*What does* $O(< expr >)$ *mean?*

1

*What does* $\Theta(< expr >)$ *mean?*

2

*What does* $\Omega(< expr >)$ *mean?*

3

*Say that the input represents a positive integer,* $x$*, what is the size of* $n$*?*

4

*What does it mean by* $O(1)$*?*

5

*What is the minimum time for any sorting algorithm that uses only number comparisons.*

6

*How do you argue correctness of Euclid's algorithm?*

7

*What would half the correctness proof be for Euclid's algorithm?*

8

*The complexity (i.e. space/running time) has the complexity proportional to $< expr >$.*

2

*The complexity (i.e. running time/space) is bounded by the $< expr >$.*

1

$\lfloor \log_b x \rfloor + 1$ *Where $b$ is the number representation, usually binary (so 2).*

4

*The complexity (i.e. running time/space) is at least by the $< expr >$.*

3

$n \log_2 n$

6

*It takes a constant time, no matter the amount of data, to perform the operation.*

5

*As $r = amodb$, $\exists q$ such that $a = bq + r$, $\therefore r = a - bq$. Suppose $x$ is a factor of $a$ and $b$, then $\exists yandz$ such that $a = xy$, $b = xz$. Hence: $r = xy - xzq$, $r = x(y - zq)$. $\therefore x$ is a factor of $r$ (and also of $b$ and $r$).*

8

*Let $r = amodb$. $hcf(a, b) = hcf(b, r)$ because all factors of $a$ and $b$ are also factors of $b$ and $r$ and vice versa. If they have the same factors, they have the same highest common factor.*

7

$(a.b) mod k =$

9

*Let p be a prime number. What is meant by a primitive root modulo p?*

10

*What does saying that algorithm A runs in time g mean?*

11

*The numbers $r_x$ between 1 and $p-1$ that, when raised by the numbers between 1 and $p-1$ compute all the numbers between 1 and $p-1$ in some order with no repetitions.*

10

$$(a.b)modk = (amodk.bmodk)modk$$

9

*Given an input of size n, the number of operations executed by A is bounded above by g(n).*

11