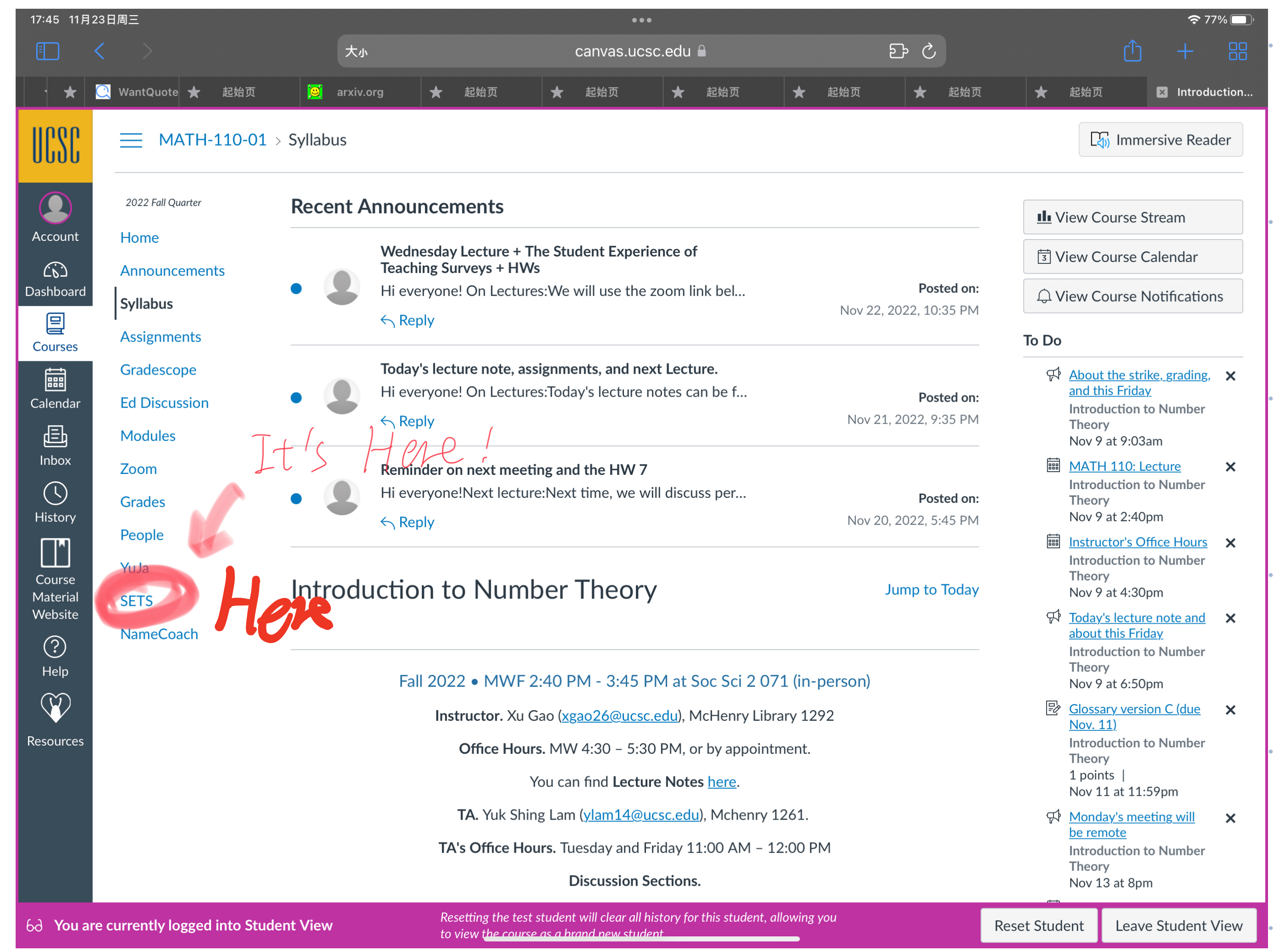
SETS:

- Will be closed on Sunday (Dec. 4)
- You can access this survey through the directlink in the email OR through Canvas
- Your feedback is Very important to us!
- Detailed comments ⟶ very helpful



Application of QRL (Quadratic Reciprocity Law)

① a prime p
② Quadratic eq.

Thm (Fermat's Christmas Theorem, Dec. 25, 1640)

Let p be a prime number & $p \equiv 1 \bmod 4$.

