Congruences

Recall: for $n \geq 1$, $\mathbb{Z}/n\mathbb{Z} = \{a \pmod n\}$ ring of residue classes $(\bmod n)$

Ex: $\mathbb{Z}/6\mathbb{Z}$ $\neq$ domain: $2 \cdot 3 \equiv 0 \pmod 6$ $\quad 2, 3 \not\equiv 0 \pmod 6$

In general:

$\mathbb{Z}/n\mathbb{Z}$ is a field $\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ is a domain

$\Uparrow$ $\qquad\qquad$ $\Downarrow =$

$n = p$ prime $\Leftarrow$ $n \neq 1$ and $n \neq ab$, $1 < a, b < n$

The case $n = p$ prime: $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ field with p elements

$\forall r \geq 1$ $\exists\, \mathbb{F}_{p^r}$ — " — p^r — " — (but $\mathbb{F}_{p^r} \neq \mathbb{Z}/p^r\mathbb{Z}$ if $r > 1$)

Invertible elements: $(\mathbb{Z}/n\mathbb{Z})^* = \{a \pmod n \mid \exists x \in \mathbb{Z} \;\; ax \equiv 1 \pmod n\}$

$\Updownarrow$

$\gcd(a, n) = 1$ $\overset{\text{Bézout}}{\Longleftrightarrow}$ $\exists x, y \in \mathbb{Z}$ $ax + ny = 1 \Rightarrow ax \equiv 1 \pmod n$

Euler's function:

$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^* = |\{a;\ 1 \leq a \leq n,\ \gcd(a, n) = 1\}|$

Ex: $n = p^r$ (p prime, $r \geq 1$) $\quad (\mathbb{Z}/p^r\mathbb{Z})^* = (\mathbb{Z}/p^r\mathbb{Z}) \setminus (p\mathbb{Z}/p^r\mathbb{Z})$, $\quad \varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$

The Chinese remainder thm: If $\gcd(m, n) = 1$, the system $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ has a unique solution $x \pmod{mn}$

Proof: Bézout $\exists u, v \in \mathbb{Z}$ $mu + nv = 1$

(existence) $nv \equiv 1 \pmod m$, $\quad \equiv 0 \pmod n$; $\quad mu \equiv 0 \pmod m$, $\quad \equiv 1 \pmod n$ $\Rightarrow$ $a(nv) + b(mu) \equiv a \pmod m$, $b \pmod n$

Abstract formulation: if $\gcd(m, n) = 1$, then the natural map

$$f: \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$x \pmod{mn} \longmapsto (x \pmod m,\ x \pmod n)$$

is bijective

f is a ring morphism: $f(1) = 1$, $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$

} f is a ring isomorphism

Useful corollary: given polynomials $f_1, \dots, f_M \in \mathbb{Z}[X_1, \dots, X_N]$, denote for any ring A

$Z(A) = \{a = (a_1, \dots, a_N) \in A^N \mid f_1(a_1, \dots, a_N) = \dots = f_M(a_1, \dots, a_N) = 0\}$ the set of solutions of the system Z: $f_1 = \dots = f_M = 0$ with values in A. Then:

$$Z(\mathbb{Z}/mn\mathbb{Z}) \simeq Z(\mathbb{Z}/m\mathbb{Z}) \times Z(\mathbb{Z}/n\mathbb{Z}) \qquad \text{if } \gcd(m, n) = 1$$
$$|Z(\mathbb{Z}/mn\mathbb{Z})| = |Z(\mathbb{Z}/m\mathbb{Z})| \times |Z(\mathbb{Z}/n\mathbb{Z})|$$

the number of solutions of $\begin{cases} f_1(x_1, \dots, x_N) \equiv 0 \pmod n \\ \vdots \\ f_M(x_1, \dots, x_N) \equiv 0 \pmod n \end{cases}$

Another corollary: if $\gcd(m, n) = 1$, then $(\mathbb{Z}/mn\mathbb{Z})^* \overset{\sim}{\Rightarrow} (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$

(group isomorphism) $\Rightarrow$ $\varphi(mn) = \varphi(m)\varphi(n)$.

Formula for $\varphi(n)$: if $n = p_1^{r_1} \cdots p_k^{r_k}$ (p_i distinct primes, $r_i \geq 1$, $k \geq 0$)

$$\Rightarrow \quad \varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{r_i}) = \prod_{i=1}^{k} p_i^{r_i}\left(1 - \frac{1}{p_i}\right) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Euler's Thm: If $\gcd(a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$ [$g \in$ finite group $G \Rightarrow g^{|G|}=1$ in G (Lagrange)]

Improvements: (1) $n=2^r$: $2 \nmid a \Rightarrow a \equiv \pm 1 \pmod 4 \Rightarrow a^2 \equiv 1 \pmod 8 \Rightarrow a^4 \equiv 1 \pmod{16} \Rightarrow \cdots$

$\Rightarrow \forall\, r \geq 3 \quad a^{2^{r-2}} = a^{\varphi(2^r)/2} \equiv 1 \pmod{2^r}$.

(2) If $n = p_1^{r_1} \cdots p_k^{r_k}$, p_i distinct primes, $r_i \geq 1$, let $m_i = \varphi(p_i^{r_i}) \times \begin{cases} \frac{1}{2} & \text{if } p_i = 2,\ r_i \geq 3 \\ 1 & \text{if not} \end{cases}$,

$m = \operatorname{lcm}(m_1, \cdots, m_k)$.

If $\gcd(a,n)=1$, then $\forall i = 1, \cdots, k \quad a^{m_i} \equiv 1 \pmod{p_i^{r_i}} \Rightarrow a^m = (a^{m_i})^{m/m_i} \equiv 1 \pmod{p_i^{r_i}}$

$\Rightarrow a^m \equiv 1 \pmod n$.

(3) If $n \neq 1, 2, 4, p^r, 2p^r$ ($p \neq 2$ prime, $r \geq 1$) $\Rightarrow m < \varphi(n)$ ($\Leftrightarrow$ the group $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic)

$\Downarrow$

$\begin{cases} n = 2^r,\ r \geq 3 \Rightarrow m = \varphi(n)/2 \\ k \geq 2,\ p_1^{r_1}, p_2^{r_2} \geq 3 \Rightarrow 2 \mid \varphi(p_1^{r_1}), \varphi(p_2^{r_2}) \Rightarrow m \mid \dfrac{\varphi(p_1^{r_1})\varphi(p_2^{r_2})}{2} \varphi(p_3^{r_3}) \cdots \varphi(p_k^{r_k}) = \dfrac{\varphi(n)}{2} \end{cases}$

Theorem. If $n = 1, 2, 4, p^r, 2p^r$ ($p \neq 2$ prime, $r \geq 1$) $\Rightarrow \exists\ a \pmod n \in (\mathbb{Z}/n\mathbb{Z})^*$ such that

$(\mathbb{Z}/n\mathbb{Z})^* = \{ \underbrace{a, a^2, \cdots, a^{\varphi(n)} \pmod n}_{\text{distinct elements}} \}$ (i.e., the group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic and $a \pmod n$ is its generator)

Proof: We need to show that $(\mathbb{Z}/p^r\mathbb{Z})^*$ is cyclic ($p \neq 2$ prime, $r \geq 1$).

Step 1. $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$ is cyclic. This is a special case of the following

Proposition. Let K be a field. A finite subgroup $G \subset K^*$ is cyclic.

Pf. Let $m = |G|$. For $g \in G$, the order of g ($= \min\{ j \geq 1 \mid g^j = 1 \}$) divides m.

For $d \mid m$, let $A(d) = \{ g \in G \mid (\text{the order of } g) = d \} \subseteq \{ g \in G \mid g^d = 1 \} \subset \mu_d(K)$

$|\mu_d(K)| = |\{ x \in K \mid x^d - 1 = 0 \}| \leq \deg(x^d - 1) = d$ (K is a field!)

If $A(d) \neq \emptyset$, $g_1 \in A(d) \Rightarrow \{ \underbrace{g_1, g_1^2, \cdots, g_1^d = 1}_{d \text{ elements}} \} \subset \underbrace{\mu_d(K)}_{\leq d \text{ elts}} \Rightarrow$ equality, hence

$A(d) = \{ g_1^i \mid \text{order of } (g_1^i) = d \} = \{ g_1^i \mid i \in (\mathbb{Z}/d\mathbb{Z})^* \}$, $|A(d)| = \varphi(d)$.

(Exercise: (order of g^i) = (order of g) / gcd((order of g), i))

So $|A(d)| = \begin{cases} 0 \\ \varphi(d) \end{cases}$ for each $d \mid m$. But

$\sum_{d \mid m} |A(d)| = |G| = m = \sum_{d \mid m} \varphi(d)$ ($m = |\mathbb{Z}/m\mathbb{Z}|$, $\varphi(d) = |\{ a \pmod m \mid \text{order of } a \pmod m = d \}|$)

$\Rightarrow \forall\, d \mid m \quad A(d) = \varphi(d) \Rightarrow \boxed{A(m) > 0}$

Step 2. Prop. If p = prime, $r \geq 1$ and $p^r > 2$, then $\left\{ \begin{matrix} x \equiv 1 \pmod{p^r} \\ x \not\equiv 1 \pmod{p^{r+1}} \end{matrix} \right\} \Rightarrow \left\{ \begin{matrix} x^p \equiv 1 \pmod{p^{r+1}} \\ x^p \not\equiv 1 \pmod{p^{r+2}} \end{matrix} \right\}$

Cor: If $n > r \geq 1$ and $p^r > 2$, then the group

$\{ x \pmod{p^n} \mid x \equiv 1 \pmod{p^r} \} = \operatorname{Ker}\left((\mathbb{Z}/p^n\mathbb{Z})^* \xrightarrow{p^r} (\mathbb{Z}/p^r\mathbb{Z})^* \right)$ is cyclic, generated by any $x \pmod{p^n}$ satisfying the above

(of order $\varphi(p^n)/\varphi(p^r) = p^{n-r}$)

Pf: $x = 1 + p^r y$, $p \nmid y$ $\quad x^p = 1 + p^{r+1} y + \underbrace{\binom{p}{2}(p^r y)^2 + \cdots + \binom{p}{p-1}(p^r y)^{p-1}}_{\equiv 0 \pmod{p^{r+2}}} + \binom{p}{p} p^{pr} y^p$ $\quad \cdot pr \geq r+2$ if $\begin{cases} p > 2 \\ p = 2, r > 1 \end{cases}$

Step 3. Prop. If $G \xrightarrow{f} H$ is a morphism of finite abelian groups such that $\gcd(|\ker(f)|, |\mathrm{Im}(f)|) = 1$, then: (1) $G \xrightarrow{f} \mathrm{Im}(f)$ has a section $G \xleftarrow{s} \mathrm{Im}(f)$ (a group morphism such that $f \circ s = id$); (2) the morphism $\alpha : \ker(f) \times \mathrm{Im}(f) \longrightarrow G$, $(g, h) \longmapsto g\, s(h)$ is a group isomorphism.

