CSE390D—Introduction to Discrete Math
Final Cheat Sheet

Ways to express the conditional statement p → q:

if p, then q	p implies q
if p, q	p only if q
p is sufficient for q	a sufficient condition for q is p
q if p	q whenever p
q when p	q is necessary for p
a necessary condition for p is q	q follows from p
q unless ¬p	

Definition: The integer n is even if there exists an integer k such that n = 2k, and n is odd if there exists an integer k such that n = 2k + 1. (Note that an integer is either even or odd, and no integer is both even and odd.)

Definition: If a and b are integers with a ≠ 0, we say that a divides b if there is an integer c such that b = ac. When a divides b we say that a is a factor of b and that b is a multiple of a. The notation a | b denotes that a divides b.

Theorem: Let a, b, and c be integers. Then
- if a | b and a | c, then a | (b + c);
- if a | b, then a | bc for all integers c;
- if a | b and b | c, then a | c.

Theorem—The Division Algorithm: Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that a = dq + r.

Definition: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides a - b. We use the notation a ≡ b (mod m) to indicate that a is congruent to b modulo m.

Theorem: Let m be a positive integer. If a ≡ b (mod m) and c ≡ d (mod m), then:

a + c ≡ b + d (mod m)   and   ac ≡ bd (mod m)

Definition: A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

Theorem—The Fundamental Theorem of Arithmetic: Every positive integer greater than 1 can be written uniquely as a prime or as a product of two or more primes where the prime factors are written in order of nondecreasing size.

Definition: An equivalence relation is reflexive, symmetric, and transitive.

Definition: A partial ordering is reflexive, antisymmetric, and transitive.

Definition: A total ordering is one where for every pair of values (a, b) in the domain, either (a, b) is in the relation or (b, a) is in the relation.

```
counting summary (choosing r items from a set of n)
                 w/o repetition              with repetition
     ordered       P(n, r) = n!/(n-r)!        n^r
     unordered     C(n, r) = n!/(r!(n-r)!)    (n+r-1)!/(r!(n-1)!)


     indistinguishable items (n1, n2, ..., nk):
     C(n, n1) * C(n-n1, n2) * ... C(nk, nk)
     = n! / (n1! * n2! * ... * nk!)
```

Bayes' Theorem

$$p(F \mid E) = \frac{p(E \mid F)p(F)}{p(E \mid F)p(F) + p(E \mid \bar{F})p(\bar{F})}$$

Principle of Inclusion/Exclusion

$$|A1 \cup A2| = |A1| + |A2| - |A1 \cap A2|$$

Conditional Probability

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)}$$

Test for Independent Events

$$p(E \cap F) = p(E)p(F)$$