Threadory, October 24

Some general definitions:
 $\begin{array}{lll} \mathcal{L}_{\text{total}} & \mathcal{L}_{$ 1) For which neZ do there exist
 $x,y \in Z$ such that $f(x,y) = n?$ Thursday, October 24 In other words, which Artegues Joine seres activitions.
• A degree d homogeneous polynomial In sthe words, which Integers are represented by f? $Lor form$ is a polynomial LIn multiple variables) where every monomial has Observation: F $f(s,y) = n$ then
 $f(dx, dy) = d^2n$. total degree d.
Example: $x^3 + y^3 + 3y^2z + 5xyz$
 $\frac{1}{2} \int \frac{1}{2} dx \text{ which } n \le 2$ do there exist $= -\frac{1}{2} \text{ days}$
= dgnee d.
Enough: $x^3 + y^3 + 3y^2z + 5xyz$ 2) For which $n \leq 2$ do there exist
a dealer $x = 2$ for which $n \leq 2$ as the third $\{(x_n)_{n\geq 2}\}$ is $\frac{2}{x}$ degree -3 form. coprime $x_iy \in \mathbb{Z}$ such that $f(x_i) = n$? - A binary form is a f_{avg} form.

Form is a form 1 - variables. In other words, which wild

adratic form is a degree-2-form. properly represented by f?

Two binary quadratic forms
 f_{avg} and $53x^2 + 52xy + 109y^2$. First goal: $f(x,y) = x^2 + y^2$. In other words, which integers are - Aigualistic form is a degree-2-form.
Example - Two bihary quadratic fame
are x^2+y^2 and $53x^2 + 52xy + 109y^2$.
Questions we like to ask about bihary First goal: $f(x,y) = x^2 + y^2$.
Which primes are represented by f? $quadratic$ forms $f(X, y)$: \cdot 2 = $1^2 + 7^2$ $\sqrt{1}$

1

Prost. Choose 2 EZ such that Lemms: If $p \equiv 3$ (anos) 4) and $p(68+y^2)$ $z^2 = -1$ (unot p). (possible since $(\frac{-1}{7})=1$) then plx 24 ply. Prof: By resumption $x^2 \equiv -y^2$ (nord p). Consider the set $5u+2v: 0 \le u < v_{P}$, 05 $v < v_{P}$? If gts, then y' (mod p) exists and Note that the number of ordered pairs $(xy')^{2} = x^{2}y^{2} = -1$ (und p), $(4,0)$ is $(1+4\pi\pi)$ = $\pi\pi^2 > (\pi\pi)^2 = p$. contradicting $(\frac{-1}{p})=-1$ when $p=3$ (mod/1). By the pigeonholo pringides there extern Hence ply, and similarly plx. 4 distinct pairs (μ, ν) and (μ', ν') with $u+zv \equiv u'+zv'$ (modp). Corollary: If p=3 (mod 4), then p is Write $x = u - u'$, you'rus then not the sum of two squares. $x \equiv 2y \pmod{p}$; squaring botholders, Prof. If $p=x^2+y^2$ then $p!x$ and $p!y$, $x = 2y^2 = -y^2(may) \ni p(x+y^2)$ $[mp!yhy p^2 (x+y^2) = p - x]$ Proposition: If p=1 (ned 4), then p is λk_0 , $0 < x^2+y^2 < (lp)^2 + lp^2 = 2p$. property represented by x^2+y^2 . $\delta x^2+y^2 = p$ exactly.

(If dl(x,y) then d^2 (x2+y) = d=±(.) De (ducto Fernist)

Prof: = If the factorization cond then Lemmon It mond note both represented by X2+V3, The so is mn. holds, then in is the preduct of numbers of the form. Proof: Choose u,v,x,y EZ with $m = u^2 + v^2$ and $n = x^2 + y^2$; Then · promos p=1 (anod 4) · 9² where 9 is prime, 93 Cmod 4); check that $mv = (uv - vy)^2 + (vy + vx)^2$. And $2=1^2+7^2$ and $q^2=9^2+0^2$ and the proposition about p=1 (mort); by (Searctly, this identity is He previous lemmes n'ilsett is the sun $|$ Cutiv χ tigi $|$ = $|$ utiv $|$ xtigi.) of two squares. Theorem: (Fernat) X+Y² represents n \Rightarrow : If $n=x^2+y^2$ and $p|n$ and if and only if: if pln and p=3 (mod4), p=3 (molt), then 4 by previous lemmed then p divides in with an even multiplicity $p|x \text{ av } p|y$; then $\frac{n}{p^2} = (\frac{x}{p})^2 + (\frac{y}{p})^2$. $56: 29.31^{2}\cdot 37^{3}$ is ∂ sur of 2 squares $I f$ pl $\frac{n}{p^2}$ then do this again ... but 29.31⁵.37⁶ is not a sun of 2 squares.

Theorem: n is properly represented by
 $x^2 + y^2 = 1$ and only if n is not divisible binary quadratic forms

by any 3 Line of primes.

