Section 11 — Quadratic Congruences

we only consider prime moduli.

Ex Find all solutions

(a) $x^2+x-6=0$ (in $\mathbb{Z}$) $\boxed{x=-3,2}$ ↘ solution in $\mathbb{Z}$ yields sol. mod p

(b) $x^2+x-6\equiv 0 \pmod{13}$ $\boxed{x\equiv -3,2}$

↑ at most 2 solutions by Lemma 2 — Section 10.

Ex Find all solutions

(a) $x^2+1=0$ (in $\mathbb{Z}$) $\boxed{\text{None}}$

(b) $x^2+1\equiv 0 \pmod{13}$ $x^2+1\equiv x^2-25 \Rightarrow \boxed{x\equiv \pm 5}$

↖ or use table

(c) $x^2+1\equiv 0 \pmod 7$ $\boxed{\text{None}}$ ← use table

Note: solution in $\mathbb{Z}$ $\Longrightarrow$ solution mod p

but converse is not always true.

Let's see when we can solve $x^2-a\equiv 0 \pmod p$, which is the same as $x^2\equiv a \pmod p$.

* in other words, when does a have a square root mod p?

Theorem 1 Let p be an odd prime. If $a \not\equiv 0 \pmod p$ then $x^2 \equiv a \pmod p$ has either 0 or 2 solutions.

Optional

Pf

By Lemma 2 – Section 10, $x^2 \equiv a$ has at most 2 solutions. Suppose it has some solution r, i.e. $r^2 \equiv a$. Then, $-r$ is also a solution. If $r \equiv -r \pmod p$, then $2r \equiv 0 \pmod p$. Since p is prime, $2 \equiv 0 \pmod p$ or $r \equiv 0 \pmod p$. Neither are possible, so $r \not\equiv -r \pmod p$. Thus, if there is some solution, there are exactly 2. $\square$

Def

$x^2 \equiv a \pmod p \longleftrightarrow a$ is a quadratic residue mod p
has a solution

$x^2 \equiv a \pmod p \longleftrightarrow a$ is a quadratic nonresidue mod p
has NO sol.

Ex Find all quadratic residues mod 11.

x	x^2
0	0
1	1
2	4
3	9
4	5
5	3
-5	6	3
-4	7	5
-3	8	9
-2	9	4
-1	10	1

Ans. 0, 1, 4, 9, 5, 3

½ of # b/w 1 and 10 are quad. res.

Lemma If p is an odd prime, there are $\frac{p-1}{2}$ nonzero quad. residues.

Q: But can we predict which numbers are quad. residues?

... is 25 a quad. residue mod 83? Sure! 5 is a sol. to $x^2 \equiv 25$

... is 7 a quad. residue mod 83? not sure...

Theorem 2 (Euler's Criterion) If p is an odd prime and $a \not\equiv 0 \pmod{p}$, then

a is a quad. residue $\iff a^{\frac{(p-1)}{2}} \equiv 1 \pmod{p}$,

a is a quad. non-residue $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

In particular, primitive roots are not quad. resides.

pf

Let $a \not\equiv 0 \pmod{p}$. Note that

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \pmod{p},$$

(Fermat)

so $a^{\frac{p-1}{2}}$ is a solution to $x^2 \equiv 1 \pmod{p}$. Thus,

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Now, we know that there exist primitive roots mod p — let g be one of them. By Thm 5 of Section 10, $a \equiv g^k$ for some k with $1 \le k \le p$.

Optional

Case 1: **k is even.**

Then $a \equiv g^k \equiv g^{2n} \pmod{p}$ for $n \in \mathbb{Z}$.

Thus,

$\circledast$ $(g^n)^2 \equiv a \pmod{p}$

so **a is a quad. residue.**

$\circledast$ $a^{\frac{p-1}{2}} \equiv (g^{2n})^{\frac{p-1}{2}} \equiv g^{n\cdot(p-1)} \equiv (g^{p-1})^n \equiv 1 \pmod{p}$

Fermat

so $\boxed{a^{\frac{p-1}{2}} \equiv 1 \pmod{p}}$

Case 2: **k is odd**

Then $a \equiv g^k \equiv g^{2n+1} \pmod{p}$

Thus,

$\circledast$ $a^{\frac{p-1}{2}} \equiv (g^{2n+1})^{\frac{p-1}{2}} \equiv g^{n(p-1)} \cdot g^{\frac{p-1}{2}}$

Fermat.

