CS1231 Discrete Structures

Number Theory

Definitions & Theorems

Bounds

- **Def 4.3.1 [Lower Bound]**: $S \subseteq \mathbb{Z}, b \in \mathbb{Z}$
  b is a lower bound for $S \iff \forall x \in S, b \leq x$
  b is an upper bound for $S \iff \forall x \in S, b \geq x$

- **Thm 4.3.2 [Well Ordering Principle]**: $S \subseteq \mathbb{Z}$
  S is non-empty and S has a lower bound
  $\implies S$ has a least element
  S is non-empty and S has an upper bound
  $\implies S$ has a greatest element

- **Prop 4.3.3 [Uniqueness of least element]**:
  $S \subseteq \mathbb{Z}$
  S has a least element $\implies$ the least element is unique

- **Prop 4.3.4 [Uniqueness of greatest element]**:
  $S \subseteq \mathbb{Z}$
  S has a greatest element $\implies$ the greatest element is unique

Parity

- **Def 1.6.1 [Even and Odd]**: $n \in \mathbb{Z}$
  n is even $\iff \exists k \in \mathbb{Z}$ such that $n = 2k$
  n is odd $\iff \exists k \in \mathbb{Z}$ such that $n = 2k+1$

- **Prop 4.6.4 (Epp) [Square number]**: $n \in \mathbb{Z}$
  n^2 is even $\implies n$ is even

Divisibility & Primality

- **Def 1.3.1 [Divisibility]**: $n, d \in \mathbb{Z}$
  $d \mid n \iff \exists k \in \mathbb{Z}$ such that $n = dk$

- **Thm 4.3.1 (Epp)**: $a, b \in \mathbb{Z}^+$
  $a \mid b \implies a \leq b$

- **Thm 4.3.3 (Epp) [Transitivity]**: $a, b, c \in \mathbb{Z}$
  $a \mid b$ and $b \mid c \implies a \mid c$

- **Thm 4.1.1 [Linear combination]**: $a, b, c \in \mathbb{Z}$
  $a \mid b$ and $a \mid c \implies \forall x, y \in \mathbb{Z}, a \mid (bx + cy)$

- **Def 4.2.1 [Prime number]**: $n \in \mathbb{Z}$
  n is prime $\iff n > 1$ and $\forall r, s \in \mathbb{Z}^+, (n = rs \implies r = n$ or $s = n)$
  n is composite $\iff \exists r, s \in \mathbb{Z}^+,$ such that $n = rs$ and $1 < r < n$ and $1 < s < n$

- **Prop 4.2.2**: p, p' is prime
  $p \mid p' \implies p = p'$

- **Prop 4.7.3 (Epp)**: p is prime, $a \in \mathbb{Z}$
  $p \mid a \implies p \nmid (a+1)$

- **Thm 4.7.4 (Epp)**: The set of primes is infinite

- **Thm 4.2.3**: p is prime, $x_i \in \mathbb{Z}$
  $p \mid x_1 x_2 \ldots x_n \implies p \mid x_i$ for some i

- **Thm 4.3.5 (Epp) [Unique Prime Factorization / Fundamental Theorem of Arithmetic]**:
  $1 < n \in \mathbb{Z}$
  $n = \prod_{i=1}^{k} p_i^{e_i}$ uniquely, for some $k > 1$, ordered primes p_i, and $e_i \in \mathbb{Z}^+$

- **Thm 4.4.1 [Quotient-Remainder Theorem]**:
  $a \in \mathbb{Z}, b \in \mathbb{Z}^+$
  $\exists! q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$

- **Def 4.5.1 [Greatest Common Divisor (GCD)]**:
  $a, b \in \mathbb{Z}$, not both zero, then $\gcd(a, b) = d$ where:
  (1) $d \mid a$ and $d \mid b$
  (2) $\forall c \in \mathbb{Z}$, $c \mid a$ and $c \mid b \implies c \leq d$

- **Prop 4.5.2 [Existence, uniqueness of GCD]**:
  $a, b \in \mathbb{Z}$, not both zero, then $\gcd(a, b)$ exists and is unique

