Geometry of numbers

Jonathan Block

Summer 2017

Office: DRL 3E2A
e-mail: blockj@math.upenn.edu

Opening exercise: Line up against the wall.
Bubble sort according to how far from
David Rittenhouse Labs you live.

How efficient is this algorithm? $O(n^2)$ $\frac{(n-1)n}{2} = \frac{n^2-n}{2} \leq Cn^2$

Orders of growth.

Number of steps $\leq Cn^2$

C constant.

Merge Sort $O(n \log n)$

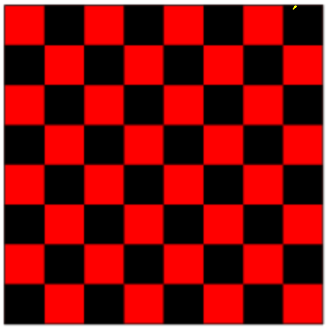
$\log_a = O(\log_b)$

Outline of what we will do:

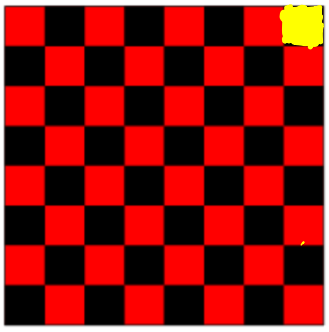
I. What is mathematics about, and proof.
II. Number theory.
    A. Pythagorean triples.
    B. Factorization into primes.
    C. Modular arithmetic.
III. Use of number theory in codes and security protocols.

Mathematics and proof:

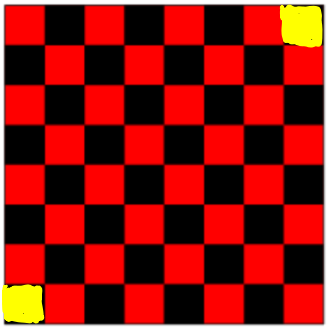
Can you tile an 8x8 chess board with a 2x1 domino?

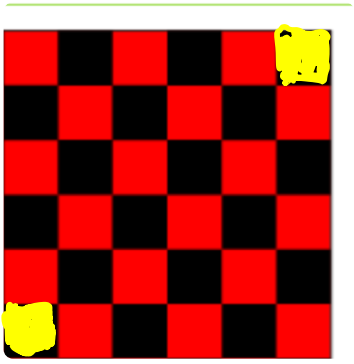


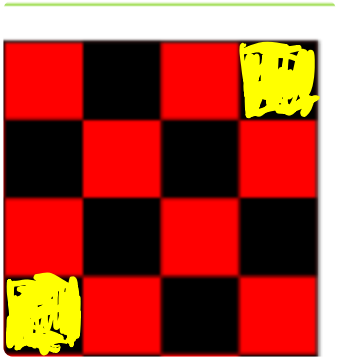
Remove a square. Can you still tile it with the domino?

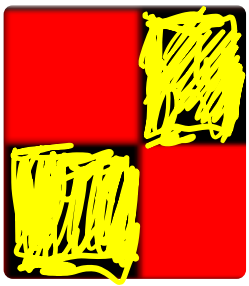


Remove the two squares shown. Can you tile it now?









Theorem. It is impossible to cover the 8x8 chess board with a 2x1 domino leaving only the lower left and upper right squares are uncovered.

Proof:
Notice that when a domino is laid down on the chess board it covers exactly two squares. Moreover, it covers exactly one red and one black square. Thus if we can

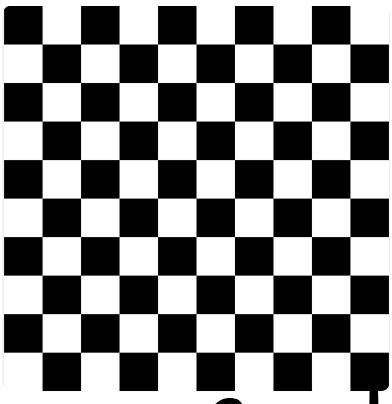
tile a region of the chess board it must cover the same number of red and black squares. On the other hand, if we remove the upper right and bottom left squares then we have 30 black squares and 32 red ones. So in all cases two red squares are left uncovered. QED

Q.E.D.