Pf: (1) Bezout: $\exists \begin{cases} a \equiv 0 \mod |\ker(f)| \\ a \equiv 1 \mod |\mathrm{Im}(f)| \end{cases}$; then $s(f(g)) = g^a$ depends only on $f(g)$ (since $g^{|\ker(f)|} = 1$ if $f(g) = 1$) and defines s, which is a group morphism and $f(s(f(g))) = f(g)^a = f(g)$ ($f(g)^{|\mathrm{Im}(f)|} = 1$).

(2) Injectivity: $g\, s(h) = 1 \Rightarrow \underbrace{f(g)}_{1}\ \underbrace{f(s(h))}_{h} = 1 \Rightarrow h = 1 \Rightarrow g = 1$, so $\ker(\alpha) = \{1\}$.

Surjectivity: $g \in G \Rightarrow g = \underbrace{g\, s(f(g))^{-1}}_{\in \ker(f)}\, s(f(g)) \in \mathrm{Im}(\alpha)$.

Corollary: (1) If $p \neq 2$ prime, $r \geq 2$, $(\mathbb{Z}/p^r\mathbb{Z})^* \xrightarrow{pr} (\mathbb{Z}/p\mathbb{Z})^*$

$|\ker(pr)| = p^{r-1}$, $|\mathrm{Im}(pr)| = p-1$

$\Rightarrow (\mathbb{Z}/p^r\mathbb{Z})^* \simeq \underbrace{\ker(pr)}_{\text{cyclic of order } p^{r-1}} \times \underbrace{\mathrm{Im}(pr)}_{\text{cyclic of order } (p-1)} \overset{\text{chinese thm}}{\simeq}$ cyclic of order $p^{r-1}(p-1)$

---

(2) **If $p=2$, $r \geq 3$:** $\{\pm 1\} \times \ker(pr') \longrightarrow (\mathbb{Z}/2^r\mathbb{Z})^*$ isomorphism

$a, b \longmapsto ab$

$pr' : (\mathbb{Z}/2^r\mathbb{Z})^* \longrightarrow (\mathbb{Z}/4\mathbb{Z})^*$, $\ker(pr')$ cyclic of order 2^{r-2}

(generated by any $a \pmod{2^r}$ such that $a \equiv 1 \pmod 4$, $a \not\equiv 1 \pmod 8$)

Another proof of Step 1: for an abelian group G and $n \geq 1$, let $G[n] = \{g \in G \mid g^n = 1\}$.

(a) $(G \times H)[n] = G[n] \times H[n]$

(b) if ℓ is a prime and G is cyclic of order ℓ^k ($k \geq 1$) $\Rightarrow G[\ell]$ is cyclic of order ℓ.

(c) every finite abelian group G of order $n = \ell_1^{k_1} \cdots \ell_m^{k_m}$ (ℓ_i distinct primes) is a product $G = G_1 \times \cdots \times G_m$, $|G_i| = \ell_i^{k_i}$; each G_i is a product of cyclic groups of ℓ-power order.

Corollary. A finite abelian group G satisfying $|G[d]| \leq d$ for all $d \geq 1$ is cyclic.

Pf: Write $G = G_1 \times \cdots \times G_m$ as in (c); then $|G_i[\ell_i]| \leq \ell_i \overset{(a),(b)}{\Longrightarrow} G_i$ is cyclic, $G_i \simeq \mathbb{Z}/\ell_i^{k_i}\mathbb{Z} \Longrightarrow$ (chinese remainder thm) $G \simeq \mathbb{Z}/\ell_1^{k_1} \cdots \ell_m^{k_m}\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$ is cyclic.

Rmk: If $x^m \equiv a \pmod n$, then ($\gcd(a, n) = 1$)

$\{x' \pmod n \mid x'^m \equiv a \pmod n\} = \{xy \pmod n \mid y^m \equiv 1 \pmod n\}$

Properties of finite (abelian) groups G

(1) $f: G \to H$ group morphism ($\forall g, g' \in G \quad f(gg') = f(g)f(g')$)

$\Rightarrow$ $\mathrm{Ker}(f) = \{g \in G \mid f(g) = 1\} \lhd G$ normal subgroup of G

$\mathrm{Im}(f) = \{f(g) \mid g \in G\} \subset H$ subgroup of H

$\bar{f}: G/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f)$ isomorphism ($\Rightarrow |G| = |\mathrm{Ker}(f)| \cdot |\mathrm{Im}(f)|$ if $|G| < \infty$)

$g\,\mathrm{Ker}(f) \longmapsto f(g)$

(2) Thm of Lagrange: $|G| < \infty \Rightarrow \forall g \in G \quad g^{|G|} = 1$

(3) K field, $|G| < \infty$, $\chi: G \to K^*$ group morphism (a "character of G")

$$\Rightarrow A = \sum_{g \in G} \chi(g) = \begin{cases} |G| \cdot 1_K \in K & \chi = 1 \\ 0 \in K & \chi \neq 1 \end{cases}$$

Pf: If $\exists\, h \in G$, $\chi(h) \neq 1 \Rightarrow$ write $g = hg' \Rightarrow A = \sum_{g' \in G} \chi(hg') = \chi(h)\,A \Rightarrow \underbrace{(1-\chi(h))}_{\neq 0} A = 0 \in K \Rightarrow A = 0$.

Notation: G abelian group, $m \in \mathbb{Z}_{>0}$, $G[m] = \{g \in G \mid g^m = 1\} \subset G$ subgroup

($m \mid n \Rightarrow G[m] \subset G[n]$) ($m = |G| \Rightarrow G = G[m]$ (Lagrange))

$(G \times H)[m] = G[m] \times H[m]$

(4) $\gcd(m,n) = 1 \Rightarrow$ product $G[m] \times G[n] \xrightarrow{\text{prod}} G[mn]$ is an isomorphism

$(g, h) \longmapsto gh$

Pf: $\exists\, a, b \in \mathbb{Z}$ $ma + nb = 1$; $\forall g_0 \in G[mn]$ $g_0 = g_0^{nb} g_0^{ma}$, $(g_0^{nb})^m = 1 = (g_0^{ma})^n \Rightarrow$ prod surjective

If $\mathrm{prod}(g,h) = 1 \Rightarrow h = g^{-1}$, $g = (g^m)^a (g^n)^b = (g^m)^a (h^n)^{-b} = 1 \Rightarrow$ prod injective

(5) $\gcd(m, |G|) = 1 \Rightarrow G[m] = \{1\} = G[1]$. This is a special case ($n = |G|$) of

(5') $G[m] \cap G[n] = G[\gcd(m,n)]$

Pf: $d = \gcd(m,n) \mid m$, $d \mid n \Rightarrow G[d] \subset G[m]$, $G[d] \subset G[n]$

If $g \in G[m] \cap G[n]$: $\exists\, a, b \in \mathbb{Z}$ $am + bn = d \Rightarrow g^d = (g^m)^a (g^n)^b = 1 \Rightarrow g \in G[d]$

(6) If $|G| < \infty$, $m \geq 1 \Rightarrow G[m] = G[m] \cap G[|G|] = G[\gcd(m, |G|)]$

(7) If $G \simeq C_N$ (cyclic group of order N; $g \in G$ any generator of G)

$m \geq 1$, $d = \gcd(m, N) \Rightarrow G[m] = G[d] \simeq C_d$, generated by $g^{N/d}$

Pf: $\exists$ isomorphism $G \xrightarrow{\sim} \mu_N(\mathbb{C})$ under which $g \longmapsto \xi_N = e^{2\pi i/N}$. Then

$G[m] = G[d] \xrightarrow{\sim} \mu_N(\mathbb{C})[d] = \mu_d(\mathbb{C})$ cyclic, generated by $\xi_d = \xi_N^{N/d}$.

(8) If G is any finite abelian group $\Rightarrow \exists$ isomorphism $G \xrightarrow{\sim} \prod_{i=1}^{k} C_{N_i}$

(C_{N_i} cyclic, $|C_{N_i}| = N_i$) $\Rightarrow \forall m \geq 1$

$$G[m] \xrightarrow{\sim} \prod_i C_{N_i}[m] = \prod_i C_{N_i}[\gcd(N_i, m)] \simeq \prod_i C_{\gcd(N_i, m)} \Rightarrow |G[m]| = \prod_i \gcd(N_i, m)$$

(9) In (7), $\{x^m \mid x \in G\} = \{y^d \mid y \in G\}$ = cyclic of order N/d, generated by g^d

If $z \in G$, $z = x_1^m \Rightarrow \{x \in G \mid x^m = z\} = \{x_1 h \mid h \in G[m]\}$ has $|G[m]| = d$ elements

Pf: $m = de$, $(e, N) = 1 \Rightarrow \exists\, e' \in \mathbb{Z}$ $ee' \equiv 1 \pmod N$ $\forall h \in G$ $h^{ee'} = h$

$x^m = (x^{m/d})^d$, $y^d = y^{dee'} = (y^{e'})^m$.

(10) $|G| < \infty \Rightarrow |\{x^m \mid x \in G\}| = |\mathrm{Im}(G \xrightarrow{f} G,\ x \longmapsto x^m)| = \dfrac{|G|}{|\mathrm{Ker}(f)|} = \dfrac{|G|}{|G[m]|} = \dfrac{|G|}{|G[d]|}$

$d = \gcd(|G|, m)$

Structure of $(\mathbb{Z}/n\mathbb{Z})^*$

Notation: C_m = a cyclic group of order m ($C_m \xrightarrow{\sim} \mu_m(\mathbb{C}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z}, +)$)

Chinese remainder thm: $\gcd(m,n)=1 \Rightarrow C_{mn} \xrightarrow{\sim} C_m \times C_n$.

Properties: (1) $n=p^r$, $p\neq 2$ prime, $r\geq 1 \Rightarrow (\mathbb{Z}/p^r\mathbb{Z})^* \simeq C_{\varphi(p^r)} \simeq C_{p-1} \times C_{p^{r-1}}$.

