

Solution to problem 51: Suppose that a, b are quadratic residues modulo p . Thus $a \equiv x^2 \pmod{p}$ and $b \equiv y^2 \pmod{p}$ for some integers x, y prime to p . Thus $ab \equiv x^2 y^2 = (xy)^2 \pmod{p}$ and ab is prime to p , so ab is a quadratic residue modulo p .

Suppose that a is a quadratic residue modulo p and b is a non-residue. If ab was a quadratic residue then we would have $a \equiv x^2 \pmod{p}$ and $ab \equiv y^2 \pmod{p}$ for some integers x, y prime to p . Since $a^{p-1} \equiv 1 \pmod{p}$, we have

$$b \equiv ba^{p-1} = aba^{p-2} \equiv y^2(x^2)^{p-2} = (yx^{p-2})^2 \pmod{p}$$

which contradicts the assumption that b is a quadratic non-residue. Thus ab cannot be a quadratic residue, i.e. it is a quadratic non-residue.

Suppose now that a is a quadratic non-residue. Consider the set of all $x \in \{1, 2, \dots, p-1\}$ such that ax is a quadratic non-residue. If this set had more than $(p-1)/2$ elements, then we would have two different members of this set x, y such that $ax \equiv ay \pmod{p}$, since the number of quadratic non-residues is $(p-1)/2$. This however means that $p|a(x-y)$ and since $\gcd(p, a) = 1$, we have $p|x-y$, i.e. $x = y$, a contradiction. It follows that our set has at most $(p-1)/2$ elements. On the other hand, we know that all quadratic residues are in this set. Since the number of quadratic residues is $(p-1)/2$, our set consists exactly of quadratic residues. Thus, if b is a quadratic non-residue, then b is not in our set, i.e. ab is a quadratic residue.

Solution to problem 52: The quadratic residues modulo 13 are the integers congruent modulo 13 to one of the numbers $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$. Modulo 13, these numbers are 1, 4, 9, 3, 12, 10. The non-residues are the integers congruent modulo 13 to one of 2, 5, 6, 7, 8, 11.