SPRING 2025: MATH 540 HOMEWORK

Homework 1. Clark: 2.1, 2.6, 2.5, 2.8, 2.9.

Homework 2. Clark, 7.3, 9.1, 9.2, 9.3. For 9.1, use the Euclidean algorithm and reverse substitution, not Blankinship's method.

Homework 3. Stein, 1.3, 1.8, 1.12 and the following problem: Suppose d, a, b are integers such that $d = sa+tb$, for some $s, t \in \mathbb{Z}$. Show that $d = s'a + t'b$ if and only if $s' = s + c$ and $t' = t + d$, where $ca + db = 0$.

Bonus Problem 1. In the number system $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, show that if $3 = ab$, with $a, b \in \mathbb{Z}[\sqrt{-5}]$, then either $a = \pm 1$ or $b = \pm 1$. (2 points)

Homework 4. (1.) Find the LCM of 1215 and 4725; (2.) Prove item (iii) from the LCM Proposition given in the lecture of January 30; (3.) Find the addition and multiplication tables for the remainders of 6 and the remainders of 7;

Homework 5. (1.) Prove the following cancellation property. If $ca \equiv cb \bmod n$, and $\gcd(c, n) = 1$, then $a \equiv b \bmod n$. (2.) Find the elements of $\mathbb{Z}_{100}$ that have multiplicative inverses. (3). Calculate $\phi(4), \phi(9), \phi(25), \phi(47)$, where $\phi(n)$ is the Euler totient function. Can you make a conjecture for the value of $\phi(p^2)$, if p is prime? You can check guess on the internet.

Homework 6. 1. Use the formulas given in class to calculate the following values of the Euler totient function: $\phi(36)$; $\phi(900)$; $\phi(2^4 3^2 5^5 11^2)$.

2. For the function $f : \mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$ defined in class, $f(\tilde{i}) = (\bar{i}, \hat{i})$, where $n = ab$ and $\gcd(a, b) = 1$, write out all of the values of f to show that f is surjective, in the case $n = 15 = 3 \cdot 5$. Note that f establishes a one-to-one and onto correspondence between the elements of $\mathbb{Z}_{15}$ that have a multiplicative inverse and the elements of $\mathbb{Z}_3 \times \mathbb{Z}_5$ that have a multiplicative inverse.

Homework 7. 1. Verify Euler's theorem for $n = 7$, $n = 12$ and all $1 \leq a < n$ such that $\gcd(a, n) = 1$. Then verify Euler's product formula for $n = 48$ and 1025,

2. Calculate: (a) 1056^{3247} modulo 9 and (b) The one's digit for 246^{135}.

3. Verify Gauss's theorem for $n = 48, n = 124, n = 1000$.

Homework 8. 1. Prove the following properties of the Euler totient function:

(i) For $a, b > 0$ and $d := \gcd(a, b)$, $\phi(ab) = \phi(a)\phi(b) \cdot \frac{d}{\phi(d)}$

(ii) If $a \mid b$, then $\phi(a) \mid \phi(b)$.

2. Calculate $\tau(360)$ and $\sigma(360)$.

Homework 9. 1. For the set $\{(a, b) \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}$ discussed in class, with equivalence classes denoted $[(a, b)]$ show that multiplication of equivalence classes given by $[(a, b)] \cdot [(c, d)] = [(ad+bc, bd)]$ is well defined.

2. Find all solutions to the linear congruences $6x \equiv 21 \bmod 27$, both in $\mathbb{Z}_{27}$ and in $\mathbb{Z}$.

Homework 10. Solve the following systems of congruences:

$$x \equiv 1 \bmod 5 \qquad 2x \equiv 1 \bmod 5$$
$$x \equiv 2 \bmod 7 \qquad 3x \equiv 2 \bmod 7$$
$$x \equiv 3 \bmod 11 \qquad 8x \equiv 3 \bmod 11$$

$$x \equiv 2 \bmod 11$$
$$x \equiv 4 \bmod 12$$
$$x \equiv 6 \bmod 13$$
$$x \equiv 5 \bmod 17.$$

Homework 11. Stein, Section 2.6: 11, 13, 23, 25a, 27a.

