Goal: \( \frac{2}{3} \) of Gauss's Theorem

best time: estimated # of solutions to cubic eqs over finite fields

This time case: proved by Gauss.

Fermat case: \( x^3 + y^3 = 1 \)

homogeneous: \( x^3 + y^3 + z^3 = 0 \)

no \((0,0,0)\)

no \((a^2, a, a^2)\).

Gauss's Thm: Let \( M_p \) be the number of projective solutions to the equation \( x^3 + y^3 + z^3 = 0 \) with \( x, y, z \in \mathbb{F}_p \).

Then

a) if \( p \neq 1 \pmod{3} \) then \( M_p = p + 1 \).

b) if \( p \equiv 1 \pmod{3} \) then there are integers \( A \) and \( B \) s.t. \( 4p = A^2 + 27B^2 \)

\( A, B \) unique up to signs. We can choose the sign of \( A \) so that \( A \equiv 1 \pmod{3} \)

\( M_p = p + 1 + A \).

Note: if \( p \equiv 1 \pmod{3} \) then \( A^2 \equiv 1 \pmod{3} \) so \( A \equiv 1 \pmod{3} \) so by replacing \( A \) with \(-A\) we can make \( A \equiv 1 \pmod{3} \).

\[ \mathbb{F}_p = \{0, 1, \ldots, p-1\} \]
\[ \mathbb{F}_p^* = \{1, 2, \ldots, p-1\} \]

Fact: \( \mathbb{F}_p^* \) is a cyclic group of order \( p-1 \).

Ex. \( \mathbb{F}_5^* \) \( \equiv \{2, 3\} \), \( 2^2 = 4, 2^3 = 3 \cdot 2^2 = 1 \)

Proof on p. 111.
Proof of Gauss's Theorem (A).

Assume that $p \not\equiv 1 \pmod{3}$.

So 3 does not divide the order $p - 1$ of $\mathbb{F}_p^*$. It follows that the map $x \mapsto x^3$ is an isomorphism from $\mathbb{F}_p^*$ to itself.

Ex. $p = 5$. $\mathbb{F}_5^*$,

| $0^3 = 0$ | $1^3 = 1$ | $2^3 = 3$ | $3^3 = 2$ | $4^3 = 4$ |

When $p \not\equiv 1 \pmod{3}$ every element of $\mathbb{F}_p$ has a unique cube root. Thus, the number of solutions to $x^3 + y^3 + z^3 = 0$ is equal to the number of solutions to $x + y + z = 0$, a line in the projective plane, so it has $p + 1$ solutions in $\mathbb{F}_p$.

$M_p = p + 1$.

Proof of (b).

Assume $p \equiv 1 \pmod{3}$, $p = 3m + 1$.

Since 3 does not divide the order of $\mathbb{F}_p^*$ the map $x \mapsto x^3$ is a homomorphism but not one-to-one onto.

The image of $x \mapsto x^3$ is $R$. $R$ has index 3 in $\mathbb{F}_p^*$.

$R = \{x^2 \ : \ x \in \mathbb{F}_p^* \}$.

The kernel of $x \mapsto x^3$ has three elements: 1, $u$, $u^2$ with $u^3 = 1$.

Ex. $p = 12$, the $R = \{\pm 1, \pm 5\}$ and the kernel of $x \mapsto x^3$ is $\{1, 3, 9\}$.

Elements of $R$ are called cubic residues.
Let $S$ and $T$ be the other 2 cosets of $R$ in $\mathbb{Z}_p^\times$.

Ex. If we take any $s \in \mathbb{Z}_p^\times$ then $S = sR$ and $T = s^2R$.

If $p = 13$, then we can choose $S = \{2\}$
$T = \{54, 7\}$

In general, $\mathbb{Z}_p^\times$ is a disjoint union
$\mathbb{Z}_p^\times = \{0\} \cup R \cup S \cup T$.

The number of elements in each of $R,S,T$ is $\frac{p}{2}$.

Note: $e = -12$ (if $2 \in R$ then $-e \in R$)
$S = \{-S\}$
$T = \{-T\}$

New symbol $[\cdot, \cdot]$.

Suppose $X, Y, Z$ are subsets of $\mathbb{Z}_p^\times$.
Let $[X,Y,Z]$ denote the number of triple $(x,y,z)$ s.t. $x \in X, y \in Y, z \in Z$ and $x+y+z = 0$.

What is $M_p$ in terms of the symbol?

First consider solutions to $x^3 + y^2 + z^2 = 0$ where none are zero. Then the one $[R,R,R]$ solution ($R = \text{cubes}$).

But for each cube there are 3 field elements that give that cube. So there are $27[R,R,R]$ solutions s.t. $x,y,z$ not zero. However, we don't want only projective solution. We need to get rid of $(ax, ay, az)$ which are $p-1$ multiplies.

$p = 3m + 1 \implies p - 1 = 3m$
27[p+2] = 9[p+2] \quad \text{projection solutions to } x^3+y^3+z^3=0 \quad \text{with } x, y, z \neq 0.

Case 1: if one of x, y, z = 0, say z = 0, then the other can't also be zero, hence we don't allow [0, 0, 0].

Pick anything nonzero for x, then there are 3 possible values for y:

\[ y^3 = -x^2 \quad \text{or} \quad y = -x, \pm x \]

Thus there are \( 3(p-1) \) triple: \((x, y, z)\) s.t. \( x^3+y^3+z^3=0 \).

Symmetric for \((0, 2)\), \((0, 1, 2)\)

So \( 9(p-1) \) triple: \((x, y, z)\) s.t. \( x^3+y^3+z^3=0 \).

So there are \( p-1 \) multipliers: \( \frac{9(p-1)}{3} = 9 \), projective solutions,

\[ M_p = 9\left[p+2\right] + 9 \quad = 9\left[p+2\right] + 1, \]

Preliminary property of brackets:

\[ [XY(2uvw)] = [XYZ] + [XTW], \quad \text{if } EUW = 0 \]

\[ XYZ = [ax_1y_1z_1] \quad a \neq 0, \]

\[ [XYZ] = [ZXY] = [YZX] = \ldots \]

\[ F_p = \bar{s}_0 S U R S U T \quad [R_2 F_p] = m^2 \]

\[ [R_2 \bar{s}_0 R] + [R_2 R] + [RST] = m^2 \]

Fix \( s \in S \) and \( t \in T \), since \([RST] = [R_s R_s r_s S]\)

\[ [RST] = [TTS], \]

\[ [R_2 \bar{s}_0 R] + [R_2 R] + [SST] + [TTS] = m^2. \]

Some skipping

\[ m + [R_s R_s] = [R_2 S]. \]

Beautiful formula: \[ M_p = 9\left[R_2 S\right], \]