(2) $n=2^r$, $r\geq 1$: $(\mathbb{Z}/2^r\mathbb{Z})^* \simeq \begin{cases} C_{\varphi(2^r)} = C_{2^{r-1}} & r=1,2 \\ C_2 \times C_{\varphi(2^r)/2} = C_2 \times C_{2^{r-2}} & r\geq 3 \end{cases}$

(3) $n=\prod_{i=1}^{k} p_i^{r_i}$, p_i distinct primes, $r_i\geq 1$, $k\geq 0 \Rightarrow (\mathbb{Z}/n\mathbb{Z})^* = \prod_{i=1}^{k} (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$

---

(4) Writing $(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_j C_{N_j}$, we obtain $\forall m\geq 1$

$$\{x\in \mathbb{Z}/n\mathbb{Z} \mid x^m \equiv 1 \pmod n\} = (\mathbb{Z}/n\mathbb{Z})^*[m] \simeq \prod_j C_{N_j}[m] \simeq \prod_j C_{\gcd(N_j,m)}$$

Ex:

$$\left|\{x \pmod n \mid x^3\equiv 1 \pmod n\}\right| = \left|(\mathbb{Z}/n\mathbb{Z})^*[3]\right| = \prod_i \underbrace{\left|(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*[3]\right|}_{\begin{cases} 1 & p_i\equiv 2 \pmod 3 \\ 3 & p_i\equiv 1 \pmod 3 \\ 1 & p_i=3,\ r_i=1 \\ 3 & p_i=3,\ r_i\geq 2 \end{cases}} = 3^{a+b}$$

$a = |\{p\mid n;\ p \text{ prime},\ p\equiv 1 \pmod 3\}|$

$b = \begin{cases} 1 & 9\mid n \\ 0 & 9\nmid n \end{cases}$

$$\{x^m \pmod n \mid x\in(\mathbb{Z}/n\mathbb{Z})^\times\} \simeq \prod_j \{g^m \mid g\in C_{N_j}\} \simeq \prod_j C_{N_j/\gcd(N_j,m)}$$

---

(5) The exponent $e(G)$ of a finite abelian group G is the smallest integer $N\geq 1$ such that $G=G[N]$. It satisfies $e(C_N)=N$, $e(G_1\times G_2)=\operatorname{lcm}(e(G_1), e(G_2))$

$\Rightarrow e(\prod_{j=1}^{k} C_{N_j}) = \operatorname{lcm}(N_1,\dots,N_k)$. As a result,

$$e\left(\prod_{i=1}^{k}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times\right) = \operatorname{lcm}(e_1,\dots,e_k),\quad e_i = e\left((\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times\right) = \varphi(p_i^{r_i}) \times \begin{cases} 1/2 & \text{if } p_i=2,\ r_i\geq 3 \\ 1 & \text{if not} \end{cases}$$

---

(6) G finite abelian group with $G=G[N]$, $m\geq 1 \Rightarrow G[m] = G[N]\cap G[m] = G[d]$ and $G^m = \{g^m \mid g\in G\} = G^d$, where $d=\gcd(m,N)$. Indeed, $g^m = (g^{m/d})^d \Rightarrow G^m \subset G^d$, and $d=mu+Nv$ $(u,v\in\mathbb{Z}) \Rightarrow g^d = (g^u)^m (g^v)^N = (g^u)^m \Rightarrow G^d \subset G^m$.

It follows that, under $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \prod_{i=1}^{k}(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$,

$$\{x^m \pmod n \mid x\in(\mathbb{Z}/n\mathbb{Z})^\times\} \xrightarrow{\sim} \prod_{i=1}^{k} \{x_i^{d_i} \pmod{p_i^{r_i}} \mid p_i\nmid x_i\},\quad d_i=\gcd(m,e_i)$$

Exercise: Write $G=(\mathbb{Z}/240\mathbb{Z})^\times$ as $\prod C_{N_j}$. What is $e(G)=?$ Compute the order of $G^{30} = \{x^{30} \pmod{240} \mid \gcd(x,240)=1\} \subset G$. For each $a\in G^{30}$, compute the number of solutions of $x^{30}\equiv a \pmod{240}$. Describe explicitly all elements of G^{30}.

Congruences $x^2 \equiv a \pmod p$ ($p \neq 2$ prime)

Note: $0 \not\equiv x^2 \equiv y^2 \pmod p \iff p \mid (x+y)(x-y) \iff y \equiv \pm x \pmod p$
($p \nmid x$; $x \not\equiv -x$ (since $1 \not\equiv -1 \pmod p$))

Def. Quadratic residues $(\bmod p)$: $QR = \mathbb{F}_p^{*2} = \{x^2 \pmod p \mid p \nmid x\} \subset \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$

Quadratic non-residues $(\bmod p)$: $QN = \mathbb{F}_p^* \setminus \mathbb{F}_p^{*2}$

Ex: $p=3$: $QR = \{1^2 \equiv 1 \pmod 3\}$, $QN = \{-1 \pmod 3\}$

$p=5$: $QR = \{(\pm 1)^2, (\pm 2)^2 \pmod 5\} = \{\pm 1 \pmod 5\}$, $QN = \{\pm 2 \pmod 5\}$

$p=7$: $QR = \{(\pm 1)^2, (\pm 2)^2, (\pm 3)^2 \pmod 7\} = \{1, 2, 4 \pmod 7\}$, $QN = \{3, 5, 6 \pmod 7\}$

Recall: $\mathbb{F}_p^* = \mu_{p-1}(\mathbb{F}_p)$ is cyclic of order $p-1$; fix a **generator** $g \pmod p \in \mathbb{F}_p^*$

Then: (1) $g^a \equiv g^b \pmod p \iff a \equiv b \pmod{(p-1)}$

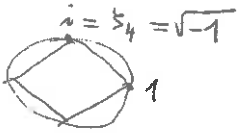
(2) $u = g^{\frac{p-1}{2}} \pmod p \in \mathbb{F}_p^*$ satisfies $u \neq 1 = u^2 \Rightarrow 0 = \frac{u^2-1}{u-1} = u+1 \Rightarrow u = -1 \in \mathbb{F}_p^*$

(3) $\mathbb{F}_p^* = \{g, g^2, \dots, \underbrace{g^{p-1} \pmod p}_{1 \in \mathbb{F}_p^*}\} \Rightarrow QR = \{\underbrace{g^2, g^4, g^6, \dots, g^{p-3}, g^{p-1} \equiv 1 \pmod p}_{\frac{p-1}{2} \text{ elements}}\}$

$QN = \{g, g^3, \dots, g^{p-4}, g^{p-2} \pmod p\}$ also $\frac{p-1}{2}$ elements

---

Moral: $\mathbb{F}_p^*$ behaves like $\mu_{p-1}(\mathbb{C})$!!



Ex: $-1 \in \mathbb{F}_p^{*2} \iff p \equiv 1 \pmod 4$

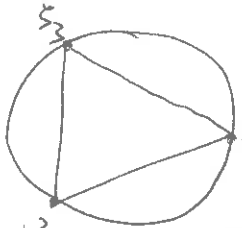
Pf: $\Rightarrow$ if $-1 \equiv x^2 \pmod p \Rightarrow \underbrace{(-1)^{\frac{p-1}{2}}}_{\pm 1} \equiv x^{p-1} \equiv 1 \pmod p$, $-1 \not\equiv 1 \pmod p$ $\Rightarrow (-1)^{\frac{p-1}{2}} = 1 \Rightarrow \frac{p-1}{2} \in 2\mathbb{Z}$.

$\Leftarrow$ if $p = 1+4n$, $g \pmod p$ has order $4n \Rightarrow g^n \pmod p$ has order $4 \Rightarrow$

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

What about $-3 \in \mathbb{F}_p^{*2}$? $\quad (p \neq 3)$

$\zeta_N = e^{2\pi i/N}$



$\sqrt{-3} = i\sqrt{3} = \zeta_3 - \zeta_3^2 = 2\zeta_3 + 1$ (root of y^2+3), $\zeta_3 = \underbrace{\frac{-1+i\sqrt{3}}{2}}_{\text{root of } \frac{x^3-1}{x-1} = x^2+x+1}$

$4(x^2+x+1) = (2x+1)^2 + 3$

Prop. If $p \neq 3$, then: $-3 \in \mathbb{F}_p^{*2} \iff p \equiv 1 \pmod 3$ $\quad (\iff p \in \mathbb{F}_3^{*2})$

Pf: $\Rightarrow$ If $y^2 \equiv -3 \pmod p$, write $y \equiv 2x+1 \pmod p$ (OK, since $2 \in \mathbb{F}_p^*$) $\Rightarrow$

$4(x^2+x+1) \equiv 0 \pmod p \Rightarrow x^2+x+1 \equiv 0 \pmod p \Rightarrow x^3 \equiv 1 \pmod p$, $x \neq 1 \pmod p$ ($x-1 \neq 0$) $\Rightarrow x \pmod p \in \mathbb{F}_p^*$ has order 3

$\Downarrow$

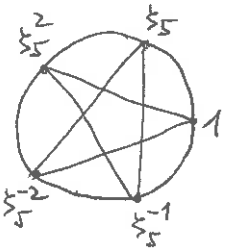
$3 \mid |\mathbb{F}_p^*| = p-1$

$\Leftarrow$ If $p \equiv 1 \pmod 3 \Rightarrow x = g^{\frac{p-1}{3}} \pmod p$ has order $= 3$ in $\mathbb{F}_p^*$

$\frac{x^3-1}{x-1} = x^2+x+1 \equiv 0 \pmod p \Leftarrow x^3 \equiv 1 \not\equiv * \pmod p \Rightarrow y = 2x+1$ satisfies

$y^2+3 \equiv 4(x^2+x+1) \equiv 0 \pmod p$.

What about $5 \in \mathbb{F}_p^{*2}$? $(p \neq 5)$ we need to relate $\sqrt{5}$ to $\zeta_5 = e^{2\pi i/5}$



ζ_5^k ($k = \pm 1, \pm 2$) = root of $0 = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1 = x^2\left(\underbrace{(x^2+x^{-2})}_{y^2-2} + \underbrace{(x+x^{-1})}_{y} + 1\right)$

$4(y^2+y-1) = (2y+1)^2 - 5$

$0 < \zeta_5 + \zeta_5^{-1}$ = a root of $\Rightarrow \zeta_5 + \zeta_5^{-1} = \frac{-1+\sqrt{5}}{2}$

$0 > \zeta_5^2 + \zeta_5^{-2}$ = — " — $\Rightarrow \zeta_5^2 + \zeta_5^{-2} = \frac{-1-\sqrt{5}}{2}$

$\Rightarrow \boxed{\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^{-2} + \zeta_5^{-1}}$

Prop: $p \equiv 1 \pmod 5 \Rightarrow 5 \in \mathbb{F}_p^{*2}$

Pf: $x = g^{\frac{p-1}{5}} \pmod p \in \mathbb{F}_p^*$ satisfies $x^5 = 1 \neq x \in \mathbb{F}_p \Rightarrow 0 = x^4+x^3+x^2+x+1 \Rightarrow$

$y = x + x^{-1} \in \mathbb{F}_p$ satisfies $(2y+1)^2 = 5 \in \mathbb{F}_p$.

Fact: $(p \neq 5)$ $5 \in \mathbb{F}_p^{*2} \Leftrightarrow p \equiv \pm 1 \pmod 5$ $(\Leftrightarrow p \in \mathbb{F}_5^{*2})$

this can be proved using $\mathbb{F}_{p^2}^*$ cyclic of order p^2-1 $(5 \mid (p^2-1) \Leftrightarrow p \equiv \pm 1 (5))$

The Legendre symbol

Def: $p \neq 2$ prime, $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \pmod p \in \mathbb{F}_p^{*2} \\ -1 & a \pmod p \notin \mathbb{F}_p^{*2} \end{cases}$ depends only on $a \pmod p \in \mathbb{F}_p$

Prop. (1) (Euler's criterion) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; (3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv -1 \pmod 4 \end{cases}$.