Also $g^{\frac{p-1}{2}} \equiv \pm 1$, but $\operatorname{ord}_p(g) = p-1$,

so $g^{\frac{p-1}{2}} \not\equiv 1$. Thus,

$$\boxed{a^{\frac{p-1}{2}} \equiv -1 \pmod{p}}$$

$\circledast$ if $r^2 \equiv a$ for some r, then

$-1 \equiv a^{\frac{p-1}{2}} \equiv (r^2)^{\frac{p-1}{2}} \equiv r^{p-1} \equiv 1 \pmod{p}$

Fermat

which can not happen unless $p=2$. Thus,

a is a quad. nonresidue.

□

Ex Which of the following have solutions?

(a) $x^2 \equiv 3 \pmod{37}$

$*$ solution $\Leftrightarrow 3^{\frac{p-1}{2}} \equiv 1 \Leftrightarrow 3^{18} \equiv 1 \pmod{37}$

$3^2 \equiv 9$

$3^4 \equiv 81 \equiv 7$

$3^8 \equiv 49 \equiv 12$

$3^{16} \equiv 144 \equiv -4$ ($37 \times 4 = 148$)

So,

$3^{18} \equiv 3^{16} \cdot 3^2$

$\equiv -4 \cdot 9$

$\equiv -36$

$\equiv 1$

Thus, 3 is a quad. res.

so YES

(b) $x^2 \equiv 6 \pmod{31}$

$*$ solution $\Leftrightarrow 6^{\frac{p-1}{2}} \equiv 1 \Leftrightarrow 6^{15} \equiv 1 \pmod{31}$

$6^2 \equiv 36 \equiv 5$

$6^4 \equiv 25 \equiv -6$

↻ cancel to get -1!!

$6^3 \equiv -1$

So,

$6^{15} \equiv (6^3)^5$

$\equiv (-1)^5$

$\equiv -1$

Thus, 6 is a quad. non residue

so NO

(c) $x^2 \equiv -1 \pmod{37}$

$*$ solution $\Leftrightarrow (-1)^{\frac{p-1}{2}} \equiv 1 \Leftrightarrow (-1)^{18} \equiv 1 \pmod{37}$

Thus, -1 is a quad. residue mod 37, so YES

Clearly, there should be an easy criterion to know when -1 is a quad. residue.

Theorem 5 Let p be an odd prime. Then -1 is a quad. residue mod p iff $p \equiv 1 \bmod 4$.

pf

-1 is a quad. res. $\iff (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$

$\iff \frac{p-1}{2}$ is even

$\iff \frac{p-1}{2} = 2k$ for $k \in \mathbb{Z}$

$\iff p-1 = 4k$ for $k \in \mathbb{Z}$

$\iff p-1 \equiv 0 \pmod 4$ □

Returning to the previous example, what if we actually wanted to find the solutions?

Ex Find the solutions to $x^2 \equiv 3 \pmod{37}$

$x^2 \equiv 40 \equiv 2^2 \cdot 10$ → $10 \equiv -27 \equiv -64$

$\equiv 2^2 \cdot 64 \cdot (-1)$

$\equiv 2^2 \cdot 8^2 \cdot (-1)$ → $-1 \equiv 36$

$\equiv 2^2 \cdot 8^2 \cdot 6^2$

$\equiv (2 \cdot 8 \cdot 6)^2$ → $2 \cdot 8 \cdot 6 \equiv 2 \cdot 48 \equiv 2 \cdot 11 \equiv 22$

$\equiv 22^2$

probably won't start doing this unless you know there is a solution, which we do

so, $\boxed{x \equiv \pm 22 \pmod{37}}$

Legendre Symbol and Quadratic Reciprocity

Motivation: speed up our ability to determine if a number is a quadratic residue or not.

