

Home work Hints:

Q2 How many ways can a factorial be written as a difference of 2 squares?

- Strategies:
- 1) try examples of the problem (eg. use a particular value)
 - 2) Try and solve a similar, but easier problem.
eg. How can you write 12 as a difference of 2 squares
 - 3) For homework for a particular class, try and use something from ~~the~~ class

eg. $4! = 5^2 - 1^2$

factoring $4! = 4 \times 3 \times 2 \times 1 = 2 \times 2 \times 3 \times 2 = 2^3 \times 3$
 $5^2 - 1^2$?

Recall $x^2 - 9 = (x-3)(x+3)$
 $a^2 - b^2 = (a-b)(a+b)$

then

$$5^2 - 1^2 = (5-1)(5+1) = 4 \cdot 6 = 2^2 \cdot 2 \cdot 3 = 2^2 \times 3$$

eg $60 = 6 \times 10$

$$= (a+b) \times (a-b)$$

$$= (8+2) \times (8-2)$$

$$= 8^2 + 2^2 = 64 - 4 = 60$$

Strategy 4) try to find a pattern

Q3 What is the smallest integer...

Factorization fact:

if $n = p_1^{a_1} \times \dots \times p_m^{a_m}$
 then $n^m = p_1^{m a_1} \times \dots \times p_m^{m a_m}$

eg. $12 = 2^2 \times 3$

eg. $12^7 = 2^{14} \times 3^7$

because $n^m = \underbrace{n \times n \times \dots \times n}_m = (p_1^{a_1} \times \dots \times p_m^{a_m}) \times \dots \times (p_1^{a_1} \times \dots \times p_m^{a_m})$

$$= \underbrace{(p_1^{a_1} p_1^{a_1} \dots p_1^{a_1})}_m \dots \underbrace{(p_m^{a_m} \dots p_m^{a_m})}_m = p_1^{ma_1} \dots p_m^{ma_m}$$

Fact $(a^m)^n = a^{mn}$ $(2^3)^5 = 8^5 = 2^{15}$

Ex. if $\frac{1}{2}$ of a is a cube (a is a ^{positive} whole number)
 if $\frac{1}{5}$ of a is a seventh power
 what is the smallest possible value of a ?

this question means: $\frac{1}{2}a = b^3$
 $\frac{1}{5}a = c^7$
 $a = 2b^3$ and $a = 5c^7$

VOTE
 A
 REDO

so assume $a = 2^r 5^s$ then $\frac{a}{2} = 2^{r-1} \times 5^s = b^3$
 and $\frac{a}{5} = 2^r \times 5^{s-1} = c^7$

$$\frac{a^b}{a^c} = a^{b-c}$$

let $b = 2^m 5^n$

then $b^3 = 2^{3m} 5^{3n}$

$$\Rightarrow 2^{3m} 5^{3n} = 2^{r-1} 5^s$$

$$\Rightarrow 3m = r-1 \quad \text{and} \quad 3n = s$$

from $\frac{a}{5} = c^7$

we deduce that

$$r = 7m, \quad m, n$$

$$s-1 = 7n, \quad \text{some integer}$$

so $r-1$ is a mult. of 3

r is a mult. of 7

$$r = 7 \quad b/c \quad 7-1 = 6 = 3 \times 2$$

8. $s-1$ is a mult. of 7
 s is a mult. of 3

$$s = 15$$

so, can take $a = 2^7 5^{15}$

check $\frac{a}{2} = 2^6 5^{15} = (2^2 \times 5^5)^3$
 $\frac{a}{5} = 2^7 5^{14} = (2 \times 5^2)^7$

Next lecture Mersenne primes eg.

$$\text{largest known prime} = 2^{24036583} - 1$$

A proposition - (in logic) is a sentence which is true or false. eg. "Hello!" is not a proposition.
"5 + 7 = 49" is a proposition

propositions are also called statements.

these have a truth value, which is true or false.

propositions are joined by connectives :

eg if p is the statement

"P is a red polygon"

if q is the statement

"P has 3 sides and is a polygon"

not \neg

and \wedge

or \vee

if... then \rightarrow

if and only if \leftrightarrow

$P \wedge Q$

P is a red triangle

$Q \wedge (\neg P)$ = P is a triangle which is not red.

$P \wedge (\neg Q)$ = P is a red polygon which is not a triangle.

$P \rightarrow Q$ = "If P is a red polygon, then P is a triangle."

Proofs - Direct proof -

eg. Theorem - the sum of two odd numbers is even

Proof: Let x and y be 2 odd numbers,

$$\text{so } x = 2r + 1, y = 2s + 1$$

$$\text{so } x + y = 2(r + s + 1)$$

$\therefore x + y$ is even.

Note this Theorem uses a definition.

Definition - an even number is a multiple of 2.

an odd number is not a number divisible by 2.

We also use the following result:

lemma: if x is a positive number then $x = 2r + 1$ for some positive integer.

Proof: let r be the largest integer with $2r < x \Rightarrow 2(r+1) > x$
 $2r < x < 2r + 2 \rightarrow x = 2r + 1$ QED = \square

In a proof by contradiction, we assume what we want to prove is false & draw an obvious contradiction, so the result must be true

Ex: lemma - a positive number has at most one prime factor bigger than its square root, unless the number itself is prime.

Proof: Suppose n is not prime & n is a positive integer, say $p|n$ & $q|n$ & $p, q > \sqrt{n}$, $p \neq q$ 2 different primes

$$\Rightarrow p \times q | n \Rightarrow pq \leq n \quad pq > \sqrt{n} \times \sqrt{n} = n$$

contradiction, so the result is true QED