Problem 1. List all quadratic residues modulo 23.

Solution: The quadratic residues modulo 23 are:

- $1^2 \equiv 22^2 \equiv 1$
- $2^2 \equiv 21^2 \equiv 4$
- $3^2 \equiv 20^2 \equiv 9$
- $4^2 \equiv 19^2 \equiv 16$
- $5^2 \equiv 18^2 \equiv 2$
- $6^2 \equiv 17^2 \equiv 13$
- $7^2 \equiv 16^2 \equiv 3$
- $8^2 \equiv 15^2 \equiv 18$
- $9^2 \equiv 14^2 \equiv 12$
- $10^2 \equiv 13^2 \equiv 8$
- $11^2 \equiv 12^2 \equiv 6$

Answer: \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}. □

Problem 2. Find all solutions of $x^2 \equiv 2 \pmod{61}$ and $x^2 \equiv -2 \pmod{61}$.

Solution: We compute that

$(-2)^{30} = 2^{30} = (2^6)^5 = (64)^5 \equiv 3^5 = 243 \equiv -1 \pmod{61}$.

It follows by Euler’s criterion that neither 2 nor $-2$ is a quadratic residue modulo 61. Therefore neither of the equations has a solution. □


Solution: Since $13 - 1 = 12$, the possible orders of elements in $\mathbb{F}_{13}^*$ are 1, 2, 3, 4, 6, 12. We are looking for an element of order 12. The first residue we will try is 2. Since $2^2 = 4, 2^3 = 8, 2^4 = 16 \equiv 3 \pmod{13}, 2^6 = 64 \equiv -1 \pmod{13}$, we conclude that 2 has order exactly 12. We are done: 2 is a primitive root of 13.

Remark. There are $\phi(12) = (4 - 2)(3 - 1) = 4$ primitive roots of 13, with 2 being just one of them. The other three primitive roots are $2^5 \equiv 6, 2^7 \equiv 11$, and $2^{11} \equiv 7$. □
Problem 4. Find all solutions of $x^8 \equiv 5 \pmod{13}$.

Solution: We will use the fact that 2 is a primitive root of 13 from the previous problem. By looking at the residues of $2, 4, 8, 16, 32, 64, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}$ modulo 13, we see that $2^9 = 512 \equiv 5 \pmod{13}$. Thus we are looking for solutions of $x^8 \equiv 2^9 \pmod{13}$.

Since 2 is a primitive root of 13, every residue is represented as $2^k$ for some $k$. So we are looking for the solutions in the form $x = 2^k$. The equation then becomes $2^8k \equiv 2^9 \pmod{13}$.

Using the cancellation property of congruences, we obtain $2^{8k-9} \equiv 1 \pmod{13}$.

Since the order of 2 is 12, the last equation is equivalent to $8k - 9 \equiv 0 \pmod{12}$. This last congruence however has no solutions, as 9 is not divisible by 4 but 8 and 12 are.

Answer: No solutions. \qed

Problem 5. Let $p \geq 5$ be a prime and $m$ a positive integer. Show that

\[
\binom{mp-1}{p-1} \equiv 1 \pmod{p}.
\]

Solution: Note that

\[
\binom{mp-1}{p-1} = \frac{(mp-1)(mp-2)\cdots(mp-(p-1))}{(p-1)!}.
\]

Given that $(p-1)!$ is coprime to $p$, the problem is equivalent to showing that

\[
(mp-1)(mp-2)\cdots(mp-(p-1)) \equiv (p-1)! \pmod{p}.
\]

As $mp \equiv 0 \pmod{p}$, we compute:

\[
(mp-1)(mp-2)\cdots(mp-(p-1)) \equiv (-1)(-2)\cdots(-(p-1))
\]

\[
\equiv (-1)^{p-1}1 \cdot 2 \cdots (p-1) \equiv (p-1)! \pmod{p}.
\]

Here we used the fact that $p-1$ is an even number. \qed

Problem 6. For an odd number $p$, let $S := 2 \cdot 4 \cdots (p-1)$ be the product of all even numbers between 1 and $p$.

