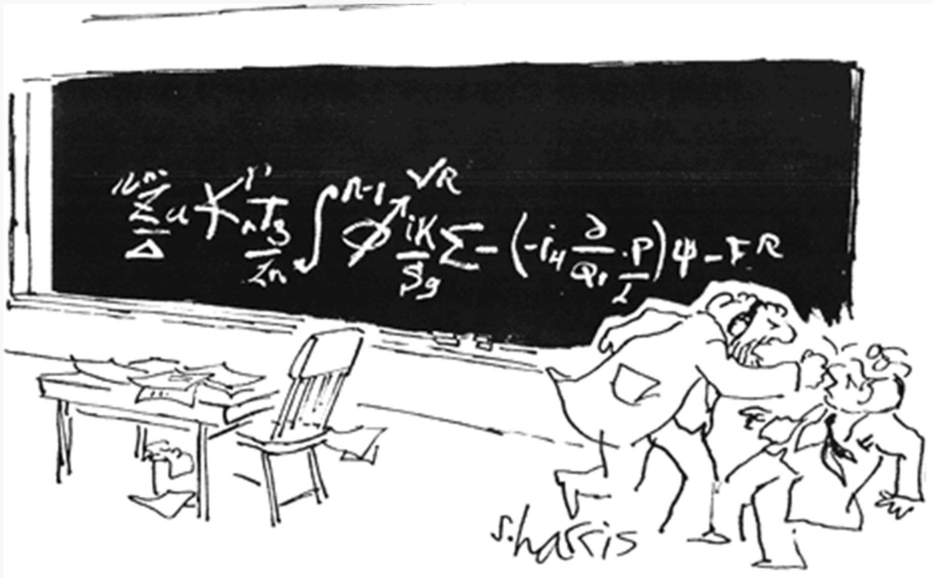
Proof

If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.

— John von Neumann



"You want proof? I'll give you proof!"

Some Facts

If we want to prove some things, we need some facts to work from.

If m and n are integers, then:

- m + n, m – n and m * n are integers
- m^n is an integer (unless n is not positive)

Def: If m and n are integers and n is not 0, then we say that *n divides m* iff there is an integer k such that m = n*k.

Symbolically, we write n | m.

Don't confuse n | m with n / m.

17 | 5 is a false statement; 17 / 5 is the number 3.4

Direct Proof

Want to prove that X implies Y.

Assume that X is true.

Show that this assumption leads to the conclusion that Y must be true.

Since this rules out the possibility that X could be true and Y could be false at the same time, it rules out the possibility that "X implies Y" could ever be false.

Example

Theorem: if A | B and A | C, then A | B + C.

proof:

Suppose that A | B and A | C.

Then by definition, there are integers K and L such that:

B = K*A and C = L*A

Then B + C = K*A + L*A = A*(K + L). Since K + L is the sum of two integers, and therefore is an integer, by definition it follows that

A | B + C.

QED

Some More Theorems

Theorem: if A is even (divisible by 2) then A^2, A^3, … , are all even.

Theorem: if A is odd (not divisible by 2) then A^2, A^3, … , are all odd.

Theorem: if A and B are even then A*B and A + B are even.

Theorem: if A and B are odd then A*B is odd and A + B is even.

Theorem: if A is even and B is odd then A + B is odd.

Theorem: if A^2 is even then A is even.

Theorem: if A^2 is odd then A is odd.

Indirect Proof (Contrapositive)

Want to prove that X implies Y.

Assume that Y is false.

Show that this assumption leads to the conclusion that X must be false.

Since "X implies Y" is logically equivalent to "not Y implies not X", this is sufficient to justify the desired conclusion.

Example

Theorem: if A^2 is odd then A is odd.

proof:

Suppose that A is not odd; then A is even. Therefore, there is an integer K such that A = 2K.

Then $A^2 = (2K)^2 = 2(2K^2)$, and so by definition A^2 is even.

So, A^2 is not odd.

QED

Contradiction

Want to prove X

Assume that X is false

Show that this assumption leads to a logical contradiction

Since the assumption must be false, X must be true

This is a direct proof of a statement of the form "not X implies Y", where Y is false. But that can only be the case if "not X" is false, and hence that X is true.

There are some mathematicians, and some logicians, who question the validity of proof by contradiction… it's a small club.

Example

Theorem: $\sqrt{2}$ is an irrational number.

proof:

Suppose that $\sqrt{2}$ is a rational number; then by definition there are integers M and N, that have no common factors, such that

$$\sqrt{2} = \frac{M}{N}$$

Square both sides and rearrange to get $2N^2 = M^2$

Now this implies that M^2 is even, and therefore that M is even.

But since M^2 is even, there is an integer L such that $M = 2L$; substituting into the equation above and simplifying gives us that

$$N^2 = 2L^2$$

But this implies that N^2 is even and so that N is even. But this contradicts the fact that M and N have no common factors.

QED