TEST #1

0 = square

(How)many positive integers btwn 1-221 are relatively prime to 221? $\phi(221) = \phi 13 \phi 17$

(C)alculate least positive residue: Euler's Thm $50^{201} \bmod 33$; $\phi 33 = \phi 3 \phi 11 = 20$; $50^{201} = 50^{20} \cdot 50 \equiv (50^{20})^{10} 50 \equiv 1^{10} 50 \bmod 33$; $50 \bmod 33$; $17 \bmod 33$

(F)ind $\mathbb{Z}$ solutions of $2x+3y=20$; note $\gcd(3,2)=1 \mid 20$. $3-2=1$ ... $(-20)+3(20)=20$; $x_0=-20$, $y_0=20$; For each $t \in \mathbb{Z}$ $x=-20+3t$, $y=20-2t$

(S)olve system of congruences: $x \equiv 3 \bmod 5$ $x \equiv 4 \bmod 17$ $M=85=M_1M_2=5(17)$; $M_1=\frac{M}{M_1}=m_2=17$ ... $[M_1]_5^{-1}=[17]_5^{-1}=[2]_5^{-1}=[3]_5 \therefore y_1=3$, $[m_2]_5^{-1}=[5]_{17}^{-1}=[7]_{17} \therefore y_2=7$

(C)RT: $x \equiv 3(17)(3)+(4)(7)(5) \bmod 85$; $x \equiv 38 \bmod 85$

(F)ind order $10 \bmod 41$: $10^2=100=18 \bmod 41$; $10^4=18^2=37 \equiv -4 \bmod 41$ ... $10^5 \equiv -4(10) \equiv -40 \equiv 1 \bmod 41$ $\therefore order_{41}(10)=5$

$\gcd(b+18,b)$ is even $\Rightarrow 2 \mid \gcd$; observe ... (l)ist poss. values for $\gcd(b+18,b)$: $\gcd(b+18,b)$; $\gcd \mid b+18$ and $\gcd \mid b$. $\Rightarrow$ ... $b+18$ and b are divided by $\gcd(b+18,b)$ ... $d \mid b+18$ & $d \mid b \Rightarrow d \mid b+18-b \Rightarrow d \mid 18$. Thus $1 \le d \le 18$. $2 \mid d$ and $d \mid 18$, $d=1,2,3,6,9,18$. only $d=6,18$ | 3 and even

(I)s $(7654321)_8$ divisible by 9:

(S)olve system congruences: $x \equiv 3 \bmod 5 \Rightarrow x=3+5j$, thus $x \equiv 4 \bmod 17 \Rightarrow 3+5j \equiv 4 \bmod 17 \Rightarrow 5j \equiv 1 \bmod 17$ (Euclidean algorithm) $1=7b-2a=7(5)-2(17) \rightarrow 7(5j) \equiv 7 \bmod 17 \Rightarrow j \equiv 7 \bmod 17$ ... $j \equiv 7 \bmod 17$ and $x=3+5j$ for $j \in \mathbb{Z}$; $j=7+17k$ for $k \in \mathbb{Z} \Rightarrow x=3+5(7+17k) \rightarrow x=38+85k \Rightarrow x \equiv 38 \bmod 85$

(I)s $(7654321)_8 \mid 9$? $8 \equiv -1 \bmod 9$, $8^2 \equiv 1 \bmod 9$, $8^3 \equiv -1 \bmod 9$ ... $1+2\cdot 8+3\cdot 8^2+4\cdot 8^3+5\cdot 8^4+6\cdot 8^5+7\cdot 8^6 \equiv 1-2+3-4+5-6+7 \bmod 9 \equiv 4 \bmod 9$

(P)rove the product of consequtive $\mathbb{Z}$ is even. Let $a \in \mathbb{Z}$ then $a+1$ is the next integer. If $a \in 2\mathbb{Z}$ then $a=2j$ for some $j \in \mathbb{Z}$ hence $a+1=2j+1$ and find $a(a+1)=2j(2j+1)=2[j(2j+1)] \Rightarrow 2 \mid a(a+1)$, $a(a+1)$ is even otherwise $a \in 2\mathbb{Z}+1$ hence $a=2j+1$ for $j \in \mathbb{Z}$ thus $a+1=(2j+1)+1=2j+2$. $\therefore a(a+1)=(2j+1)(2j+2)=2[(2j+1)(j+1)] \Rightarrow 2 \mid a(a+1)$.