Pf. (1) $p \mid a \Rightarrow 0 \equiv 0 \pmod p$; if $p \nmid a$, then $a \equiv g^i \pmod p$ and

$\left(\frac{a}{p}\right) = \begin{cases} 1 & 2 \mid i \\ -1 & 2 \nmid i \end{cases}$, $a^{\frac{p-1}{2}} \equiv (g^{\frac{p-1}{2}})^i \equiv (-1)^i \pmod p \equiv \left(\frac{a}{p}\right) \pmod p$.

(2) $\underbrace{\left(\frac{ab}{p}\right)}_{\pm 1} \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \underbrace{\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)}_{\pm 1} \pmod p$, $-1 \not\equiv 1 \pmod p$ $\Rightarrow$ equality $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(3) $\left(\frac{-1}{p}\right) \overset{(1)}{\equiv} (-1)^{\frac{p-1}{2}} \pmod p \overset{-1 \not\equiv 1}{\Longrightarrow} \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Quadratic Reciprocity Law (QRL)

$p \neq 2$ primes $\neq 2 \Rightarrow$ $\boxed{\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)}$, $\boxed{q^* = (-1)^{\frac{q-1}{2}} q \ (\equiv 1 \pmod 4)}$

(so $\left(\frac{q^*}{p}\right)$ depends only on $p \pmod q$)

$\boxed{p \in \mathbb{F}_q^{*2} \Leftrightarrow q^* \in \mathbb{F}_p^{*2}}$

Complements:

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

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$

The Jacobi symbol

Def: $a, b \in \mathbb{Z}\setminus\{0\}$, $b>0$, $\gcd(2a,b)=1$; write $b=\prod p_i^{k_i}$, $p_i \neq 2$ primes

$$\left(\frac{a}{b}\right) = \prod_i \left(\frac{a}{p_i}\right)^{k_i} \in \{\pm 1\} \quad \text{(depends only on } a \pmod b\text{)}$$

Properties: (1) $b=p$ prime $\Rightarrow \left(\frac{a}{b}\right)$ = the Legendre symbol $\left(\frac{a}{p}\right)$

(2) $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$; (3) $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$; (4) if $a \equiv x^2 \pmod b \Rightarrow \left(\frac{a}{b}\right) = \left(\frac{x}{b}\right)^2 = 1$

[**Warning:** ($\Leftarrow$) does not hold in general: $\exists x \quad a \equiv x^2 \pmod{15} \iff \left(\frac{a}{3}\right)=\left(\frac{a}{5}\right)=1$, but

$$\left(\frac{a}{15}\right)=1 \iff \begin{cases} \left(\frac{a}{3}\right)=\left(\frac{a}{5}\right)=1 \\ \left(\frac{a}{3}\right)=\left(\frac{a}{5}\right)=-1 \end{cases}$$

]

(5) $b>0$, $2\nmid b \Rightarrow \left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$, $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$

(6) **Reciprocity Law:** $a, b>0$, $2\nmid ab$, $\gcd(a,b)=1 \Rightarrow \boxed{\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}\left(\frac{b}{a}\right)}$

Pf: use QRL + complements, and $\frac{b-1}{2}+\frac{b'-1}{2} \equiv \frac{bb'-1}{2} \pmod 2$, $\frac{b^2-1}{8}+\frac{b'^2-1}{8} \equiv \frac{(bb')^2-1}{8} \pmod 2$

Ex: 691 = prime; does $x^2 \equiv 259 \pmod{691}$ have a solution? Yes!

$691 = 2\cdot 259 + 173$
$259 = 173 + 86$
$173 = 4\cdot 43 + 1$

$$\left(\frac{259}{691}\right) = -\left(\frac{691}{259}\right) = -\left(\frac{173}{259}\right) = -\left(\frac{259}{173}\right) = -\left(\frac{86}{173}\right) = -\underbrace{\left(\frac{2}{173}\right)}_{-1}\left(\frac{43}{173}\right) = \left(\frac{173}{43}\right) = \left(\frac{1}{43}\right) = 1$$

Note: For fixed $a \in \mathbb{Z}\setminus\{0\}$, the function

$$b \longmapsto \left(\frac{a}{b}\right) \qquad (b \in \mathbb{Z},\ b>0,\ (b,2a)=1)$$

depends only on the class $b \pmod{4|a|} \in (\mathbb{Z}/4|a|\mathbb{Z})^*$

and is multiplicative: $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$

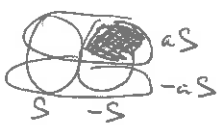
Gauss' Lemma. Fix $S \subset \mathbb{F}_p^*$ such that $\mathbb{F}_p^* = S \sqcup \underbrace{(-S)}_{\{-s \mid s\in S\}}$ disjoint union ($\Rightarrow |S| = \frac{1}{2}|\mathbb{F}_p^*| = \frac{p-1}{2}$)

(ex: $S = \{1 \pmod p, 2 \pmod p, \dots, \frac{p-1}{2} \pmod p\}$). For $a \in \mathbb{F}_p^*$, let $aS = \{as \mid s\in S\} \subset \mathbb{F}_p^*$.

(1) $aS \sqcup (-a)S = \mathbb{F}_p^*$; (2) $\boxed{\left(\frac{a}{p}\right) = (-1)^{|aS \cap (-S)|}}$.

Pf: (1) multiplication by $a^{\pm 1}$ induces bijections $S \underset{a^{-1}}{\overset{a}{\rightleftarrows}} aS$, $-S \underset{a^{-1}}{\overset{a}{\rightleftarrows}} a(-S) = (-a)S$

(2)



$\forall s \in S \quad as = s'\varepsilon_{s'} \qquad s' \in S,\ \varepsilon_{s'} = \pm 1$

If $s_1 \neq s_2 \in S \Rightarrow s_1 \neq \pm s_2 \Rightarrow as_1 \neq \pm as_2$ $\Big\}$ $\begin{matrix} S \longrightarrow S \\ s \longmapsto s' \end{matrix}$ is a bijection

So $a^{\frac{p-1}{2}} \underbrace{\prod_{s\in S} s}_{A} = \prod_{s\in S}(as) = \prod_{s'\in S} s'\varepsilon_{s'} = A \prod_{s\in S}\varepsilon_{s'} = A\,(-1)^{|aS\cap(-S)|} \in \mathbb{F}_p^*$

$A \in \mathbb{F}_p^* \Rightarrow \underbrace{\left(\frac{a}{p}\right)}_{\pm 1} \equiv \underbrace{a^{\frac{p-1}{2}}}_{\pm 1} \equiv \underbrace{(-1)^{|aS\cap(-S)|}}_{\pm 1} \pmod p \overset{1\neq -1}{\Longrightarrow} \boxed{\left(\frac{a}{p}\right) = (-1)^{|aS\cap(-S)|}}$.

Cor: For S as in Gauss' lemma and $a=2$, $s' \in 2S \cap S \iff s = 1, 2, \dots, \left\lfloor \frac{p-1}{4} \right\rfloor$; $s' \in 2S \cap (-S) \iff s = 1 + \left\lfloor \frac{p-1}{4} \right\rfloor, \dots, \frac{p-1}{2}$

$$\Rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor}, \quad \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor = 2n + \begin{cases} 0 \\ 1 \\ 1 \\ 2 \end{cases} \text{ if } p = 8n + \begin{cases} 1 \\ 3 \\ 5 \\ 7 \end{cases} \Rightarrow \left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$$

Proof of QRL: need to generalise $i\sqrt{3} = \zeta_3 - \zeta_3^2$, $\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$

$p \neq 2$ (+2) primes $= 1 + 2\zeta_3$ $= 1 + 2\zeta_5 + 2\zeta_5^4$

$\zeta_2 = e^{2\pi i/2}$

Def. Quadratic Gauss sums $(a \in \mathbb{F}_2^*)$

$$S_a = \sum_{b \in \mathbb{F}_2^*} \left(\frac{b}{2}\right) \zeta_2^{ab} = \sum_{x \in \mathbb{F}_2} \zeta_2^{ax^2} \quad \left(\text{since } \sum_{y \in \mathbb{F}_2} \zeta_2^y = \frac{\zeta_2^2 - 1}{\zeta_2 - 1} = 0\right)$$

Facts:

(1) $S_a \underset{\uparrow\, b = a^{-1}c}{=} \sum_{c \in \mathbb{F}_2^*} \left(\frac{a^{-1}}{2}\right)\left(\frac{c}{2}\right)\zeta_2^c = \left(\frac{a}{2}\right)^{-1} S_1 = \left(\frac{a}{2}\right) S_1$; (2) $\overline{S_a} = \sum_b \left(\frac{b}{2}\right)\zeta_2^{-ab} = S_{-a} = \left(\frac{-1}{2}\right) S_a$

(3) $|S_a|^2 = |S_1|^2 = S_1 S_{-1} = \sum_{b,c \in \mathbb{F}_2^*} \left(\frac{b}{2}\right)\left(\frac{c}{2}\right)\zeta_2^{b-c} \underset{\uparrow\, b = cd}{=} \sum_{c,d \in \mathbb{F}_2^*} \left(\frac{d}{2}\right)\zeta_2^{c(d-1)} = \sum_{d \in \mathbb{F}_2^*} \left(\frac{d}{2}\right) \begin{cases} 2-1 & d=1 \\ -1 & d \neq 1 \end{cases} =$

$= 2 - \sum_{d \in \mathbb{F}_2^*} \left(\frac{d}{2}\right) = 2.$ (4) $\boxed{S_1^2 = \left(\frac{-1}{2}\right) 2 = 2^*}$

ζ_2 is a root of $\frac{x^2-1}{x-1} = x^{2-1} + x^{2-2} + \cdots + x + 1 = 0$

$\Rightarrow$ $\underbrace{\{a_0 + a_1\zeta_2 + \cdots + a_{2-2}\zeta_2^{2-2} \mid a_i \in \mathbb{Z}\}}_{\mathbb{Z}[\zeta_2]}$ is a subring of $\mathbb{C}$

$\mathbb{Z}[\zeta_2]$ (= the smallest — " — — " — containing $\mathbb{Z}$ and ζ_2).