Then the Diophantine equation $X^2 + Y^2 = p$ has a solution in $\mathbb{Z}$.

$X^2 + Y^2 = pZ^2$ (ref. Lec.12)

Rmk:

- It was discovered (not proved) by Fermat on Christmas day
- Many great mathematician used different methods to prove it.
- We'll use a "geometry of number" method to prove it. (due to Minkowski)

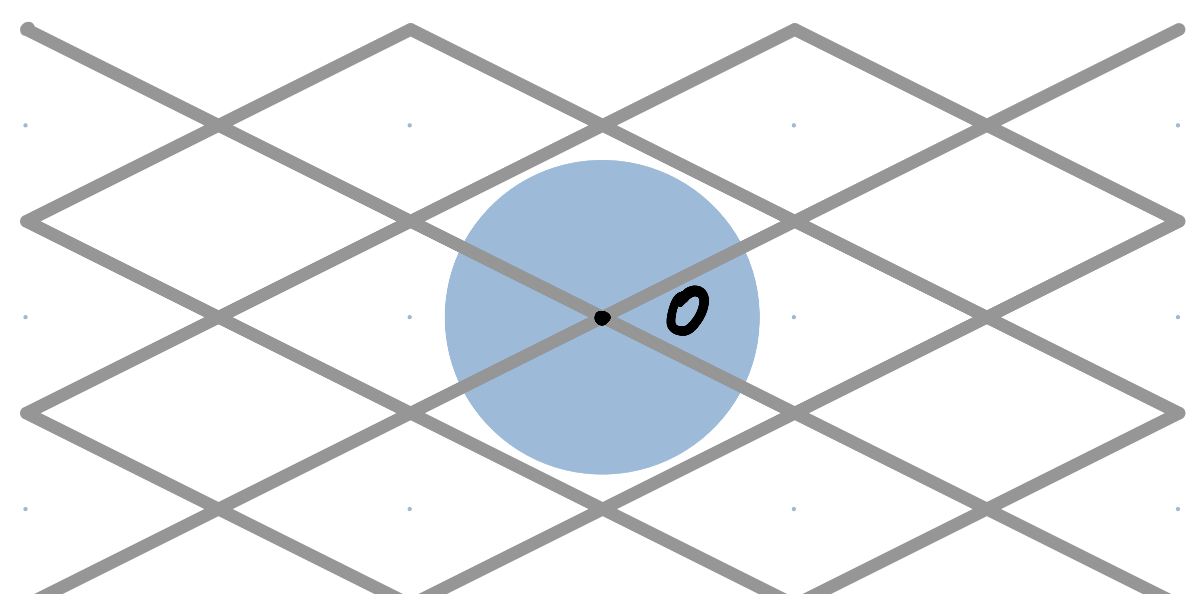
Thm. (Minkowski's theorem, plane case)

Consider a grid of parallelograms in the plane, with the origin at a grid-point
$\mathbb{Z}\vec{u} + \mathbb{Z}\vec{v}$ $\vec{u},\vec{v}$ are vectors in the plane

and a circle centered at the origin. If the area of the circle is greater than
$\{(x,y) \mid x^2+y^2 \leq r^2\}$ $A_{circle} = \pi \cdot r^2$

4 times the area of a parallelogram, then the circle contains a grid-point
$A_{parallelogram} = |\det(\vec{u},\vec{v})|$ $\exists (x,y) \mid \begin{array}{l} 0 < x^2+y^2 \leq r^2 \\ (x,y) = a\vec{u} + b\vec{v} \end{array}$ for some $a, b \in \mathbb{Z}$

besides the origin. $\begin{array}{l}\vec{u} = (a,b) \\ \vec{v} = (c,d)\end{array} \Rightarrow A = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$



Proof. pp. 200 in TEXTBOOK

Proof of Fermat's Christmas.

Let p be a prime number & $p \equiv 1 \mod 4$.

By the reciprocity of -1, we see that -1 is a QR mod p.

Let $u \in \mathbb{Z}$ s.t. $u^2 \equiv -1 \mod p$.