(1) Show that $S = 2^{\frac{p-1}{2}} \left( \binom{p-1}{2} \right)!$

(2) Let $r$ be the number of even numbers strictly greater than $(p-1)/2$ and less than $p$. Prove that $S \equiv (-1)^r \left( \binom{p-1}{2} \right)! \pmod{p}$.

(3) Prove that if $p$ is an odd prime, then $x^2 \equiv 2 \pmod{p}$ has a solution if and only if $p \equiv 1, 7 \pmod{8}$. 

Solution: (1)
\[2 \cdot 4 \cdots (p - 1) = (2 \cdot 1)(2 \cdot 2) \cdots (2 \cdot \frac{p-1}{2}) = 2^{(p-1)/2} \cdot 2 \cdots \left(\frac{p-1}{2}\right) = 2^{(p-1)/2} \left(\frac{p-1}{2}\right)!\]

(2) If \(x\) is an even number strictly greater than \((p - 1)/2\) and less than \(p\), then \(p - x\) is an odd number less or equal than \((p - 1)/2\) and greater than 0. In fact, every odd number from 1 to \((p - 1)/2\) is written in a unique way as \(p - x\), where \(x\) is an even number strictly greater than \((p - 1)/2\) and less than \(p\).

It follows that
\[S \equiv 2 \cdot 4 \cdots (p-5)(p-3)(p-1) \equiv (-1)(-3)(-5) \cdots \left(\pm \frac{p-1}{2}\right) \pmod{p}\]

In the product on the right, every even number in the interval \([1, (p - 1)/2]\) appears exactly once, with positive sign, and every odd number in the interval \([1, (p - 1)/2]\) appears exactly once, but with negative sign. There are precisely \(r\) negative signs in the product. It follows that
\[S = (-1)2(-3)4(-5) \cdots \left(\pm \frac{p-1}{2}\right) = (-1)^r \left(\frac{p-1}{2}\right)!\]

(3) Putting (1) and (2) together we see that
\[2^\frac{p-1}{2} \left(\frac{p-1}{2}\right)! = S \equiv (-1)^r \left(\frac{p-1}{2}\right)! \pmod{p}\]

Since \(\left(\frac{p-1}{2}\right)!\) is coprime to \(p\), the cancellation property of congruences implies that
\[2^\frac{p-1}{2} \equiv (-1)^r \pmod{p}\]

By Euler’s criterion, 2 is a quadratic residue if and only if \(r\) is even. We now consider separately 4 cases: \(p \equiv 1, 3, 5, 7 \pmod{8}\).

If \(p = 8k + 1\), then \((p - 1)/2 = 4k\) and so \(r\) is the number of even numbers in the interval \([4k + 1, 8k]\). Counting, we see that \(r = 2k\). Thus 2 is a quadratic residue modulo \(p\) in this case.

If \(p = 8k + 3\), then \((p - 1)/2 = 4k + 1\) and so \(r\) is the number of even numbers in the interval \([4k + 2, 8k + 2]\). Counting, we see that \(r = 2k + 1\). Thus 2 is NOT a quadratic residue modulo \(p\) in this case.

If \(p = 8k + 5\), then \((p - 1)/2 = 4k + 2\) and so \(r\) is the number of even numbers in the interval \([4k + 3, 8k + 4]\). Counting, we see that \(r = 2k + 1\). Thus 2 is NOT a quadratic residue modulo \(p\) in this case.

If \(p = 8k + 7\), then \((p - 1)/2 = 4k + 3\) and so \(r\) is the number of even numbers in the interval \([4k + 4, 8k + 6]\). Counting, we see that \(r = 2k + 2\). Thus 2 is a quadratic residue modulo \(p\) in this case.