Congruences (mod p) in $\mathbb{Z}[\zeta_2]$: for $x, y \in \mathbb{Z}[\zeta_2]$ define

$x \equiv y \pmod{p\mathbb{Z}[\zeta_2]} \iff x - y \in p\mathbb{Z}[\zeta_2]$.

usual properties: $x \equiv x' \pmod{p\mathbb{Z}[\zeta_2]}$, $y \equiv y' \pmod{p\mathbb{Z}[\zeta_2]} \Rightarrow x+y \equiv x'+y'$, $xy \equiv x'y'$, $\boxed{(x+y)^p \equiv x^p + y^p \pmod{p\mathbb{Z}[\zeta_2]}}$

Therefore: $S_1^p = \left(\sum_b \left(\frac{b}{2}\right)\zeta_2^b\right)^p \equiv \sum_b \left(\frac{b}{2}\right)^p \zeta_2^{pb} = \sum_b \left(\frac{b}{2}\right)\zeta_2^{pb} = S_p = \left(\frac{p}{2}\right) S_1 \pmod{p\mathbb{Z}[\zeta_2]}$

$\Rightarrow$ $\underbrace{S_1^{p+1}}_{S_1^2 (S_1^2)^{\frac{p-1}{2}} = 2^*(2^*)^{\frac{p-1}{2}} \equiv 2^*\left(\frac{2^*}{p}\right) \pmod{p\mathbb{Z}[\zeta_2]}} \equiv \left(\frac{p}{2}\right) S_1^2 = 2^*\left(\frac{p}{2}\right) \pmod{p\mathbb{Z}[\zeta_2]}$

$\Rightarrow$ $\boxed{2^*\left(\left(\frac{p}{2}\right) - \left(\frac{2^*}{p}\right)\right) \in \mathbb{Z} \cap p\mathbb{Z}[\zeta_2]}$

Lemma: $\mathbb{Q} \cap \mathbb{Z}[\zeta_2] = \mathbb{Z}$ $(\Rightarrow \mathbb{Z} \cap p\mathbb{Z}[\zeta_2] = p\mathbb{Z} \Rightarrow \left(\frac{p}{2}\right) \equiv \left(\frac{2^*}{p}\right) \pmod p \Rightarrow \boxed{\left(\frac{p}{2}\right) = \left(\frac{2^*}{p}\right)})$

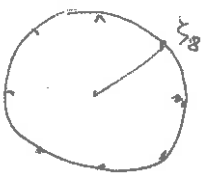
Pf: Later

(two methods: (1) $1, \zeta_2, \ldots, \zeta_2^{2-2}$ are linearly independent over $\mathbb{Q}$ (since $\frac{x^2-1}{x-1}$ is irreducible in $\mathbb{Q}[x]$)

(2) $\mathbb{Z}[\zeta_2] \subset \overline{\mathbb{Z}}$ {= the ring of algebraic integers} and $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.)

Remark: $S = \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7 = \sqrt{8} \in \mathbb{Z}[\zeta_8]$; let $\chi_8(q) = \begin{cases} 1 & q \equiv \pm 1 \ (8) \\ -1 & q \equiv \pm 3 \ (8) \end{cases}$

$= \sum_{a \in (\mathbb{Z}/8\mathbb{Z})^*} \chi_8(a)\zeta_8^a$



Again, $S^p \equiv \chi_8(p) S \pmod{p\mathbb{Z}[\zeta_8]}$

$\Rightarrow$ $\underbrace{S^2}_{8}\left(\underbrace{(S^2)^{\frac{p-1}{2}}}_{8^{\frac{p-1}{2}}} - \chi_8(p)1\right) \in \mathbb{Z} \cap p\mathbb{Z}[\zeta_8] = p\mathbb{Z} \Rightarrow \left(\frac{8}{p}\right) \equiv \chi_8(p) \pmod p$

$\Rightarrow$ $\boxed{\left(\frac{2}{p}\right) = \chi_8(p)}$

Special cases of Dirichlet's thm on primes

$\mathcal{P} = \{2, 3, 5, 7, \dots\} = \{\text{prime numbers}\}$; $\mathcal{P}_{a \pmod m} = \{p \in \mathcal{P} \mid p \equiv a \pmod m\}$

Euler: $\sum_{p \in \mathcal{P}} \frac{1}{p} = +\infty$

Dirichlet: If $m \geq 2$, $\gcd(a, m) = 1 \Rightarrow \sum_{p \in \mathcal{P}_{a \pmod m}} \frac{1}{p} = +\infty$ $\left(\Rightarrow |\mathcal{P}_{a \pmod m}| = \infty\right)$

Prop. $|\mathcal{P}_{\pm 1 \pmod 4}| = \infty$

$\mathcal{P} = \{2\} \sqcup \mathcal{P}_{1 \pmod 4} \sqcup \mathcal{P}_{-1 \pmod 4}$

Pf: $-1 \pmod 4$: given $p_1, \dots, p_r \in \mathcal{P}_{-1 \pmod 4}$ $(r \geq 0)$, let $N = 4p_1 \cdots p_r - 1 \geq 3$

$N \equiv -1 \pmod 4$, $N = \prod_{q_j \in \mathcal{P}, q_j \neq 2} q_j^{a_j}$. If all $q_j \equiv 1 \pmod 4 \Rightarrow N \equiv 1 \pmod 4$ – contradiction.

So $\exists\, p \mid N$, $p \equiv -1 \pmod 4$. If $p = p_i$ for some $i = 1, \dots, r$, then $\left.\begin{matrix} p \mid N+1 \\ p \mid N \end{matrix}\right\} \Rightarrow p \mid 1$ impossible

Therefore $p \in \mathcal{P}_{-1 \pmod 4} \setminus \{p_1, \dots, p_r\}$.

$1 \pmod 4$: given $p_1, \dots, p_r \in \mathcal{P}_{1 \pmod 4}$ $(r \geq 0)$, let $N = (2p_1 \cdots p_r)^2 + 1 \geq 5$, $2 \nmid N$.

$\exists$ prime $p \mid N \Rightarrow p \neq 2$. As $(2p_1 \cdots p_r)^2 \equiv -1 \pmod p \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod 4$.

Again, if $p = p_i$ for some $i = 1, \dots, r$, $\left.\begin{matrix} p \mid N-1 \\ p \mid N \end{matrix}\right\} \Rightarrow p \mid 1$ impossible $\Rightarrow p \in \mathcal{P}_{1 \pmod 4} \setminus \{p_1, \dots, p_r\}$

Exercise: Given $p_1, \dots, p_r \in \mathcal{P} \setminus \{2\}$, let $N_1 = (2p_1 \cdots p_r)^4 + 1$,

$N_3 = (p_1 \cdots p_r)^2 + 2$, $N_5 = (p_1 \cdots p_r)^2 + 4$, $N_7 = (3p_1 \cdots p_r)^2 - 2$.

Show that $\forall\, i \in \{1, 3, 5, 7\}$ $\exists\, p \mid N_i$, $p \in \mathcal{P}_{i \pmod 8} \setminus \{p_1, \dots, p_r\}$.

$\left(\Rightarrow |\mathcal{P}_{i \pmod 8}| = \infty\right)$.

Exercise: (1) If $p \neq 2$ prime, $a \in \mathbb{Z}$, $p \mid (a^{2^n} + 1) \Rightarrow p \equiv 1 \pmod{2^{n+1}}$.

(2) $\forall n \geq 1$ $\quad |\mathcal{P}_{1 \pmod{2^{n+1}}}| = \infty$

Rmk: these elementary methods only show that $|\mathcal{P}_{a \pmod m}| = \infty$ if $a^2 \equiv 1 \pmod m$.

Applications of $\left[-1 \in \mathbb{F}_p^{*2} \iff p \equiv 1 \pmod 4\right]$

Prop. If $a, b \in \mathbb{Z}$, $p \neq 2$ prime, $p \mid (a^2+b^2) \Rightarrow \begin{cases} p \nmid ab, & p \equiv 1 \pmod 4 \\ p \mid a, & p \mid b \end{cases}$

If: if $p \mid b \Rightarrow p \mid a^2 \Rightarrow p \mid a$. If $p \nmid b \Rightarrow \exists c \ \ bc \equiv 1 \pmod p \Rightarrow 0 \equiv (a^2+b^2)c^2 \equiv (ac)^2 + 1 \pmod p$

$\Downarrow$

$\left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod 4$

Prop. Let $m, n \in \mathbb{Z}$, $n \equiv 1 \pmod 4$, no prime $p \equiv -1 \pmod 4$ divides m. Then

$y^2 + 4m^2 = x^3 - n^3 = (x-n)(x^2+nx+n^2)$ has no solution $x, y \in \mathbb{Z}$. (*Ex*: $m = n = 1$, $y^2 + 5 = x^3$)

If. If $2 \nmid y \Rightarrow 2 \mid x \Rightarrow x^3 - n^3 \equiv -1 \pmod 4 \not\equiv 1 \equiv y^2 + 4m^2 \pmod 4$.

If $2 \mid y \Rightarrow 4 \mid (x^3 - n^3) \Rightarrow x \equiv 1 \pmod 4$, $x^2+nx+n^2 \equiv -1 \pmod 4 \Rightarrow \exists$ prime $p \mid (x^2+nx+n^2)$, $p \equiv -1 \pmod 4$

$\Rightarrow p \mid (y^2+4m^2) \overset{\text{Prop.}}{\Rightarrow} p \mid 4m^2$ impossible.

Exercise. If $2 \nmid mn$ and if no prime $p \equiv -1 \pmod 4$ divides m, then

$y^2 + m^2 = x^3 - (2n)^3 = (x-2n)(x^2+2nx+4n^2)$ has no solution $x, y \in \mathbb{Z}$.

Thm (Fermat, Euler) Let $p \neq 2$ be a prime. (1) $\exists x, y \in \mathbb{Z}$ $p = x^2 + y^2 \iff p \equiv 1 \pmod 4$.

(2) $(p \neq 3)$ $\exists x, y \in \mathbb{Z}$ $x^2 + 3y^2 = p \iff p \equiv 1 \pmod 3$.

Pf. (1) $x^2, y^2 \equiv 0, 1 \pmod 4 \Rightarrow x^2 + y^2 \equiv 0, 1, 2 \pmod 4$; if odd, $x^2 + y^2 \equiv 1 \pmod 4$.

If $p \equiv 1 \pmod 4 \Rightarrow \exists a \in \mathbb{Z}$ $a^2 + 1 \equiv 0 \pmod p \Rightarrow p \mid (a+i)(a-i)$ in $\mathbb{Z}[i]$.

But $p \nmid a \pm i$ and Euclid's Lemma holds in $\mathbb{Z}[i] \Rightarrow p \neq$ irreducible in $\mathbb{Z}[i] \Rightarrow$

$\Rightarrow p = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha, \beta \notin \mathbb{Z}[i]^*$. Then $N(p) = p^2 = \underbrace{N(\alpha)}_{>1} \underbrace{N(\beta)}_{>1} \Rightarrow N(\alpha) = N(\beta) = p$.

Writing $\alpha = x + iy$ $(x, y \in \mathbb{Z})$ we get $p = N(\alpha) = x^2 + y^2$ (and $\beta = N(\alpha)/\alpha = \overline{\alpha}$).

---

(2) $\Rightarrow$ is automatic. $\Leftarrow$ if $p \equiv 1 \pmod 3$, $1 = \left(\frac{p}{3}\right) = \left(\frac{-3}{p}\right) \Rightarrow \exists a \in \mathbb{Z}$ $a^2 + 3 \equiv 0 \pmod p$

$\Rightarrow p \mid (a + i\sqrt{3})(a - i\sqrt{3})$ in $\underbrace{\mathbb{Z}[\xi_3] = \mathbb{Z}\left[\frac{-1+i\sqrt{3}}{2}\right]}_{\text{UFD}} \Rightarrow p \neq$ irreducible in $\mathbb{Z}[\xi_3]$.

