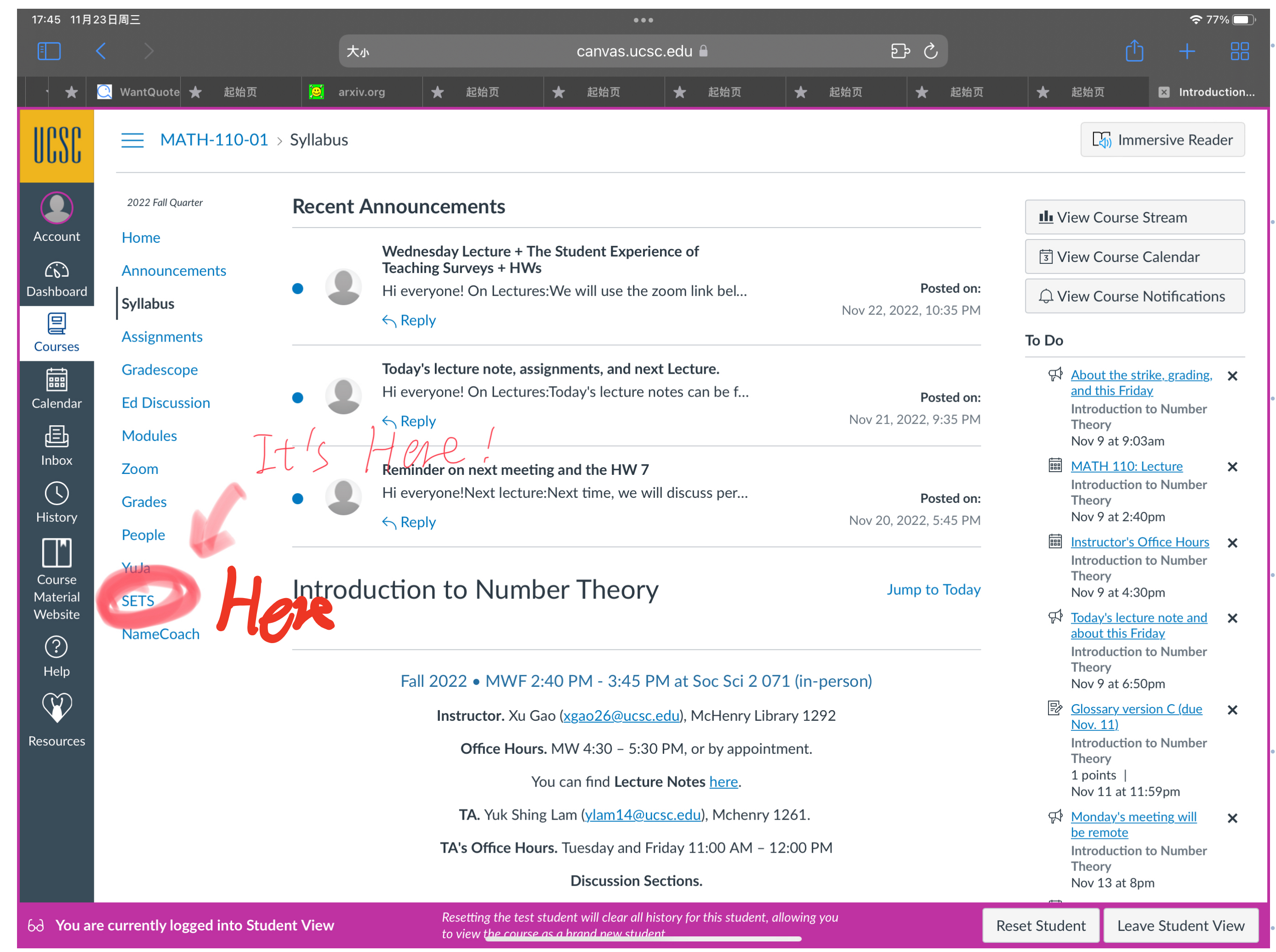
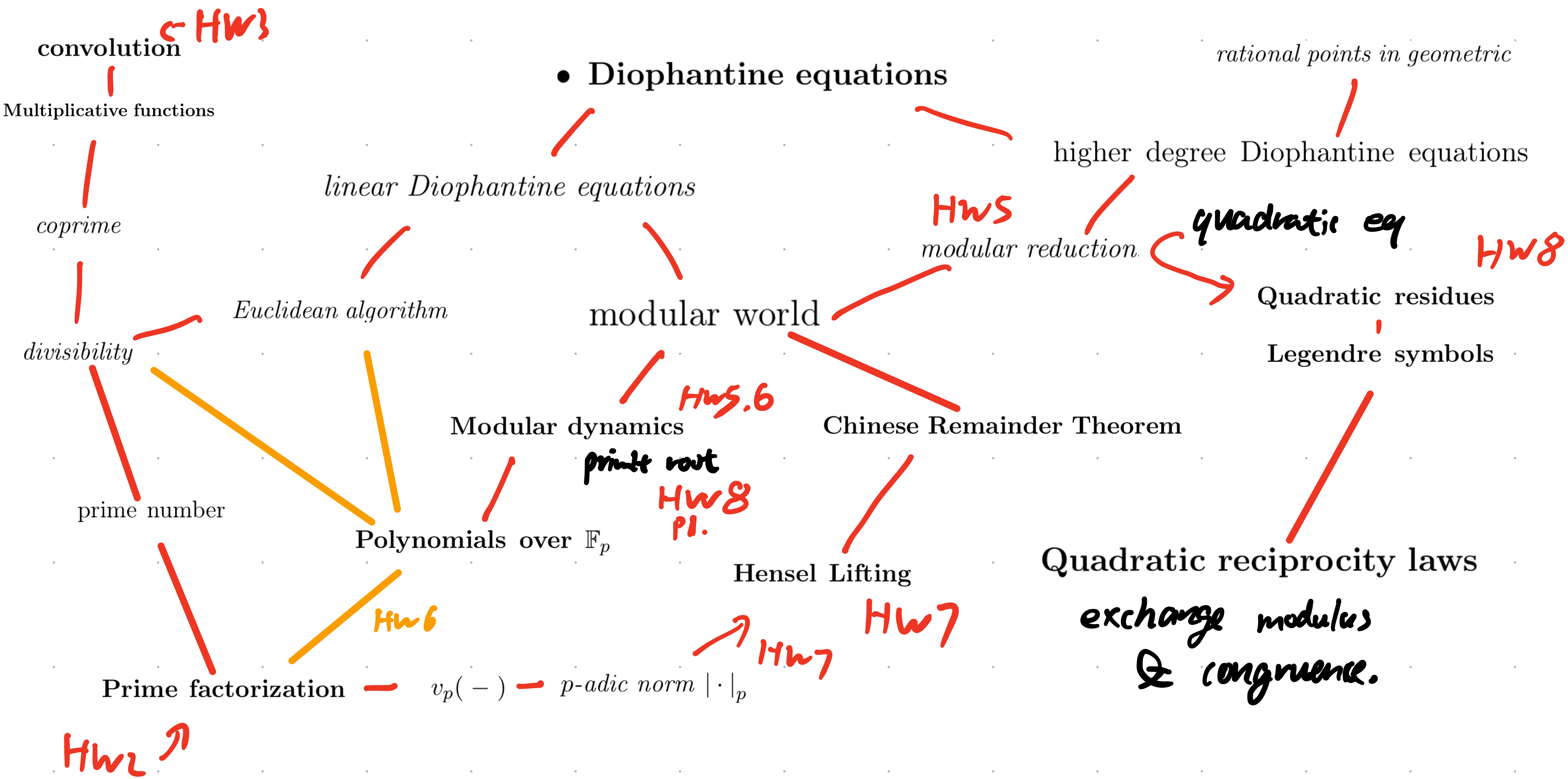
SETS:

