Math 115 - Midterm 1+2 Definitions

1. The product of sets $A \times B$ is the Cartesian product of the sets, where $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

2. A relation on a set A is a subset of $A \times A$. Elaborately, a relation on a set A takes two values from A and puts them into a class based on how they are compared.

3. A relation is reflexive if for any $a \in A$, aRa, symmetric if $aRb \implies bRa$, and transitive if $aRb \wedge bRc \implies aRc$, where $b, c \in A$.

4. A relation on a set A is an equivalence relation if it is reflexive, symmetric, and transitive. An equivalence class of an element $a \in A$ is the set $\{x \in A \mid a \sim x\}$, which is the set of all members that are in a's equivalence class.

5. A partition of a set A is a collection of disjoint subsets of A (with each subset nonempty) such that their union is A.

6. a and b are relatively prime if $\gcd(a, b) = 1$.

7. The integers $b_1, \ldots, b_n$ are relatively prime if $\gcd(b_1, \ldots, b_n) = 1$. They are pairwise relatively prime if $\gcd(b_i, b_j) = 1$ for all $i \neq j$.

8. A prime number is an integer at least two whose factors are 1 and itself. A composite number is a number that isn't prime.

9. The prime factorization of a number n is denoted $\prod_p p^{\alpha(p)}$, where this product symbolizes the product of all primes and the function α returns the exponent of a prime when considering that prime as its input.

10. A congruence class (modulo m) is a set of all integers that are congruent modulo m.

11. A complete residue system (modulo m) is a set of integers $r_1, \dots, r_n$ such that any integer x is congruent modulo m to exactly of the r_i's.

12. A reduced residue system (modulo m) is a set of integers $s_1, \dots, s_k$ coprime to m such that any integer coprime to m is congruent modulo m to exactly one of the s_i's.

13. Euler's totient function, $\phi(m)$, returns the number of elements in a reduced residue system modulo m. Equivalently, $\phi(m)$ is the number of integers t, with $0 < t \leq m$, such that t is coprime to m.

14. Consider the integers modulo m. Then, take the integer a in modulo m. Then, a has a unique inverse (modulo m) a^{-1} such that $aa^{-1} \equiv 1 \pmod{m}$.

15. A Gaussian integer is a complex number of the form $a + bi$, where $a, b \in \mathbb{Z}$.

16. $\mathbb{Z}[x]$ is the set of all polynomials with integer coefficients.

17. The number of solutions to the congruence $f(x) \equiv g(x) \pmod{m}$ is the number of congruence classes that satisfy $f(x) - g(x) \equiv 0 \pmod{m}$.

18. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, with $a_i \in \mathbb{Z}$ for all i. The degree of the congruence $f(x) \equiv 0 \pmod{m}$ is the highest value of i such that $m \nmid a_i$, and undefined if $m \mid a_i$ for all i. To find the degree of the congruence $f(x) = g(x) \pmod{m}$ (with $f, g \in \mathbb{Z}[x]$), find the degree of $(f - g)(x) \equiv 0 \pmod{m}$.

19. A polynomial-time algorithm is an algorithm whose run time is a polynomial function of the length of its input.

20. A weak probable prime to the base a is a number $p > 1$ that satisfies $a^{p-1} \equiv 1 \pmod{p}$. A weak pseudoprime to the base a is a number $p > 1$ that satisfies $a^{p-1} \equiv 1 \pmod{p}$ but p is composite.

21. Consider the following algorithm:

    (a) Find j and d odd such that $m - 1 = 2^j d$.

    (b) If $a^d \equiv \pm 1 \pmod{m}$, then m is a strong probable prime, stop.

(c) Square a^d to get a^{2d}. If $a^{2d} \equiv 1 \pmod{m}$, then m is composite. If $a^{2d} \equiv -1 \pmod{m}$, then m is a strong probable prime, stop.

(d) Repeat this procedure for the list $a^{4d}, \ldots, a^{2^{j-1}d}$.

(e) If the procedure has not yet terminated, m is composite.

If the test is inconclusive, then m is composite. m is a strong pseudoprime to the base a if the test with m is conclusive but m is both odd and composite.

22. A Carmichael number is a composite number m which is a weak pseudoprime to the base a for all integers a coprime to m.

23. p^α exactly divides n (denote: $p^\alpha \mid\mid n$) if $p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$.

---

24. **Root of $f \in \mathbb{Z}[x]$ modulo m.** Let $f \in \mathbb{Z}[x]$ and let $m \in \mathbb{Z}_{>0}$. Then, a root of f modulo m is an integer a such that $f(a) \equiv 0 \pmod{m}$.

25. **Monic Polynomial.** A polynomial in $\mathbb{C}[x]$ (or $\mathbb{Z}[x]$) is monic if (it is nonzero) its leading coefficient is 1.