Def Let p be an odd prime. Assume $p \nmid a$. We define the Legendre symbol $\left(\frac{a}{p}\right)$ by ↑ equiv. to $a \not\equiv 0 \pmod p$

"a on p" → $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quad. res. mod } p \\ -1 & \text{if } a \text{ is a quad. non res. mod } p \end{cases}$

* $\left(\frac{a}{p}\right)$ is often defined to be 0 if $p \mid a$, but Dudley leaves this undefined.
* Euler's Criterion $\Rightarrow \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

Ex Compute

(a) $\left(\frac{4}{7}\right) = 1$ b/c $x^2 \equiv 4 \pmod 7$ has a sol.

(b) $\left(\frac{-1}{11}\right) = -1$ b/c $(-1)^{\frac{10}{2}} = -1$

(c) $\left(\frac{1}{101}\right) = 1$

Theorem 3 (Basic Props. of the Legendre Symbol)

Let p be an odd prime. Assume $a, b \not\equiv 0 \pmod p$.

(a) If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

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

(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

pf

By Euler, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

(a) if $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right)$

(b) a is a sol. to $x^2 \equiv a^2 \bmod p$, so $\left(\frac{a}{p}\right) = 1$

(c) $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ □

Ex Does $x^2 \equiv -4 \pmod{103}$ have a solution?

* $x^2 \equiv -4 \pmod{103}$ has a sol. $\iff$ -4 is a quad. res. mod 103
$\iff \left(\frac{-4}{103}\right) = 1$

* $\left(\frac{-4}{103}\right) = \left(\frac{-1}{103}\right)\left(\frac{4}{103}\right)^{1} = \left(\frac{-1}{103}\right)^{-1} = \boxed{-1}$

* $\left(\frac{-1}{103}\right) = 1 \iff 103 \equiv 1 \pmod 4$ ← Thm 5

but $103 \equiv 3 \pmod 4$

so $\left(\frac{-1}{103}\right) = -1$

So $\boxed{\text{NO}}$, no solution.

Quadratic Reciprocity — comparing $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$

Theorem 4 (Quadratic Reciprocity) Let p and q be different odd primes. Then

* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if $p \equiv 1 \pmod 4$ OR $q \equiv 1 \pmod 4$

* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if $p \equiv 3 \equiv q \pmod 4$

Equivalently,

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

↑ -1 only when $p \equiv q \equiv 3 \pmod 4$

pf see Section 12 of the book.

Ex Compute

(a) $\left(\frac{5}{101}\right) \overset{QR}{=} (-1)^{\frac{4}{2}\cdot\frac{100}{2}} \cdot \left(\frac{101}{5}\right)$

$= \left(\frac{101}{5}\right)$

$= \left(\frac{1}{5}\right)$ ← $101 \equiv 1 \pmod 5$

$= \boxed{1}$

not prime!

(b) $\left(\frac{77}{131}\right) = \left(\frac{7\cdot 11}{131}\right)$

$= \left(\frac{7}{131}\right)\cdot\left(\frac{11}{131}\right)$

$\overset{QR}{=} (-1)^{\frac{130}{2}\cdot\frac{6}{2}} \cdot \left(\frac{131}{7}\right) \cdot (-1)^{\frac{130}{2}\cdot\frac{10}{2}} \cdot \left(\frac{131}{11}\right)$

$= (-1)\left(\frac{131}{7}\right)\cdot(-1)\left(\frac{131}{11}\right)$

$= \left(\frac{5}{7}\right)\cdot\left(\frac{10}{11}\right)$ ← $131 \equiv 5 \pmod 7$, $131 \equiv 10 \pmod{11}$

$= \left(\frac{5}{7}\right)\left(\frac{-1}{11}\right)$

$\overset{QR}{=} (-1)^{\frac{4}{2}\cdot\frac{6}{2}}\left(\frac{7}{5}\right)\cdot\left(\frac{-1}{11}\right)$

$= \left(\frac{7}{5}\right)\cdot\left(\frac{-1}{11}\right)$ ← $7 \equiv 2 \pmod 5$

