1(a) $x^2 + 7x + 10 \equiv 0 \pmod{11}$

$\iff 4x^2 + 28x + 40 \equiv 0 \pmod{11}$

$(2x+7)^2 - 9 \equiv 0 \pmod{11}$

$(2x+7)^2 \equiv 9 \pmod{11}$

$y^2 \equiv 9 \pmod{11}$

$2x+7 \equiv 3 \pmod{11}$ OR $2x+7 \equiv 8 \pmod{11}$

$2x \equiv -4 \pmod{11}$

$x \equiv -2 \pmod{11}$

$x \equiv 9 \pmod{11}$

$x = 9$

$2x \equiv 1 \pmod{11}$

$x \equiv 6$

$x = 6$

In general: $ax^2 + bx + c \equiv 0 \pmod p$, p an odd prime & $\gcd(a,p) = 1$

$\Longleftrightarrow$ ~~$4a^2x^2 + 4bx + 4c \equiv 0 \pmod p$~~

~~$(2ax+b)^2$~~

$\Longleftrightarrow$ $4a^2x^2 + 4acbx + 4ac \equiv 0 \pmod p$

$(2ax+b)^2 + 4ac - b^2 \equiv 0 \pmod p$

$(2ax+b)^2 \equiv b^2 - 4ac \pmod p$

i.e., $\underline{y^2 \equiv d \pmod p}$, $y = 2ax + b$, $d = b^2 - 4ac$.

Defns * p an odd prime, $\gcd(a,p) = 1$

(1) a is a quadratic residue of p iff

there is a solution of $x^2 \equiv a \pmod{p}$.

(2) a is a quadratic nonresidue of p iff

there is no solution of $x^2 \equiv a \pmod{p}$.

---

we know that $x^2 \equiv a \pmod{p}$ has a solution iff

ind a is even: $2 \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}$,

solvable iff $2 \mid \operatorname{ind} a$.

There are $\frac{p-1}{2}$ such values of a, so p has

$\frac{p-1}{2}$ quadratic residues.

Thm a is a quadratic residue of p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod p$;

a is a quadratic nonresidue of p iff $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Euler's criterion

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

pf. Suppose that a is a quadratic nonresidue of p. If c is any integer from the set $\{1, \dots, p-1\}$, then the congruence $cx \equiv a \pmod p$ has a unique solution $x = c'$ s.t. $c \not\equiv c' \pmod p$. Now pair these up:

$k = \frac{p-1}{2}$

$$\begin{cases} c_1 c_1' \equiv a \pmod p \\ c_2 c_2' \equiv a \pmod p \\ \vdots \\ c_k c_k' \equiv a \pmod p \end{cases} \implies (p-1)! \equiv a^{\frac{p-1}{2}} \pmod p$$

$$\implies a^{\frac{p-1}{2}} \equiv -1 \pmod p \text{ by Wilson's Thm.}$$

On the other hand, if a is a quadratic residue,

then $x^2 \equiv a \pmod p$ has a solution $x_1 \in \{1, \dots, p-1\}$,

and $p - x_1$ is the other solution. Pair up the other numbers

from $\{1, \dots, p-1\}$:

$$k = \frac{p-3}{2}$$

$$\begin{cases} c_1 c_1' \equiv a \pmod p \\ c_2 c_2' \equiv a \pmod p \\ \vdots \\ c_k c_k' \equiv a \pmod p \\ x_1(p - x_1) \equiv -a \pmod p \end{cases} \Longrightarrow (p-1)! \equiv -a^{\frac{p-1}{2}} \pmod p$$

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

by Wilson's Thm.

Legendre's symbol: $\left(\frac{a}{p}\right) := \begin{cases} +1 & \text{if } a \text{ is a quadratic residue of } p \\ 0 & \text{if } p \mid a \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p \end{cases}$

Euler's criterion a is a quadratic residue of p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. ($p$ an odd prime, $\gcd(a,p)=1$)

pf.: a is a quadratic residue of p, then $x^2 \equiv a \pmod p$ for some x, and $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$.

if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, then $a \equiv r^k \pmod p$ for some $k \in \{1,\dots,p-1\}$ and some primitive root r of p. Then

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

$\Rightarrow k$ is even $\Rightarrow k = 2j$ for some j

and $a \equiv (r^j)^2 \pmod p$.