$p \nmid (a \pm i\sqrt{3})$

We obtain again $p = \alpha\overline{\alpha}$, $\alpha = u + v\xi_3$ $(u, v \in \mathbb{Z})$. After possibly replacing α by $\alpha\xi_3 = -v + (u-v)\xi_3$ or $\alpha\xi_3^2 = (v-u) - u\xi_3$ we can assume that $v = 2y \in 2\mathbb{Z}$; then $\alpha = x + iy\sqrt{3}$ $(x, y \in \mathbb{Z}) \Rightarrow p = x^2 + 3y^2$.

Exercise: Let $p \neq 2$ be a prime. Then: $\exists x, y \in \mathbb{Z}$ $x^2 + 2y^2 = p \iff p \equiv 1, 3 \pmod 8$.

Rmk: if $p \equiv 1 \pmod 4$, $p = x^2 + y^2 \Rightarrow x \not\equiv y \pmod 2$. If, say, $2 \nmid x$, then $y = 2z$ and $p = x^2 + 4z^2$ $(\Rightarrow p \equiv 1 + 4z^2 \equiv 1 + 4z \pmod 8)$.

It follows that: $p \equiv 1 \pmod 8 \iff 2 \mid z \iff \exists x, t \in \mathbb{Z}$ $p = x^2 + 16t^2$.

Question: does this continue? What about $p = x^2 + 64u^2$?

Exercise (irreducible elements of $\mathbb{Z}[i]$) Let $\alpha \in \mathbb{Z}[i]$.

(1) If $N(\alpha) = p$ is a prime $\Rightarrow \alpha$ is irreducible in $\mathbb{Z}[i]$.

(2) If α is irreducible in $\mathbb{Z}[i] \Rightarrow \exists$ prime p such that $\alpha \mid p$ in $\mathbb{Z}[i]$.

(3) If $p \equiv 3 \pmod 4$ is a prime $\Rightarrow$ p is irreducible in $\mathbb{Z}[i]$.

(4)

$$\{\alpha \text{ irreducible} \mid \alpha \mid p\} = \left\{ \begin{array}{ll} i^k(1+i) & (N(\alpha)=2) \text{ if } p=2 \\ i^k p & (N(\alpha)=p^2) \text{ if } p \equiv 3 \pmod 4 \\ i^k(x \pm iy) & (N(\alpha)=p) \text{ if } p = x^2+y^2 \equiv 1 \pmod 4 \end{array} \right\}$$

Exercise (irreducible elements of $\mathbb{Z}[\zeta_3]$) Let $\beta \in \mathbb{Z}[\zeta_3]$.

(1) $N(\beta) = p$ prime $\Rightarrow \beta$ irreducible

(2) β irreducible $\Rightarrow \exists$ prime p, $\beta \mid p$.

(3) $p \equiv 2 \pmod 3$ prime $\Rightarrow$ p irreducible in $\mathbb{Z}[\zeta_3]$.

(4)

$$\{\beta \text{ irreducible} \mid \beta \mid p\} = \left\{ \begin{array}{lll} \zeta_6^k(1-\zeta_3) & (N(\beta)=3) & \text{if } p=3 \\ \zeta_6^k p & (N(\beta)=p^2) & \text{if } p \equiv 2 \pmod 3 \\ \zeta_6^k(x \pm iy\sqrt{3}) & (N(\beta)=p) & \text{if } p = x^2+3y^2 \equiv 1 \pmod 3 \end{array} \right\}$$

Corollary:

$$\{x^2+y^2 \mid x,y \in \mathbb{Z}\} = \{N(\alpha) \mid \alpha \in \mathbb{Z}[i]\} = \{0\} \cup \left\{ \prod_{p \text{ prime}} p^{a_p} \;\middle|\; a_p \equiv 0 \pmod 2 \text{ if } p \equiv 3 \pmod 4 \right\}$$

$$\{x^2-xy+y^2 \mid x,y \in \mathbb{Z}\} = \{N(\beta) \mid \beta \in \mathbb{Z}[\zeta_3]\} = \{0\} \cup \left\{ \prod_{p \text{ prime}} p^{b_p} \;\middle|\; b_p \equiv 0 \pmod 2 \text{ if } p \equiv 2 \pmod 3 \right\}$$

$$\| \qquad \{u^2+3v^2 \mid u,v \in \mathbb{Z}\}$$

Congruences $x^r \equiv a \pmod p$ (p prime, $p \nmid a$, $r>1$)

Ex: $\mathbb{F}_5^{*3} = \{(\pm 1)^3, (\pm 2)^3 \pmod 5\} = \mathbb{F}_5^*$ $\quad 3 \nmid (5-1)$

$\mathbb{F}_7^{*3} = \{(\pm 1)^3, (\pm 2)^3, (\pm 3)^3 \pmod 7\} = \{\pm 1 \pmod 7\}$ $\quad 3 \mid (7-1)$

Prop. Let p = prime, $r>1$, $d = \gcd(p-1, r)$; $r = dm$, $\gcd(p-1, m) = 1$

$\exists m'$ $\quad mm' \equiv 1 \pmod{(p-1)}$

(1) $\mathbb{F}_p^* \rightleftarrows \mathbb{F}_p^*$ are mutually inverse group isomorphisms

$x \longmapsto y = x^m$

$x = y^{m'} \longleftarrow y$

(2) For $a \in \mathbb{F}_p^*$, $\quad x^r = a$ has a solution in $\mathbb{F}_p^*$ $\quad [\text{so } \mathbb{F}_p^{*r} = \mathbb{F}_p^{*d}]$

$\Updownarrow$

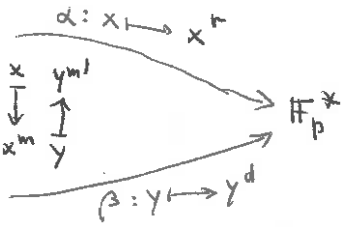
$y^d = a$ ——— $\Updownarrow$ ——— $\iff a^{\frac{p-1}{d}} = 1$

If this is the case, the number of solutions of $x^r = a$ in $\mathbb{F}_p^*$ is equal to d.

Pf: (1) $(x^m)^{m'} = x$, $(y^{m'})^m = y$ for all $x, y \in \mathbb{F}_p^*$, since $mm' = 1 + (p-1)n$, $x^{p-1} = y^{p-1} = 1$.

(2) If $x_0^r = a$, then there are bijections

$$\begin{array}{ccccc} \{x \in \mathbb{F}_p^* \mid x^r = a\} & \xleftarrow[\text{bij.}]{\text{mult. by } x_0} & \mu_r(\mathbb{F}_p) = \ker(\alpha) & \subset & \mathbb{F}_p^* \\ \text{bij.} \uparrow\downarrow & & \text{bij.} \uparrow\downarrow & & \text{bij.} \uparrow\downarrow \\ \{y \in \mathbb{F}_p^* \mid y^d = a\} & \xleftarrow[\text{bij}]{\text{mult. by } y_0} & \mu_d(\mathbb{F}_p) = \ker(\beta) & \subset & \mathbb{F}_p^* \end{array}$$



($y_0 = x_0^m$)

- if $a = y^d \Rightarrow a^{\frac{p-1}{d}} = y^{p-1} = 1$.
- if $a^{\frac{p-1}{d}} = 1$, write $a = g^u$ (g a generator of the cyclic group $\mathbb{F}_p^*$) $\Rightarrow$ $g^{(p-1)u/d} = 1 \iff (p-1) \mid \frac{(p-1)u}{d} \iff d \mid u \Rightarrow a = (g^{u/d})^d \in \mathbb{F}_p^{*d}$.

Ex: $p \neq 2$ prime; (1) if $p \equiv 3 \pmod 4$ & $r = 4 \Rightarrow d = 2$, $\mathbb{F}_p^{*4} = \mathbb{F}_p^{*2}$

(2) if $p \equiv 1 \pmod 4$, $r = 4 \Rightarrow d = 4$; $a \in \mathbb{F}_p^{*4} \iff a^{\frac{p-1}{4}} \equiv 1 \pmod p$.

Therefore $-1 \in \mathbb{F}_p^{*4} \iff (-1)^{\frac{p-1}{4}} \equiv 1 \pmod p \iff (-1)^{\frac{p-1}{4}} = 1 \iff p \equiv 1 \pmod 8$

When is $2^{\frac{p-1}{4}} \equiv 1 \pmod p$? Dirichlet: if $p = a^2+b^2$, $\pi = a+bi$ ($2 \nmid a$, $2 \mid b$, say) $\Rightarrow$ $\boxed{2^{\frac{p-1}{4}} \equiv i^{ab/2} \pmod{\pi\mathbb{Z}[i]}}$

So $2 \in \mathbb{F}_p^{*4} \iff i^{ab/2} = 1 \iff 8 \mid b \iff p = a^2 + 64(b/8)^2$ (conjectured by Euler)

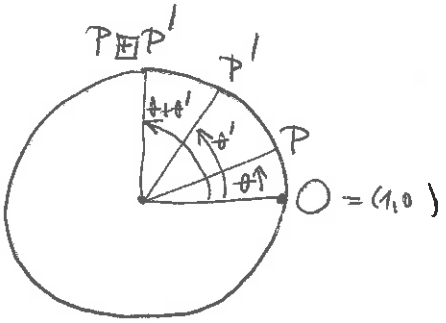
Proof of Dirichlet's congruence:

- $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = \left(\frac{b^2}{a}\right) = \left(\frac{b}{a}\right)^2 = 1$
- $(a+b)^2 = p + 2ab \equiv 2ab \pmod p \Rightarrow \left(\frac{a+b}{p}\right) \equiv (a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} \pmod p$
- $\pi i = ai - b \Rightarrow b \equiv ai \pmod{\pi\mathbb{Z}[i]}$, $ab \equiv a^2 i \pmod{\pi\mathbb{Z}[i]}$,

$$(ab)^{\frac{p-1}{4}} \equiv a^{\frac{p-1}{2}} i^{\frac{p-1}{4}} \equiv \left(\frac{a}{p}\right) i^{\frac{p-1}{4}} \equiv i^{\frac{p-1}{4}} \pmod{\pi\mathbb{Z}[i]}$$

- $\left(\frac{2p}{a+b}\right) = \left(\frac{(a+b)^2 + (a-b)^2}{a+b}\right) = \left(\frac{(a-b)^2}{a+b}\right) = \left(\frac{a-b}{a+b}\right)^2 = 1$
- $\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right) = \left(\frac{2p}{a+b}\right)\left(\frac{2}{a+b}\right) = \left(\frac{2}{a+b}\right) = (-1)^{\frac{(a+b)^2-1}{8}} = (-1)^{\frac{p-1+2ab}{8}} = i^{\frac{p-1}{4}} i^{ab/2}$
- $2^{\frac{p-1}{4}} \equiv \frac{(2ab)^{\frac{p-1}{4}}}{(ab)^{\frac{p-1}{4}}} \equiv \frac{i^{\frac{p-1}{4}} i^{ab/2}}{i^{\frac{p-1}{4}}} \equiv i^{ab/2} \pmod{\pi\mathbb{Z}[i]}$.

