In this exam all variables are integers. Solutions mean integer solutions.

1. (25 points) Let $n > 1$. Assume that $\mu(\phi(n)) \neq 0$.

Show that primitive roots modulo $n$ exist.

2. (25 points) Show that there are infinitely many odd prime numbers $p$ such that both $2$ and $-2$ are quadratic *non*-residues modulo $p$.

3. (25 points) Assume $n > 1$ and $n = p_1 p_2 \cdots p_k$ where $p_i$'s are distinct prime numbers, and $k$ is even. Show that

$$\sum_{d \mid n, 0 < d < \sqrt{n}} \mu(d) = 0.$$ 

4. (25 points) How many mutually incongruent solutions do the following equations have? Explain your answers. (Fact: $304$ is a primitive root modulo $2017$.)

(1). $x^2 \equiv 304 \pmod{2017^2}$
(2). $x^{27} \equiv 304 \pmod{2017^2}$
(3). $x^{2017} + x \equiv 304 \pmod{2017^2}$

Solutions on next page
Solutions:

1. Note that if $4 \mid \phi(n)$ then $\mu(\phi(n)) = 0$. If there exist two different odd prime factors of $p \mid n$ and $q \mid n$, then $(p-1)(q-1) \mid \phi(n)$. Both $p-1$ and $q-1$ are even, so $4 \mid n$. Therefore $n$ must be the form of $2^k \cdot p^\alpha$, or $2^k \cdot p^\alpha$ where $p$ is odd prime. If $n = 2^k$ and $k > 2$, then $4 \mid \phi(n) = 2^{k-1}$. If $n = 2^k \cdot p^\alpha$ and $k > 1$, then $\phi(n) = 2^{k-1} \cdot p^{\alpha-1} \cdot (p-1)$ is also a multiple of 4. So the only possible such $n$ are 2, 4, $p^\alpha$, $2p^\alpha$ ($p$ odd prime, and in fact $\alpha \leq 2$) which all have primitive roots by results of exercises in §7.2.

2. The assumption means $\left(\frac{2}{p} \right) = -1$ and $\left(\frac{-2}{p} \right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = -1$. These hold if and only if $p \equiv 5 \pmod{8}$.

To show there exists infinitely many prime number of $8k + 5$: Assume there are only finitely many prime numbers that are congruent to 5 modulo 8. Call them $p_1, \ldots, p_r$. Consider $N = (p_1 p_2 \ldots p_r)^2 + 4$ (or $(2p_1 p_2 \ldots p_r)^2 + 1$). Then $N \equiv 5 \pmod{8}$. If $p \mid N$ is a prime factor, then $(p_1 p_2 \ldots p_r)^2 \equiv -4 \pmod{p}$. Therefore $\left(\frac{-2}{p} \right) = \left(\frac{1}{p}\right) = 1$ which means $p \equiv 1 \pmod{8}$ or $p \equiv 5 \pmod{8}$. However $N \equiv 5 \pmod{8}$ so it has at least one prime factor $q$ such that $q \equiv 5 \pmod{8}$. By assumption, $q \mid p_1 p_2 \ldots p_r$ and $q \mid N$. Thus $q \mid 4$ which is a contradiction.

3. For each $d \mid n$ and $0 < d < \sqrt{n}$, we have the corresponding $\frac{n}{d} \mid n$ and $\sqrt{n} < \frac{n}{d} < n$. Since $n$ is square free and has even number of factors, $\mu(d) = \mu\left(\frac{n}{d}\right)$. Also $\sqrt{n} \notin \mathbb{Z}$. Therefore

$$\sum_{d \mid n, \ 0 < d < \sqrt{n}} \mu(d) = \sum_{d \mid n, \ \sqrt{n} < d < n} \mu(d)$$

so

$$\sum_{d \mid n, \ 0 < d < \sqrt{n}} \mu(d) = \frac{1}{2} \sum_{d \mid n} \mu(d) = 0$$

by Theorem 6-5.

4. (1). You can do a direct computation $\left(\frac{304}{2017}\right) = \left(\frac{16}{2017}\right)\left(\frac{19}{2017}\right) = \left(\frac{19}{2017}\right) = \left(\frac{3}{19}\right) = \left(\frac{2}{19}\right) = -1$. So the equation $x^2 \equiv 304 \pmod{2017}$ has no solution. However you could see immediately that the fact that 304 is a primitive root modulo 2017 implies it is not a quadratic residue. In any case $x^2 \equiv 304 \pmod{2017^2}$ does not have solution either.

(2). This is similar to part (1). The equation does not have any solution: If $a^{27} \equiv 304 \pmod{2017^2}$, then $a^{27} \equiv 304 \pmod{2017}$. But then $304^{2016} \equiv (a^{27})^{2016} \equiv (a^{2016})^9 \equiv 1 \pmod{2017}$, which is a contradiction since 304 is a primitive root modulo 2017. See Exercise #7 in §7.1.

(3). First look at the equation $x^{2017} + x - 304 \equiv 0 \pmod{2017}$. By Fermat’s Theorem $x^{2017} \equiv x \pmod{2017}$. So the equation is $2x - 304 \equiv 0 \pmod{2017}$ which has a unique solution $m \equiv 152 \pmod{2017}$. Now $(x^{2017} + x - 304)' = 2017x^{2016} + 1$, so $2017 \mid (x^{2017} + x - 304)'_{x=m}$. Therefore by Exercise 3 and 4 in §5.4, there exists a unique $r \pmod{2017}$ such that $m + 2017r$ is a solution of $x^{2017} + x - 304 \equiv 0 \pmod{2017^2}$. Thus the solution exists and is unique (up to congruence modulo 2017²).