Consider the set:

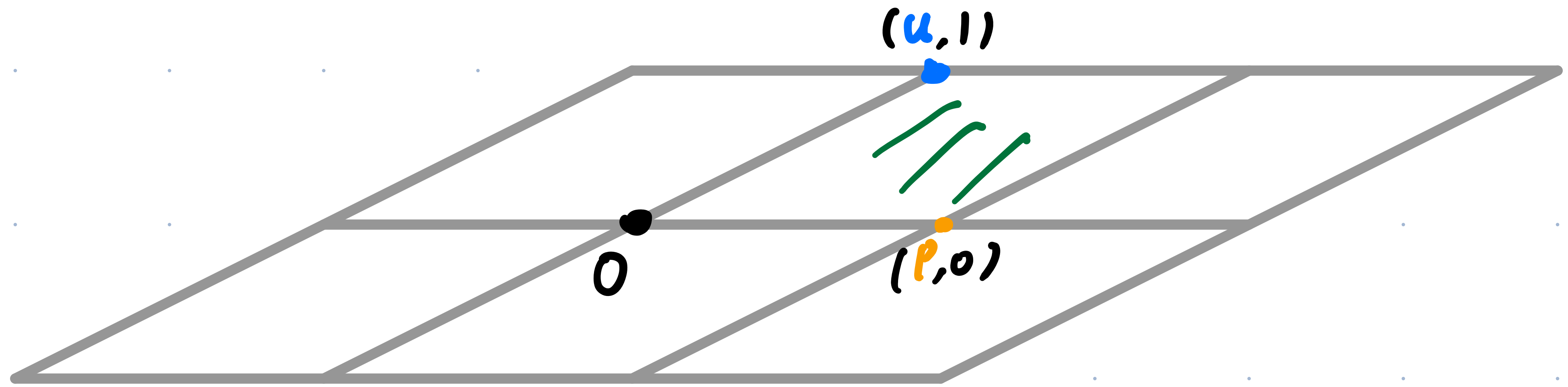
$$S = \{ (x, y) \in \mathbb{Z}^2 \mid x \equiv uy \mod p \}$$

$$x^2 \equiv u^2 y^2 \equiv -y^2 \mod p$$

Note that

$$S = \mathbb{Z}(u, 1) + \mathbb{Z}(p, 0)$$

So S = grid-point of a grid of parallelograms



Area of a parallelogram $= \begin{vmatrix} u & 1 \\ p & 0 \end{vmatrix} = p$

Put a circle of area $\cancel{4p}$ or $5p$ at O. Then Minkowski's theorem implies that there is a grid-point (x,y) inside the circle (including its edge) besides O.

Now we have :

(x, y) is a grid-point $\Rightarrow (x, y) \in S \Rightarrow x \equiv u y \mod p$

Note that $u^2 \equiv -1 \mod p$.

Hence $x^2 \equiv u^2 y^2 \equiv -y^2 \mod p$

$\Rightarrow \quad p \mid x^2 + y^2 \qquad ①$

(x, y) is contained in the circle $\Rightarrow x^2 + y^2 \leq \frac{\overset{5}{\cancel{4}}}{\pi} p < 2p \qquad ②$