- **Thm 4.5.3 [Bézout's Identity]**:
  $a, b \in \mathbb{Z}$, not both zero, and $d = \gcd(a, b)$
  $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$

- **Def 4.5.4 [Relatively Prime]**: $a, b \in \mathbb{Z}$
  a and b are relatively prime $\iff \gcd(a, b) = 1$

- **Prop 4.5.5**: $a, b \in \mathbb{Z}$, not both zero
  $c \mid a$ and $c \mid b \implies c \mid \gcd(a, b)$

- **Prop * Num. Th. P2**: $a, b \in \mathbb{Z}^+$
  $a \mid b \iff \gcd(a, b) = a$

- **Prop * Num. Th. P2**: $a, b \in \mathbb{Z}$, not both zero, $d = \gcd(a, b)$
  $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime

- **Prop * Num. Th. P2**: $a, b \in \mathbb{Z}^+$
  $\gcd(a, b) \mid \operatorname{lcm}(a, b)$

- **Def 4.6.1 [Least Common Multiple (LCM)]**:
  $a, b \in \mathbb{Z} \setminus \{0\}$, then $\operatorname{lcm}(a, b) = m \in \mathbb{Z}^+$ where:
  (1) $a \mid m$ and $b \mid m$
  (2) $\forall c \in \mathbb{Z}^+$, $a \mid c$ and $b \mid c \implies m \leq c$

Modular Congruence

- **Def 4.7.1 [Congruence modulo]**: $m, n \in \mathbb{Z}$, $d \in \mathbb{Z}^+$
  $m \equiv n \pmod{d} \iff d \mid (m - n)$

- **Def 8.4.1 (Epp) [Modular equivalences]**:
  $a, b \in \mathbb{Z}$, $1 < n \in \mathbb{Z}^+$, then these are equivalent:
  (1) $n \mid (a - b)$
  (2) $a \equiv b \pmod{n}$
  (3) $\exists k \in \mathbb{Z}$ such that $a = b + kn$
  (4) $a \bmod n = b \bmod n$

- **Thm 8.4.3 (Epp) [Modulo Arithmetic]**:
  $a, b, c, d \in \mathbb{Z}$, $1 < n \in \mathbb{Z}^+$
  If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then these are true:
  (1) $(a + b) \equiv (c + d) \pmod{n}$
  (2) $(a - b) \equiv (c - d) \pmod{n}$
  (3) $ab \equiv cd \pmod{n}$
  (4) $a^m \equiv c^m \pmod{n}, \forall m \in \mathbb{Z}^+$

- **Cor 8.4.4 (Epp)**: $a, b \in \mathbb{Z}$, $1 < n \in \mathbb{Z}^+$
  (1) $ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n}$
  (2) $ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n$
  (3) $a^m \equiv (a \bmod n)^m \pmod{n}, \forall m \in \mathbb{Z}^+$

- **Def 4.7.2 [Multiplicative inverse modulo n]**:
  $a \in \mathbb{Z}$, $1 < n \in \mathbb{Z}^+$
  $s = a^{-1}$ is a multiplicative inverse of a modulo n
  $\iff as \equiv 1 \pmod{n}$

- **Thm 4.7.3 [Existence of multiplicative inverse]**: $a \in \mathbb{Z}$, $1 < n \in \mathbb{Z}^+$
a^{-1} exists $\iff$ a and b are relatively prime

- **Col 4.7.4 [Multiplicative inverses for primes]**: $a \in \mathbb{Z}$, p is prime
$\forall a \in \mathbb{Z}$ in range $0 < a < p$, a^{-1} exists

- **Thm 8.4.9 (Epp) [Cancellation Law]**: $a, b, c \in \mathbb{Z}$, $1 < n \in \mathbb{Z}^+$, a and n are relatively prime
$ab \equiv ac \pmod{n} \implies b \equiv c \pmod{n}$

- **Thm 8.4.10 (Epp) [Fermat's Little Theorem]**: If p is prime, $a \in \mathbb{Z}$, $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$