26. **$\mathbb{Z}/m\mathbb{Z}$.** This is the set of congruence classes modulo m.

27. $(\mathbb{Z}/m\mathbb{Z})^*$ This set is defined to be the set $\{\tilde{a} \in \mathbb{Z} : \gcd(a, m) = 1\}$. This set is well-defined and contains $\phi(m)$ elements.

28. **Order of a modulo m.** Let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}_{>0}$ with $\gcd(a, m) = 1$. Then the order of a modulo m is the smallest integer $h > 0$ such that $a^h \equiv 1 \pmod{m}$. If $\gcd(a, m) \neq 1$, then the order of a modulo m is undefined.

29. **Primitive root modulo m.** A primitive root modulo m is an integer g whose order modulo m is $\phi(m)$.

30. **Quadratic residue modulo m.** Let $m \in \mathbb{Z}_{>0}$. A quadratic residue modulo m is an integer a coprime to m such that $x^2 \equiv a \pmod{m}$ has a solution.

31. **Quadratic non-residue modulo m.** Let $m \in \mathbb{Z}_{>0}$. A quadratic non-residue modulo m is an integer a coprime to m such that $x^2 \equiv a \pmod{m}$ does not have a solution.

32. **Legendre Symbol, $\left(\frac{a}{p}\right)$.** Let $a \in \mathbb{Z}$. Then, $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue modulo p, -1 if a is a quadratic non-residue modulo p, and 0 if $p \mid a$.

33. **Jacobi Symbol, $\left(\frac{P}{Q}\right)$.** Let Q be an odd positive integer with prime factors $Q = q_1 \cdot \cdots \cdot q_s$, where all the q_i are odd primes, not necessarily distinct. Then, the Jacobi Symbol $\left(\frac{P}{Q}\right)$ is defined by:

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right)$$

where $\left(\frac{P}{q_j}\right)$ is the Legendre Symbol.

34. **Binary Quadratic Form.** A binary quadratic form is a polynomial of the form $ax^2 + bxy + cy^2$, where x, y are the variables, and a, b, c are the coefficients.

35. **Binary Quadratic Form represents n.** A binary quadratic form $f = f(x, y)$ represents an integer n if $f(x_0, y_0) = n$ for some $x_0, y_0 \in \mathbb{Z}$ with $(x_0, y_0) \neq (0, 0)$.

36. **Binary Quadratic Form properly represents n.** The binary quadratic form $f = f(x_0, y_0)$ properly represents n if $f(x_0, y_0) = n$ with $x_0, y_0 \in \mathbb{Z}$ relatively prime.

37. **Discriminant of a binary quadratic form.** The discriminant of a binary quadratic form $ax^2 + bxy + cy^2$ is the quantity $d = b^2 - 4ac$.

38. **Types of binary quadratic forms.** A binary quadratic form $f(x, y)$ is:

    (a) indefinite if it takes on both positive and negative values.

    (b) positive semidefinite if $f(x_0, y_0) \geq 0$ for all x_0, y_0.

    (c) positive definite if $f(x_0, y_0) > 0$ for all x_0, y_0 with $(x_0, y_0) \neq (0, 0)$.

(d) negative semidefinite if $f(x_0, y_0) \leq 0$ for all x_0, y_0.

(e) negative definite if $f(x_0, y_0) < 0$ for all x_0, y_0 with $(x_0, y_0) \neq (0, 0)$.

(f) definite if it is positive definite or negative definite.

(g) semidefinite if positive semidefinite or negative semidefinite.

(note: we let $x_0, y_0 \in \mathbb{R}, \mathbb{Q}, \mathbb{Z}$).

39. **T_M, where M is a 2x2 matrix.** Given a 2x2 matrix M, let $T_M : \mathbb{R}^2 \to \mathbb{R}^2$ be the function $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto M \begin{pmatrix} x \\ y \end{pmatrix}$. In other words, if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $T_M \begin{pmatrix} x \\ y \end{pmatrix} = (ax + by, cx + dy)$.

40. **Modular group, Γ.** The modular group Γ is the set $\Gamma = \{$2x2 matrices with integer entries and determinant 1$\}$.

41. **Determinant of a matrix M.** If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then the determinant of M is given by $\det M = ad - bc$.

42. **M takes f to g.** A matrix $M \in \Gamma$ takes f to g (where f and g are forms) if $f \circ T_M = g$.

43. **Equivalent Forms.** The forms f and g are equivalent if $\exists M \in \Gamma$ that takes f to g.

44. **Reduced binary quadratic form.** Let $f(x, y) = ax^2 + bxy + cy^2$ be a form whose discriminant is not a perfect square. Then, f is reduced if $-|a| < b \leq |a| < |c|$ or $0 \leq b \leq |a| = |c|$.