)+3 \equiv 2^4 + 4 \cdot 2^3 \cdot 7t + 2 + 7t + 3 \equiv 21 + 33 \cdot 7t \equiv 7 \cdot 3 + (-2 + 7 \cdot 5)7t \equiv 7(3 - 2t) \pmod{7^2}$. Therefore $f(2 + 7t) \equiv 0 \pmod{7^2} \iff 3 - 2t \equiv 0 \pmod 7 \iff 2t \equiv 3 \pmod 7 \iff 4 \cdot 2t \equiv 4 \cdot 3 \pmod 7 \iff t \equiv 5 \pmod 7$. We get the solutions $x = 2 + 7(5 + 7n) = 37 + 49n$ for some $n \in \mathbb{Z}$.

ANSWER: $x = 37 + 49n$, where $n \in \mathbb{Z}$

(4) First we expand 101 into a continued fraction using the usual algorithm (see the textbook, the calculations are not written down here) We get $\sqrt{101} = [10; \overline{20}]$ and since the period length is one the positive solutions of $x^2 - 101y^2$ are given by $(x_j, y_j) = (p_{(2j-1)\cdot 1-1}, q_{(2j-1)\cdot 1-1}$ for $j = 1, 2, \dots$, where $\frac{p_k}{q_k}$ is the k'th convergent of the continued fraction $[10; \overline{20}]$. Thus the first solution is $(x_1, y_1) = (p_0, q_0) = (10, 1)$. The next one is $(x_2, y_2) =$

(p_2, q_2), which we get by computing

$$\frac{p_2}{q_2} = [10; 20, 20] = 10 + \cfrac{1}{20 + \cfrac{1}{20}} = 10 + \frac{20}{401} = \frac{4030}{401}$$

ANSWER: The two smallest solutions in positive integers are $(10, 1)$ and $(4030, 401)$.

(5) (a) $2^6 = 64 \equiv -9 \pmod{73}$, $2^9 = 2^3 \cdot 2^6 \equiv 8(-9) \equiv -72 \equiv 1 \pmod{73}$ Hence the order of 2 modulo 73 divides 9. Since it is not 1 or 3, it must be 9.

(b) Let d be the order of 5 modulo 73. It must be a divisor of $\varphi(73) = 72 = 2^3 3^2$. The computations we have to show that $d = 72$, that is that 5 is a primitive root, can be done as follows. Note that $5^4 = 625 = 10 \cdot 73 - 105 \equiv -32 \equiv -2^5 \pmod{73}$. Hence $5^{4 \cdot 9} \equiv (-2^5)^9 \equiv -(2^9)^5 \equiv -1 \pmod{73}$. It follows that d does not divide 36. We just have to exclude that $d = 8$ or $d = 24$. But this follows from $5^{24} = (5^4)^6 \equiv (-2^5)^6 \equiv 2^{30} \not\equiv 1 \pmod{73}$, since the order of 2 does not divide 30.

ANSWER: (a): 9 (b): For example 5 is a primitive root of 73.

(6) If p is a prime number that divides n, then necessarily $p - 1$ divides $\varphi(n) = 500 = 2^2 5^3$. Therefore the only primes that possibly could divide n are $2, 3, 5, 11, 101, 251$. Also when p^2 divides n, then $p | \varphi(n)$. Hence 3, 11, 101 and 251 can occur only to the first power in the prime factorisation of n. If $251 | n$ then $n = 251m$ and since m and 251 must be relatively prime $\varphi(n) = 250\varphi(m)$ and therefore $\varphi(m) = 2$. Hence $m = 2^2$, 3 or $2 \cdot 3$. In this case we get $n = 753, 1004, 1506$. If $101 | n$ then $n = 101m$ and thus $\varphi(m) = 5$, and no such m exists, because $\varphi(m)$ is always even for $m > 2$. If $11 | n$, then $n = 11m$ and we get $\varphi(m) = 50 = 2 \cdot 5^2$ and it is easily seen that there are no such numbers m. If the prime divisors of n are among $2, 3, 5$ then $n = 5^4$ or $n = 2 \cdot 5^4$.

ANSWER: $n = 625, 753, 1004, 1250, 1506$.