∎

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^{p-1} - 1 \equiv 0 \pmod p$$

$$\Rightarrow \underbrace{p \mid a^{\frac{p-1}{2}} - 1}_{a^{\frac{p-1}{2}} \equiv 1 \pmod p} \quad \text{or} \quad \underbrace{p \mid a^{\frac{p-1}{2}} + 1}_{a^{\frac{p-1}{2}} \equiv -1 \pmod p} \quad \text{(not b.k!)}$$

$$a^{p-1} \equiv 1 \pmod p$$

p : an odd prime ; a : integer s.t. $\gcd(a,p)=1$

- a is a quadratic residue of p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ (Euler's criterion)
- a is a quadratic nonresidue of p iff $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Defn $\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{if } a^{\frac{p-1}{2}} \equiv 1 \pmod p \\ 0 & \text{if } p \mid a \\ -1, & \text{if } a^{\frac{p-1}{2}} \equiv -1 \pmod p \end{cases}$

Properties

(1) $a \equiv b \pmod p \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ ✓

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

(3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$: $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{(p-1)}{2}\frac{(p-1)}{2}} b^{\frac{(p-1)}{2}\frac{(p-1)}{2}} \pmod p$

$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ & $2 \nmid p$

(4) $\left(\frac{a}{p}\right)^2 = 1$ ✓ $\Longrightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. ✓

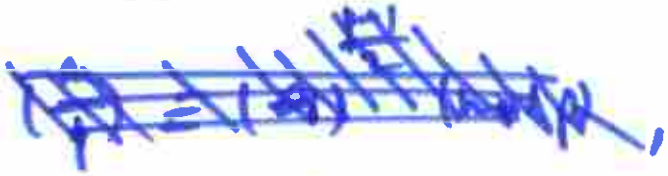
$\left(\frac{1}{p}\right) = 1$ since $1^2 \equiv 1 \pmod p$ ✓

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

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

(we proved earlier that $x^2+1 \equiv 0 \pmod p$ is solvable iff $p \equiv 1 \pmod 4$.)

FACT: $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$: Let r be a primitive root of p.



$$\Longleftarrow \quad \sum_{1}^{p-1} \left(\frac{a}{p}\right) = \sum_{k=1}^{p-1} (-1)^k = 0.$$

$\left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} \pmod p$, $a \equiv r^k$ for some k ⇑

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

Gauss's Lemma

Let n = # of integers in $\{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a\}$

whose remainders are $> \frac{p}{2}$ modulo p.

Then $\left(\frac{a}{p}\right) = (-1)^n$.

pf. ka, $1 \le k \le \frac{p-1}{2}$ when the multiples of a

where has remainder t_k, $1 \le t_k \le p-1$.

Let $r_1, \ldots, r_m$ be the t_k's that are $< \frac{p}{2}$;

let $s_1, \ldots, s_n$ " " " " " $> \frac{p}{2}$.

Then $\{r_1, \ldots, r_m, p-s_1, p-s_2, \ldots, p-s_n\}$ are all $< \frac{p}{2}$.