$\pi > 2.5$

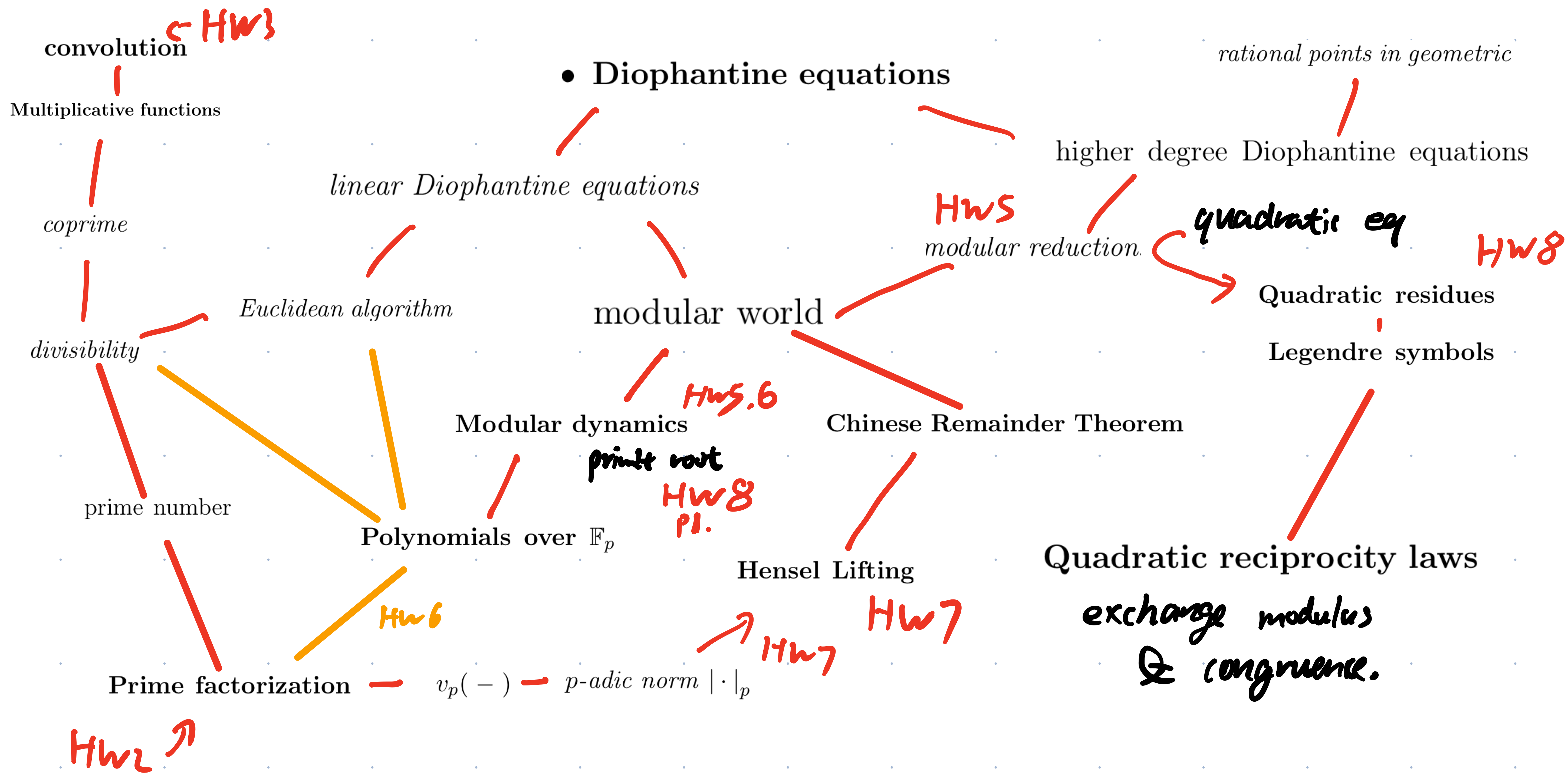
$(x, y) \neq 0 \quad \Rightarrow \quad x^2 + y^2 > 0 \qquad ③$

$① + ② + ③ \Rightarrow x^2 + y^2 = p$

证

Outline of Final

MATH 110 | Introduction to Number Theory | Fall 2022



The followings are topics in each lecture

Lecture 1: Euclidean algorithm

Lecture 2: GCD and the solvability of the linear Diophantine equation $ax + by = c$.

Lecture 3: LCM and the solution set of the homogeneous linear Diophantine equation $ax + by = 0$.

HW1

Lecture 4: General solutions of the linear Diophantine equation $ax + by = c$.

Lecture 5: Hasse diagram, prime numbers, coprime, and Prime Factorization.

Lecture 6: Unique Prime Factorization property, the function $V_p(-)$.

HW2

Lecture 7: Distributions of prime numbers, divisor set, and multiplicative functions.

HW3 convolution

Lecture 8: Multiplicative functions, Mersenne primes, rational numbers.

Lecture 9: Irrational number, algebraic number, and transcendental number.

Lecture 10: Diophantine approximation, Ford circles, and kiss of fractions.

Lecture 11: Dirichlet's approximation theorem and mediant of fractions.

HW4

Lecture 12: Pythagorean triples, rational points in circles, and modular world.

Lecture 13: Modular world and additive modular dynamics.

HW5

Lecture 14: Modular dynamics.

Lecture 15: Fermat's little theorem and primality testings.

Lecture 16: Similarity between additive modular dynamics and multiplicative modular dynamics, primitive roots.

HW8 P1

HW6

Lecture 17: primitive root theorem

Lecture 18: Polynomials mod p

Lecture 19: Polynomials mod p and Chinese remainder theorem

Lecture 20: Chinese remainder theorem Practice it by yourself !!

Lecture 21: Hensel's lemma HW7

Lecture 22: Quadratic residue

Lecture 23: Legendre symbols and Quadratic Reciprocity Law HW8

Prob 3.

Lecture 24-26: prove the Quadratic Reciprocity Law

Lecture 26-27: applications of Quadratic Reciprocity Law