Quiz 1

---

1. Which set is in one-to-one correspondence with the collection of subsets of a set of size n?

→*A*. The set of integers from 0 to $2^n - 1$.

B. The set of integers from 0 to 2^{n-1}.

C. The set of integers which can be expressed in binary form.

D. None of the above.

---

2. The integer part of x is the integer k such that

A. $k - 1 \leq \log_{10}(x) < k$.

→*B*. $k \leq x < k + 1$.

C. $|x - k| < 1$.

D. None of the above.

---

3. Sets A and B are disjoint when

→*A*. their intersection is the empty set.

B. their union is the empty set.

C. their union equals their intersection.

D. All of the above.

E. None of the above.

---

4. How likely is it to be dealt the same bridge hand you had last time?

A. 1 in $\dfrac{52!}{5!}$.

B. 1 in $\dfrac{52!}{13!}$.

C. 1 in $\dfrac{52!}{5! \cdot 13!}$.

→*D*. None of the above.

---

5. If A is a set then $|A|$ denotes

A. the collection of subsets of A.

B. the set of all permutations of A.

→*C*. the cardinality of A.

D. None of the above.

Quiz 2

---

1. $\sum_{k=0}^{n} \binom{n}{k} =$

A. $n!$.

B. n^k.

→*C.* 2^n.

D. None of the above.

---

2. The number of *unordered* k-subsets of a set with n elements is

→*A.* $\binom{n}{k}$.

B. $n!/k!$.

C. $n!/(n-k)!$.

D. None of the above.

---

3. The number of *ordered* k-subsets of a set with n elements is

A. $\binom{n}{k}$.

B. $n!/k!$.

→*C.* $n!/(n-k)!$.

D. None of the above.

---

4. Let S be a set with n elements. How many decimal digits are there in the number of subsets of S.

A. $1 + \lfloor 10 \log_2(n) \rfloor$

B. $1 + \lfloor n \log_2(10) \rfloor$

→*C.* $1 + \lfloor n \log_{10}(2) \rfloor$

D. None of the above.

---

5. The decision tree for selecting a permutaion of n elements has how many nodes in the bottom level?

A. $n - 1$

B. n

→*C.* $n!$

D. None of the above.

Quiz 3

---

1. What is the $\sum_{k=1}^{n}(2k-1)$?

A. $2n-1$.

B. $(2n-1)^2$.

→*C.* n^2.

D. None of the above.

---

2. Suppose we have a property of positive integers. Suppose also that 1 has this property, and that whenever $n-1$ has this property then so does n. True or false: Every positive integer has this property.

True.

---

3. Suppose we have n boxes and we place more than n objects into them. True or false: At least one box will contain more than 1 object.

True.

---

4. True or false: For all n, $2^{n-1} \leq n! \leq n^{n-1}$.

True.

---

5. Stirling's Formula tells us that

A. $n! \sim (n/e)^n \sqrt{2\pi n}$.

B. The ratio of $n!$ to $(n/e)^n \sqrt{2\pi n}$ approaches 1 as $n \to \infty$.

C. The difference between $\log(n!)$ and $\log\left[(n/e)^n \sqrt{2\pi n}\right]$ approaches 0 as $n \to \infty$.

→*D.* All of the above.

E. None of the above.

Quiz 4

---

1. What is the difference between the n-th square and the $(n+1)$-st?

A. The $(n-1)$-st square.

B. The $(n-1)$-st odd number.

C. The n-th odd number.

→*D*. None of the above.

---

2. What information can we get from Stirling's formula?

A. An asymptotic estimate for the factorial.

B. An estimate for the number of decimal digits of the factorial.

C. An estimate for the number of binary bits of the factorial.

→*D*. All of the above.

E. None of the above.

---

3. What does the "$\sim$" in Stirling's Formula mean?

→*A*. The ratio of the two expressions approaches 1 as $n \to +\infty$.