Discussion of a properly represents

Discussion of a properly represents

Theorem: If a 1 Theorem: n is properly represented by General connections: $X^{2}+y^{2}$ if and only \hat{T} in is not divisible binary quadratic form by any 3 Lonor 4 poinces. $3x^{2}+6x4+2y^{2}$ of discriminant Other cool quodrotic-form results: $\Delta = b^2 - 4ac$ Theorem (Lagrange): Every nonnegative sented by General connections:

not divisible binary quadratic for

a) $x^2 + bxy^2 + 2y^2$ of di

nonnegative $\Lambda = b^2-bx$

womegative if $\Lambda = b^2-bx$

integer coeffs Λ $Nb8e-15$ represented by $W^2+\chi^2+\gamma^2+Z^2$. Noteger is represented by $w + x + y + z$. Legendre symbol
Winteger coeffs $\begin{pmatrix} 1 \ 0 \end{pmatrix}$ and algebraic number vumber of variables represents $1,3,3,...$ $\frac{1}{290}$ $\frac{1}{290}$ and ratio extensions Theorem. If a quadratic form ($\frac{M}{m}$ any $\left(\frac{A'}{P}\right)$ and theory of variables) represents $1,3,3,..,290$ quadratic extraction of variables) represents $1,3,3,..,290$ quadratic extraction of variables) $\frac{M}{M}$ then it represents all positive integers. terms $X_i X_{\hat{\nu}}$ are all even, then 390 can closs group of $\left(\frac{1}{2}\right)$ ($E = \frac{1}{2}$ the coefficients of the cross
come $X_i X_i$ are all even, then 390 come class s_i
be reduced to 15. closses of binary quadratic forms

Book to the beganize symbol $\begin{pmatrix} \frac{a}{c} \end{pmatrix}$

where P is on and prime. Extension:
 $\int \frac{a}{c} \cdot d\theta$ = $\frac{c}{c} \cdot \frac{b}{c}$, θ are 35 (m) $\frac{c}{c}$
 $\int \frac{a}{c} \cdot d\theta$ is defined by θ
 $\int \frac{a}{c} \cdot d\theta$ and θ 1 Bock to the Legendre symbol $\begin{pmatrix} \mathbb{Z} \\ \mathbb{P} \end{pmatrix}$
where \mathbb{P} is an add prime. Extension? $-(\frac{2}{Q})=(-1)^{-(q^2-1)/8}-\{-1, +2\}=3.5$ Cmn (8) Jacobi symbol $\left(\frac{a}{a}\right)$ is defined for . Quadratic Reciprocity: it
all act and all positive integers Q_i , P_iQ be one positive integers the Quodrobic Reciprocity : if all $ac\,Z$ and all odd positive integers Q_i p is an add prime. Extension:

sbi symbol $\left(\frac{a}{a}\right)$ is defined for . Quadrotic Reciprocity: if
 ϵ $\frac{a}{b}$ and all odd positive integers Q_i ; $P_i \&$ be one positive integers then if $Q = p_1^{\prime\prime} p_2^{\prime\prime} - p_k^{\prime\prime}$ then we define $\begin{pmatrix} \frac{1}{p} & \frac{1}{p$ Unfortunate property of Jacobi symbol: $\left(\frac{a}{Q}\right)^{1}$ Legendre symbol $\begin{pmatrix} 2 \\ p \end{pmatrix}$
and prime. Extension?
($\begin{pmatrix} \frac{\Delta}{\alpha} \\ \frac{\Delta}{\alpha} \end{pmatrix}$ is defined for
all add positive integers Q_i
($\begin{pmatrix} 2 \\ p_i \end{pmatrix}$ is then we define
($\begin{pmatrix} 2 \\ p_i \end{pmatrix}$ is $\begin{pmatrix} \frac{\Delta}{\alpha} \\ \frac{\Delta}{\$ $\left(\frac{a}{2}\right) = 1$ does not imply that back to the Legendre symbol $\begin{pmatrix} 2 \\ 3 \end{pmatrix}$ is $\begin{pmatrix} 3 \\ 4 \end{pmatrix}$ = $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ is $\begin{pmatrix} 3 & -1 \\ 4 & 5 \end{pmatrix}$

Legendre ($\begin{pmatrix} 3 \\ 2 \end{pmatrix}$) is defined for
 $\begin{pmatrix} 2 & -1 \\ 3 & 2 \end{pmatrix}$ is defined for
 $\begin{pmatrix}$ Jocobi Legendre Symbols -Jacobi symbol is muttiplicative in either Example: 0=11 and Q=221 = 13. D Is a quadrative residue (mod Q)! $argum$ ert . your Tuesday group work, you shoved
no solutiona, Properties of Jacobi symbol: · It equils the Legendre symbol $x^2 \equiv 11$ (mod 221) has no salitone, b y colculating $\left(\frac{11}{13}\right)=-1, \left(\frac{11}{17}\right)=-1$ 1 . unert.
Ales of Jacobi symbol:
It Q is on odd prime.
If Q is on odd prime. · Le to the legendre symbol $\frac{1}{2}$
 $\frac{1}{2}$ is on and prime. Extensions:
 $\frac{1}{2}$ is on and prime. Extensions:
 $\frac{1}{2}$ is defined for
 $\alpha = p_1^2 p_2^2$ is defined for
 $\alpha = p_1^2 p_2^2$ is defined for
 $\alpha = p_1^2 p_2^2$

Example: 53,681 is a prime congruent $53,681 = -70$ ω $1,311$ t_0 1 (mod 4). Does $x^2 \equiv 1,311$ (mod 53,68/1) $1,311 = 16$ (nood 35) have solutions? Answer: We exploit Quadratic Reciprocity $1,34 \equiv 7$ (most 8) $\left(\frac{53,681}{1,311}\right) \le \left(\frac{-70}{1,311}\right) = \left(\frac{-1}{1,311}\right)\left(\frac{2}{1,311}\right)\left(\frac{35}{1,311}\right)$ $= (-1)(+1)(-\frac{(1,311)}{35})$ Neut topic. Anthmetic Functions $= +(\frac{16}{35}) = (\frac{4}{35})(\frac{4}{35}) = +1.$ $(f:IN\rightarrow R)$ Hence the Legendre symbol $\left(\frac{1,311}{53,531}\right)$ =1 to the congruence does have solutions.