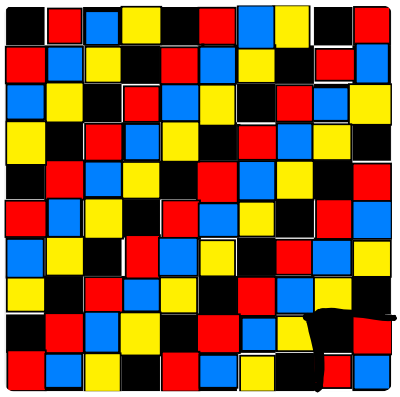
This article is about the Latin phrase. For the physical theory, see quantum electrodynamics. For other uses, see QED (disambiguation).

Q.E.D. (also written QED) is an initialism of the Latin phrase ***quod erat demonstrandum***, meaning "what was to be demonstrated", or, less formally, "thus it has been demonstrated". The phrase is traditionally placed in its abbreviated form at the end of a mathematical proof or philosophical argument when the original proposition has been exactly restated as the conclusion of the demonstration.[1] The abbreviation thus signals the completion of the proof.

Change it up a little. Consider a 10x10 chess board. Can You tile it with a 4x1 domino.



How about an mxn chess board? Conjecture: Can only do this if m or n is divisible by 4.



Each domino covers all four colors.
So any tiling will cover equal numbers of each color.
But there are not equal numbers of each color

The language of mathematics

Mathematicians care about truth. We make statements that we can then determine their "truthyness" or falseness. An important component of such statements is precision. Without precision, we are not sure what the statement we are trying to determine the truth of actually is.

We will do our best to make unambiguous, yet meaningful, sentences, that are either true or false. Nothing can be both true and false. If a sentence is both, it has two meanings: a true one and a false one.
Let me begin by putting together sentences and seeing how they combine.

Here we use capital letters to denote possible statements, i,e, propositions.

Not Not A is true means that A is false. To say that "A dog is not a reptile" is exactly to deny the truth of "The dog is a reptile".

And When we say that A and B are true, we mean that both A is true and B is true. To say that dinner was delicious and not fattening, means that dinner was delicious and not fattening.

You have to watch out when people say that Goebbels was a good Nazi. It looks like they mean to say he was good and he was a Nazi. But, what they mean was that he was good at Naziness. So sometimes ambiguity sneaks in because of the english language.

Or When we say that A or B is true, then we mean that A is true or B is true. It could be that both are true. So, for instance if A is true, then no matter what B is, A or B is true. "Shiela plays the oboe or the clarinet, " means Shiela plays the oboe or Shiela plays the clarinet, or both.

Implies (or if ... then ...) We say that A implies B, if whenever A is true, B is true. Consider "If you give your teacher an apple every day, then you will pass the course." I can only complain if I don't pass having given my teacher an apple every day. Of course, I could pass if I learn the material as well.

It is sometimes useful to write down a "truth table". Here it is easier to give some examples rather than a definition:

A	B	Not A -A	A and B A&B	A or B AVB	A implies B A→B
T	T	F	T	T	T
T	F	F	F	T	F
F	T	T	F	T	T
F	F	T	F	F	T

On the top line we wrote in words the operations, and on the second line, we wrote a symbolic form of the sentence above.

So, when you are being cross examined by this enormous policeman on the road and he asks, “Did you drink before driving or did you not?”, you produce a truth table:
A = I drank and –A = I did not drink. The policeman is asking A V –A. I produce a table like the following:

A	-A	A V –A
T	F	T
F	T	T

And, therefore, you must answer “True, sir.”

Of course, what you mean, and I am sure your lawyer will point this out, that it is true that you either drank or did not drink before driving.

So, if I say that “Being the best candidate will get you elected”, I am committed to accepting the sentence that “Being the best candidate or the biggest buffoon will get you elected”. Am I not?

No, not really. What went wrong? Let’s look at “implication”.

Let A = “You are the best candidate”. And let B = “You are the biggest buffoon”.
Does A → A V B?

