Instructor: Leo Goldmakher

Williams College
Department of Mathematics and Statistics

MATH 200 : DISCRETE MATH

Results proved in class

[1] *Proposition.* The n^{th} triangular number (denoted T_n) is $\frac{n(n+1)}{2}$. (Two proofs.)

[2] *Theorem.* $\sqrt{2}$ is irrational (two proofs, both using the well-ordering principle).

[3] *Lemma.* Every integer $n \geq 2$ has a prime factor.

[4] *Theorem.* There are infinitely many primes.

[5] *Theorem.* A conditional and its contrapositive are logically equivalent.

[6] *Proposition.* Given $n \in \mathbb{Z}$. Then $n^2 - 1$ is a perfect square if and only if $n = \pm 1$.

[7] *Proposition.* The function $f : \mathbb{Z}_{>0}^2 \to \mathbb{Z}_{>0}$ defined by $(x, y) \mapsto 2^x 3^y$ is injective, but not surjective.

[8] *Proposition.* $\mathbb{Q}_{>0}$ is countable.

[9] *Theorem.* The set $(0, 1)$ is uncountable.

[10] *Theorem.* Given any set S, the cardinality of its power set $\mathcal{P}(S)$ is strictly larger than that of S.

[11] *Proposition.* $(0, 1) \approx (-1, 1)$.

[12] *Theorem.* $(0, 1) \approx \mathbb{R}$. (A visualization with explanation suffices for this one.)

[13] *Proposition.* In any set of 51 distinct integers from $\{1, 2, \ldots, 100\}$, two must be consecutive.

[14] *Proposition.* In any set of five points on the surface of a sphere, four of them must lie on a single hemisphere.

[15] *Theorem.* (Induction) If $\mathcal{A} \subseteq \mathbb{Z}_{>0}$ satisfies

(i) $1 \in \mathcal{A}$ and

(ii) $n \in \mathcal{A} \implies n + 1 \in \mathcal{A}$,

then $\mathcal{A} = \mathbb{Z}_{>0}$.

[16] *Proposition.* $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2$ for any positive integer n.

[17] *Theorem.* (Strong Induction) If $\mathcal{A} \subseteq \mathbb{Z}_{>0}$ satisfies

(i) $1 \in \mathcal{A}$ and

(ii) $\{k \in \mathbb{Z}_{>0} : k < n\} \subseteq \mathcal{A} \implies n \in \mathcal{A}$,

then $\mathcal{A} = \mathbb{Z}_{>0}$.

[18] *Theorem.* Every positive integer has a unique binary expansion.

[19] *Theorem.* The n^{th} Fibonacci number is

$$f_n = (-1)^n \frac{\beta^{n+1} - \alpha^{n+1}}{\beta - \alpha}$$

where α, β are the roots of $1 - x - x^2$.

[20] *Proposition.* If f_n denotes the n^{th} Fibonacci number, then $\lim\limits_{n\to\infty} \frac{f_{n+1}}{f_n} = \frac{1+\sqrt{5}}{2}$.

[21] *Quotient-Remainder Theorem.* Given $a, n \in \mathbb{Z}$ with $n > 0$, there exist unique choices of $q, r \in \mathbb{Z}$ such that $a = qn + r$ and $0 \le r < n$.

[22] *Proposition.* Given $a \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, and $r \in \{0, 1, 2, \ldots, n-1\}$. Then $a \pmod{n} = r$ iff $n \mid a - r$.

[23] *Proposition.* Consider the a^{th} row of the multiplication table $\pmod{p}$. The sum of the k^{th} and $(p-k)^{\text{th}}$ entries is p.

[24] *Proposition.* The following are equivalent:

(i) *The Sudoku Rule*: Every row and column of the $\pmod{p}$ multiplication table contains each of the numbers $\{1, 2, \ldots, p-1\}$ exactly once.

(ii) If $a \not\equiv 0 \pmod{p}$ and $ax \equiv ay \pmod{p}$, then $x \equiv y \pmod{p}$.

(iii) If $k\ell \equiv 0 \pmod{p}$, then one of k or ℓ must be $\equiv 0 \pmod{p}$.

(iv) If $p \mid k\ell$, then $p \mid k$ or $p \mid \ell$.

[25] *Theorem.* If p is prime and k and ℓ are positive integers such that $p \mid k\ell$, then $p \mid k$ or $p \mid \ell$.

[26] *Fermat's Little Theorem.* Given a prime p, $a^{p-1} \equiv 1 \pmod{p}$ for every $a \not\equiv 0 \pmod{p}$.

[27] *Newton's Binomial Theorem.* We have

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$

where $\binom{n}{k}$ denotes the number of ways of picking k objects out of a set of n objects.

[28] *Proposition.* $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

[29] *Theorem.* Given a finite set S, let $\mathcal{P}(S)$ denote its power set. Then $|\mathcal{P}(S)| = 2^{|S|}$.

[30] *Proposition.* The number of optimal routes from the origin to a point (m, n) on the integer grid is $\binom{m+n}{m}$.

[31] *Proposition.* There's no way to cross each of the seven bridges of Königsberg exactly once.