Real Numbers — Appendix A (Epp)
All entities are real numbers in this section

- **T11 [Zero Product Property]**: $ab = 0 \implies a = 0$ or $b = 0$

- **T17 [Trichotomy Law]**:
Exactly one of these three statements are true:
(1) $a < b$ (2) $b < a$ (3) $a = b$

- **T18 [Transitive Law]**: $a < b$ and $b < c \implies a < c$

- **T19**: $a < b \implies a + c < b + c$

- **T20**: $a < b$ and $c > 0 \implies ac < bc$

- **T21**: $a \neq 0 \implies a^2 > 0$

- **T23**: $a < b$ and $c < 0 \implies ac > bc$

- **T24**: $a < b \implies -a > -b$ $(\therefore a < 0 \implies -a > 0)$

- **T25**:
$ab > 0 \implies (a > 0$ and $b > 0)$ or $(a < 0$ and $b < 0)$

- **T26**: $a < c$ and $b < d \implies a + b < c + d$

- **T27**: $0 < a < c$ and $0 < b < d \implies 0 < ab < cd$

Rational Numbers

- **Thm 4.6.3 (Epp)**: The sum of any rational number and any irrational number is irrational

- **Thm 4.7.1 (Epp)**: $\sqrt{2}$ is irrational

Useful Information & Presentation

- **Smallest primes**: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199

- **Euclid's algorithm**: Calculate $\gcd(1320, 714)$:

$$
\begin{aligned}
& & \gcd(1320, 714) & \quad (1) \\
1320 &= 714 \times 1 + 606 & \longleftarrow \gcd(714, 606) & \quad (2) \\
714 &= 606 \times 1 + 108 & \longleftarrow \gcd(606, 108) & \quad (3) \\
606 &= 108 \times 5 + 66 & \longleftarrow \gcd(108, 66) & \quad (4) \\
108 &= 66 \times 1 + 42 & \longleftarrow \gcd(66, 42) & \quad (5) \\
66 &= 42 \times 1 + 24 & \longleftarrow \gcd(42, 24) & \quad (6) \\
42 &= 24 \times 1 + 18 & \longleftarrow \gcd(24, 18) & \quad (7) \\
24 &= 18 \times 1 + 6 & \longleftarrow \gcd(18, 6) & \quad (8) \\
18 &= 6 \times 3 + 0 & \longleftarrow \gcd(6, 0) & \quad (9)
\end{aligned}
$$

Solve $\gcd(1320, 714) = 1320x + 714y$:

$$
\begin{aligned}
6 &= 24 + 18(-1) & \text{from line (8)} \\
&= 24 + (42 - 24)(-1) & \text{from line (7)} \\
&= 42(-1) + 24(2) & \\
&= 42(-1) + (66 - 24)(2) & \text{from line (6)} \\
&= 66(2) + 42(-3) & \\
&= 66(2) + (180 - 66)(-3) & \text{from line (5)} \\
&= 180(-3) + 66(5) & \\
&= 180(-3) + (606 - 108 \times 5)(5) & \text{from line (4)} \\
&= 606(5) + 108(-28) & \\
&= 606(5) + (714 - 606)(-28) & \text{from line (3)} \\
&= 714(-28) + 606(33) & \\
&= 714(-28) + (1320 - 714)(33) & \text{from line (2)} \\
&= 1320(33) + 714(-61) &
\end{aligned}
$$

$\therefore x = 33$ and $y = -61$ is a valid solution

$(x, y) = \left(33 + \dfrac{714k}{6}, -61 + \dfrac{1320k}{6}\right)$ is a valid solution for any $k \in \mathbb{Z}$

- **Mathematical induction**:
1. Let P(n) = (n has a prime factorization), for any integer $n > 1$.
2. Base case: $n = 2$:
2.1. Since 2 is prime, $2 = 2$ is a trivial prime factorization.
2.2. Thus P(2) is true.
3. Inductive step: For any integer $k > 1$:
3.1. Assume P(i) is true for $1 < i \leq k$. *(Note: for regular induction, assuming $P(k)$ is true is sufficient.)*
3.2. That is, all integers i in the range $1 < i \leq k$ have prime factorizations.
3.2.1. Consider the integer k+1:
3.2.*. ...
4. Therefore, by strong induction, the statement is true.