The abelian group law on the unit circle



$C : x^2+y^2 = 1$

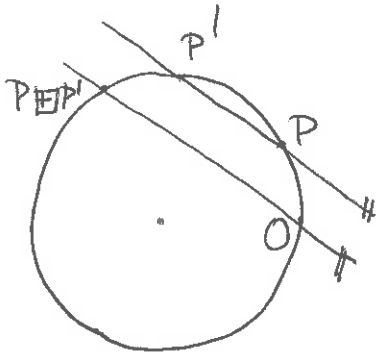
$C(\mathbb{R}) \xrightarrow{\sim} U(1) = \{z \in \mathbb{C} \mid z\bar{z} = 1\}$ abelian group under multiplication

$P = (x,y) \longmapsto x+iy = z$

$P' = (x',y') \longmapsto x'+iy' = z'$

$P \boxplus P' \longmapsto zz' = (xx'-yy') + i(xy'+yx')$

$(xx'-yy', xy'+yx')$



inverse:

$-P = (x,-y) \longleftrightarrow z^{-1} = \frac{1}{x+iy} = x-iy$

the group law $\boxplus$ and the inverse are given by polynomials $xx'-yy', xy'+yx', x, -y \in \mathbb{Z}[x,y,x',y']$ with coefficients in $\mathbb{Z}$ $\Rightarrow$ these formulas make $C(A) = \{(x,y) \mid x,y \in A,\ x^2+y^2=1\}$ into an abelian group, for every ring A.

We know, by Hilbert's Theorem 90, that

$$\begin{array}{ccc} \mathbb{C}^* & \longrightarrow & U(1) \simeq C(\mathbb{R}) \\ \cup & z \longmapsto z/\bar{z} & \cup \\ \mathbb{Q}(i)^* & \longrightarrow & C(\mathbb{Q}) \end{array}$$

are surjective group morphisms, with respective kernels $\mathbb{R}^*$ and $\mathbb{R}^* \cap \mathbb{Q}(i)^* = \mathbb{Q}^*$

$\Rightarrow$ group isomorphisms

$$\begin{array}{ccc} \mathbb{C}^*/\mathbb{R}^* & \xrightarrow{\sim} & C(\mathbb{R}) \\ \cup & & \cup \\ \mathbb{Q}(i)^*/\mathbb{Q}^* & \xrightarrow{\sim} & C(\mathbb{Q}) \end{array}$$

Exercise: use the description of irreducible elements of $\mathbb{Z}[i]$ (and the fact that $\mathbb{Z}[i]$ is a UFD) to show that

$$\mathbb{Q}(i)^*/\mathbb{Q}^* \simeq \left(\text{cyclic group of order 4}\right) \circledast \bigoplus_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \mathbb{Z}$$

The number of solutions of $f(x_0,\dots,x_n)\equiv a \pmod p$

Notation: K field, $g\in K[x_1,\dots,x_m]$ polynomial in $\underbrace{m}$ variables $x_1,\dots,x_m$ coordinates in the affine space $\mathbb{A}^m$

$Z_g=\{g=0\}\subset\mathbb{A}^m$ the zero locus of g

For any ring $B\supset K$, $Z_g(B)=\{(b_1,\dots,b_m)\mid b_i\in B,\ g(b_1,\dots,b_m)=0\}$

Our case: $K=\mathbb{F}_p$, $p\neq 2$ prime, $f=f(x_0,\dots,x_n)$ non-degenerate quadratic form over $\mathbb{F}_p$ of $\dim(f)=n+1\geq 1$, $a\in\mathbb{F}_p$, $g=f-a$.

We know: $f\sim a_0x_0^2+\cdots+a_nx_n^2$, $a_i\in\mathbb{F}_p^*$, $d(f)=a_0\cdots a_n\in\mathbb{F}_p^*/\mathbb{F}_p^{*2}$.

Thm:
$$\left|Z_f(\mathbb{F}_p)\right|-p^n=\begin{cases}0 & 2\mid n\\ (p-1)p^{\frac{n-1}{2}}\left(\dfrac{(-1)^{\frac{n+1}{2}}d(f)}{p}\right) & 2\nmid n\end{cases}$$

Pf: $n=0$: $a_0x_0^2=0$: 1 solution $x_0=0$ $\quad\underline{|Z_f(\mathbb{F}_p)|=1}$.

$n=1$: $a_0x_0^2+a_1x_1^2=0\iff(a_0x_0)^2=-d(f)x_1^2$; if $x_1=0\Rightarrow x_0=0$ 1 solution

if $\underbrace{x_1\in\mathbb{F}_p^*}_{p-1\text{ solutions}}\Rightarrow(a_0x_0/x_1)^2=-d(f)$, which has $1+\left(\frac{-d(f)}{p}\right)$ solutions for $\frac{a_0x_0}{x_1}$

$\Rightarrow|Z_f(\mathbb{F}_p)|-p=1+(p-1)\left(1+\left(\frac{-d(f)}{p}\right)\right)-p=(p-1)\left(\frac{-d(f)}{p}\right)$.

$n\geq 2$: $\dim(f)=n+1\geq 3\Rightarrow f\sim x_0x_1\perp f_1$, f_1 non-degenerate, $d(f)=-d(f_1)$, $\dim(f_1)=n-1$, $f_1=f_1(\underbrace{x_2,\dots,x_n}_{y})$

$f(x)=0\iff|Z_f(\mathbb{F}_p)|$ sol.

- $x_0x_1=0=f_1(y)$: $(2p-1)$ sol. $\quad|Z_{f_1}(\mathbb{F}_p)|$ sol.
- $x_1\neq 0\neq f_1(y)$: $(p-1)$ sol. $\quad(p^{n-1}-|Z_{f_1}(\mathbb{F}_p)|)$ sol. $\quad x_0=-\frac{f_1(y)}{x_1}$

$$\boxed{|Z_f(\mathbb{F}_p)|-p^n=p\left(|Z_{f_1}(\mathbb{F}_p)|-p^{n-2}\right)}$$

Induction $n-2\mapsto n$ gives the result.

Fibration:

$\left(-\frac{f_1(y)}{x_1},x_1,y\right)\in Z_f$	$\cong$	$Z_{x_0x_1}\times Z_{f_1}$	$\sqcup$	$(\mathbb{A}^1\setminus\{0\})\times(\mathbb{A}^{n-1}\setminus Z_{f_1})$	$\to$	(x_1,y)
$\downarrow f_1$		$\downarrow$		$\downarrow$		$\downarrow$
$\mathbb{A}^1$	$=$	$\{0\}$	$\sqcup$	$(\mathbb{A}^1\setminus\{0\})$	$\to$	$f_1(y)$

Thm. If $a\in\mathbb{F}_p^*$,
$$\left|Z_{f-a}(\mathbb{F}_p)\right|-p^n=\begin{cases}p^{n/2}\left(\dfrac{(-1)^{n/2}d(f)a}{p}\right) & 2\mid n\\ -p^{(n-1)/2}\left(\dfrac{(-1)^{\frac{n+1}{2}}d(f)}{p}\right) & 2\nmid n\end{cases}$$

Pf: Consider $g=f\perp\langle -a\rangle=f(x_0,\dots,x_n)-at^2$. If $\underbrace{t\neq 0}_{p-1\text{ values}}$, $g(x,t)=0\iff f\left(\frac{x}{t}\right)=a$ $\iff\frac{x}{t}\in Z_{f-a}$

If $t=0$, then $g(x,t)=0\iff f(x)=0$.

So $(p-1)\left|Z_{f-a}(\mathbb{F}_p)\right|+|Z_f(\mathbb{F}_p)|=\left|Z_{f\perp\langle -a\rangle}(\mathbb{F}_p)\right|$.

Rmk: the image of $Z_f(\mathbb{F}_p)\setminus\{(0,\dots,0)\}$ in the projective space $\mathbb{P}^n(\mathbb{F}_p)=(\mathbb{F}_p^{n+1}\setminus\{(0,\dots,0)\})/\mathbb{F}_p^*$ is a non-singular projective quadric $PZ_f\subset\mathbb{P}^n$ of $\dim=n-1$, with $|PZ_f(\mathbb{F}_p)|=\dfrac{|Z_f(\mathbb{F}_p)|-1}{p-1}$ points over $\mathbb{F}_p$.

Application (quadratic reciprocity law)

$p, q \neq 2$ primes, $p \neq q$.

$f = x_0^2 + \cdots + x_q^2$ quadratic form over $\mathbb{F}_p$

the cyclic group C_q of order q acts on

$Z_f(\mathbb{F}_p) = \{(x_0, \dots, x_q) \mid x_i \in \mathbb{F}_p,\ x_0^2 + \cdots + x_q^2 = 0\}$ as follows:

a fixed generator $s \in C_q$ sends $(x_0, x_1, \dots, x_q)$ to $(x_0, x_2, \dots, x_q, x_1)$.

the set of fixed points is $\{(x_0, \underbrace{y, \dots, y}_{q \text{ times}}) \mid x_0, y \in \mathbb{F}_p,\ x_0^2 + q y^2 = 0\}$.

Fact: If C_q acts on a finite set A, then $|\underbrace{A^{C_q}}_{\text{fixed points}}| \equiv |A| \pmod q$

$[\ A \setminus A^{C_q} = \bigsqcup \underbrace{\text{orbits of } C_q \text{ different from single points}}_{\text{each such orbit has } q \text{ elements}}\ ]$

So: $\underbrace{|Z_f(\mathbb{F}_p)|}_{p^q + p^{\frac{q-1}{2}}(p-1)\left(\frac{(-1)^{\frac{q+1}{2}}}{p}\right)} \equiv |Z_f(\mathbb{F}_p)^{C_q}| = \underbrace{|Z_{x^2+qy^2}(\mathbb{F}_p)|}_{p + (p-1)\left(\frac{-q}{p}\right)} \pmod q$

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

$\Rightarrow \underline{(p-1)\left(\left(\frac{p}{q}\right) - \left(\frac{q^*}{p}\right)\right) \equiv 0 \pmod q}$, $q^* = (-1)^{\frac{q-1}{2}}$

If $p \equiv 1 \pmod q$ ($\Rightarrow p > q$), exchange $p \leftrightarrow q$, so we can assume that $p \not\equiv 1 \pmod q \Rightarrow \left(\frac{p}{q}\right) \equiv \left(\frac{q^*}{p}\right) \pmod q$

$\Rightarrow \left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$.

Congruences of small degree

Prop. If p = prime, $a, b \in \mathbb{F}_p^*$, $c \in \mathbb{F}_p \Rightarrow$ $ax^2 + by^2 = c$ has a solution $x, y \in \mathbb{F}_p$.

Pf: OK if $p=2$. If $p \neq 2$: $A = \{ax^2 \mid x \in \mathbb{F}_p\} = \{0\} \cup a\mathbb{F}_p^{*2} \Rightarrow |A| = 1 + |\mathbb{F}_p^{*2}| = 1 + \frac{p-1}{2} = \frac{p+1}{2}$.

Also, $B = \{c - by^2 \mid y \in \mathbb{F}_p\}$ has $|B| = \frac{p+1}{2} \Rightarrow |A \cap B| = |A| + |B| - \underbrace{|A \cup B|}_{\leq |\mathbb{F}_p| = p} \geq \frac{p+1}{2} + \frac{p+1}{2} - p = 1$.