- 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



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

Q1: Solve $x^2 \equiv 22 \mod 63$

Step 1: Prime factorization $63 = 7 \times 9$

Step 2: Solve $x^2 \equiv 22 \mod 63$

$\iff x^2 \equiv 22 \mod 7$ & $x^2 \equiv 22 \mod 9$

2.1) $x^2 \equiv 22 \mod 7$
$\equiv 1 \mod 7$
has solutions $x \equiv 1 \mod 7$
and $x \equiv 6 \mod 7$

2.2) $x^2 \equiv 22 \mod 9$
$\equiv 4 \mod 9$
has solutions $x \equiv 2 \mod 9$
and $x \equiv 7 \mod 9$

Step 3: Use CRT to combine the solutions.

$x \equiv 1 \bmod 7$ or $x \equiv 6 \bmod 7$

$x \equiv 2 \bmod 9$ or $x \equiv 7 \bmod 9$

$2 \times 2 = 4$ cases:

	1 mod 7	6 mod 7
2 mod 9	$1 \cdot (-3) \cdot 9 + 2 \cdot (4) \cdot 7 = 29$	$6 \cdot (-3) \cdot 9 + 2 \cdot (4) \cdot 7 = -106 \equiv 20$
7 mod 9	$1 \cdot (-3) \cdot 9 + 7 \cdot (4) \cdot 7 \equiv 43$	$6 \cdot (-3) \cdot 9 + 7 \cdot (4) \cdot 7 \equiv 34$

M = product of moduli

$M_i = M / m_i$ $\quad M = 63$

$m_1 = 7 \quad m_2 = 9$

$M_1 = 9 \quad M_2 = 7$

$N_1 M_1 + N_2 M_2 = 1$

$-3 \cdot 9 \quad 4 \cdot 7$

$x \equiv a_i \bmod m_i$ for all i

$a_1 = 1 \quad a_2 = 2$

$$x \equiv \sum a_i N_i M_i \bmod M$$

Ref lec 20 & 21

Only need the final answer being natural rep.

