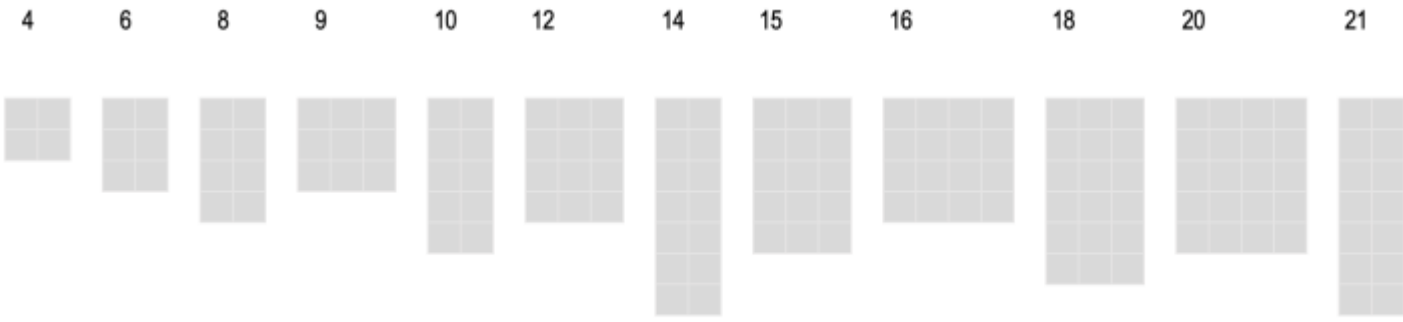
Primes

Description

Some secure encryption methods make use of prime numbers. Iâ??ll examine the method in the next post, but hereâ??s some properties of primes relevant to encryption, presented via simple grid geometry. Hopefully that connects this esoteric field with spatial shapes such as rectangular rooms on a gridded plan.

Composites

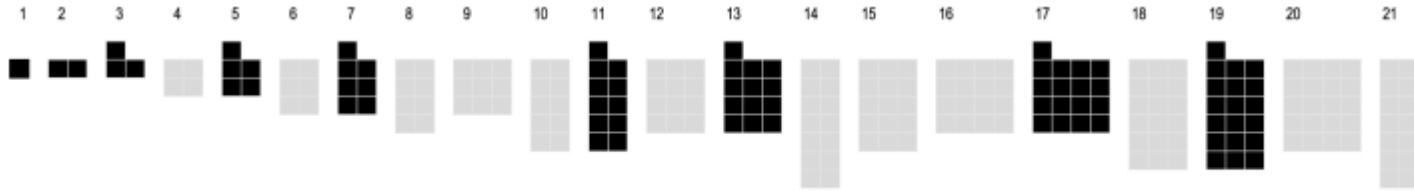
A composite number is a positive integer that is the product of two integers other than 1 or itself. If you draw a rectangle constrained by a regular grid, then the number of grid cells covered by the rectangle will also be a composite number (unless the rectangle occupies just 1 or 2 grid units). Here are the first 13 composite numbers as numbers of grid units as rectangles. There are alternative rectangular shapes for some of these. Any even composite number is divisible by two. So for even composites there will always be a version that is 2 grid units wide.



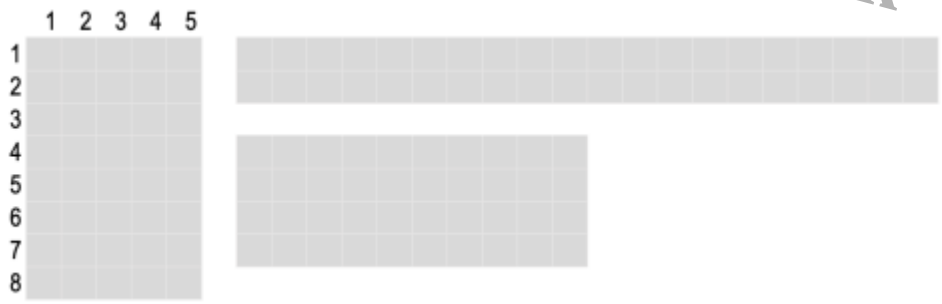
Any composite number can be factored, i.e. broken down into two integers that when multiplied result in that composite number, e.g. the factors of 16 are 4 and 4, or 8 and 2.

Primes

Integers that are not factorable are known as prime numbers. A prime number is a positive integer that is *not* the product of two other integers (except 1 or itself). If you try and draw a rectangle on a regular grid that only takes up a prime number of grid units then there will always be at least a grid cell left over. Prime numbers are always odd (apart from the number 2). You can always turn a prime into a composite by subtracting 1 from it (except for the first 3 primes in the series). I show the first 10 primes in black in the following.

