(SKETCHES OF) SOLUTIONS, NUMBER THEORY, TATA 54, 2016-06-09

(1) Since $108 = 2^2 \cdot 3^3$, we show that $n^{21} \equiv n^3 \pmod 4$ and $n^{21} \equiv n^3 \pmod{3^3}$ for all n.

If n is even, then both n^{21} and n^3 are divisible by 4. If n is odd, then $n^2 \equiv 1 \pmod 4$ and therefore $n^{21} \equiv n(n^2)^{10} \equiv n \equiv n^3 \pmod 4$. Hence the first congruence holds.

If $3|n$, then both sides in the second congruence are congruent to 0 modulo 3^3. If $3 \nmid n$, then by Euler's theorem $n^{18} \equiv 1 \pmod{3^3}$. Observe that $\varphi(3^3) = 3^2 \cdot 2 = 18$. Hence $n^{21} = n^3 \cdot n^{18} \equiv n^3 \pmod{3^3}$.

(2) A positive integer can be written as the sum of the squares of two integers if and only if each prime of the form $4k + 3$ in its prime factorization occurs to an even power.

(a) $4949 = 7^2 \cdot 101$

(b) $3069 = 3^2 \cdot 11 \cdot 31$

(c) If $n = x^2+y^2$, then n is congruent to 0, 1 or 2, since a square is congruent to 0 or 1 modulo 4. However $100000000003 \equiv 3 \pmod 4$.

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

(3) First 3751 is a composite number, namely $3751 = 11 \cdot 341 = 11^2 \cdot 31$. (Note that $1 - 5 + 7 - 3 = 0$ and $1 - 4 + 3 = 0$). We want to show that the second condition for a number to be a pseudoprime is satisfied, namely in our case that $3^{3750} \equiv 1 \pmod{3751}$. Now $3^5 = 243 \equiv 1 \pmod{11^2}$ and since $5|3750$ therefore $3^{3750} \equiv \pmod{11^2}$. Since $30|3750$, using Fermat‘s little theorem we also get $3^{3750} \equiv 1 \pmod{31}$. Hence the second condition is satisfied.

(4) (a) Since $4036 \equiv 10 \pmod{2013}$, we get

$$(\frac{4036}{2013}) = (\frac{10}{2013}) = (\frac{2}{2013})(\frac{5}{2013}).$$

But $(\frac{2}{2013}) = -1$, since $2013 \equiv 5 \pmod 8$ and using the law of quadratic reciprocity

$$(\frac{5}{2013}) = (\frac{2013}{5}) = (\frac{3}{5}) = (\frac{5}{3}) = (\frac{2}{3}) = -1.$$

Hence $(\frac{4036}{2013}) = (-1) \cdot (-1) = 1$.

(b) Since $11|2013$,the congruence $x^2 \equiv 4036 \pmod{2013}$ is equivalent to $x^2 \equiv 10 \pmod{2013}$. If this congruence is satisfied then $x^2 \equiv 10 \pmod{11}$ and therefore $x^2 \equiv -1 \pmod{11}$, would have a solution, which is not the case. The prime number 11 is namely congruent to 3 modulo 4.

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

(5) (a) Use the algoritm

$\alpha_0 = \alpha$

$a_k = [\alpha_k]$

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

to compute the continued fraction expansion $[a_0; a_1, a_2, \ldots ...]$ of an irrational number α. You will find that $\sqrt{15} = [3; \overline{1, 6}]$,

(b) Since the periodlength is even (= 2), there are no integer solutions to $x^2 - 15y^2 = -1$. This can also been seen in a different way. If x and y are integers such that $x^2 - 15y^2 = -1$, then $x^2 \equiv -1 \pmod{3}$, but that is impossible.

ANSWER: (a): $[3; \overline{1, 6}]$ (b): No, it has no solutions.

(6) We will use that $\operatorname{ord}_{43} a | 42$ for all integers a not divisible by 43.

(a) $2^7 = 128 = 129 - 1 \equiv -1 \pmod{43}$ and therefore $2^{14} \equiv 1 \pmod{43}$. Hence $\operatorname{ord}_{43} 2 | 14$ Since $\operatorname{ord}_{43} 2 \neq 1, 2, 7$ necessarily $\operatorname{ord}_{43} 2 = 14$.

(b) The calculations $3^4 = 81 = -5 + 2 \cdot 43 \equiv -5 \pmod{43}$, $3^6 = 3^2 \cdot 3^4 \equiv -45 \equiv -2 \pmod{43}$, $3^7 \equiv -6 \pmod{43}$, $3^{14} \equiv 36 \equiv -7 \pmod{43}$, $3^{21} \equiv (-6)(-7) \pmod{43}$, show that $\operatorname{ord}_{43} 3 = 42$. Hence 3 is a primitive root of 43.

(c) Let $d = \operatorname{ord}_{43^2} 3$. Then $d \mid \varphi(43^2) = 43 \cdot 42$. Since $3^d \equiv 1 \pmod{43^2}$ also $3^d \equiv 1 \pmod{43}$. Therefore $42 = \operatorname{ord}_{43} 3 \mid d$. Hence there are just two possibilities, namely $d = 42$ or $d = 43 \cdot 42$. We will exlude the first one by showing that 3^{42} is not congruent to 1 modulo 43^2. So we start to calculate and we use the binomial theorem.

$3^4 = 81 = -5 + 2 \cdot 43$,

$3^6 = 9(-5 + 2 \cdot 43) = -45 + 18 \cdot 43 = -2 + 17 \cdot 43$,

$3^{42} = (3^6)^7 = (-2 + 17 \cdot 43)^7 \equiv -2^7 + 7 \cdot 2^6 \cdot 17 \cdot 43 \equiv -128 + 64 \cdot 119 \cdot 43 \equiv 1 - 3 \cdot 43 + (21 + 43)(-10 + 3 \cdot 43) \cdot 43 \equiv 1 - 3 \cdot 43 - 210 \cdot 43 \equiv 1 - 213 \cdot 43 \equiv 1 - (5 \cdot 43 - 2)43 \equiv 1 + 2 \cdot 43 \pmod{43^2}$.

Hence the first possibility is excluded and 3 is therefore a primitive root of 43^2.

Answer: (a) $\operatorname{ord}_{43} 2 = 14$.