A	B	AVB	“A→AVB”
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

So, no matter what, A does imply AVB.

Let’s now think about the proposition that (A ⇒ C) ⇒ (AVB ⇒ C).
Is that necessarily true?

Here, C is the statement that “You will be elected”. We believe that A → C, i.e. that if you are the best candidate, you will be elected.

A	B	C	(A ⇒ C)	AVB	(AVB ⇒ C)	(A ⇒ C) ⇒ (AVB ⇒ C)
T	T	T	T	T	T	T
T	T	F	F	T	F	T
T	F	T	T	T	T	T
T	F	F	F	T	F	T
F	T	T	T	T	T	T
F	T	F	T	T	F	F
F	F	T	F	F	F	T
F	F	F	T	F	T	T

So it's not true.

The problem, we now see, is that in listening to spoken English, we are not always so good at hearing parentheses. We meant (A ⇒ C) V (B⇒C) but heard (AVB⇒C).

By the way, notice how complicated the table got. The more clauses that can have truth values, the larger the table. Because there are now 3 letters, A,B and C, we have 8 possible truth assignments (and only one of the eight led to a problem --- it was the one that said “If you are the biggest buffoon, you will be elected”)
In practice, one has to simply get used to parsing sentences very carefully to know what they mean and do not mean. When you’re stuck, you can produce a truth table and check to be absolutely sure you haven’t neglected any possibilities.

Another useful relationship between statements that mathematicians love is

If and only if. A⇔C means that A is true exactly if C is true. So the truth table looks like:

A	C	A⇔C
T	T	T

T	F	F
F	T	F
F	F	T

In an ideal world, with the previous interpretations of what A and C mean, I would be very happy if A$\Rightarrow$C.
Exercise: Convince yourself that (A$\Leftrightarrow$ B)$\Leftrightarrow$ (A$\Rightarrow$B) & (B$\Rightarrow$A). Express this in words.

Here is a shockingly useful and sometimes confusing tautology.

Proposition: (A$\Rightarrow$B)$\Leftrightarrow$ (-B$\Rightarrow$ -A)

We will first check this by truth tables (there are four cases, because there are two independent parts A and B) and then we'll think about what this means.

A	B	-A	-B	(A$\Rightarrow$B)	(-B$\Rightarrow$ -A)	(A$\rightarrow$B)$\Leftrightarrow$(-B$\rightarrow$ -A)
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

The proposition says that saying that A implies B is exactly the same as saying that not B implies that not A is true i.e. that A is false. In other words, to say that A implies B is exactly the same as saying that if B does not hold, it must be that A is false. For if A were true, B would have to be.

This proposition is the basis for a technique called proof by contradiction that we will use several times.

Another important relation is that
-(AVB)$\Leftrightarrow$ (-A)&(-B).

Also

-(A&B)$\Leftrightarrow$ (-A) V (-B)

“Not” switches around “ands” and “ors”. To say that I am not (both) gorgeous and smart means that I am not gorgeous or I am not smart. I only need fail to have one of these characteristics to fail having them both (if you see what I mean).

It is important to observe how “not” interacts with “every”. ∀ = for all ∃ = there exists

When I deny that “All Americans are open, honest, and friendly” what actually happens?
Denying “open, honest, and friendly” is asserting “un-open or dishonest or unfriendly”. But the “All Americans” becomes “There is some American”.
The denial of “All Americans are open, honest, and friendly” is “There is some American who is un-open, dishonest, or unfriendly”.

And, of course the denial of “There exists” is either of the two equivalent statements “There does not exist...” or “For all things, it is not the case that...”

For example, to deny that “There is a free lunch” means either of the two entirely equivalent statements: “There is no free lunch” or “All lunches are unfree.”

Now, for notation: We will write “∀x” to say “For all x” and we write “∃y” to say “There exists a y.”
So –(∀x P) is “It is not the case that P is true of all x”. It is equivalent to ∃y –P, that is “There is a y so that P is not true of y".

$$-(\forall \text{ A American, A is HOF})$$

$$\exists \text{ A an American so that } (A \neg H) \vee (A \neg O) \vee (A \neg F)$$