Math 5653. Solutions to the Second test.

Problem 1: Find all integers n for which $\phi(n)$ is NOT divisible by 4.

Solution: First note that $\phi(1) = 1$ is not divisible by 4. Assume now that $n \geq 2$, so we can write $n = \prod_{i=1}^{k} p_i^{a_i}$ where p_i are distinct primes and $a_i \in \mathbb{N}$. Then $\phi(n) = \prod_{i=1}^{k} \phi(p_i^{a_i})$, and $\phi(n)$ is NOT divisible by 4 if and only if at most one of the numbers $\phi(p_i^{a_i})$ is even and none of them is divisible by 4.

We know that $\phi(p^a)$, with $a \geq 1$, is even unless $p = 2$ or $a = 1$, so at most one prime power in the factorization of n is larger than 2, so n must be of the form 2^a, p^a or $2p^a$ for some odd prime p. Since $\phi(2^a) = 2^{a-1}$, we have $4 \nmid \phi(2^a) \iff a = 1$ or 2. If p is an odd prime, then $\phi(2p^a) = \phi(p^a) = p^{a-1}(p-1)$, and this number is not divisible by 4 if and only if $p \equiv 3 \mod 4$.

So the final answer is as follows: $\phi(n)$ is not divisible by 4 if and only if $n = 1, 2, 4, p^a$ or $2p^a$ where $p \equiv 3 \mod 4$.

Problem 2: Find the number of reduced solutions to the congruence

$$x^2 + 8x \equiv 54 \mod 1423.$$

The number 1423 is prime (you do not need to verify this).

Solution: Completing the square, we see that our congruence is equivalent to $(x+4)^2 \equiv 70 \mod 1423$. The map $x \mapsto x+4$ from $\mathbb{Z}$ to $\mathbb{Z}$ is bijective and preserves congruence classes mod 1423, so the number of reduced solutions to $(x+4)^2 \equiv 70 \mod 1423$ is equal to the largest number of pairwise noncongruent solutions to $(x+4)^2 \equiv 70 \mod 1423$ is equal to the largest number of pairwise noncongruent solutions to $y^2 \equiv 70 \mod 1423$ is equal to the number of reduced solutions to $y^2 \equiv 70 \mod 1423$. We know that the latter number $1 + \left(\frac{70}{1423}\right)$.

We compute $\left(\frac{70}{1423}\right)$ using quadratic reciprocity and the formula for $\left(\frac{2}{p}\right)$. Note that $1423 = 8 \cdot 7 \cdot 5 \cdot 5 + 23$, so $1423 \equiv 7 \mod 8$, $1423 \equiv 3 \mod 4$, $1423 \equiv 3 \mod 5$ and $1423 \equiv 2 \mod 7$. Since $70 = 2 \cdot 5 \cdot 7$, we have

$$\left(\frac{70}{1423}\right) = \left(\frac{2}{1423}\right)\left(\frac{5}{1423}\right)\left(\frac{7}{1423}\right) = 1 \cdot \left(\frac{1423}{5}\right) \cdot (-1) \cdot \left(\frac{1423}{7}\right)$$
$$= (-1) \cdot \left(\frac{3}{5}\right) \cdot \left(\frac{2}{7}\right) = (-1) \cdot \left(\frac{5}{3}\right) \cdot 1 = -\left(\frac{2}{3}\right) = -(-1) = 1.$$

So the given congruence has 2 reduced solutions.

Problem 3: Prove that the group $U_p = \mathbb{Z}_p^\times$ is cyclic for any prime p.

Solution: See Corollary 8.3 in Lecture 8 notes.

Problem 4: Let p be a prime of the form $4k+3$. Prove that the congruence

$$x^4 \equiv 25 \mod p$$

has a solution.

Solution: Suppose that $x^4 \equiv 25 \mod p$ has no solutions. Since $x^2 \equiv \pm 5 \mod p$ implies[1] that $x^4 \equiv 25 \mod p$, it follows that none of the congruence $x^2 \equiv 5 \mod p$ and $x^2 \equiv -5 \mod p$ has solutions. This means that $\left(\frac{5}{p}\right) = -1$ and $\left(\frac{-5}{p}\right) = -1$. On the other hand, $\left(\frac{-5}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{-1}{p}\right) = -\left(\frac{5}{p}\right)$ since $p \equiv 3 \mod 4$, so we reached a contradiction.

Problem 5: Find the largest integer n for which $exp(U_n) = 2$.

Solution: Write $n = \prod_{i=1}^k p_i^{a_i}$ where p_i are distinct primes and $a_i \in \mathbb{N}$. Then $U_n \equiv U_{p_1^{a_1}} \times \ldots \times U_{p_k^{a_k}}$, so $exp(U_n) = LCM(U_{p_1^{a_1}}, \ldots, U_{p_k^{a_k}})$.

Thus $exp(U_n) = 2$ if and only if $exp(U_{p_i^{a_i}}) = 1$ or 2 for each i, and at least one of these exponents is equal to 2 (note that both 1 and 2 may appear more than once).

If p is an odd prime, then U_{p^a} is cyclic, then $exp(U_{p^a}) = |U_{p^a}| = \phi(p^a) = p^{a-1}(p-1)$ which is never equal to 1 and equals 2 if and only if $p^a = 3$.

On the other hand, we know that $exp(U_{2^a}) = 2^{a-1}$ for $a = 1$ or 2 and $exp(U_{2^a}) = 2^{a-2}$ for $a \geq 3$, so $exp(U_{2^a}) = 1$ or 2 if and only if $2^a = 2, 4$ or 8.

Thus, the largest n for which $exp(U_n) = 2$ is $n = 3 \cdot 8 = 24$.

[1] The opposite implication is also true by Euclid's lemma, but we do not need it for this problem