Logic

Useful Information & Presentation

- **Verifying argument validity**
Sandra knows Java and Sandra knows C++.
∴ Sandra knows C++.
  1. Let p = (Sandra knows Java).
  2. Let q = (Sandra knows C++).
  3. $p \wedge q$. (Premise)
  4. $\therefore q$. (Valid by specialization)

If at least one of these two numbers is divisible by 6, then the product of these two numbers is divisible by 6.
Neither of these two numbers is divisible by 6.
∴ The product of these two numbers is not divisible by 6.
  1. Let p = (At least one number is divisible by 6).
  2. Let q = (Their product is divisible by 6).
  3. $p \to q$. (Premise)
  4. $\sim p$. (Premise)
  5. // $\therefore \sim q$. (Invalid; inverse error)

Counting & Probability

- **Thm 9.1.1 [Num. of elements in list]**:
  For any $m, n \in \mathbb{Z}$ s.t. $m \le n$, there are $n - m + 1$ integers from m to n inclusive
- **Thm 9.2.1 [Multiplication rule]**:
  Total num. of ways $= \prod$(num. ways of each step)
- **Thm 9.2.2 [Permutation]**: Num. of permutations of a set with n elements ($n \ge 1$) is $n!$
- **Thm 9.2.3 [$\mathbf{P(n,\ r)}$]**: Num. of r-permutations from a set with n elements ($1 \le r \le n$) is $n(n-1)(n-2)\cdots(n-r+1) \equiv \dfrac{n!}{(n-r)!}$
- **Thm 9.3.1 [Addition rule]**:
  If A is the union of distinct mutually disjoint subsets A_i, then $N(A) = \sum N(A_i)$
- **Thm 9.3.2 [Difference rule]**: If B is a subset of A, then $N(A - B) = N(A) - N(B)$
- **Thm 9.3.3 [Principle of inclusion & exclusion for 2 or 3 sets]**
- **Thm 9.4.1 [Pigeonhole principle]**:
  A function from one finite set to a smaller finite set cannot be injective
- **Generalized pigeonhole principle**:
  For any function from a finite set X to a finite set Y and for any $k \in \mathbb{Z}^+$:
  $k < \frac{|X|}{|Y|} \implies$ there is some $y \in Y$ s.t. y is the image of at least $k+1$ distinct elements
- **Generalized pigeonhole principle (contrapositive form)**:
  For any function from a finite set X to a finite set Y and for any $k \in \mathbb{Z}^+$:
  For every $y \in Y$, $f^{-1}(y)$ has at most k elements $\implies |X| \le k|Y|$
- **Thm 9.4.2 [Bijectivity of same-sized sets]**:
  If X and Y are finite sets of the same size, and $f\colon X \to Y$ then:
  f is injective $\iff$ f is surjective
- **Thm 9.5.1 [$\binom{n}{r}$]**: Num. of r-combinations from a set with n elements is $\dfrac{\mathrm{P}(n,r)}{r!} = \dfrac{n!}{r!(n-r)!}$
- **Thm 9.5.2 [Permutations of sets of indistinguishable objects]**: $\dfrac{n!}{n_1!n_2!\cdots n_k!}$
- **Thm 9.6.1 [r-combinations with repetition allowed]**: Num. of r-combinations with repetition allowed (multisets of size r) that can be selected from a set of n elements is $\binom{r+n-1}{r}$
- **Thm 9.7.1 [Pascal's formula]**:
  $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$
- **Thm 9.7.1 [Binomial theorem]**:
  $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$
- **Conditional probability**: $P(B|A) = \dfrac{P(A \cap B)}{P(A)}$
  $P(B|A) \cdot P(A) = P(A \cap B) = P(A|B) \cdot P(B)$
- **Thm 9.9.1 [Bayes' theorem]**: If the sample space S is a union of mutually disjoint events $B_1, \dots, B_n$ and $1 \le k \le n$, then:
  $P(B_k|A) = \dfrac{P(A|B_k) \cdot P(B_k)}{P(A|B_1)\cdot P(B_1) + \cdots + P(A|B_n)\cdot P(B_n)}$
- **Independent events**: A and B are independent $\iff P(A \cap B) = P(A) \cdot P(B)$
- **Pairwise/mutually independent**:
  Pairwise independent:
  Any two different events are independent
  Mutually independent:
  For any subset T of events, $P\left(\bigcap T\right) = \prod_{A \in T} P(A)$
  (when $n > 2$, pairwise indep. $\not\Longrightarrow$ mutually indep.)