B. The difference of the two expressions approaches 0 as $n \to +\infty$.

C. The two expressions are nearly equal for all sufficiently large n.

D. All of the above.

E. None of the above.

---

4. True or false: If n is even then the number of even-size subsets of an n-set is one less than the number of odd-size subsets of an n-set.

False.

---

5. True or false: The Pigeonhole Principle implies the Twin Paadox.

False.

Quiz 5

---

1. True or false: The number of digits in the decimal expression of $n!$ is roughly proportional to $n \log(n/e) + \frac{1}{2} \log(n) + C$, for some constant C.

True.

---

2. True or false: The number of bits in the binary expression of $n!$ is roughly proportional to $n \log(n/e) + \frac{1}{2} \log(n) + C$, for some constant C.

True.

---

3. True or false: There are more than 100 subsets of $\{0, 1, 2, 3, 4, 5, 6\}$.

True.

---

4. True or false: There are more than 1000 subsets of $\{0, 1, 2, 3, 4, 5, 6, 7\}$.

False.

---

5. True or false: There are more 2-letter strings (of lower-case letters) than there are permutations of the set $\{0, 1, 2, 3, 4, 5\}$.

False.

Quiz 6

---

1. The Binomial Theorem was discovered by

A. An English physicist.

B. A French philosopher.

C. A Greek astronomer.

→*D*. None of the above.

---

2. $\sum_{k=0}^{n} \binom{n}{k} =$

A. $n!$.

→*B*. 2^n.

C. $\binom{2n}{n}$.

D. None of the above.

---

3. $\sum_{k=0}^{n} \binom{n}{k}^2 =$

A. $n!$.

B. 2^n.

→*C*. $\binom{2n}{n}$.

D. None of the above.

---

4. The number of ways to distribute n identical pennies to k children so that each child gets at least one is

A. $\binom{n}{k}$.

B. $\binom{n+k-1}{k-1}$.

→*C*. $\binom{n-1}{k-1}$.

D. None of the above.

---

5. The number of ways to distribute n identical pennies to k children is

A. $\binom{n}{k}$.

→*B*. $\binom{n+k-1}{k-1}$.

C. $\binom{n-1}{k-1}$.

D. None of the above.

Quiz 7

---

1. Which word has more anagrams: CONNECT or ALFALFA?

→*A*. CONNECT

B. ALFALFA

C. They have the same number.

---

2. Fix a very large positive integer n, and plot $\binom{2n}{k}$ versus k. What does the graph look like?

A. A "bell" curve with mean n.

B. A gaussian distribution with mean n.

C. A normal distribution with mean n.

→*D*. All of the above.

E. None of the above.

---

3. $\sum_{j=0}^{k} \binom{n+j}{j} =$

→*A*. $\binom{n+k+1}{k}$.

B. $\binom{n+k}{k+1}$.

C. $\binom{n+k+1}{k+1}$.

D. None of the above.

---

4. $\sum_{j=0}^{n} (-1)^j \binom{n}{j} =$

A. $\binom{2n}{n}$.

B. $(-1)^n \binom{2n}{n}^2$.

C. $(-2)^n$.

→*D*. None of the above.

---

5. $\sum_{j=0}^{n} 2^j \binom{n}{j} =$

A. 2^{n+1}.

B. $2^n + 1$.

→*C*. $(2+1)^n$.

D. None of the above.

Quiz 8

---

1. The number of binary bits of N is

A. roughly $\log(10)/\log(2)$ times the number of decimal digits of N.

B. roughly proportional to $\log(N)$.

C. exactly equal to $\lfloor \log_2(N) \rfloor + 1$.

→*D*. All of the above.

E. None of the above.

---

2. True or false: De Moivre's version of Stirling's Formula can be proved by estimating $\int_1^n \log(x)\,dx$ using the Trapezoidal Rule.

True.

---

3. In python, the expression `a%b` evaluates to

A. a raised to the power b.

B. the integral part of $a \div b$.

→*C*. the remainder of $a \div b$.

D. None of the above.

---

4. The identity $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ can be proved

→*A*. combinatorially.