$= \left(\frac{2}{5}\right)\cdot\left(\frac{-1}{11}\right)$

$= (-1)\cdot(-1)$

$= \boxed{1}$

There are 2 options

$\left(\frac{2}{5}\right) \equiv 2^{\frac{p-1}{2}} \equiv 2^2 \equiv -1 \pmod 5$

$\left(\frac{-1}{11}\right) \equiv -1^{\frac{10}{2}} \equiv (-1) \pmod{11}$

WARM UP

Ex Compute $\left(\frac{8}{131}\right)$

$\left(\frac{8}{131}\right) = \left(\frac{2}{131}\right)\cdot\left(\frac{4}{131}\right) = \left(\frac{2}{131}\right) = ?$ $\left(\frac{4}{131}\right) = 1$

No QR b/c 2 is not odd ☹

Theorem 6 Let p be an odd prime. Then

$\left(\frac{2}{p}\right) = 1$ if $p \equiv 1, 7 \pmod 8$

$\left(\frac{2}{p}\right) = -1$ if $p \equiv 3, 5 \pmod 8$.

~~pf~~ Later.

Ex Compute

(a) $\left(\frac{8}{131}\right) = \left(\frac{2}{131}\right)\cdot\left(\frac{4}{131}\right) = \left(\frac{2}{131}\right) = \boxed{-1}$

$\left(\frac{4}{131}\right) = 1$; -1 b/c $131 \equiv 3 \pmod 8$

(b) $\left(\frac{34}{71}\right) = \left(\frac{2}{71}\right)\left(\frac{17}{71}\right) \overset{QR}{=} (-1)^{\frac{70}{2}\cdot\frac{16}{2}}\left(\frac{71}{17}\right) = \left(\frac{3}{17}\right) \overset{QR}{=} (-1)^{\frac{16}{2}\cdot\frac{2}{2}}\left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = \boxed{-1}$

$\left(\frac{2}{71}\right) = 1$

Ex Consider the sequence: $1, 5, 10, 17, 26, \ldots, n^2+1, \ldots$

Find an element of the sequence that is divisible by 11, if possible.

Rephrase: is there a solution to $n^2 + 1 \equiv 0 \pmod{11}$?

Answer: $n^2 \equiv -1 \pmod{11}$ has a sol. iff $\left(\frac{-1}{11}\right) = 1$

but by Thm 5 $\left(\frac{-1}{11}\right) = -1$ since $11 \equiv 3 \pmod 4$.

Thus, no element of the seq. is div. by 11.

Ex Determine if $x^2 - 37x + 27 \equiv 0 \pmod{43}$ has any solutions.

Idea: complete the square!

$$x^2 + bx + c = x^2 + bx + \left(\frac{b}{2}\right)^2 - \left(\frac{b}{2}\right)^2 + c$$
$$= \left(x + \frac{b}{2}\right)^2 + c$$

↑ need to divide b by 2!

Answer: add 43 to make even

$$x^2 - 37x + 27 \equiv x^2 + 6x + 27 \pmod{43}$$
$$\equiv x^2 + 6x + 9 - 9 + 27 \pmod{43}$$
$$\equiv (x+3)^2 + 18 \pmod{43}$$

So,

$x^2 - 37x + 27 \equiv 0 \pmod{43}$ has a sol.

$\iff (x+3)^2 + 18 \equiv 0 \pmod{43}$ has a sol.

let $u = x+3$

$\iff u^2 + 18 \equiv 0 \pmod{43}$ has a sol.

$\iff u^2 \equiv -18 \pmod{43}$ has a sol.

$\iff \left(\frac{-18}{43}\right) = 1$

So, let's compute $\left(\frac{-18}{43}\right)$.

$$\left(\frac{-18}{43}\right) = \left(\frac{-1}{43}\right)\cdot\left(\frac{2}{43}\right)\cdot\left(\frac{9}{43}\right) = 1$$

-1 ($43 \equiv 3 \pmod 4$), -1 ($43 \equiv 3 \pmod 8$), 1 (9 is a square)

So, **YES**, there is a solution to the original congruence.

pf idea for Theorem 6

Recall

Theorem 6 Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = 1 \quad \text{if} \quad p \equiv 1, 7 \pmod 8$$
$$\left(\frac{2}{p}\right) = -1 \quad \text{if} \quad p \equiv 3, 5 \pmod 8.$$

The proof can be divided into 2 cases: $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.

($p \equiv 1, 5 \pmod 8$; $p \equiv 3, 7 \pmod 8$.)

