Math 104A - Additional Practice Problems for Final Exam

Topics:

(1) Prime factorization over the integers and in arbitrary domains. Prime versus irreducible. Euclidean domains, UFDs.
(2) Greatest common divisor. Euclid’s algorithm. Linear diophantine equations.
(3) Chinese Remainder Theorem and linear systems of equations.
(4) Higher degree congruences, in particular quadratic congruences. Lagrange’s theorem modulo primes. Taylor’s theorem and congruences modulo powers of primes.
(5) The ring \( \mathbb{Z}_m \). Units. Inverses.
(6) Euler’s function. Multiplicative functions.
(7) Euler and Fermat’s Theorems. Wilson’s theorem.
(9) Exponential congruences. Finding \( n \)th roots modulo primes or powers of primes.
(10) Quadratic residues. Legendre symbol.

Practice problems.

1. Consider the ring \( R = \mathbb{Z}[\sqrt{-37}] \). Is 2 irreducible in \( R \)? Is 2 prime in \( R \)? Is \( R \) an UFD? Is \( R \) an Euclidean domain?

2. (i) For each fixed integer \( m \), write down the general solution to the equation

\[
71x + 50y = m.
\]

(ii) Find the inverse of 50 in \( \mathbb{Z}_{71} \).

(iii) How many units are there in the ring \( \mathbb{Z}_{50} \times \mathbb{Z}_{71} \)?

3. Solve the system of linear congruences

\[
5x \equiv 7 \pmod{24}, \quad x \equiv 3 \pmod{50}, \quad 2x \equiv 1 \pmod{45}.
\]

4. (i) Solve the quadratic congruence \( 2x^2 - x - 25 \equiv 0 \pmod{19^2} \).

(ii) Solve the congruence \( x^{421} + x^{44} + 5 \equiv 0 \pmod{7^2} \).

5. Let \( p > 2 \) be prime. Solve the congruence

\[
x^{p^2} - px^2 - 1 \equiv 0 \pmod{p^3}.
\]
6. Let $f : \mathbb{N} \rightarrow \mathbb{R}$ be a multiplicative function. Let
\[
g(n) = \sum_{d|n, d>0} f(d).
\]
Show that $g$ is also multiplicative.

7. 
   (i) Find the last three digits of $7^{1999}$.
   (ii) What is the smallest integer $m$ such that for all $(a, 231) = 1$, we have $a^m \equiv 1 \mod 231$?

8. 
   (i) Find a primitive root modulo 19. List all the other primitive root modulo 19.
   (ii) Find a primitive root modulo $2 \cdot 19^e$. How many primitive roots modulo $2 \cdot 19^e$ are there?
   (iii) List all the cubic residues modulo 19.

9. How many solutions do the following congruences have?
   (i) $x^2 \equiv -1 \mod 365$;
   (ii) $x^2 \equiv -1 \mod 244$;
   (iii) $x^4 \equiv 1 \mod 2^e \cdot 7^f$;
   (iv) $x^{16} \equiv -1 \mod p$ for $p$ prime. Discuss depending on the class of $p$ modulo 32.
   (v) $x^{12} \equiv 16 \mod 17$;
   (vi) $x^{20} \equiv 13 \mod 17$;
   (vii) Solve the congruence $3^{4x+1} \equiv 1 \mod 49$.

10. Show that for all primes $p$, and for all integers $m$, we have
\[
\sum_{a=0}^{p-1} \left( \frac{ma}{p} \right) = 0.
\]

11. Show that $n$ does not divide $2^n - 1$, if $n > 1$.
   
   *Hint: take $p$ the smallest prime dividing $n$. What can the order of $2$ modulo $p$ possibly be?*

12. Let $p$ be a prime. Find the product of all nonzero cubic residues modulo $p$. 