11/3

Goal: 2/3 of Gauss's Theorem

Last time: estimated # of solutions to cubic eqns over finite fields.

This time case: proved by Gauss.

Fermat curve: $x^3+y^3=1$ Projective solutions only

homogeneous: $X^3+Y^3+Z^3=0$ no $(0,0,0)$ no (aX, aY, aZ).

<u>Gauss's Thm</u> 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 $p \not\equiv 1 \pmod 3$ 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 $A \equiv 1 \bmod 3$

$$M_p = p+1+A.$$

Note: if $p \equiv 1 \bmod 3$ then $A^2 \equiv 1 \bmod 3$ so $A \equiv \pm 1 \bmod 3$ so by replacing A with $-A$ we can make $A \equiv 1 \bmod 3$.

$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$

$\mathbb{F}_p^* = \{1, \ldots, p-1\}$

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

Ex. $\mathbb{F}_5^*$ gen $= 2$. $2, 2^2=4, 2^3=3$ $2^4=1$

Proof on p. 111.

Proof of Gauss's Thm Part (A).

Assume that $p \not\equiv 1 \mod 3$.

So 3 does not divide the order $p-1$ of $\mathbb{F}_p^*$.

It follows that the map $x \longmapsto x^3$ 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 $p \not\equiv 1 \mod 3$ 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 # of solutions to $x+y+z=0$, $\longrightarrow$ a line in the projective plane, so it has $p+1$ solutions in $\mathbb{F}_p$.

$M_p = p+1$.

Proof of (b).

Assume $p \equiv 1 \mod 3$. $p = 3m+1$

Since 3 does divide the order of $\mathbb{F}_p^*$ the map $x \longrightarrow x^3$ is a homomorphism but neither one-to-one nor onto.

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

$R = \{ x^3 : x \in \mathbb{F}_p^* \}$.

The kernel of $x \longrightarrow x^3$ has three elements: $1, \omega, \omega^2$ with $\omega^3 = 1$

Ex. $p=13$ then $R = \{\pm 1, \pm 5\}$ and the kernel of $x \rightarrow x^3$ is $\{1, 3, 9\}$

Elements of R are called <u>cubic residues</u>.

Let S and T be the other 2 cosets of R in $\mathbb{F}_p^*$

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

If $p = 13$ then we can choose $s = 2$

$$S = \{\pm 2, \pm 10\}$$
$$T = \{\pm 4, \pm 7\}$$

In general $\mathbb{F}_p$ is a disjoint union

$$\mathbb{F}_p = \{0\} \cup R \cup S \cup T.$$

The number of elements in each of R, S, T is m.

Note: $R = -R$ (if $r \in R$ then $-r \in R$)

$$S = -S$$
$$T = -T$$

New symbol $[\ \ ]$

Suppose X, Y, Z are subsets of $\mathbb{F}_p$.

Let $[XYZ]$ denote the number of triples (x, y, z) s.t. $x \in X$, $y \in Y$, $z \in Z$ and $x + y + z = 0$.

<u>What is M_p in terms of the symbol?</u>

First consider solutions to $x^3 + y^3 + z^3 = 0$ where none are zero. Then there are $[RRR]$ solutions (R = cubes).

But for each cube there are 3 field elements that give that cube. So there are $27[RRR]$ solutions s.t. x, y, z not zero. However, we don't want only projective solutions. We need to get rid of (aX, aY, aZ) There are $p-1$ multipliers

$p = 3m+1 \quad p-1 = 3m$

$\frac{27[RRR]}{3m} = \frac{9[RRR]}{m}$ projective solution to $x^3+y^3+z^3=0$ $\quad x,y,z \neq 0$.

Case 2. if one of $x,y,z = 0$, say z, then the other can't also be zero, because we don't allow $[0,0,0]$.

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

$$y^3 = -x^3 \;:\; y = -x,\ -\omega x,\ -\omega^2 x$$

Then there are $3(p-1)$ triples $(x,y,0)$ s.t. $x^3+y^3=0$.

Symmetric for $(x,0,z)$ $(0,y,z)$

So $9(p-1)$ triples (x,y,z) s.t. $x^3+y^3+z^3=0$.

So there are $p-1$ multipliers $\frac{9(p-1)}{3m} = 9$ projective solutions. with 1 coord. 0.

$$M_p = \frac{9[RRR]}{m} + 9. = 9\left(\frac{[RRR]}{m}+1\right).$$

Marvellous properties of bracket:

$[XY(Z\cup W)] = [XYZ]+[XYW]$. if $Z\cap W = \emptyset$.

$[XYZ] = [aX, aY, aZ]$ $\quad a \neq 0$.

$[XYZ] = [ZYX] = [YXZ] = \ldots\ldots$

$\mathbb{F}_p = \{0\} \cup R \cup S \cup T \quad [RR\,\mathbb{F}_p] = m^2$

$[RR\{0\}] + [RRR] + [RRS] + [RRT] = m^2$

Fix $s \in S$ and $t \in T$. Since $[RRS] = [sR, sR, sS]$

$= [SST]$

$[RRT] = [TTS]$.

$[RR\{0\}] + [RRR] + [SST] + [TTS] = m^2$.

$\vdots$ some skipping

$m + [RRR] = [RTS]$.

Beautiful formula: $M_p = \frac{9[RTS]}{m}$.