Graphs & Trees

Basic Graph Theory

- **Basic definitions**:
  Simple graph: no loops or parallel edges
  Complete graph: simple graph with one edge per pair of distinct edges
  Total degree of graph: sum of degrees of all vertices
- **Thm 10.1.1 [Handshake theorem]**: For any graph G, total degree of G = num. of edges in G
- **Col 10.1.2**: Total degree of a graph is even
- **Prop 10.1.3**: There are even num. of vertices with odd degree
- **More definitions**:
  Walk from v to w: finite alternating sequence of adjacent vertices and edges, i.e. $v_0 e_1 v_1 e_2 \dots v_{n-1} e_n v_n$ where $v_0 = v$ and $v_n = w$
  Trail from v to w: walk without repeated edge
  Path from v to w: walk without repeated vertex
  Trivial walk from v to v: walk with single vertex v
  $\boxed{\text{walk} \supseteq \text{trail} \supseteq \text{path} \supseteq \text{trivial walk}}$
  Closed walk: start and end at same vertex
  Circuit (or cycle): non-trivial closed walk without repeated edge
  Simple circuit (or simple cycle): circuit with no repeated vertex apart from start/end
  $\boxed{\text{closed walk} \supseteq \text{circuit} \supseteq \text{simple circuit}}$
  Connected vertices: there is a walk from v to w
  Connected graph: all pairs of vertices are connected
  Connected component: connected subgraph of G that is not a subgraph of any other connected subgraph of G
- **Lemma 10.2.1 [Circuit edge removal]**:
  For any graph G:
  (1) G is connected $\implies$ there is a path between any two distinct vertices in G
  (2) If v and w are part of a circuit and one edge from the circuit is removed, then there still exists a trail from v to w
  (3) G is connected and contains a circuit $\implies$ any edge of the circuit can be remove without disconnecting G

Euler Circuits

- **Euler circuit definitions**:
Euler circuit: circuit that uses every edge exactly once and uses every vertex at least once
Eulerean graph: graph with a Euler circuit
Euler trail: trail between distinct start and end vertices that uses every edge exactly once and uses every vertex at least once

- **Thm 10.2.2**:
G has Euler circuit $\implies$ every vertex of G has positive even degree

- **Thm 10.2.4 [Existence of Euler circuit]**:
G has Euler circuit $\iff$ G is connected and every vertex of G has positive even degree

- **Col 10.2.5 [Existence of Euler trail]**:
G has Euler trail from v to w $\iff$ G is connected, v and w have (positive) odd degree, all other vertices of G have positive even degree

Hamiltonian Circuits

- **Hamiltonian circuit definitions**:
Hamiltonian circuit: simple circuit that uses every vertex exactly once
(Hamiltonian circuits with the same path but different start/end are the same circuit)
Hamiltonian graph: graph with a Hamiltonian circuit

- **Prop 10.2.6 [Hamiltonian circuit properties]**:
If G has a Hamiltonian circuit, then there exists a subgraph H such that:
(1) H contains every vertex of G
(2) H is connected
(3) H has the same number of edges as vertices
(4) Every vertex of H has degree 2
(The contrapositive form may be used to show G does not have a Hamiltonian circuit)

Adjacency Matrices

- **Basic usage**: $a_{ij} = i^{\text{th}}$ row, j^{th} column
Directed graph: a_{ij} = num. of edges from v_i to v_j
Undirected graph: Symmetric adjacency matrix

- **Thm 10.3.1 [Block diagonal = connected components]**: G is made up of connected components $G_1, \ldots, G_k \implies A = \text{diag}[A_1, \ldots, A_k]$

