MATH 4573: PRACTICE FINAL PROBLEMS

INSTRUCTOR: TYLER GENAO

Here's the topics we've covered that can be addressed on the final exam.

- §2.8, primitive roots and power residues:
  - definition of a primitive root mod m;
  - a primitive root mod an odd prime power p^2 is a primitive root mod p^e, for all $e \geq 2$ ([NZM91, Theorem 2.40]);
  - definition of an n'th power residue mod m;
  - Euler's criterion for n'th power residues mod p.
- §4.1, the floor function:
  - basic properties of the floor function;
  - de Polignac's formula.
- §4.2, arithmetic functions:
  - mathematical definitions for $\phi(n), d(n), \sigma(n), \omega(n)$ and $\Omega(n)$ (if these appear on the final, I will describe them to you using *words,* e.g., $d(n)$ is the number of positive divisors of n);
  - multiplicativity of $d(n)$ and $\sigma(n)$;
  - if $f(n)$ is multiplicative, then so is $F(n) := \sum_{d|n} f(d)$.
- §4.3, the Möbius inversion formula:
  - definition of the Möbius function $\mu(n)$;
  - the Möbius inversion formula.

  §3.1, quadratic residues:
  - Euler's criterion when $n = 2$;
  - definition of quadratic residues and non-residues;
  - the Legendre symbol and its basic properties.
- §3.2, quadratic reciprocity:
  - the statement of quadratic reciprocity;
  - the supplemental laws of quadratic reciprocity, for $\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right)$.
- §3.3, the Jacobi symbol:
  - the Jacobi symbol and its basic properties;
  - quadratic reciprocity and its supplemental laws for the Jacobi symbol.
- §5.0, "introduction to Diophantine equations":
  - definition of a Diophantine equation;
  - definition of integral, rational and real solutions;
  - Showing integral solutions don't exist for some Diophantine equations by reducing them modulo primes p ("local considerations," see for example Exercise 3 and 4 in HW 8, or Exercise 7 in HW 9);
  - definition of plane curves in $\mathbb{R}^2$.
- §5.1, the equation $ax + by = c$:

  - statement of the linear Diophantine theorem ([NZM91, Theorem 5.1]);
  - algorithm to parametrize all integral solutions to a line, using the proof of the linear Diophantine theorem.
- §5.3, Pythagorean triples:
  - definition of Pythagorean triples and primitive solutions;
  - (I won't ask you to memorize the characterization for positive primitive Pythagorean triples).
- §5.6, rational points on curves:
  - nonsingular points;
  - algorithm for parametrizing rational points on nonsingular conics;
  - homogenizing and de-homogenizing polynomials;
  - turning an affine curve into a projective curve, and vice-versa;
  - points at infinity.
- §5.7: elliptic curves:
  - definition of a general elliptic curve, a projective elliptic curve and an elliptic curve in short Weierstrass form;
  - the group law on an elliptic curve;
  - torsion points on an elliptic curve.

1. Statements

Here are some statements for reference that will be included on the final exam.

1. **(Quadratic reciprocity):** if p, q are distinct odd primes, then

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}} \cdot \left(\frac{p}{q}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod 4 \textbf{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \pmod 4 \textbf{ and } q \equiv 3 \pmod 4. \end{cases}.$$

2. **(Euler's criterion for n'th power residues):** for $n, a, p \in \mathbb{Z}^+$ with p prime: if $\gcd(p, a) = 1$, then the congruence $x^n \equiv a \pmod p$ has a solution if and only if $a^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod p$, in which case it has $\gcd(n, p-1)$ solutions.

3. **(Formula for point sum):** let $E_{/\mathbb{Q}} : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve (in "normal Weierstrass form"). Then given two points $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{Q})$, if $x_1 \neq x_2$ then one has

$$P_1 \oplus P_2 := (x_3, y_3) = (m^2 - a - x_1 - x_2, -y_1 - m(x_3 - x_1)),$$

where m is the secant slope between P_1 and P_2.

Problem 1. Determine the number of solutions to the following congruences. You can assume that each modulus is prime.

a) $x^{12} \equiv 16 \pmod{17}$;
b) $x^4 \equiv 1 \pmod{163}$;
c) $x^{20} \equiv 2 \pmod{29}$;
d) $x^2 \equiv -1 \pmod{997}$;
e) $x^2 \equiv -5 \pmod{1009}$.

Problem 2.

a) Evaluate the sum

$$\sum_{n\geq 1} \mu(n!)$$

where $\mu\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ is the Möbius function.

b) Find the least positive integer n such that $d(n) = 6$, where $d(n)$ counts the number of positive divisors of n.

Problem 3. Parametrize all integral solutions to the following lines, if they exist.

a) $L_1 : 12x + 50y = 1$.

b) $L_2 : 15x + 7y = 111$.

Problem 4. This exercise concerns the arithmetic of the elliptic curve $E : y^2 = x^3 - 5x + 1$.

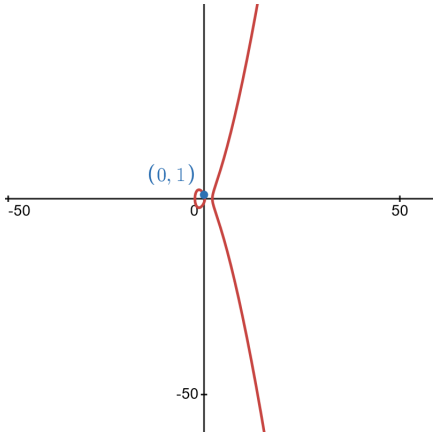

FIGURE 1. The elliptic curve $E : y^2 = x^3 - 5x + 1$.

a) We have the point $P = (0, 1) \in E(\mathbb{Q})$. Show that $2P := P \oplus P = \left(\frac{25}{4}, \frac{117}{8}\right)$.
b) Suppose that $\alpha \in \mathbb{R}$ satisfies

$$\alpha^3 - 5\alpha + 1 = 0.$$

Then $Q := (\alpha, 0) \in E(\mathbb{R})$. Show that $2Q := Q \oplus Q = O$, where $O := [0 : 1 : 0]$.

References

[NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th Ed., John Wiley & Sons, Inc., New York (1991).