$r_i \equiv p - s_j \pmod p \Rightarrow r_i + s_j \equiv 0 \pmod p$

can't happen! $\Rightarrow$ $ka + ma \equiv 0 \Rightarrow k + m \equiv 0 \pmod p$

Thus: $\{r_1, \dots, r_n, p-s_1, \dots, p-s_n\} = \{1, 2, 3, \dots, \frac{p-1}{2}\}$

$\Rightarrow \quad r_1 \cdot r_2 \cdot \dots \cdot r_n \cdot (p-s_1) \cdot \dots (p-s_n) \equiv (\frac{p-1}{2})! \pmod p$

$(-1)^n \, a \cdot 2a \cdot \dots \cdot (\frac{p-1}{2})a \equiv (\frac{p-1}{2})! \pmod p$

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

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

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

$\Rightarrow \quad (\frac{a}{p}) \equiv (-1)^n \pmod p \quad \Rightarrow \quad (\frac{a}{p}) = (-1)^n.$

□

$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{8}}$:

$\left(\frac{2}{p}\right) = (-1)^n$ where $n = \#\{2, 4, 6, \ldots, (p-1)\}$

whose remainders mod p exceed $\frac{p}{2}$.

$2k < \frac{p}{2} \iff k < \frac{p}{4} \Rightarrow \lfloor \frac{p}{4} \rfloor = \#$ of these $< \frac{p}{2}$

$\Rightarrow n = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$

$p \equiv 1 \pmod 8 \Rightarrow p = 8k+1 \Rightarrow n = \frac{8k+1-1}{2} - \lfloor \frac{8k+1}{4} \rfloor$

$= 4k - 2k = 2k$ even

$p = 8k+3 \Rightarrow n = \frac{8k+3-1}{2} - \lfloor \frac{8k+3}{4} \rfloor = 4k+1-2k = 2k+1$ odd

$p = 8k+5 \Rightarrow n = 4k+2 - (2k+1) = 2k+1$ odd

$p = 8k+7 \Rightarrow n = 4k+3 - (2k+1) = 2k+2$ even

FACT: There are infinitely many primes of the form $4k+1$.

pf: Suppose not — let $p_1, \dots, p_n$ be all of the primes of the form $4k+1$. Then define

$$N = (2p_1p_2\cdots p_n)^2 + 1.$$

Then some odd prime $p \mid N$, so

$$(2p_1p_2\cdots p_n)^2 \equiv -1 \pmod{p} \implies p \equiv 1 \pmod{4}$$

$$\implies p \mid 1. \quad \times$$

FACT: There are infinitely many primes of the form $8k-1$.

pf.: if not, let $p_1, \dots, p_n$ be the primes of the form $8k-1$, and define

$$N = (4p_1p_2\cdots p_n)^2 - 2.$$

This has some odd prime divisor p, so

$$(4p_1p_2\cdots p_n)^2 \equiv 2 \pmod{p} \implies p \equiv \pm 1 \pmod{8}.$$

$$\implies p \equiv -1 \pmod{8}$$

for some p.

$$\implies p \mid 2. \quad \times$$

Theorem p an odd prime, a an odd integer

Then $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}$.

pf. For each k, $ka = \left\lfloor \frac{ka}{p} \right\rfloor p + t_k$, $1 \le k \le \frac{p-1}{2}$

$$\text{Then } \sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor p + \sum_{1}^{m} r_i + \sum_{1}^{n} s_j$$

$$\Longrightarrow \quad a \sum_{1}^{\frac{p-1}{2}} k = p \sum_{1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{1}^{m} r_i + \sum_{1}^{n} s_j \qquad (1)$$

Recall from Gauss's Lemma that

$$\{r_1, \dots, r_m, p-s_1, \dots, p-s_n\} = \{1, 2, \dots, \tfrac{p-1}{2}\}.$$

Thus: $$\sum_{1}^{\frac{p-1}{2}} k = \sum_{1}^{m} r_i + \sum_{1}^{n} p - s_j = np + \sum_{1}^{m} r_i - \sum_{1}^{n} s_j \qquad (2)$$

(1) − (2): $$(a-1) \sum_{1}^{\frac{p-1}{2}} k = p \sum_{1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - np + 2 \sum_{1}^{n} s_j .$$

mod 2: $$0 \equiv \sum_{1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor - n \pmod 2$$

$$\Rightarrow n \equiv \sum_{1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \pmod 2$$

$$\Rightarrow \left(\frac{a}{p}\right) = (-1)^n = (-1)^{\sum_{1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}$$

∎