Thm (Chevalley – Warning) Let $f_1, \dots, f_r \in \mathbb{F}_p[x_1, \dots, x_n]$, $d_i = \deg(f_i)$.

Let $Z_{f_1, \dots, f_r} = \{f_1 = \dots = f_r = 0\} \subset \mathbb{A}^n$ be the locus of common zeroes of $f_1, \dots, f_r$.

If $\boxed{\sum_{i=1}^r d_i < n}$, then $\left| Z_{f_1, \dots, f_r}(\mathbb{F}_p) \right| \equiv 0 \pmod p$.

Cor: If each f_i is homogeneous, then $(0, \dots, 0) \in Z_{f_1, \dots, f_r} \Rightarrow \exists\, P \in Z_{f_1, \dots, f_r}(\mathbb{F}_p)$, $P \neq (0, \dots, 0)$

Pf: **Lemma:** For $a \geq 0$, the sum $\sum_{x \in \mathbb{F}_p} x^a \in \mathbb{F}_p$ is equal to $\begin{cases} -1, & (p-1) \mid a,\ a > 0 \\ 0, & \text{otherwise.} \end{cases}$ (Exercise)

Consider $F(x_1, \dots, x_n) = \prod_{i=1}^r \left(1 - f_i(x_1, \dots, x_n)^{p-1}\right) = \sum_{a_1, \dots, a_n} c(a_1, \dots, a_n)\, x_1^{a_1} \cdots x_n^{a_n} \in \mathbb{F}_p[x_1, \dots, x_n]$.

For $b = (b_1, \dots, b_n) \in \mathbb{F}_p^n$, $f_i(b)^{p-1} = \begin{cases} 1 \\ 0 \end{cases}$ $\begin{matrix} f_i(b) \neq 0 \\ f_i(b) = 0 \end{matrix}$ $\Rightarrow F(b) = \begin{cases} 1 & b \in Z_{f_1, \dots, f_r}(\mathbb{F}_p) \\ 0 & b \notin Z_{f_1, \dots, f_r}(\mathbb{F}_p) \end{cases}$

So $\left| Z_{f_1, \dots, f_r}(\mathbb{F}_p) \right| \pmod p = \sum_{x \in \mathbb{F}_p^n} F(x) = \sum_{a_1, \dots, a_n} c(a_1, \dots, a_n) \prod_{i=1}^n \left(\sum_{x_i \in \mathbb{F}_p} x_i^{a_i} \right) = 0 \quad \in \mathbb{F}_p$.

(If $c(a_1, \dots, a_n) \neq 0 \Rightarrow a_1 + \dots + a_n \leq (p-1) \sum \deg(f_i) < (p-1)n \Rightarrow \exists i \;\; a_i < p-1 \Rightarrow \sum_{x_i \in \mathbb{F}_p} x_i^{a_i} = 0$)

Thm. If p = prime and $a_1, \dots, a_{2p-1} \in \mathbb{Z}$, then $\exists\, 1 \leq i_1 < \dots < i_p \leq 2p-1$ such that $p \mid (a_{i_1} + \dots + a_{i_p})$.

Pf. Consider $F(x_1, \dots, x_{2p-1}) = \sum_{1 \leq i_1 < \dots < i_p \leq 2p-1} (x_{i_1} + \dots + x_{i_p})^{p-1} \in \mathbb{Z}[x_1, \dots, x_{2p-1}]$.

If $p \nmid (a_{i_1} + \dots + a_{i_p})$ for all $i_1 < \dots < i_p$, then

$$F(a_1, \dots, a_{2p-1}) \equiv \sum_{1 \leq i_1 < \dots < i_p \leq 2p-1} 1 = \binom{2p-1}{p} \not\equiv 0 \pmod p.$$

However, all coefficients of F are divisible by p: F is a symmetric polynomial and the coefficient at $x_1^{k_1} \cdots x_k^{k_k}$ ($k_1 \geq \dots \geq k_k \geq 1$, $\sum_{i=1}^k k_i = p-1$) is divisible by the number of terms with $i_1 = 1, \dots, i_k = k$, which is equal to $\binom{2p-1-k}{p-k} = \binom{2p-1-k}{p-1}$. (this number is divisible by p since $k \leq p-1$ and $2p-1-k \geq p$.

Therefore $F \in p\mathbb{Z}[x_1, \dots, x_{2p-1}]$ and $F(a_1, \dots, a_{2p-1}) \equiv 0 \pmod p$.

Counting solutions of $a_0 x_0^{r_0} + \cdots + a_n x_n^{r_n} \equiv 0 \pmod p$

Lemma $N \geq 1$, $a \in \mathbb{Z} \Rightarrow \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \zeta_N^{ay} = \begin{cases} N & N \mid a \\ 0 & N \nmid a \end{cases}$ $\quad (\zeta_N = e^{2\pi i/N})$

Given: p prime, function $f: \mathbb{F}_p^{n+1} \longrightarrow \mathbb{F}_p$; let $Z_f = \{x = (x_0, \dots, x_n) \in \mathbb{F}_p^{n+1} \mid f(x) = 0\}$

$$|Z_f| = \sum_{x \in \mathbb{F}_p^{n+1}} \begin{cases} 1 & f(x)=0 \\ 0 & f(x)\neq 0 \end{cases} = \frac{1}{p} \sum_{\substack{x \in \mathbb{F}_p^{n+1} \\ y \in \mathbb{F}_p}} \zeta_p^{y f(x)} = \frac{1}{p}\left(\sum_{y=0} + \sum_{y \neq 0} \cdots\right) = p^n + \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p^{n+1}} \zeta_p^{y f(x)}$$

$f(x) = a_0 x_0^{r_0} + \cdots + a_n x_n^{r_n}$, $a_i \in \mathbb{F}_p^*$, $r_i \geq 1$

$$\boxed{|Z_f| = p^n + \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \prod_{i=0}^{n} \sum_{x_i \in \mathbb{F}_p} \left(\zeta_p^{y a_i}\right)^{x_i^{r_i}}}$$

$r_i = d_i m_i$, $d_i = (p-1, r_i)$, $(m_i, p-1) = 1$, $d_i \mid (p-1)$

$\mathbb{F}_p \longrightarrow \mathbb{F}_p$, $x_i \longmapsto x_i^{m_i} = y_i$ bijection, $x_i^{r_i} = y_i^{d_i}$

So $\sum_{x_i \in \mathbb{F}_p} \left(\zeta_p^{y a_i}\right)^{x_i^{r_i}} = \sum_{y_i \in \mathbb{F}_p} \left(\zeta_p^{y a_i}\right)^{y_i^{d_i}}$.

Fix a generator g of $\mathbb{F}_p^*$

For $i = 0, \dots, n$, let $\chi_i : \mathbb{F}_p^* \longrightarrow \mu_{d_i}(\mathbb{C})$, $\chi_i(g^b) = \zeta_{d_i}^b$ $(\Rightarrow \chi_i(aa') = \chi_i(a)\chi_i(a'))$.

Facts: (1)
$$\begin{cases} a = g^b \in \mathbb{F}_p^{*d_i} \Longleftrightarrow d_i \mid b \Longleftrightarrow \chi_i(a) = 1 \overset{\text{Lemma}}{\Longleftrightarrow} \sum_{j=0}^{d_i - 1} \chi_i(a)^j = d_i \\ a = g^b \notin \mathbb{F}_p^{*d_i} \Longleftrightarrow \chi_i(a) \neq 1 \overset{\text{Lemma}}{\Longleftrightarrow} \sum_{j=0}^{d_i-1} \chi_i(a)^j = 0. \end{cases}$$

(2) If $a \in \mathbb{F}_p^{*d_i}$, then there are d_i elements $y_i \in \mathbb{F}_p^*$ such that $y_i^{d_i} = a$.

Therefore: $\forall u \in \mathbb{F}_p^*$ $\sum_{y_i \in \mathbb{F}_p} \zeta_p^{u y_i^{d_i}} = 1 + \sum_{a \in \mathbb{F}_p^*} (1 + \chi_i(a) + \cdots + \chi_i(a)^{j-1}) \zeta_p^{ua} = 1 + \sum_{j=0}^{d_i - 1} G_u(\chi_i^j)$,

$G_u(\chi_i^j) = \sum_{a \in \mathbb{F}_p^*} \chi_i(a)^j \zeta_p^{ua}$ (Gauss sum – analogue of $\int_0^\infty e^{-t} t^{s-1} dt = \Gamma(s)$)

(3) $j = 0 \Rightarrow$ $G_u(\chi_i^0) = \sum_{b \in \mathbb{F}_p^*} \zeta_p^b = -1$.

(4) $j \neq 0 \Rightarrow$ $|G_u(\chi_i^j)|^2 = \sum_{a, b \in \mathbb{F}_p^*} \chi_i(a)^j \chi_i(b)^{-j} \zeta_p^{u(a-b)} \overset{a = bc}{=} \sum_{c \in \mathbb{F}_p^*} \chi_i(c)^j \left(\sum_{b \in \mathbb{F}_p^*} \left(\zeta_p^{u(c-1)}\right)^b\right) =$

$\overset{\text{Lemma}}{=} \sum_{c \in \mathbb{F}_p^*} \chi_i(c)^j \begin{cases} p-1 & c = 1 \\ -1 & c \neq 1 \end{cases} = p \underbrace{\chi_i(1)^j}_{1} - \sum_{c \in \mathbb{F}_p^*} \chi_i(c)^j \overset{\text{Lemma}}{=} p$.

Cor: $\left| \sum_{x_i \in \mathbb{F}_p} \left(\zeta_p^{y a_i}\right)^{x_i^{r_i}} \right| \leq (d_i - 1) p^{1/2}$, hence

$$\boxed{\left| |Z_f| - p^n \right| \leq p^{\frac{n-1}{2}} (p-1) \prod_{i=0}^{n} (d_i - 1)}$$

Special case $r_0 = \cdots = r_n = 2$: $\sum_{x_i \in \mathbb{F}_p} \left(\zeta_p^{y a_i}\right)^{x_i^2} = \left(\frac{y a_i}{p}\right) S$, $S = \sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) \zeta_p^a$, $S^2 = p^* = (-1)^{\frac{p-1}{2}} p$

$d = a_0 \cdots a_n$

$$|Z_f| - p^n = \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \left(\prod_{i=0}^{n} \left(\frac{y a_i}{p}\right) S \right) = \frac{1}{p} S^{n+1} \left(\frac{d}{p}\right) \underbrace{\sum_{y \in \mathbb{F}_p^*} \left(\frac{y}{p}\right)^{n+1}}_{\begin{cases} p-1 & 2 \mid n \\ 0 & 2 \nmid n \end{cases}} = \begin{cases} 0, & 2 \nmid n \\ (p-1) p^{\frac{n-1}{2}} \left(\frac{(-1)^{\frac{n+1}{2}} d}{p}\right), & 2 \mid n \end{cases}$$