- **Thm 10.3.2 [Walks of length *n*]**: ij^{th} entry of A^n = num. of walks of length n from v_i to v_j

Isomorphisms

- **Isomorphic graph**: G is isomorphic to $G' \iff$ exists bijections $g\colon V(G) \to V(G')$ and $h\colon E(G) \to E(G')$ preserving edge-endpoint functions of G and G',
i.e. $\forall v \in V(G)$, $e \in E(G)$, (v is an endpoint of e $\iff$ $g(v)$ is an endpoint of $h(e)$)

- **Thm 10.4.1 [Equivalence relation]**:
Graph isomorphism is an equivalence relation

- **Thm 10.4.2 [Invariants for isomorphism]**:
(1) has n vertices
(2) has m edges
(3) has a vertex of degree k
(4) has m vertices of degree k
(5) has a circuit of length k
(6) has a simple circuit of length k
(7) has m simple circuits of length k
(8) is connected
(9) has an Euler circuit
(10) has a Hamiltonian circuit

- **Simple isomorphic graph**: For simple G and G':
G is isomorphic to $G' \iff$ exists bijection $g\colon V(G) \to V(G')$ preserving edge-endpoint functions of G and G',
i.e. $\forall u, v \in V(G)$, ($\{u, v\}$ is an edge in G $\iff$ $\{g(u), g(v)\}$ is an edge in G')

Trees

- **Basic definitions**:
Circuit-free: graph with no circuits
Tree: graph that is circuit-free and connected
Trivial tree: graph with only one vertex
Forest: graph that is circuit-free and not connected

- **Leaf / terminal vertex definition**:
If T has only 1 or 2 vertices, then all vertices are leaves *(leaf of trivial tree has degree 0)*
If T has at least 3 vertices then:
— degree 1 = leaf
— degree greater than 1 = internal vertex
(In a rooted tree, a root with only one child is also a leaf)

- **Lemma 10.5.1**: Any non-trivial tree has at least one vertex of degree 1

- **Thm 10.5.2 [*n*–1 edges]**:
Any tree with n vertices ($n \geq 0$) has $n - 1$ edges

- **Lemma 10.5.3 [Circuit edge removal]**:
If G is connected and C is any circuit in G, removing any edge of C from G will not disconnect the graph

- **Thm 10.5.4 [Tree condition]**:
G is a connected graph with n vertices and $n - 1$ edges $\implies$ G is a tree

Rooted Trees

- **Basic definitions**:
Level of a vertex: num. of edges along the (unique) path between it and the root
Height: max. vertex level
Full binary tree: each parent has exactly two children

- **Thm 10.6.1 [Full binary tree theorem]**:
T is a full binary tree with k internal vertices $\implies$ T has a total of $2k + 1$ vertices and $k + 1$ leaves

- **Thm 10.6.2 [Max. leaves given tree height]**:
T is a binary tree with height h and t leaves $\implies$ $t \leq 2^h$ (equiv. $\log_2 t \leq h$)
(Root with ≤1 child is also a leaf)

Spanning Trees

- **Basic definition**:
  Spanning tree of a graph: subgraph that contains every vertex of G and is a tree
  Minimum spanning tree: spanning tree with least possible total weight

- **Prop 10.7.1**:
  (1) Every connected graph has a spanning tree
  (2) Any two spanning trees for a graph have the same num. of edges

Useful Sequences

Prime Numbers

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	$\cdots$

Fibonacci Numbers

1	1	2	3	5	8	13	21	34	55
89	144	233	377	610	987	1597	2584	4181	$\cdots$

Triangular Numbers

1	3	6	10	15	21	28	36	45	55
66	78	91	105	120	136	153	171	190	210
231	253	276	300	325	351	378	406	435	465
496	528	561	595	630	666	703	741	780	$\cdots$

Square Numbers

1	4	9	16	25	36	49	64	81	100
121	144	169	196	225	256	289	324	361	400
441	484	529	576	625	676	729	784	841	900
961	1024	1089	1156	1225	1296	1369	1444	1521	$\cdots$