Case 1: $p \equiv 1 \pmod 4$ (i.e. when $p \equiv 1, 5 \bmod 8$)

We use Euler's Criterion: $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p$

So we need to compute $2^{\frac{p-1}{2}}$. We use a trick...

Consider the number

$$z = \overbrace{2 \cdot 4 \cdot 6 \cdots (p-3) \cdot (p-1)}^{\text{there are } \frac{p-1}{2} \text{ terms}}$$

Aside: if $p = 17$, this quantity is

$$z = 2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 14 \cdot 16$$

(8 terms)

we compute $z \pmod p$ 2 different ways.

(i) $$Z = 2 \cdot 4 \cdot 6 \cdots (p-3)\cdot(p-1)$$

$$= 2^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right)$$

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

Aside: if $p = 17$,

$$Z = 2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 14 \cdot 16 = 2^8 \cdot 8!$$

(ii) Break Z into two pieces.

$$Z = 2 \cdot 4 \cdot 6 \cdots (p-3)(p-1)$$

There are $\frac{p-1}{2}$ terms. Since $p \equiv 1 \pmod 4$, $p - 1 = 4k$ for some $k \in \mathbb{Z}$, so $\frac{p-1}{2} = 2k$ is <u>even</u>.

$$Z = \underbrace{\left[2 \cdot 4 \cdot 6 \cdots \left(\frac{p-1}{2}\right)\right]}_{\frac{p-1}{4} \text{ terms}} \underbrace{\left[\left(\frac{p+3}{2}\right) \cdots (p-3)\cdot(p-1)\right]}_{\frac{p-1}{4} \text{ terms}}$$

Aside: if $p = 17$

$$Z = [2 \cdot 4 \cdot 6 \cdot 8][10 \cdot 12 \cdot 14 \cdot 16]$$

$$\equiv [2 \cdot 4 \cdot 6 \cdot 8][(-7)(-5)(-3)(-1)] \pmod p$$

$$\equiv [2 \cdot 4 \cdot 6 \cdot 8][1 \cdot 3 \cdot 5 \cdot 7] \cdot (-1)^4 \pmod p$$

$$\equiv (-1)^4 \cdot 8! \pmod p$$

Thus,

$$Z \equiv \left[2 \cdot 4 \cdot 6 \cdots \frac{p-1}{2}\right]\left[\left(-\left(\frac{p-1}{2}-1\right)\right)\cdots(-3)(-1)\right] \pmod p$$

evens $\leq \frac{p-1}{2}$; neg. of odds $< \frac{p-1}{2}$

$\uparrow \frac{p-1}{4}$ terms!

$$\equiv \left[2 \cdot 4 \cdot 6 \cdots \frac{p-1}{2}\right] \cdot \left[1 \cdot 3 \cdot 5 \cdots \left(\frac{p-1}{2}-1\right)\right] \cdot (-1)^{\frac{p-1}{4}}$$

$$\equiv (-1)^{\frac{p-1}{4}} \cdot \left(\frac{p-1}{2}\right)! \pmod p$$

In conclusion,

$$2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! = Z \equiv (-1)^{\frac{p-1}{4}} \cdot \left(\frac{p-1}{2}\right)! \pmod p$$

$$\Longrightarrow \quad 2^{\frac{p-1}{2}} \cdot \cancel{\left(\frac{p-1}{2}\right)!} \equiv (-1)^{\frac{p-1}{4}} \cdot \cancel{\left(\frac{p-1}{2}\right)!} \pmod p$$

cancellable b/c not div. by p

$$\Longrightarrow \quad 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod p$$

Thus, when $p \equiv 1 \pmod 4$, we have

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \equiv \begin{cases} +1 & \text{if } \frac{p-1}{4} = 2m \\ -1 & \text{if } \frac{p-1}{4} = 2m+1 \end{cases}$$

$p-1 = 8m \Rightarrow p = 1+8m$

$p-1 = 8m+4 \Rightarrow p = 5+8m$

So,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \\ -1 & \text{if } p \equiv 5 \pmod 8 \end{cases}.$$

Case 2: $p \equiv 3 \pmod 4$ (i.e. when $p \equiv 3, 7 \bmod 8$)

Similar to the previous case, but the product doesn't split down the middle anymore. But, this essentially causes no problems.

□