Q2: Solve $x^3+x^2+x+1 \equiv 0 \mod 27$

It is already a prime power. So No CRT.

Step 1 (Reduce to prime modulus)

$$x^3+x^2+x+1 \equiv 0 \mod 3$$

The solutions are : $\cancel{0}$ $\cancel{1}$ -1

Step 2 (Hensel's lifting)

First check $f'(a) \not\equiv 0 \mod 3$ $f'(x) = 3x^2+2x+1 \equiv 2x+1 \mod 3$

$$f'(-1) = 2\cdot(-1)+1 = -1 \not\equiv 0 \mod 3$$

Then we can lift it :

$$x_1 \equiv -1 \mod 3 \ \& \ f(x_1) \equiv 0 \mod 9.$$

$$\boxed{x_1 = -1 + 3\cdot t}$$

$x^3 + x^2 + x + 1$

$3x^2 + 2x + 1$

$$f(-1) + f'(-1)\cdot 3\cdot t \equiv 0 \mod 9$$

TWO WAYS TO find t:

① lifting of multiplicative inverse

in general, could be nonzero

$$0 + 2\cdot 3\cdot t \equiv 0 \mod 9$$

obtained by lift inverse of 2 mod 3 to mod 9.

$$3\cdot t \equiv \boxed{2^{-1}}\cdot 0 \mod 9$$

$$\equiv 0 \mod 9$$

② descend to mod 3 $p \mid f(a)$, $p \mid P$, $p \mid 0$

$$0 + 2\cdot t \equiv 0 \mod 3$$

9/3

just the inverse of 2 mod 3.

$$t \equiv \boxed{2^{-1}}\cdot 0 \mod 3$$

$$x_1 = -1 + 2 \cdot t = -1 \equiv 8 \mod 9$$

Let's lift $x_1 = 8$ to mod 27.

$x^3 + x^2 + x + 1$

$3x^2 + 2x + 1$

$$x_2 = 8 + 9 \cdot T$$

$$f(x_1) + f'(x_1) \cdot 9 \cdot T \equiv 0 \mod 27$$

$$8^3 + 8^2 + 8 + 1 + (3 \cdot 8^2 + 2 \cdot 8 + 1) \cdot 9 \cdot T \equiv 0 \mod 27$$

$$18 + 20 \cdot 9 \cdot T \equiv 0 \mod 27$$

① lift $20^{-1} \mod 9$ to mod 27

②

$$2 + 20 \cdot T \equiv 0 \mod 9$$

$$2 + 2T \equiv 0 \mod 9$$

$$T \equiv 8 \mod 9$$

$$x_2 = 8 + 9 \cdot 8$$

$$= 80 \mod 27$$

$$\equiv 26 \mod 27.$$

Q3: For which p, $2x^2 \equiv 5 \mod p$ has a solution?

$p=2$: $LHS \equiv 0$ $\quad 0 \not\equiv 5 \mod 2$ no sol.

p is odd.

$2x^2 \equiv 5 \mod p$ has a solution

$\Updownarrow$

$x^2 \equiv 2^{-1} \cdot 5 \mod p$ has a solution.

$\Updownarrow$

$\overline{2}^{-1} \cdot \overline{5}$ is a QR mod p

$\Updownarrow$

$$\left(\frac{2}{p}\right)^{-1} \cdot \left(\frac{5}{p}\right) = \left(\frac{2^{-1} \cdot 5}{p}\right) = \text{either } 0 \text{ or } 1$$

$\left(\frac{5}{p}\right)=1 \Leftrightarrow \left(\frac{p^*}{5}\right)=1 \Leftrightarrow p \equiv ? \mod 5$

$\left(\frac{2}{p}\right)^{-1} = \left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \mod 8$

either 0 $\Updownarrow$ $p \mid 5$ i.e. $p=5$

1 $\Updownarrow$ $\left(\frac{2^{-1} \cdot 5}{p}\right) = 1$

$\Phi(p) \ni g^e \longleftrightarrow \bar{e} \in \mathbb{Z}/_{p-1}$

$\uparrow$ primitive root.

