CSE390D—Introduction to Discrete Math
Final Cheat Sheet

Ways to express the conditional statement $p \rightarrow q$:

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 $\neg p$	

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 $a \neq 0$, 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 $a \mid b$ denotes that a divides b.

Theorem: Let a, b, and c be integers. Then

- if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
- if $a \mid b$, then $a \mid bc$ for all integers c;
- if $a \mid b$ and $b \mid c$, then $a \mid c$.

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 $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m.

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}$$

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

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