Thursday, October 24

Some general definitions:

- A degree-d <u>homogeneous polynomial</u> (or <u>form</u>) is a polynomial (in multiple variables) where every monomial has total degree d.

<u>Example</u>: $X^3+Y^3+3Y^2Z+5XYZ$ is a degree-3 form.

- A <u>binary</u> form is a form in 2 variables.
- A <u>quadratic form</u> is a degree-2 form.

<u>Example</u>: Two binary quadratic forms are x^2+y^2 and $53x^2+152xy+109y^2$.

Questions we like to ask about binary quadratic forms $f(x,y)$:

1) For which $n \in \mathbb{Z}$ do there exist $x,y \in \mathbb{Z}$ such that $f(x,y)=n$? In other words, which integers are <u>represented</u> by f?

Observation: If $f(x,y)=n$ then $f(dx,dy)=d^2n$.

2) For which $n \in \mathbb{Z}$ do there exist <u>coprime</u> $x,y \in \mathbb{Z}$ such that $f(x,y)=n$? In other words, which integers are <u>properly represented</u> by f?

First goal: $f(x,y)=x^2+y^2$. Which primes are represented by f?

- $2=1^2+1^2$ ✓

Lemma: If $p \equiv 3 \pmod 4$ and $p \mid (x^2+y^2)$, then $p \mid x$ and $p \mid y$.

Proof: By assumption $x^2 \equiv -y^2 \pmod p$.

If $p \nmid y$, then $y^{-1} \pmod p$ exists and

$(xy^{-1})^2 \equiv x^2 y^{-2} \equiv -1 \pmod p$,

contradicting $\left(\frac{-1}{p}\right) = -1$ when $p \equiv 3 \pmod 4$.

Hence $p \mid y$, and similarly $p \mid x$. //

Corollary: If $p \equiv 3 \pmod 4$, then p is not the sum of two squares.

Proof: If $p = x^2+y^2$ then $p \mid x$ and $p \mid y$, implying $p^2 \mid (x^2+y^2) = p$. $\times$ //

Proposition: If $p \equiv 1 \pmod 4$, then p is properly represented by X^2+Y^2. ☆

(due to Fermat)

Proof: Choose $z \in \mathbb{Z}$ such that $z^2 \equiv -1 \pmod p$. (possible since $\left(\frac{-1}{p}\right) = 1$)

Consider the set

$$\{u + zv : 0 \le u < \sqrt{p},\ 0 \le v < \sqrt{p}\}.$$

Note that the number of ordered pairs (u,v) is $(1 + \lfloor \sqrt{p} \rfloor)^2 = \lceil \sqrt{p} \rceil^2 > (\sqrt{p})^2 = p$.

By the pigeonhole principle there exist distinct pairs (u,v) and (u',v') with $u + zv \equiv u' + zv' \pmod p$.

Write $x = u - u'$, $y = v' - v$; then

$x \equiv zy \pmod p$; squaring both sides,

$x^2 \equiv z^2 y^2 \equiv -y^2 \pmod p \Rightarrow p \mid (x^2+y^2)$.

Also, $0 < x^2+y^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p$.

So $x^2+y^2 = p$ exactly. //

☆ (If $d \mid (x,y)$ then $d^2 \mid (x^2+y^2) = p \Rightarrow d = \pm 1$.)

Lemma: If m and n are both represented by x^2+y^2, then so is mn.

Proof: Choose $u,v,x,y \in \mathbb{Z}$ with $m=u^2+v^2$ and $n=x^2+y^2$; then ... check that

$$mn=(ux-vy)^2+(uy+vx)^2. \quad //$$

wut...

(Secretly, this identity is $|(u+iv)(x+iy)| = |u+iv|\,|x+iy|$.)

Theorem: (Fermat) x^2+y^2 represents n if and only if: if $p \mid n$ and $p \equiv 3 \pmod 4$, then p divides n with an even multiplicity.

Ex: $29 \cdot 31^2 \cdot 37^3$ is a sum of 2 squares but $29^4 \cdot 31^5 \cdot 37^6$ is not a sum of 2 squares.

Proof: $\Leftarrow$ If the factorization condition holds, then n is the product of numbers of the form:

- 2
- primes $p \equiv 1 \pmod 4$
- q^2 where q is prime, $q \equiv 3 \pmod 4$;

And $2=1^2+1^2$ and $q^2=q^2+0^2$ and the proposition about $p \equiv 1 \pmod 4$; by the previous lemma, n itself is the sum of two squares.

$\Rightarrow$: If $n=x^2+y^2$ and $p \mid n$ and $p \equiv 3 \pmod 4$, then (by previous lemma) $p \mid x$ and $p \mid y$; then $\frac{n}{p^2}=\left(\frac{x}{p}\right)^2+\left(\frac{y}{p}\right)^2$.

