$(n|p) = +1$

$(n|p) = -1$

$$\boxed{(nm|p) = (n|p)(m|p)}$$

res × res = res

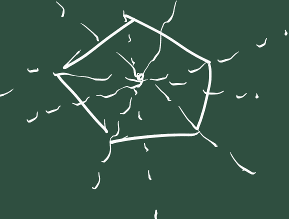
n.res × n.res = res

n.res × res = n.res.

$$(p|q) = \begin{cases} -(q|p), & q \equiv p \equiv 3 \bmod 4 \\ (q|p), & \text{otherwise.} \end{cases}$$

D_n = group of symmetries of n-sided regular polygon.

eg. D_3  , D_4 

, D_5 

$D_n = \langle r, s \rangle$, $r^n = e$, $s^2 = e$

$sr = r^{-1}s$ $\quad |D_n| = 2n$

So $D_n = \{e, r, r^2, r^3, \ldots, r^{n-1},$
$s, rs, r^2s, r^3s, \ldots, r^{n-1}s\}$

There is the subgroup

$R = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$

R is a subgroup of D_n. $|R| = n$.

$R = \langle r \rangle$

Now in general R itself will have subgroups which will also be subgroups of D_n.

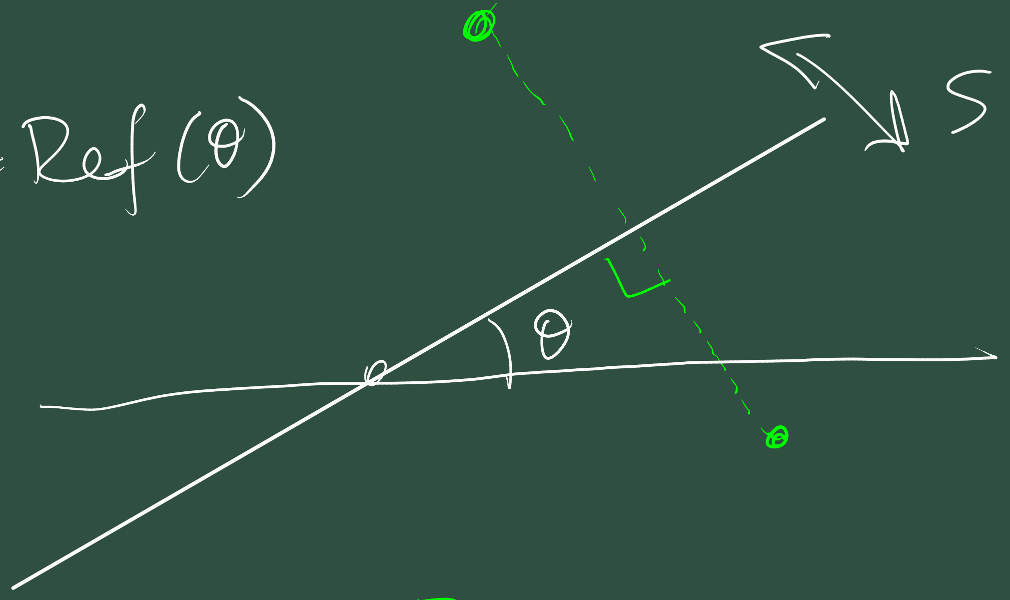
There is also the subgroup

$\langle s \rangle = \{e, s\}$ of D_n.

and other subgroups containing reflections too. $|\langle s \rangle| = 2$

$e \cdot e = e$

$s = \mathrm{Ref}(\theta)$



$$s^2 = e$$

$$s.s = e.$$

For a reflection $s : \mathbb{R}^2 \to \mathbb{R}^2$ can represent it with a reflection matrix

$$s = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$

can show $s^{-1} = s$

$s^2 =$ identity matrix.

$$s.s = I.$$

$$\Rightarrow s = s^{-1}$$

Recall: there an infinite number of primes.

how are they distributed in $\mathbb{Z}$.

think of $\mathbb{Z}$ modulo 4.

any integer $z \equiv 0, 1, 2, 3 \pmod 4$

If p is an odd prime

$$p \equiv 1, 3 \pmod 4$$

$3, 5, 7, 11, 13, 17, 19, 23, \ldots$

$3 \quad 1 \quad 3 \quad 3 \quad 1 \quad 1 \quad 3 \quad 3, \ldots$

in fact there are an infinite number of primes $\equiv 1 \mod 4$
$\equiv 3 \mod 4$.

in fact there is a general result Dirichlet's Theorem which says if $\gcd(a, n) = 1$

then there is an infinite number of primes $\equiv a$ (modulo n).

We can prove some special cases of Dirichlet's theorem (i.e. for certain a, n)

Ex 8.5 Q3 (a).

Claim: there an infinite number of primes p of the form $p = 4n-1$.

Proof By contradiction.

Assume there's an only a finite number of primes $p = 4n-1$.

Then let P be the largest one.