B. inductively.

C. both combinatorially and inductively.

D. neither combinatorially nor inductively.

---

5. Who was Omar Khayyam?

A. Some guy from Nishapur, Iran, born almost a thousand years ago, whose name means "tent maker".

B. A Persian mathematician and astronomer often credited with both the Binomial Theorem and the Jalali calendar.

C. The author of several hundred Farsi rubaiyat, which have become popular in translation the world over.

→*D*. All of the above.

E. None of the above.

Quiz 9

---

1. True or false: If a sequence a_n satisfies the recursive relation $a_{n+1} = a_n + a_{n-1}$ then $a_n = F_n$, the n-th Fibonacci number.

False.

---

2. True or false: If n is large then $F_{n+1} \approx \frac{1}{2}(1 + \sqrt{5})F_n$.

True.

---

3. True or false: If $x = \lim_{n\to\infty} \dfrac{F_{n+1}}{F_n}$ then $x = 1 + \dfrac{1}{x}$.

True.

---

4. True or false: $\displaystyle\sum_{k=0}^{n} F_k = F_{n+1}$.

False.

---

5. True or false: $\displaystyle\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} = F_n$.

True.

Quiz 10

1. What was Fibonacci's real name?

A. Guilielmo

→*B*. Leonardo

C. Bigollo

D. None of the above.

---

2. Where was Fibonacci born?

→*A*. Pisa

B. Bugia

C. Palermo

D. None of the above.

---

3. Where was Fibonacci educated?

A. Present-day Egypt

B. Present-day Italy

C. Present-day Germany

D. All of the above.

→*E*. None of the above.

---

4. In what century was Fibonacci active?

A. 11th

B. 12th

→*C*. 13th

D. All of the above.

E. None of the above.

---

5. What book did Fibonacci write?

A. *Liber abaci*

B. *Liber quadratorum*

C. *Practica geometriae*

→*D*. All of the above.

E. None of the above.

Quiz 11

---

1. If A and B are independent events then

→*A*. $P(A \cap B) = P(A)P(B)$.

B. $P(A \cup B) = P(A)P(B)$.

C. $P(A \cup B) = P(A) + P(B)$.

D. All of the above.

E. None of the above.

---

2. A subset of a sample space is called

A. a sample.

B. an outcome.

→*C*. an event.

D. All of the above.

E. None of the above.

---

3. The set of all possible outcomes is called

→*A*. the sample space.

B. the probability distribution.

C. exclusive event.

D. All of the above.

E. None of the above.

---

4. True or false: In a uniform probability distribution all outcomes have the same probability.
True.

---

5. True or false: If we toss a fair (balanced) coin n times then the probability that we observe exactly k heads is $2^{-n}\binom{n}{k}$.
True.

Quiz 12

---

1. True or false: The Law of Very Large Numbers says that coincidences often occur when we look at very large data sets.

True.

---

2. True or false: The Law of Small Numbers says that if you look at small examples then you can find many strange or interesting patterns that do no generalize to larger numbers.

True.

---

3. True or false: The Law of Very Large Numbers implies Law of Large Numbers.

False.

---

4. True or false: If A and B are exclusive events then they are independent.

False.

---

5. If ϕ is the golden ration then the number of decimal digits of F_n (the n-th Fibonacci number) is approximately

$\rightarrow$*A*. $n \log_{10} \phi$.

B. $\phi \log_{10} n$.

C. $10 \log_{\phi} n$.

D. None of the above.

Quiz 13

1. What is the sieve of Eratosthenes good for?

A. To prove that there are infinitely many primes.

B. To solve the Chinese Remainder Problem.

C. To locate perfect numbers.

D. All of the above.

→*E*. None of the above.

---

2. What is the extended euclidean algorithm good for?

A. To prove that there are infinitely many primes.

→*B*. To solve the Chinese Remainder Problem.