If $p \mid \frac{n}{p^2}$ then do this again ... //

Theorem: n is properly represented by x^2+y^2 if and only if n is not divisible by any $3 \pmod 4$ primes.

Other cool quadratic-form results:

Theorem (Lagrange): Every nonnegative integer is represented by $w^2+x^2+y^2+z^2$.

w/ integer coeffs

Theorem: If a quadratic form (in any number of variables) represents $1,2,3,\dots,290$, then it represents all positive integers.

– If the coefficients of the cross terms x_ix_j are all even, then 290 can be reduced to 15.

General connections:

binary quadratic form $ax^2+bxy+cy^2$ of discriminant $\Delta = b^2-4ac$

Legendre symbol $\left(\frac{\Delta}{p}\right)$ $\longleftrightarrow$ algebraic number theory of quadratic extensions $\mathbb{Q}(\sqrt{\Delta})$

class group of $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$

$\updownarrow$

classes of binary quadratic forms

Back to the Legendre symbol $\left(\frac{a}{p}\right)$ where p is an odd prime. Extension:

<u>Jacobi symbol</u> $\left(\frac{a}{Q}\right)$ is defined for all $a \in \mathbb{Z}$ and all odd positive integers Q:

if $Q = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ then we define

$$\underbrace{\left(\frac{a}{Q}\right)}_{\text{Jacobi}} = \underbrace{\left(\frac{a}{p_1}\right)^{r_1} \left(\frac{a}{p_2}\right)^{r_2} \cdots \left(\frac{a}{p_k}\right)^{r_k}}_{\text{Legendre symbols}}$$

- Jacobi symbol is multiplicative in either argument.

Properties of Jacobi symbol:

- It equals the Legendre symbol if Q is an odd prime.
- $\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2} = \begin{cases} 1, & \text{if } Q \equiv 1 \pmod 4, \\ -1, & \text{if } Q \equiv 3 \pmod 4 \end{cases}$
- $\left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8} = \begin{cases} 1, & \text{if } Q \equiv 1, 7 \pmod 8 \\ -1, & \text{if } Q \equiv 3, 5 \pmod 8 \end{cases}$
- Quadratic Reciprocity: if P, Q be odd positive integers, then $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$

Unfortunate property of Jacobi symbol:

- $\left(\frac{a}{Q}\right) = 1$ does <u>not</u> imply that a is a quadratic residue $\pmod Q$!

Example: $a = 11$ and $Q = 221 = 13 \cdot 17$.

In your Tuesday group work, you showed $x^2 \equiv 11 \pmod{221}$ has no solutions, by calculating $\left(\frac{11}{13}\right) = -1$, $\left(\frac{11}{17}\right) = -1$.

But $\left(\frac{11}{221}\right) = \left(\frac{11}{13}\right)\left(\frac{11}{17}\right) = (-1)(-1) = +1$.

<u>Exercise</u>: If $\left(\frac{a}{Q}\right) = -1$ then a is a quadratic nonresidue $\pmod Q$.

Example: 53,681 is a prime congruent to $1 \pmod 4$. Does $x^2 \equiv 1{,}311 \pmod{53{,}681}$ have solutions?

Answer: We exploit

$$\underbrace{\left(\frac{1{,}311}{53{,}681}\right)}_{\text{Legendre}} = \underbrace{\left(\frac{1{,}311}{53{,}681}\right)}_{\text{Jacobi}} = \left(\frac{53{,}681}{1{,}311}\right)$$

Quadratic Reciprocity for Jacobi

Since $53{,}681 \equiv -70 \pmod{1{,}311}$:

$1{,}311 \equiv 7 \pmod 8$

$$\left(\frac{53{,}681}{1{,}311}\right) = \left(\frac{-70}{1{,}311}\right) = \left(\frac{-1}{1{,}311}\right)\left(\frac{2}{1{,}311}\right)\left(\frac{35}{1{,}311}\right)$$

$$= (-1)(+1)\left(-\left(\frac{1{,}311}{35}\right)\right)$$

$$= +\left(\frac{16}{35}\right) = \left(\frac{4}{35}\right)\left(\frac{4}{35}\right) = +1.$$

Hence the Legendre symbol $\left(\frac{1{,}311}{53{,}681}\right) = 1$, so the congruence does have solutions. ✓

$53{,}681 \equiv -70 \pmod{1{,}311}$

$1{,}311 \equiv 16 \pmod{35}$

Next topic:

Arithmetic functions

$(f : \mathbb{N} \to \mathbb{R})$