$\overline{-1} \longleftrightarrow \frac{p-1}{2}$

Homework 8 (due Dec. 2)

MATH 110 | Introduction to Number Theory | Fall 2022

Problem 1. Let p be an odd prime. Recall that a primitive root modulo p is an integer g such that $p-1$ is the smallest positive integer e such that

$$g^e \equiv 1 \pmod{p}.$$

The map preserves the binary operation on $\mathbb{F}_p^\times$: multi, $\bar{1}$ on $\mathbb{Z}/_{p-1}$: add, $\bar{0}$

(a) (5 pts) Consider $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{\bar{0}\}$. Show that there is an *isomorphism* of groups (a bijective map preserving ~~addition,~~ multiplication, zero, ~~and~~ one) from $\mathbb{F}_p^\times$ to $\mathbb{Z}/(p-1)$. $g^e \mapsto \bar{e}$

Hint. First show that $\mathbb{F}_p^\times = \{g^e \mid 0 \leqslant e < p-1\}$, where g is a primitive root. (Why there is a primitive root?) 1. $x \in \mathbb{F}_p$ is a unit $\iff x \neq \bar{0}$ 2. By PRT, $\exists g$, $\ell(g) = \varphi(p)$

(b) (5 pts) Use a primitive root g to demonstrate that -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$.

$\exists x \in \mathbb{F}_p^\times$ s.t. $x^2 = \overline{-1} = g^{\frac{p-1}{2}}$, $x = g^e$ $\Updownarrow$ $e = \frac{p-1}{4}$

(c) (5 pts) Use a primitive root g to prove the *Wilson Theorem*: $(p-1)! \equiv -1 \pmod{p}$.

Hint. First show that $(p-1)! \equiv g^{1+2+\cdots+(p-2)} \pmod{p}$.

$(p-1)!$ prod of all elem in $\mathbb{F}_p^\times$ $\longleftrightarrow$ sum of all ele in $\mathbb{Z}/_{p-1}$ $0+1+\cdots+p-2$

$1+\cdots+p-2 = \frac{(p-2)(p-1)}{2}$

$\left(g^{\frac{p-1}{2}}\right)^{p-2}$ has to be -1

(d) (5 pts) Given a primitive root g, and an integer $a \in \Phi(p)$, prove that a is a quadratic residue modulo p if and only if $a \equiv g^e \pmod{p}$ for an even number e. Use this to prove the *Euler's Theorem on quadratic residues*:

$a = g^e$ is QR; $\exists x$ s.t. $x^2 = a$; $x = g^f$ $g^{2f} = g^e$ $2f \equiv e \bmod \varphi(p)$ even $\Uparrow$ force $p-1$ even

$$a \text{ is a quadratic residue} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

$g^{e\cdot\frac{p-1}{2}} = \left(g^{\frac{p-1}{2}}\right)^e = (-1)^e = \begin{cases} 1 & \text{even} \\ -1 & \text{odd} \end{cases}$

Problem 2 (10 pts)**.** Let p be an odd prime. Compute the Legendre symbols

$$\left(\frac{\frac{p-1}{2}}{p}\right) \quad \text{and} \quad \left(\frac{\frac{p+3}{2}}{p}\right) \left(\frac{2}{p}\right) = \left(\frac{p+3}{p}\right) = \left(\frac{3}{p}\right)$$

The results should be stated in language of congruence class of p modulo a certain modulus independent of p. Namely, the conditions in the results should be of the form:

$$p \equiv \underline{\qquad} \pmod{m},$$

where m is a modulus independent of p.

Hint. Use the complete multiplicativity of Legendre symbol.

Problem 3. Consider the polynomial $f(T) = T^2 + T + 1$. The purpose of this problem is to figure out for which prime p, $f(T)$ is irreducible modulo p.

(a) (3 pts) Show that $f(T)$ is irreducible modulo 2.

Hint. Use Problem 2 (a) from HW 6.

Hence, we may assume p is odd. In what follows, we keep this assumption.

(b) (3 pts) Find an integer polynomial of the form $(T+a)^2 \cancel{+} - q$ such that

$$f(T) \equiv (T+a)^2 \cancel{+} - q \pmod{p}.$$

Hint. Note that p is odd.

(c) (3 pts) Argue that $f(T)$ is irreducible if and only if q (the leftover term in 3.(b)) is a quadratic non-residue modulo p. $\Leftrightarrow \exists \alpha$ s.t. $f(\alpha) \equiv 0 \bmod p$

$\qquad = (\alpha + a)^2 - q \equiv 0 \bmod p$

Equivalently, $f(T)$ is irreducible if and only if

$$\left(\frac{q}{p}\right) = -1.$$

(d) (6 pts) Conclude the condition for $f(T)$ being irreducible modulo p in language of congruence of p modulo a certain modulus independent of p. Namely, the condition should be of the form:

$$p \equiv \underline{\qquad} \pmod{m},$$

where m is a modulus independent of p.