C. To locate perfect numbers.

D. All of the above.

E. None of the above.

---

3. True or false: if p is a prime and a is any integer then $p \mid a^p - a$.
True.

---

4. True or false: for every positive integer k there exist a positive integer a such that $a, a+1, a+2, \ldots, a+k$ are all composite.
True.

---

5. True or false: $\pi(x) \sim x \log(x)$, where $\pi(x)$ denotes the number of primes less than x.
False.

Quiz 14

---

1. The statement that the density of primes near n is approximately $1/\log(n)$ is known as

A. Goldbach's Conjecture.

B. the Riemann Hypothesis.

→*C*. the Prime Number Theorem.

D. None of the above.

---

2. Euler proved that the infinite sum $\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\cdots$

→*A*. diverges.

B. converges to $\frac{1}{\pi}$.

C. converges to some as yet unidentified limit.

D. None of the above.

---

3. In the third century Sun Tzu stated that a system of simultaneous congruences $x \equiv a_i \bmod n_i$ could be solved provided that

A. $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

→*B*. $\gcd(n_i, n_j) = 1$ whenever $i \neq j$.

C. $\gcd(a_i, n_j) = 1$ whenever $i \neq j$.

D. All of the above.

E. None of the above.

---

4. True or false: The extended euclidean algorithm can be used to solve the Chinese Remainder Problem.
True.

---

5. True or false: The Sieve of Eratosthenes can be used to find all of the primes up to a given bound.
True.

Quiz 15

---

1. The Prime Number Theorem states that

A. the density of primes near N is $1/\log(N)$.

B. the number of primes less than N is roughly $\displaystyle\int_2^N \frac{dt}{\log(t)}$.

C. the number of primes less than N is asymptotic to $N/\log(N)$.

→*D*. All of the above.

E. None of the above.

---

2. The Riemann Hypothesis

A. states that the nonreal zeroes of the zeta function have real part equal to 1/2.

B. implies the Prime Number Theorem.

C. is one of the most important unsolved problems in mathematics.

→*D*. All of the above.

E. None of the above.

---

3. True or false: If p is a prime and $p \mid ab$ then either $p \mid a$ or $p \mid b$.
True.

---

4. True or false: If $p \mid a^{p-1} - 1$ whenever $\gcd(a, p) = 1$ then p is prime.
False.

---

5. True or false: If p is a prime then $p \mid (p-1)! + 1$.
True.

Quiz 16

1. In the third century Sun Tzu stated that a system of simultaneous congruences $x \equiv a_i \bmod n_i$ could be solved provided that

→*A*. $\gcd(n_i, n_j) = 1$ whenever $i \neq j$.

B. $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

C. $\gcd(a_i, n_j) = 1$ whenever $i \neq j$.

D. All of the above.

E. None of the above.

---

2. What is the extended euclidean algorithm good for?

A. To prove that there are infinitely many primes.

→*B*. To solve the Chinese Remainder Problem.

C. To locate perfect numbers.

D. All of the above.

E. None of the above.

---

3. The Prime Number Theorem states that

A. the density of primes near N is $\log(N)/N$.

→*B*. the number of primes less than N is roughly $\displaystyle\int_2^N \frac{dt}{\log(t)}$.

C. the number of primes less than N is asymptotic to $\log(N)$.

D. All of the above.

E. None of the above.

---

4. True or false: Suppose $p \mid ab$ implies either $p \mid a$ or $p \mid b$. Then we can conclude that p is a prime.
True.

---

5. True or false: Suppose that p is prime. Then we can conclude that $p \mid a^{p-1} - 1$ whenever $\gcd(a, p) = 1$.
True.

Quiz 17

---

1. Alice is trying to
- *A*. fiddle her tax returns.
- *B*. plan a coup d'etat.
- *C*. save on her phone bill.
- →*D*. All of the above.
- *E*. None of the above.

---

2. Alice
- *A*. can barely hear Bob on the telephone.
- *B*. suspects Bob is working with the secret police.
- *C*. has never met Bob.
- →*D*. All of the above.
- *E*. None of the above.

