(SKETCHES OF) SOLUTIONS, NUMBER THEORY, TATA 54, 2015-06-10

(1) (a) $\varphi(\varphi(113)) = \varphi(112) = \varphi(2^4 \cdot 7) = 2^3 \cdot 6 = 48$.

(b) The order of 2 modulo 113 is a divisor of $112 = 2^4 \cdot 7$. $2^7 = 128 \equiv 128 \equiv 15 \pmod{113}$, $2^{14} \equiv 15^2 \equiv 225 \equiv -1 \pmod{113}$, $2^{28} \equiv 1 \pmod{113}$. Therefore the order of 2 must divide 28 and it is not $1, 2, 4, 7$ or 14, so it must be 28. Hence it is not a primitive root.

ANSWER: (a): 48

(2) The norm of a gaussian prime dividing $\alpha = 11 - 8i$ must be a divisor of the norm of α, i.e of $185 = 5 \cdot 37$. The norm of $\pi = 2 - i$ is 5 and since 5 is a (rational) prime, π is a gaussian prime. Let us test if it divides α. Yes, $\frac{11-8i}{2-i} = 6 - i$. Also $6 - i$ is a gaussian prime, since its norm is the prime number 37.

ANSWER: $(2 - i)(6 - i)$

(3) $5^{12} - 1 = (5^6 - 1)(5^6 + 1)$, $5^6 - 1 = (5^3 - 1)(5^3 + 1) = (5 - 1)(5^2 + 5 + 1)(5 + 1)(5^2 - 5 + 1) = 4 \cdot 31 \cdot 6 \cdot 21$. $5^6 + 1 = 25^3 + 1 = (25 + 1)(25^2 - 25 + 1) = 2 \cdot 13 \cdot 601$. Hence $5^{12} - 1 = 2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$. It remains to show that 601 is a prime number. Since $\sqrt{601} < 25$, we have just to show that no prime less than and equal to 23 divides $601 = 25^2 - 25 + 1 = 25 \cdot 24 + 1$. This is evident for $2, 3, 5$. $601 \equiv 4 \cdot 3 + 1 \equiv 13 \pmod 7$, $601 \equiv 1 - 0 + 6 \equiv 7 \pmod{11}$, $601 \equiv (-1)(-2) + 1 \equiv 3 \pmod{13}$, $601 \equiv 8 \cdot 7 + 1 \equiv 4 \pmod{17}$, $601 \equiv 6 \cdot 5 + 1 \equiv 12 \pmod{19}$, $601 \equiv 2 \cdot 1 + 1 \equiv 3 \pmod{23}$.

ANSWER: (a): $2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$.

(4) (a) We use the reciprocity law for the Jacobi symbol, observing that $143 \equiv 7 \equiv 3 \pmod 4$.
$(\frac{28}{143}) = (\frac{7}{143}) = -(\frac{143}{7}) = -(\frac{3}{7}) = (\frac{7}{3}) = (\frac{1}{3}) = 1$

(b) But $143 = 11 \cdot 13$ is composite, so we cannot use that the Jacobisymbol is 1, in order to conclude that the congruence is solvable. However, since the Legendre symbol $(\frac{28}{13}) = (\frac{2}{13}) = -1$, on the contrary the congruence has no solutions.

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

(5) (a) can be solved by expanding $\sqrt{7}$ in a continued fraction and noting that its periodlength is even. However it is a special case of (b); If there are integers x, y, such that $x^2 - ny = -1$,

then the congruence $x^2 \equiv -1 \pmod{p}$ has a solution, for each prime p, dividing n. But when $p \equiv 3 \pmod{4}$, it cannot have a solution!

(6) Evidently we should use Fermat's litle theorem.
$n \sum_{d|n} d^{p-2} = \sum_{d|n} \frac{n}{d} d^{p-1} \equiv \sum_{d|n} \frac{n}{d} \cdot 1 \equiv \sum_{d|n} d \equiv \sigma(n) \pmod{p}$, since $d^{p-1} \equiv 1 \pmod{p}$ for each divisor d of n, when the prime p does not divide n. If n is a perfect number, then $\sigma(n) = 2n$. Hence from (a) we get that $n \sum_{d|n} d^{p-2} \equiv 2n \pmod{p}$. Since $(n, p) = 1$, we can cancel p and we get the congruence in (b).