

**Problem**

- a) Find  $b \in \mathbb{Z}$  such that  $\left(\frac{b}{p}\right) = -1$  for all odd primes  $p \equiv 2 \pmod{3}$
- b) Find  $b \in \mathbb{Z}$  such that  $\left(\frac{b}{p}\right) = -1$  for all odd primes  $p \equiv 2 \pmod{5}$
- c) Let  $q$  be an odd prime, and let  $a \in \mathbb{Z}$  such that  $\left(\frac{a}{q}\right) = -1$ . Show that there exists  $b \in \mathbb{Z}$  such that  $\left(\frac{b}{p}\right) = -1$  for all odd primes  $p \equiv a \pmod{q}$
- d) Now suppose instead that  $\left(\frac{a}{q}\right) = 1$ . Show that there does not exist  $b \in \mathbb{Z}$  such that  $\left(\frac{b}{p}\right) = -1$  for all odd primes  $p \equiv a \pmod{q}$

**Solution**

a)

I will prove that -3 is quadratic non-residue modulo  $p$ , if  $p$  is congruent to 2 modulo 3.

To do this, I will use Lagrange symbol and its properties, such as quadratic reciprocity law:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

So,

$$\begin{aligned} \left(\frac{-3}{p}\right) &= \left(\frac{-1 * 3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = (\text{using reciprocity law}) \\ &= (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{3-1}{2}\right)} = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) \\ &= (p \text{ is congruent to } 2 \text{ modulo } 3) = \left(\frac{2}{3}\right) = -1 \end{aligned}$$

So, we just proved required statement for  $b = -3$ .

b)

I will in the same way prove that 5 is quadratic non-residue modulo  $p$ , if  $p$  is congruent to 2 modulo 5.

$$\begin{aligned} \left(\frac{5}{p}\right) &= (\text{reciprocity}) = \left(\frac{p}{5}\right) (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{5-1}{2}\right)} = \left(\frac{p}{5}\right) (-1)^{p-1} = (p \text{ is odd}) = \left(\frac{p}{5}\right) \\ &= \left(\frac{2}{5}\right) = -1 \end{aligned}$$

So, the statement is proved.

c)

Lets look at two cases.

First .  $\frac{q-1}{2}$  is even. Then number  $b=(q)$  is non-residue modulo  $p$ . Proof:

$$\left(\frac{q}{p}\right) = (\text{reciprocity}) = \left(\frac{p}{q}\right) (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = \left(\frac{a}{p}\right) = -1$$

Second.  $\frac{q-1}{2}$  is odd.  $b=-q$  is required number. Proof:

$$\begin{aligned} \left(\frac{-q}{p}\right) &= \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \\ &= (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) (-1)^{\left(\frac{p-1}{2}\right)} = \left(\frac{p}{q}\right) = \left(\frac{a}{q}\right) = -1 \end{aligned}$$

So, we found  $b$  for all odd primes congruent to  $a$  modulo  $q$ , where  $\left(\frac{a}{q}\right) = -1$ , such that  $\left(\frac{b}{p}\right) = -1$

d)

Suppose there exist such number  $b$ .

Then, using quadric reciprocity law we have:

$$1 = \left(\frac{b}{p}\right) = \left(\frac{p}{b}\right) (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{b-1}{2}\right)}$$

Again we have two cases.

First :  $\frac{b-1}{2}$  is even.

Then we have that  $\left(\frac{p}{b}\right) = 1$

But, using Dirichlet's theorem, we may choose prime  $p$ , such that:  $(p \equiv a \pmod q)$  and  $(p \equiv b_0 \pmod b)$ , where  $b_0$  is any non - residue modulo  $b$ .

For such prime  $\left(\frac{p}{b}\right) = \left(\frac{b_0}{b}\right) = -1$ .

Contradiction.

Second case.

$\frac{b-1}{2}$  is odd

$$\left(\frac{p}{b}\right) (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{b-1}{2}\right)} = \left(\frac{p}{b}\right) (-1)^{\left(\frac{p-1}{2}\right)}$$

But again, using Dirichlet's theorem we may choose  $p$ , such that  $p \equiv 1 \pmod{4}$  (then  $\frac{p-1}{2}$  is even),  $p \equiv a \pmod{q}$  and  $p \equiv b_0 \pmod{b}$

Then  $\left(\frac{p}{b}\right) (-1)^{\left(\frac{p-1}{2}\right)} = \left(\frac{p}{b}\right) = \left(\frac{b_0}{b}\right) = -1$

We have contradiction again.

In proofs I used multiple conditions on  $p$ , while choosing it by Dirichlet's theorem. But they may be done as one, firstly used Chinese remainder theorem.

So, the proof is finished.