---

3. A coding theorist is someone who
- *A*. thinks Alice is crazy.
- *B*. thinks Bob is crazy.
- *C*. thinks both are crazy.
- →*D*. None of the above.

---

4. Which of these are part of coding theory?
- *A*. source coding
- *B*. channel coding
- *C*. secrecy coding
- →*D*. All of the above.
- *E*. None of the above.

---

5. Cryptography is a kind of
- *A*. source coding
- *B*. channel coding
- →*C*. secrecy coding
- *D*. All of the above.
- *E*. None of the above.

Quiz 18

This quiz concerns `primes_and_composites.py` and `time_trials.py`.

---

1. What python structure does the function `sieve` use to keep track of primes and composites?

A. Separate lists of primes and composites, which grow at each iteration of the main loop.

→*B*. A dictionary whose keys are all integers and whose values are marked False when the key is determined to be composite.

C. A dictionary whose keys are all integers and whose values are marked True when the key is determined to be prime.

D. None of the above.

---

2. Under what condition does `brute_force_test` break the main loop?

A. When a number is determined to be prime.

→*B*. When a number is determined to be composite.

C. Either of the above.

D. None of the above.

---

3. What does the function `fermat_test` return?

A. True if `powermod(b,n-1,n)` equals 1.

B. False if `powermod(b,n-1,n)` does not equal 1.

→*C*. Both of the above.

D. None of the above.

---

4. What does `fermat_false_positives` return?

A. The number of primes `fermat_test` misidentifies as composite.

→*B*. The number of composites `fermat_test` misidentifies as prime.

C. Neither of these.

---

5. What does `fermat_timer` return?

→*A*. The time required to run `fermat_test` on prime candidate n, for k randomly chosen bases b.

B. The time required to run `fermat_test` on k given bases, for r randomly chosen prime candidates n.

C. Neither of these.

Quiz 19

Questions 3–5 concern the code in `primes_and_composites.py`.

---

1. True or false: The Miller-Rabin Test is a strengthening of the Fermat Test designed to overcome the difficulty of Carmichael numbers.

True.

---

2. True or false: A Carmichael number is a Fermat pseudoprime for every base relatively prime to it.

True.

---

3. What does `fermat_test` return?

A. `powermod(b,n-1,n)`

B. `powermod(n-1,b,n)`

C. `powermod(n,n-1,b)`

→*D*. None of the above.

---

4. What is the last line of `sieve`?

A. `return P.keys()`

B. `return P.values()`

C. `return [P[n] for n in P]`

→*D*. None of the above.

---

5. What is the line which causes the main loop of `brute_force_test` for a composite n?

A. `if n % x > 0:`

→*B*. `if n % x == 0:`

C. `if n % x < 0:`

D. None of the above.

Quiz 20

1. What does Alice use when she wants to save on her phone bills?

A. Secret coding.

B. Channel coding.

→*C*. Source coding.

D. All of the above.

E. None of the above.

---

2. What does Alice use when she has a difficult time hearing Bob?

A. Secret coding.

→*B*. Channel coding.

C. Source coding.

D. All of the above.

E. None of the above.

---

3. True or false: When Bob receives a message from Alice encypted using a one-time pad then Bob should encrypt his response with the same random bit-string Alice used.

False.

---

4. True or false: Modern cryptography began with the idea that the only thing that can protect Alice and Bob's communication from Eve is Eve's lack of the knowledge of the secret key that Alice and Bob are using.

False.

---

5. True or false: The security of the number-theoretic "drop box" which Alice and Bob use to save chess moves is based on the computational complexity of factoring integers into primes.

True.

Quiz 21

---

1. True or false: It is possible for a bank ATM to verify the password of a customer without knowing what the password is.

True.

---

2. How does Alice hide her n-digit secret x in an $(m+n)$ prime, using the "envelope" method?

A. Use primality tests to locate the first prime after $x \cdot 10^m$.

→*B*. Apply primality tests to random $(m+n)$-digit numbers congruent to $x \bmod 10^m$.