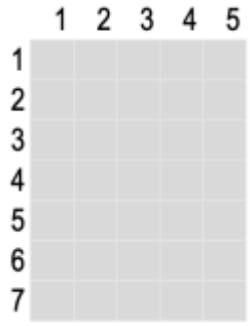


Two numbers (prime or not) multiplied together produce a composite. e.g. 8Ã?5=40. If one of the factors is a composite then there will be more than one rectangle, as well as rotations. In this case 40 units form rectangles of shape 8Ã?5, 20Ã?2 or 4Ã?10.



You canâ??t factor a prime number (i.e. identify 2 integers that when multiplied make that number) , but one or both of the factors of a composite number can be a prime.

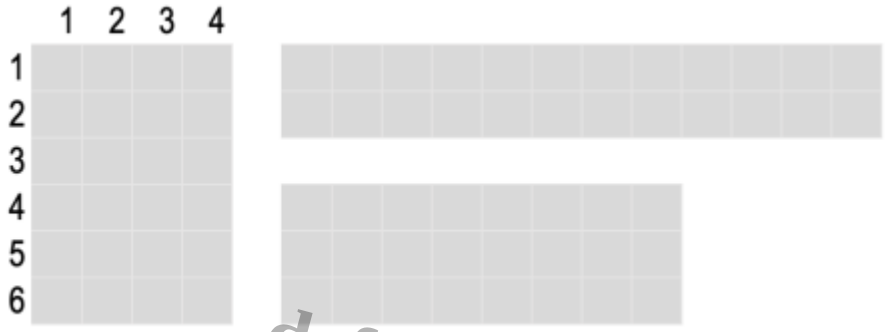
Two primes multiplied together produce a composite number. The factors of that composite will only be those two primes. So, if you multiply the two primes 5 and 7 that produces 35. 35 can only be factored into 5 and 7. Apart from a 90 degree rotation, there is no other arrangement of 35 grid units that is a rectangle. That rule applies to any primes multiplied together. The primes will be unique factors of the resultant composite.



You can check that composites made from multiplying two primes are the only factors of that composite via a helpful website that factors numbers: Prime Factorization Calculator

- https://www.mathsisfun.com/numbers/prime-factorization-tool.html

So rectangles with prime dimensions are rigid. Subtract 1 from each side of each rectangle and you have a rectangle with dimensions that are composites, allowing several arrangements in some cases.



Calculating the prime factors for a number that is prime-factorable is trivial for small composite numbers. The simplest method is to try every number combination, though there are a few rules of thumb that can filter out certain unproductive combinations. Whatever the method, itâ??s very difficult for large numbers, and by â??largeâ?• cryptographers mean numbers of the order of 400 digits long. A helpful tutorial paper by Kathryn Mann explains the scale of the challenge.

> â??The lifetime of the universe is approximately 10^{18} seconds â?? an 18 digit number. Assuming a computer could test one million factorizations per second, in the lifetime of the universe it could check 10^{24} possibilities. But for a 400 digit product, there are 10^{200} possibilities. This means the computer would have to run for 10^{176} times the life of the universe to factor the large number.â?•

In terms of my geometrical grid, such large numbers would assume the distance between gridlines is smaller than the distance between subatomic particles. Interestingly, a hypothetical rectangle of sides that are of huge prime dimensions would still be of fixed dimensions, as opposed to a rectangle of sides that are a huge dimension, one of which is not a prime.

Itâ??s easy to calculate a huge composite number by multiplying two very large primes. Itâ??s virtually â??impossibilityâ?• to reverse engineer the composite to derive the two primes by which it was created.

With modification, thatâ??s the basis of a method for encrypting a message. Establish a method that would require a codebreaker to embark on the impossible task of calculating the two primes of an extremely large number in order to read the message. If the designated recipient has a key by which she can derive the original primes, then she can read the message. Iâ??ll explain the method in the next post.

Reference

- Mann, Kathryn. 2017. The science of encryption: prime numbers and mod n arithmetic. Available online: https://math.berkeley.edu/~kpmann/encryption.pdf (accessed 3 May 2021).

Note

- Banner image is a fragment of Eduardo Paolozziâ??s Newton After Blake sculpture at the Museum of Modern Art in Edinburgh, run through a Photoshop Camera filter (Spectrum).

Category

1. Architecture

Tags

1. cryptography
2. prime numbers

Date Created
May 8, 2021
Author
rcoyne99