COT5405 Homework 1 Solutions

Maksim Levental

November 28, 2014

I'm not good at Algebra. Supposedly there are two camps in math, the geometers and the algebraists, and never the twain shall meet. I'm loathe to affirm such a pseudo-scientific hypothesis but I simply cannot reason about purely algebraic ideas as well as I can about even slightly geometric forms. Case in point: I do not have an intuitive understanding of the Euclidean Algorithm for computing the GCD of two numbers. Sure I understand the proof perfectly well and it's short enough that I can hold it all in short term memory when I'm reading it, but I have trouble recreating it because there's no kernel that's manifestly commonsensical to me. Juxtapose that idea with, for example, Gram-Schmidt orthonormalization. If I never do math again I'd still be able to construct an orthonormal basis for a vector space on my death bed, with my eyes closed, and just after having my hands amputated.

Euclidean algorithm to the rescue (or maybe Euclid to the rescue). Look at this image of a rectangle that's 24 by 60 units.

The idea is that finding the GCD of 24 and 60, from here on denoted by $\gcd(24, 60)$, corresponds to tiling the rectangle with the largest squares of uniform area possible, i.e. some number that all have the same area, with the characteristic dimension of the tiling square being that GCD. Why is this the case? Well firstly, for such a tiling is the characteristic dimension of the tiling square even a common divisor at all? Sure. Any row of the tiling evenly divides the width dimension of the rectangle and any column of the tiling divides the height dimension of the rectangle. In this instance (in the above image) it's a little confusing but the tiling squares are the ones with embossed edges - the tiling is 2x4 with squares of characteristic dimension 12. So $24 \div 2 = 12$ and $60 \div 4 = 12$ and so 12 is a common divisor. Why is this common divisor the ¡strong¿greatest¡/strong¿ common divisor? That takes a little more work, and admittedly requires a fact that's not so geometric, but simple enough to prove that I'm comfortable with it anyway.

The deal is that the tiling above was, presumably (or potentially), derived using the full Euclidean algorithm for computing greatest common divisors. Here's an illustration of the geometric representation of said algorithm (albeit on a rectangle with dimension 462x1071):

What's happening here? The tiling proceeds by attempting to tile the rectangle by the largest possible square that's possibly a divisor of both 462 and 1071, namely a square with characteristic dimension 462. Clearly it falls short - there's a remainder of $1071 - 2 \cdot 462 = 147$. Why then does the tiling proceed with the blue squares (then on down to the red ones)? Here's the part that's purely algebraic (at least as far as I can tell) and justification for iteration with smaller squares: I claim that

$\gcd(a, b) = \gcd(a, b - at)$ for any $t \in \mathbb{Z}$

Proof:

Let $d = gcd(a, b)$. Then d divides a and b, and then d divides at (you get at least one factor of d from a). So d divides $b - at$ (d "factors" out) and therefore $d \leq \gcd(a, b - at)$. Let $d' = \gcd(a, b - at)$. Then d' divides a and $b - at$ and so d' divides $(b - at) + at$, i.e. d' divides b. Therefore $d' \leq \gcd(a, b)$. Finally $d = d'$. Bringing it back - what does this small fact do for us? Look at the gif. If tiling the