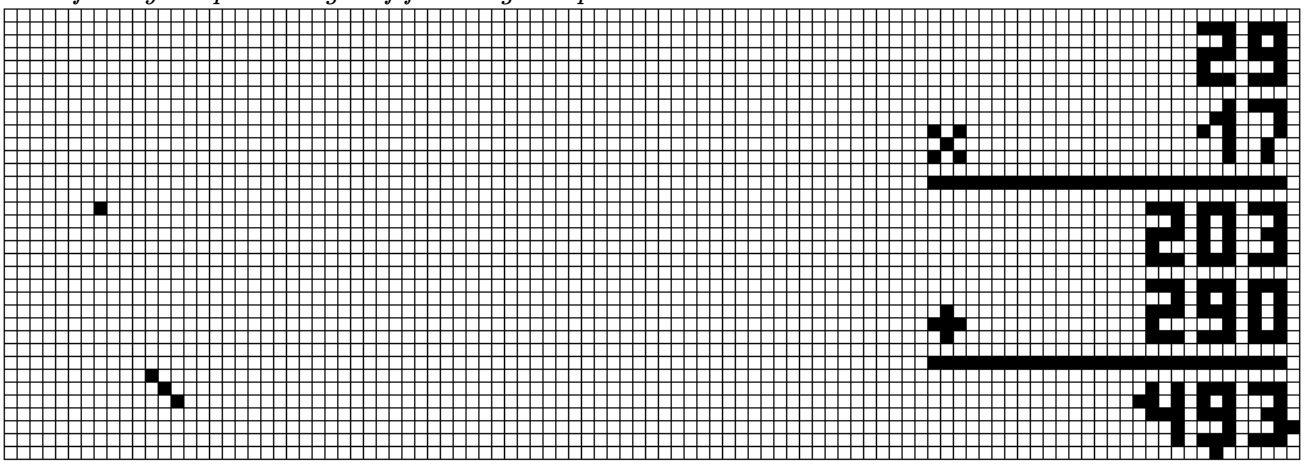
Cryptanalysis through combinatoric correctness

One of many low-pixel images of factoring semiprime 493



Acceptable artifacting in a set of similar images

Acceptable legibility in a set of similar images

In combinatorics, this sample image has a name or index that is somewhere between 1 and 2^n inclusive where n is the number of total squares. And the index of this image WITHOUT artifacting can be incomprehensibly distant from the same image index WITH artifacting. The same can be said for differences in digit styles, colors, and legibility boundaries.

Are there consistent and scalable relationships between similar images? Can these relationships help you jump to nearby similar images and group them together? If so, how would you manipulate the actual index values? And most importantly, how quickly can you find this sample image given only "493" as pixelated above? What if there's something about the sample correctness that makes it stand out… Can you find what it is or prove that it's nothing?

Here's a quote by mathematician Leila Schneps on Grothendieck's example of Galios theory applied to relationships: "It's this idea that any simple picture, made of vertices and segments—whatever you can draw in this way—that there's a natural connection between each and every one of those drawings and an actual equation with coefficients that are algebraic numbers—and this is so weird."

Database compromise through inference

« R » Public study x H B _ X

publicstudyserver.org/Happiton (tracker warning: 16 redirects)

Town of Happiton wellness study

How many participants	own a dog	?				36
How many participants	play music	?				30
How many participants	own a dog	and	earn 200k	?		6
How many participants	own a dog	and	earn 100k	?		30
How many participants	play music	and	earn 100k	?		30
How many participants	▼	▼	▼	?		**Compile!**

Dog owners are split by 2 categories of income.

—*Dog owners earning* 200*k don't play music, therefore your target makes* 200*k—a detail meant to sit confidential on the compiling server.*

Suppose you discover that some target of yours participated in this particular study. So far, you know they own a dog and don't play music, but you wish to know how much money they're making. In this example, you compromised the database and got what you wanted to know, by asking only 5 questions. This is possible even if the numbers are imperfect where you must then infer from quite a few new questions to ensure perfect sums. And there are heavily-researched, applied (US army,) and theoretical formulas which determine compromise for n questions, however, by fudging results, this can be made nearly impossible.

The point is that you can extend this attack and try extracting what emerges from any other database such as a range of primes which failed to factor 1 or more semiprimes. Might 1 tested prime cluster say something about another untested? Can you prove it's impossible for whatever function in question? And most importantly, are extensions of this attack bound to any particular functions—extensions dependent on function particularities?