Bonus Problem. For $n \geq 1$ give, with proof, a complete description of the complex numbers that are primitive nth roots of unity. (5 points)

HW 12. Work the following problems.

(i) Find the roots of $f(x) = 3x^2 + 4x + 4 \bmod 11$.
(ii) Give an example of a quadratic polynomial in $\mathbb{Z}[x]$ that does not have a root mod 11.
(iii) Show that a quadratic residue mod p cannot be a primitive root of 1 mod p (for p an odd prime).

Homework 13. Stein, Section 4.6: 1, 3, 5.

Bonus Problem. Stein, Section 4.6: 6. (10 points)

Homework 14. Stein, Section 4.6: 8, 9.

Bonus Problem. From Lecture 14, prove that (2) and (2') are equivalent and (3) and (3') are equivalent. (6 points)

Homework 15. 1. Find all primes primes $p \leq 37$ such that $(\frac{5}{p}) = 1$.

2. Give an example to show that $(\frac{a}{n}) = 1$ need not imply that a is a quadratic residue mod n. Here $(\frac{a}{n})$ denotes the Jacobi symbol.

3. Assuming $\gcd(a, n) = 1 = \gcd(b, n)$, prove the following properties of the Jacobi symbol.

(i) If $a \equiv b \bmod n$, then $(\frac{a}{n}) = (\frac{b}{n})$.
(ii) $(\frac{ab}{n}) = (\frac{a}{n}) \cdot (\frac{b}{n})$.

Homework 16. 1. Verify Gauss' Lemma for $(\frac{11}{13})$.

2. Use Gauss' Lemma to prove the cases $p = 8k + 7$ and $p = 8k + 5$ of quadratic reciprocity for $(\frac{2}{p})$.

Homework 17. 1. Use the law of quadratic reciprocity to show that $(\frac{3}{p}) = \begin{cases} 1, & \text{if } p \equiv \pm 1, \bmod 12 \\ -1, & \text{if } p \equiv \pm 5 \bmod 12. \end{cases}$

2. Verify the Numerical Lemma from Lecture 17 directly (by calculating both sides of the equation), for $p = 7, q = 11$, and also by counting the number of lattice points above and below the line, as given in Lecture 17.

Homework 18. 1. Give an example showing that the quotient and remainder found in the division algorithm over the Gaussian integers need not be unique.

2. Find a GCD for $u = 11 + 16i$ and $v = 10 + 11i$ in the Gaussian integers, and write it as a Gaussian integer combination of u and u, *ala* Bezout's principle.

Homework 19. Find prime factorization in the Gaussian integers for $6 + 6i$, $10 + 15i$, $100 + 20i$.

Homework 20. Stein, Section 5.8: 8, 9, 11.

Homework 21. 1. Verify Jacobi's formula for $n = 100$.

2. Verify the following properties about Pythagorean triples x, y, z. These show that 3, 4, 5 are lurking around all primitive Pythagorean triples.

(i) Exactly one of x, y, z is divisible by 5.
(ii) If the triple is primitive, either x or y is divisible by 3.
(iii) At least one of x, y, z is divisible by 4.

Homework 22. 1. Show that if a and b are integers, then the arithmetic progression $a, a + b, a + 2b, \ldots$ contains an arbitrary number of consecutive composite terms.

2. Show that if a and b are positive integers, then $a^2 \mid b^2$ implies $a \mid b$.

3. Show that if $a, b,$ and c are positive integers with $\gcd(a, b) = 1$ and $ab = c^n$, then there are positive integers d and e such that $a = d^n$ and $b = e^n$.

Homework 23. 1. Calculate $\Phi_8(x), \Phi_{12}(x), \Phi_{24}(x)$.

2. Follow the proof of the theorem from the lecture of May 1 to find the ten primes in the arithmetic progression $\{6t + 1\}_{t \geq 1}$. You may use a calculator or computer.