C. Multiply x by a randomly chosen m-digit prime.

D. None of the above.

---

3. What formula does Bob use to encrypt his plain text x with Alice's RSA public key (e, m)?

→*A*. $x^e \bmod m$

B. $m^e \bmod x$

C. $e^x \bmod m$

D. None of the above.

---

4. If (e, m) is Alice's RSA public key, what property must her private key d have?

A. $de = 1 \bmod m$

B. $dm = 1 \bmod e$

→*C*. $de = 1 \bmod \phi(m)$

D. None of the above.

---

5. How can Bob use RSA to convince Alice the message he sends did in fact come from him, and not an imposter?

A. First encrypt it with his public key, then add his signature, then encrypt using Alice's private key.

→*B*. First encrypt it with his private key, then add his signature, then encrypt using Alice's public key.

C. First encrypt it with Alice's private key, then add his signature, then encrypt using his public key.

D. None of the above.

Quiz 23

1. True or false: Every graph has an even number of nodes of even degree.
False.

2. True or false: Every graph has an odd number of nodes of odd degree.
False.

3. True or false: If nodes a and b are in the same connected component of a graph G then there is a path in G containing both a and b.
True.

4. True or false: It is easy to determine whether a graph contains an eulerian walk.
True.

5. True or false: It is easy to determine whether a graph contains an hamiltonian cycle.
False.

Quiz 24

1. What characterizes a tree?

A. A connected graph containing no cycle.

B. A connected graph which is disconnected by the deletion of any edge.

C. A graph with no cycles but into which the addition of an edge creates a cycle.

→*D*. All of the above.

E. None of the above.

---

2. What is the root of a tree?

A. The node of highest degree.

B. The node of lowest degree.

→*C*. Any old node specified as such.

D. All of the above.

E. None of the above.

---

3. Every tree with n nodes has how many edges?

A. n

→*B*. $n-1$

C. $n+1$.

D. None of the above.

---

4. How many labeled trees on n nodes are there?

A. $n!$

B. $(n!)^2$.

C. $n!/2^n$.

→*D*. None of the above.

---

5. The number of unlabeled trees with n nodes is

A. at least $n^{n-2}/n!$.

B. at most 4^{n-1}.

→*C*. All of the above.

D. None of the above.

Quiz 25

---

1. The Father Code is used to encode

→*A*. labeled trees.

B. unlabeled trees.

C. Both.

D. Neither.

---

2. The Planar Code is used to encode

A. labeled trees.

→*B*. unlabeled trees.

C. Both.

D. Neither.

---

3. Cayley's Theorem is proved using

A. the Father Code.

→*B*. the Prüfer Code.

C. the Planar Code.

D. All of the above.

E. None of the above.

---

4. True or false: a tree is a minimally connected graph.
True.

---

5. True or false: a tree is a maximally acyclic graph.
True.

Quiz 26

---

1. The problem of finding a cycle such that the total edge-cost is minimum is called

A. Kruskal's Problem.

B. the Perfect Matching Problem.

→*C*. the Traveling Salesman Problem.

D. None of the above.

---

2. The Greedy Algorithm can be used to solve

A. the Traveling Salesman Problem.

B. the Hamiltonian Cycle Problem.

→*C*. the Minimal Spanning Tree Problem.

D. All of the above.

E. None of the above.

---

3. True or false: The Tree Shortcut Algorithm solves the Traveling Salesman Problem.
False.

---

4. True or fasle: If every node of a bipartite graph has the same (positive) degree then it contains a perfect matching.
True.

---

5. True or false: If a bipartite graph contains a perfect matching then every subset A of one part has at least $|A|$ neighbors in the other part.
True.

Quiz 27

---

1. Which of the following is an accurate statement about the Tree Shortcut Algorithm (TSA)?

A. Given an arbitrary graph G, TSA finds a minimal spanning tree in G which satisfies the triangle inequality.

B. TSA finds a minimal spanning tree in a graph G, *provided* G satisfies the triangle inequality.

C. TSA finds a solution to the Traveling Salesman Problem in a graph G, *provided* G satisfies the triangle inequality.

D. All of the above.

→*E*. None of the above.

