GENERATING AND DECONSTRUCTING PRIME NUMBERS

L. M. IONESCU

Abstract. Prime numbers have a rich structure, when viewed as sizes of finite fields. Iteration of an analysis as Klein geometry yields their deconstruction into simpler primes: the POSet structure.

Reversing the process is Euclid's trick of generating new primes. A generalization of this is used by McCanney to cover the set of primes away from primorials as centers. This fast algorithm has a "propagation" flavor.

Generating primes in this manner is also related with Goldbach's Conjecture.

1. Introduction

Prime numbers are sizes of primary finite fields F_p, which in turn can be viewed as the tautological representation of the symmetry group of the corresponding abelian group $(Z/p, +)$:

$$(F_p^*, \cdot) \cong Aut(Z/p, +) \to Aut(Z/p, +).$$

As such, the set of prime numbers exhibits a much richer structure than just viewed ordered by size in the set of natural numbers, where they appear in a chaotic manner. The later is expected when discarding all the other information due to the mentioned algebraic structures.

In this article we present a faster method for *generating prime numbers*, inspired by the work of McCanney [2]. It is based on a generalization of *Euclid's trick* $N = p_1 p_2 ... p_k + 1$ used to prove there are infinitely many primes:

$$N = p_1 p_2 ... p_k \pm q,$$

where q is a previously generated prime number, which always turns out to be larger than the primes p_i used.

Then, instead of using the Erathostene sieve to discard composite numbers resulting in the former procedure, we can just factorize the resulting number, yielding possibly more than just on new prime at a time. The computational burden due to factorization is not considered at this stage. The more economic way would still be to use Erathostene sieve method.

This method for generating prime numbers is in fact inverse to the *deconstruction method* yielding the POSet structure on the prime numbers due to the previously

Date: May 2022.

mentioned richer algebraic structure, which is based on factoring $N-1$ for a prime number N.

The work is based on the articles [3, 1] and the presentation [4].

2. Deconstructing Prime Numbers

The POSet of prime numbers is introduced in [3]. Recall that in the POSet, a prime p has descendants the primes dividing $p-1$ (symmetries of F_p^*).

So, how can we use the POSet structure to generate the prime numbers?

2.1. Generating Prime Numbers.

Generalizing Euclid's trick starting from primorials gives a fast way to conjecturally generate all prime numbers. With reference to the POSEt of primes, obtained by deconstructing primes, this procedure works "upward" in the POSet.

Primorials result from multiplying primes consecutive in the linear order of their sizes. They are the "most composite" numbers, and in fact are *step functions when regarding numbers as functions on the spectrum of* $Spec(Z)$. Yet when decomposing prime numbers we have "gaps", e.g. $2\cdot 3\cdot 7+1=43$ "misses" 5, and the corresponding simple function has two components.

Then the natural question is "What such characteristic functions yield primes?".

2.1.1. *Other Production rules.* Other methods to construct primes involve more general polynomials in prime numbers, e.g. $p_1p_2+p_1p_3+p_2p_3$ etc.

Other production rules for primes have the flavor of a fusion rule for primary fields[1]:

$$p * q = (p-1)(q-1)+1, \quad p \star q = 2\cdot(p-1)/2\cdot(q-1)/2+1.$$

Proposition 2.1. *The two operations $*$ and $\star$ define a commutative (and associative) monoid structure on the POSet of prime numbers P. $(P,*,2)$ is unital.*

Proof 1. *Direct check.*

In fact they correspond to splicing the symmetries of the abelian groups $(Z/p,+)$ and $(F_q,+)$. Since the result is not necessarily a prime number, one may wish to study the corresponding fusion rule coefficients $C^r_{pq} =< p*q, r >$, the power of the prime r in the "tensor product" [2].

In what follows we restrict our attention to the simple polynomials used by McCannes, generalizing Euclid's trick.

[1] Note that F_2 acts as a unit for $*$.

[2] $Z/p\otimes Z/q=\sum C^r_{pq}Z/r$

3. A Fast Prime Numbers Generation Procedure

The procedure is iterative. Start with the prime 2 on our list of primes. Then with $p_{\#1} = 2$ define $N = p_{\#1} \pm 1$ obtaining 1 (discard) and 3. Using the 2nd primorial $p_{\#2} = 2 \cdot 3$, define $N = 6 \pm 1$, yielding 5 and 7 (factor or use sieve method to discard multiples of 2 and 3). Now with the same primorial $6 \pm 5, 7$ retain the positive ones 11 and 13. Again $6+11 = 17$ and $6+13 = 19$ give two more primes; then $6+17 = 23$ while $6 + 19 = 25$ is discarded; $6 + 23 = 29$. Keep iterating and also advancing at the next primorials, used as markers of complexity, ordered by size on the real line. In the previous example, the third primorial $p_{\#3} = 30$ is a center with $30 - 1 = 29$ yielding a previously generated prime.

The detailed algorithm is described in [2]. For optimization there are details that need further study.

Note also that underlying the above procedure there is a weak form (variant) of Goldbach conjecture: any number, here a primorial, is a sum (or difference) of prime numbers.

4. Conclusions

The prime numbers have a rich structure when viewed beyond their order by size: the POSet structure due to the symmetry structure of primary Abelian groups $(Z/p, +)$; specifically, prime numbers are sizes of primary finite fields F_p, viewed as "representations" (Klein geometry). This allows to deconstruct prime numbers into simpler constituent prime numbers.

Reversing the process is Euclid's "trick". A generalization of this, related to Goldbach conjecture, allows to generate prime numbers in a fast "propagating" manner. Primorials are centers of symmetric neighborhoods on the real line, allowing to organize this algorithm of "propagation" of prime numbers outward from this centers.

Further generalizations are suggested, when viewing natural numbers as functions on the set of primes, $Spec(Z)$ and when considering more general polynomials, as decompositions of a prime number.

References

[1] L. M. Ionescu, On prime numbers and the Riemann zeros, https://arxiv.org/abs/2204.00899

[2] J. McCanney, Calculate Primes - Direct Propagation Of The Prime Numbers, Paperback – January 1, 2007.

[3] L. M. Ionescu, A natural POSet structure on the set of prime numbers, https://arxiv.org/abs/1407.6659

[4] L. M. Ionescu, On prime numbers and Riemann zeros, ISU Algebra Seminar presentation, April 14 2022, https://about.illinoisstate.edu/lmiones/research/