

## 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  $b_1, \dots, b_n$  are relatively prime if  $\gcd(b_1, \dots, b_n) = 1$ . 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  $\alpha$  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 one 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  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ , 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  $f(x) \equiv g(x) \pmod{m}$  (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  $a^{4d}, \dots, a^{2^{j-1}d}$ .
- (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.  $p^\alpha$  exactly divides  $n$  (denote:  $p^\alpha \parallel n$ ) if  $p^\alpha \mid n$  but  $p^{\alpha+1} \nmid n$ .

24. ADD MIDTERM 2 DEFINITIONS FROM HERE ONWARDS