---

2. Which of the following is an accurate statement about a bipartite graph G?

A. If G contains a perfect matching, then the Greedy Algorithm will match at least half of the nodes in G.

B. If every node has degree d, and if $d > 0$, then G contains a perfect matching.

C. If G does not contain a perfect matching then there is a set A of nodes in one part with fewer than $|A|$ neighbors in the other.

→*D*. All of the above.

E. None of the above.

---

3. True or false: There is an efficient algorithm to find a minimal spanning tree.
True.

---

4. True or false: There is an efficient algorithm to find a perfect matching in a bipartite graph (or to determine that there is none).
True.

---

5. True or false: There is an efficient algorithm to solve the Traveling Salesman Problem.
False.

Quiz 28

---

1. True or false: If a bipartite graph G contains a perfect matching then there is a positive d such that each node has degree d.

False.

---

2. True or false: If G is a bipartite graph such that every subset A of one part has at least $|A|$ neighbors in the other, then G contains a perfect matching.

True.

---

3. True or false: If a bipartite graph G contains a perfect matching, then the Greedy Algorithm will find one of them.

False.

---

4. True or false: If G is a bipartite graph which contains a perfect matching, then G has the same number of nodes in the left and the right parts.

True.

---

5. True or false: If G is a bipartite graph with the same number of nodes in the left and the right parts, and if A is subset of the left part with fewer than $|A|$ neighbors on the right, then there is a subset B of the right part with fewer than $|B|$ neighbors on the left.

True.

Quiz 28

(Computational)

---

1. Let E be the elliptic curve $y^2 = x^3 - 6x + 16$, $P = (0, -4)$, and $Q = (3, 5)$. What is $P + Q$?
Slope of $\overline{PQ}$ is 3, hence $P + Q = (6, -14)$.

---

2. Let E be the elliptic curve $y^2 = x^3 - 7x + 6$ and $P = (0, 4)$. What is $2P$?
Slope of tangent at P is $-3/4$, hence $2P = (9/16, 27/64)$.

---

3. Let E be the elliptic curve $y^2 - 2y = x^3 + 2x$ and $P = (0, 0)$. What is $-P$?
The line of symmetry is $y = 1$, hence $-P = (0, 2)$.

---

4. Let E be the elliptic curve $y^2 = x^3 - 7x + 6$. What are the points of order 2 on E?
$(-3, 0)$, $(1, 0)$, and $(2, 0)$.

---

5. Let E be the elliptic curve $y^2 = x^3 + 2$. What are the inflection points of E?
$(0, \sqrt{2})$, $(0, -\sqrt{2})$, $(2, \sqrt{10})$, and $(2, -\sqrt{10})$.

Quiz 30

(Computational)

---

1. Compute $\left(\frac{2}{179}\right)$.
Since 179 mod 16 = 3, $\left(\frac{2}{179}\right) = -1$

---

2. Compute $\left(\frac{179}{181}\right)$.
Since $181 = 1 \bmod 4$, $\left(\frac{179}{181}\right) = \left(\frac{181}{179}\right) = \left(\frac{2}{179}\right) = -1$.

---

3. Is 179 a square modulo 181. (Note: 181 is prime.)
Since $\left(\frac{179}{181}\right) = -1$, 179 is not a square module 181.

---

4. Compute $\left(\frac{3^{16}}{1039}\right)$. (Hint: think!)
Since 3 does not divide 1039, $\left(\frac{3^{16}}{1039}\right) = \left(\frac{3}{1039}\right)^{16} = 1$.

---

5. Compute $\left(\frac{71943}{38187}\right)\left(\frac{38187}{71943}\right)$. (Hint: think!)
$\gcd(71943, 38187) \neq 1$ (3 divides both arguments) hence the Jacobi symbols equal 0.