Lecture 33

April 1st

Final ex : April 20 (Monday) 9–12 EX 200

OH: April 7, 3-4pm, April 14, 3-4pm, April 16, 3-4pm.

Remember: Pythagorean triple (thm), FLT, CRT, Primitive Root Thm, QRL, Sum of 2 □ (Thm), pell's thm, Gaussian prime thm, Euclidean Algorithm

12 problems (3 have 2 parts)

#28.5

g primitive root mod 37

g^k primitive root mod 37 $\Leftrightarrow \gcd(k,36)=1$

$k=1,5,7,\cdots 35$ (total 12)

#28.9

q prime $\equiv 1 \bmod 4$

$p=2q+1$ prime

2 is a primitive root mod p

$2^{p-1}\equiv 1 \bmod p$, $2^u \not\equiv 1 \bmod p$ for any $u<p-1$ (to show)

Sps $2^u \equiv 1 \bmod p$

$u \mid p-1$, but $p-1=2q$, q is a prime, $u=\underline{1}, \underline{2}, \underline{q}, 2q=p-1$

3 candidates

$2 \not\equiv 1 \bmod p$

$2^2 \equiv 1 \bmod p$

only need to show $2^q \not\equiv 1 \bmod p$

Euler's Criterion for Legendre symbol

$2^q = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right)$

$p\equiv 3 \bmod 8$

$\left(\frac{2}{p}\right) = -1 \not\equiv 1 \bmod p$

#28.10 p prime, $p \nmid k$, b has kth root mod p.

g primitive root mod p

Let $b \equiv g^u \bmod p$

$x=g^v$, $g^{kv}=x^k \equiv b = g^u$

$kv \equiv u \bmod p-1$

This has a solution, it has $\gcd(k,p-1)$ sol.

$\gcd(k,p-1) \mid u$

#29.4 $x^k \equiv a \bmod p$ has a solution

$\Leftrightarrow k\,I(x) \equiv I(a) \bmod p-1$ has a solution

$\Leftrightarrow \gcd(k,p-1) \mid I(a)$

e.g. $x^3 \equiv b \bmod p$ has a sol $\Leftrightarrow 3\,I(x) \equiv I(b) \bmod p-1$ has a sol

$\Leftrightarrow \gcd(3,p-1) \mid I(b)$

In particular, if $p\equiv 2 \bmod 3$, it always have a solution

$\downarrow$

$p-1 \not\equiv 1 \bmod 3$

$x^{111} \equiv 729 \bmod 1987$

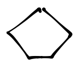
$\equiv 3^6$

$111\, I(x) \equiv 6 I(3) \bmod 1986$, $\gcd(111,1986)=3$ and $3 \mid 6I(3)$. There are 3 solutions

#31.4

n^{th} pentagonal number $\frac{3n^2-n}{2}$

$n=2$, $\frac{12-2}{2}=5$



#32.4 pentagonal number which is also triangular number.

$\frac{3n^2-n}{2}=\frac{m(m+1)}{2}$ (asking for + integer sol'ns)

$\Rightarrow$ By completing squares:

$(6n-1)^2=3(2m+1)^2-2$

$x^2=3y^2-2$

$x^2-3y=-2$

Solve $x^2-3y^2=1$ (pell's thm. by remembering, the smallest solutions are $(2,1)$.
& $x_k+y_k\sqrt{3}=(2+\sqrt{3})^k$)

so $x_k+y_k\sqrt{3}=(1+\sqrt{3})(2+\sqrt{3})^k$

Not all x_k & y_k will give integer m,n

k odd $\rightsquigarrow$ $\left.\begin{array}{l} x_k\equiv -1 \bmod 6 \\ y_k\equiv 1 \bmod 2\end{array}\right\} \mapsto$ give int. m,n

#35.9

$R=\{\alpha=a+b\sqrt{3}: a,b\in\mathbb{Z}\}$

$N(\alpha)=a^2-3b^2$

α unit $\Leftrightarrow N(\alpha)=\pm 1$ $\qquad a^2-3b^2\neq -1$

$N(\alpha)=1$ (has to be 1)

$a^2-3b^2=N(\alpha)=1$ (exactly a pell's thm)

α unit $\Leftrightarrow \alpha=\pm(2+\sqrt{3})^k$, $k=0,\pm1,\pm2,\cdots$

$(2+\sqrt{3})^{-1}=2-\sqrt{3}$

#36.6 $R=\{\underbrace{a+b\sqrt{-5}}_{\alpha=}, a,b\in\mathbb{Z}\}$

$N(\alpha)=a^2+5b^2$

R does not have unique factorization

$6=2\times3=(1+\sqrt{-5})(1-\sqrt{-5})$

$2,3,1\pm\sqrt{-5}$ are all irreducibles

$2=\alpha\cdot\beta$, α,β not units

$N(2)=4=N(\alpha)N(\beta)$, $N(\alpha)=2=a^2+5b^2$

no int solutions

#36.5

$\gcd(\underset{\beta}{\underset{\parallel}{8+38i}}, \underset{\alpha}{\underset{\parallel}{9+59i}})$

$\alpha=\beta q+r$

$N(r)<N(\beta)$ $\qquad \frac{\alpha}{\beta}=\frac{9+59i}{8+38i}=\frac{2314}{1508}+\frac{130}{1508}i$

$q=1+0\cdot i$, $r=\alpha-\beta q=1+21i$ $\qquad$ repeat write $\beta=rq_1+r_1$, $N(r_1)<N(r)$

$r = r_1 q_2 + r_2$
$r_1 = r_2 q + 0$
$r_2 = -1 + 5i = (-i)(5+i)$ ...... $\gcd(\alpha, \beta)$