Then consider the integer N.

$$N = (\underbrace{2^2 \times 3 \times 5 \times 7 \times \ldots \times P}_{\text{product of all the primes from 3 to } P}) - 1$$

product of all the primes from 3 to P.

we know N has prime factors q

note that $q > P$.

because if $q \le P$ then q is

in this factor $3 \times 5 \times \dots \times P$

in which case $q \mid N$

and $q \mid (2^2 \times 3 \times \dots \times P)$

~~and~~ and so $q \mid 1$.

since $1 = -N + (2^2 \times 3 \times 5 \times \dots \times P)$.

which is a contradiction.

so all prime factors q of N are

satisfying $q > P$.

so all these q must have

the form $4n+1$ for ~~some~~

various n, ie. $q \equiv 1 \pmod 4$

$\Rightarrow N \equiv 1 \pmod 4$

as N is the product of all its prime divisors.

But this contradicts the definition of N

as

$$N = 4 \times (3 \times \dots \times \underline{P}) - 1.$$

$$\equiv 3 \pmod 4$$

So we've got a contradiction.

So we conclude there is no largest prime $\underline{P}$ of the form $4n-1$, so there is an infinite number of them.

(b). There are an <u>infinite number</u> of primes of the form $p = 8k+3$.

3, 5, 7, 11, 13, 17, 19, 23, , O . . O O

Proof (by contradiction)

Assume there's only a finite number. $p_1, \dots, p_s \equiv 3 \pmod 8$

Then consider.

$$N = (p_1 \cdots p_s)^2 + 2.$$

note $N \equiv ? \pmod 8$

$$N = p_1^2 p_2^2 \cdots p_s^2 + 2.$$

$$\equiv 1 \cdot 1 \cdots\cdots 1 + 2 \pmod 8$$

$$\equiv 3 \pmod 8$$ so N is odd.

Let q be an odd prime divisor of N.

Also notice that -2 is a quadratic residue modulo N.

$$-2 \equiv -N + (p_1 \cdots p_s)^2$$

$$-2 = -mq + (p_1 \cdots p_s)^2$$

so $(-2|N) = +1$. so $(-2|q) = +1$

$\Rightarrow \left(-1 \middle| q\right)\left(2 \middle| q\right) = +1.$

Two cases

either $\left(-1 \middle| q\right) = -1 \Rightarrow q \equiv 3 \bmod 4.$

& $\left(2 \middle| q\right) = -1 \Rightarrow q \equiv 3, 5 \bmod 8.$

OR

$\left(-1 \middle| q\right) = +1 \Rightarrow q \equiv 1 \bmod 4.$

$\left(2 \middle| q\right) = +1 \Rightarrow q \equiv 1, 7 \bmod 8$

Therefore $q \equiv 1$ or $3 \pmod 8$

But the prime divisors q of N cannot all $\equiv 1 \bmod 8$ since then $N \equiv 1 \bmod 8$ but this contradicts $N \equiv 3 \bmod 8$.

So N must have at least one prime divisor $q \equiv 3 \bmod 8$.

So $q = p_i$ for some $1 \leq i \leq s$

But we get that $q \mid N$ and

$q \mid (p_1 \cdots p_s)^2$

and so $q \mid 2$ since

$2 = N - (p_1 \cdots p_s)^2$

$\Rightarrow q = 2.$

This contradicts the fact that

N is odd.

So there must be an infinite

number of primes of the form

$\equiv 3 \pmod 8$

Ex 8.4. Q10. $x^2 \equiv 29 \pmod{53}$

$$(29|53) = (53|29), \text{ by Q.R.}$$

$= (24|29)$, reduction. $53 \equiv 24 \pmod{29}$

$= (2|29)^3 (3|29)$, factorization.

$= (2|29)(3|29)$

$= -(3|29)$, by $(2|p)$ result and $29 \equiv 5 \bmod 8$

$= -(29|3)$

$= -(2|3)$

$= -(-1)$, 2 is a non-residue modulo 3.

$= +1$

So 29 is a quadratic residue modulo 53.

Q1 (c)

Consider $5x^2 + 6x + 1 \equiv 0 \pmod{23}$

Solutions if they exist are given by

$$x = (-6 + u)(10)^{-1} \bmod 23$$

where u is an element satisfying

$$u^2 \equiv \underbrace{6^2 - 4 \cdot 5}_{\text{discriminant.}} \pmod{23}$$

$$\equiv 36 - 20$$

$$\equiv 16 \pmod{23}$$

$$\equiv (\pm 4)^2$$

So $u \equiv 4, 19 \pmod{23}$

So there are two solutions.

Notice $7 \cdot 10 = 70 \equiv 1 \bmod 23$.

So $10^{-1} \equiv 7 \pmod{23.}$

$-6 \equiv 17 \bmod 23.$

sols are

$$x = (17 + 4) \cdot 7.$$

$$= 21 \cdot 7.$$

$$= 147$$

$$\equiv \underline{\underline{9}} \bmod 23.$$

$$x \equiv (17+19)\cdot 7.$$
$$= (36)\cdot 7.$$
$$\equiv 13\cdot 7 \qquad \text{mod } 23.$$
$$\equiv 91$$
$$\equiv \underline{\underline{22}} \pmod{23}$$