(SKETCHES OF) SOLUTIONS, NUMBER THEORY, TATA 54, 2015-08-29

(1) Observe that $21 \equiv -2 \pmod{23}$ and we show that -2 is a primitive root modulo 23. Now $\varphi(23) = 22 = 2 \cdot 11$. Since $\operatorname{ord} -2|23$, we have to exclude that $(-2)^{11} \equiv 1 \pmod{23}$. First $(-2)^8 = 256 \equiv 3 \pmod{23}$, hence $(-2)^{11} = (-2)^3 \cdot (-2)^8 \equiv -8 \cdot 3 \equiv -24 \equiv -1 \pmod{23}$

(2) A positive integer is the sum of two squares if and only if each prime divisor, which is $\equiv 3 \pmod 4$ occurs to an even power in the prime factorization.

(a) $605 = 5 \cdot 121 = 5 \cdot 11^2$

(b) $697 = 17 \cdot 41$

(c) $711 = 3^2 \cdot 79$

ANSWER: Only the two first ones.

(3) The number 103 is a prime number. $x^4 \equiv 4 \pmod{103} \iff (x^2 - 2)(x^2 + 2) \equiv 0 \pmod{103} \iff x^2 - 2 \equiv 0 \pmod{103}$ or $x^2 + 2 \equiv 0 \pmod{103}$. The first congruence congruence is equivalent to $x^2 \equiv 2 \pmod{103}$, which has solutions, since the Legendre symbol $(\frac{2}{103}) = 1$. Note that $103 \equiv -1 \pmod 8$.

ANSWER: Yes.

(4) (a) Since $\varphi(17) = 16 = 2^4$, $\operatorname{ord}_{27} 5$ divides 2^4. The following computations will show that 5 has order 16 modulo 17 and thus is a primitive root. $5^2 \equiv 8 \pmod{17}$, $5^4 \equiv 8^2 \equiv 64 \equiv -4 \pmod{17}$, $5^8 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$.

(b) By definition $\operatorname{ind}_5 a$ is the integer k, such that $5^k \equiv a \pmod{17}$ and $1 \leq k \leq 16$. E.g $5^3 \equiv 6 \pmod{17}$ and thus $\operatorname{ind}_5 6 = 3$. In order to find your table of indices just compute the least positive residues of the powers of 5. Some indices can be more quickly found by using the logarithmic laws for indices applied to previously computed ones. All your computations should of course be presented.

(c) $8^x + 18 \equiv 0 \pmod{17} \Leftrightarrow 8^x \equiv -13 \pmod{17}$
$\Leftrightarrow 8^x \equiv 4 \pmod{17} \Leftrightarrow x \operatorname{ind}_5 8 \equiv \operatorname{ind}_5 4 \pmod{16}$
$\Leftrightarrow 2x \equiv 12 \pmod{16} \Leftrightarrow x \equiv 6 \pmod 8$
$\Leftrightarrow x = 6 + 8n$, $n = 0, 1, 2, \ldots$

ANSWER: (b): $16, 6, 13, 12, 1, 3, 15, 2, 10, 7, 11, 9, 4, 5, 14, 8$.
(c): $x = 6 + 8n$, $n = 0, 1, 2, \ldots$

(5) The number 561 is composite; $561 = 11 \cdot 51 = 3 \cdot 11 \cdot 17$ We have also to show that

$$35^{\frac{561-1}{2}} \equiv \left(\frac{35}{561}\right)$$

Now $35 \equiv 2 \pmod 3$, $35 \equiv 2 \pmod{11}$ and $35 \equiv 1 \pmod{17}$. $(\frac{35}{561}) = (\frac{35}{3})(\frac{35}{11})(\frac{35}{17}) = (\frac{2}{3})(\frac{2}{11})(\frac{1}{17}) = (-1) \cdot (-1) \cdot 1 = 1$, $35^{280} \equiv (-1)^{280} \equiv 1 \pmod 3$, $35^{280} \equiv 1 \pmod{11}$, by Fermat's little theorem , since $10|280$. $35^{280} \equiv 1^{280} \pmod{17}$ Hence we can conclude that the desired congruence is valid.

(6) (a) We compute the periodic continued fraction expansion of $\alpha = \sqrt{7}$, using the algorithm

$$\alpha_0 = \alpha$$
$$a_n = [\alpha_n]$$
$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$$

To see how such computations (which I do not write out here) are performed, see the solutions of other exams. It turns out to be $[2; \overline{1, 1, 1, 4}]$.

(b) The convergents

$$C_k = \frac{p_k}{q_k} = [a_0; a_1, a_2, \ldots, a_k]$$

satisfy the inequalities

$$|\alpha - C_k| < \frac{1}{{q_k}^2}$$

Testing with $k = 4$, we get

$$C_4 = [2; 1, 1, 1, 4] = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4}}}}$$

We get $C_4 = \frac{37}{14}$ and thus

$$|\sqrt{7} - \frac{37}{14}| < \frac{1}{14^2}$$

Alternatively use the algorithm for computing the numbers p_k and q_k, see the textbook. **ANSWER:**(a) $[2; \overline{1, 1, 1, 4}]$, (b) For example $r = \frac{37}{14}$