(I)f $[a] \in \mathbb{Z}_n$ has order $k>1$. & $b \in \mathbb{Z}$ has $ab \equiv 1 \pmod n$. Prove $[b]$ has order k: If $[a]$ has order $k>1$ then $[a]^k=[1]$ and $[a]^\ell \ne [1]$ for $1 \le \ell \le k$. we are given $ab \equiv 1 \bmod(n)$ hence $[a][b]=[1]$. Notice, $([a][b])^k=[a]^k[b]^k=[b]^k \Rightarrow [b]^k=[1]$. & $[b]^j=[1] \Rightarrow [a]^j[1]=[1] \Rightarrow [a]^j=[1]$ $\rightarrow\!\leftarrow$ $k>j$. Thus $[b]^j \ne [1]$ for $1 \le j \le k$ yet $[b]^k=[1]$ thus order of $[b]$ is also k

After making Caley Table: $H=\{1,4\}$ show G is partioned by the cosets of H. pick anything not in H, $2H=\{2,8\}=\{2,3\}$. $H \cup 2H=\{1,4\} \cup \{2,3\}$

Lagrange's Theorem: The order of any subgroup of a finite group G then the order of H divides the order of G. (aka) Let G be a group w/ $|G|<\infty$, then $H \le G \Rightarrow |H| \mid |G|$ Proof: $|H|=|gH|$ $\forall g \in G$. This is clear given bijection btwn H and gH. $\Psi: H \to gH$ by $\Psi(x)=g(x)$. Ψ is well defined. In addition, Ψ is onto as is seen from nothing $y \in gH \Rightarrow \exists h \in H \ni y=gh$. Observe $\Psi(h)=gh=y$. Thus Ψ onto. Next, $\Psi(x)=\Psi(y) \rightarrow gx=gy \Rightarrow g^{-1}gx=g^{-1}gy \rightarrow x=y \Rightarrow \Psi$ is 1-1. If $g_1H \ne g_2H$, then $g_1H \cap g_2H=\emptyset$. $g_1 \in g_2H$ then $g_1H=g_2H$ & $g_1 \in g_2H$ then $\exists h \in H \ni g_1=g_2h \Rightarrow g_2=g_1h^{-1}$ Let $x \in g_1H \Rightarrow \exists h_1 \in H \ni x=g_1h_1=g_2hh_1$ & as $hh_1 \in H$ as $H \le G$, thus $y=g_1h^{-1}h_2 \in g_1H$. $g_2H \le g_1H$. $\therefore g_1H=g_2H$ By showing all cosets $|gH|=|H|$ and cosets partition G into disjoint subsets $|G|=|H|+|g_2H|+$

TEST #2

PPT: If $x^2+y^2=z^2$; $x=u^2+v^2$ and $y=2uv$. $z=u^2+v^2$

Find a solution of $x^2-65y^2=1$. solve for $x^2-65y^2=-1$ w/ $y=1$ $(x_1x_2+ny_1y_2, x_1y_1+y_1x_2)$

& $d \in \mathbb{Z}$ is □free and $a,b,x,y \in \mathbb{Z}$. Prove if $a+b\sqrt{d}=x+y\sqrt{d}$, $a=x$, $b=y$. & $a \ne x$. $a+b\sqrt{d}=x+y\sqrt{d}$; $a-x=y\sqrt{d}-b\sqrt{d}$; $a-x=(y-b)\sqrt{d}$ since $y-b \ne 0$, $\sqrt{d}=a-x/y-b$ $\rightarrow\!\leftarrow$ irr. of $\sqrt{n}$

Find distinct units: solve $a^2+5b^2=1$ for $a,b \in \mathbb{Z}$ $(\ ,\ ) \Rightarrow$ units $(\_+\_\sqrt{\ })$ and $(\_-\_\sqrt{5})$. use BG compnile

Determining primes:
- Prime in $\mathbb{Z}[i]$; if $p=4n+1$, $p=a^2+b^2$; $13=2^2+3^2=(2+3i)(2-3i)$; $norm(2\pm 3i)=13<norm(13)=169$

Finding gcd in $\mathbb{Z}[i]$: $\gcd(a,b)=\frac{a}{b} \Rightarrow$ rationalize $\Rightarrow$ approximate fraction; $a-(app)(b)=$ new b. repeat until unit.

Show $a-ib$ is a Gaussian prime. & $a-ib$ is not GP. Then $a-bi=\alpha\beta$ which is not prime $\rightarrow norm(\alpha), norm(\beta) \ne 1$ also $norm(a-bi) \ne 1$. Thus unique. so $a+bi=\overline{\alpha\beta}$ $\rightarrow\!\leftarrow$

Find GP factorization: $102=2\cdot 51=2\cdot 3\cdot 17=(1+i)(1-i)3(4+i)(4-i)$.

Give an ex. how prime divisor property fails for non-real primes in the Hurwitz: $\alpha=1+j+k$; $\beta=-1-j-k$; $\alpha\beta=(1+j+k)(-1-j-k)=-1^2-j^2-k^2-ij-j(i-1k-ki-jk-kj)=3$. $Norm(\alpha)=norm(\beta)=3$, hence α,β are Hurwitz primes. $p=(1+j+k)/2+1=(3+1+j+k)/2$ has norm $(p)=(9+1+1+1)/4=12/4=3$ is p and $p\bar{p}=3 \Rightarrow p \mid 3$ or $p \mid \alpha\beta$ yet $p \nmid \alpha$ and $p \nmid \beta$ as $\alpha \in \beta$ are primes of Hurwitz #'s

Quaternion: $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$

$\begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta}_1 & \bar{\alpha}_1 \end{pmatrix}\begin{pmatrix} \alpha_2 & \beta_2 \\ -\bar{\beta}_2 & \bar{\alpha}_2 \end{pmatrix}=\begin{pmatrix} \alpha_3 & \beta_3 \\ -\bar{\beta}_3 & \bar{\alpha}_3 \end{pmatrix}$ where $\alpha_3=\alpha_1\alpha_2-\beta_1\bar{\beta}_2$, $\beta_3=\alpha_1\beta_2+\beta_1\bar{\alpha}_2$

Remainder $2^{432} \div 7$: $[2^9]^{48}=[512]^{48}=[1]^{48}$

If a is rel. prime to 72 then $a^{12} \equiv 1 \pmod{72}$
Proof: $72=8\cdot 9$, thus $a^{12} \equiv 1 \bmod 8$ and $a^{12} \equiv 1 \bmod 9$. so $\gcd(a,72)=1 \Rightarrow \gcd(a,8)=\gcd(a,9)=1$. using Eul. Th^m $a^{\phi(8)}=a^4 \equiv 1 \bmod(8) \Rightarrow a^{12} \equiv 1 \pmod{72}$ for any integer a relatively prime to 72

Let $a \in \mathbb{Z}$. Show $a^{12}-1$ is divisible by 35 whenever $\gcd(a,35)=1$. same as above.

What is remainder 4^{232} when divided by 7? $4^{\phi(7)} \equiv 1 \bmod 7 \Rightarrow 4^6 \equiv 1 \bmod 7 \Rightarrow 4^{(38)6+4} \equiv (1)^{38}4^4 \equiv 4^4 \bmod 7 \Rightarrow 256 \bmod 7 \equiv 4 \bmod 7$

suppose $2\_99561=[3(523+x)]^2$
$32+x \equiv 0 \bmod 9 \Rightarrow 5+x \equiv 0 \bmod 9 \Rightarrow x \equiv -5 \bmod 9 \Rightarrow x \equiv 4$

Pigeonhole principle: If more than k pigeons go into k boxes then at least one box contains at least 2 pigeons; (∞) if ∞ many pigeons go into k boxes, then at least one box contains infinetly many pigeons

TEST #3

$P(t)=13t-7$ observe $P(\frac{7}{13})=7-7=0$. Thus $\alpha=7/13$ is an algebraic number. Is it an integer? $P(t)$ is not monic $\alpha=7/13$ is not algebraic int.

Prove if $1 \in I$, then $I=R$. & $1 \in I$ and I an ideal then for all $x \in I$ and $r \in R$, $xr \in I$. But $x=1$, $r \in R$ gives $xr=r \in I$ thus $r \in R \Rightarrow r \in I$, thus $r \in R \Rightarrow r \in I \rightarrow R \subseteq I$. conversely $I \subseteq R$ is assumed at outset $\therefore I=R$.

Show $1 \in (2)+(1+\sqrt{-14})$. $(1+\sqrt{-14})^2=1+2\sqrt{-14}-14=-13+2\sqrt{-14} \in (1+\sqrt{-14})$ But $-2\sqrt{-14} \ni y$, $2(7) \in (2)$. Thus $x+y+z=1 \in (2, 1+\sqrt{-14})$

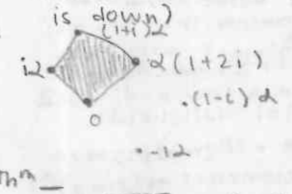
Find units in $\mathbb{Z}[\sqrt{-14}]$: $norm(a+b\sqrt{-14})=a^2+14b^2 \ge 0$ thus $norm(a+b\sqrt{-14})=a^2+14b^2=1 \Rightarrow a=\pm 1, b=0$

For ideals A, B, show $\overline{AB}=\bar{A}\cdot\bar{B}$:
$AB=\{a_1b_1+\dots+a_kb_k \mid a_i \in A, b_i \in B\}$ by def^n of product $\overline{AB}=\{\overline{a_1b_1+\dots+a_kb_k} \mid a_i \in A, b_i \in B\}$. Consider $z \in \bar{A}\cdot\bar{B} \Rightarrow z=\bar{a}_1\bar{b}_1+\dots+\bar{a}_n\bar{b}_n=\overline{a_1b_1+\dots a_nb_n} \in \overline{AB}$. Thus $\bar{A}\cdot\bar{B} \subseteq \overline{AB}$. conversely $z \in \overline{AB} \rightarrow \exists a_i \in A, b_i \in B \ni z=\overline{a_1b_1+\dots+a_nb_n}=\bar{a}_1\bar{b}_1+\dots+\bar{a}_n\bar{b}_n \in \bar{A}\cdot\bar{B}$ Thus $\overline{AB} \subseteq \bar{A}\cdot\bar{B} \Rightarrow \overline{AB}=\bar{A}\bar{B}$.

Prove $(3-\sqrt{-14})$ is prime in $\mathbb{Z}[\sqrt{-14}]$. Find norm $=23=$ prim(e)
Show $(3-\sqrt{-14})$ is max in $\mathbb{Z}[\sqrt{-14}]$. Prime $\Rightarrow$ max

Mordell's Equation: cube (group real w/ imaginary) $y+1\sqrt{-26}=(a^3-78ab^2)+(3a^2b-26b^3)\sqrt{-26}$
$1=(3a^2b-26b^3)b \rightarrow b=\pm 1$. Find a when $b=\_$ Solve for y then plug in to solve for x.

Lattice: pick point then just add $1+2i$ (1 is right, i is down)



$\mathbb{Z}[\sqrt{?}]=a^2+?b^2=1$