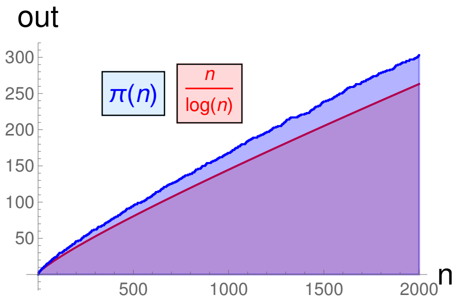
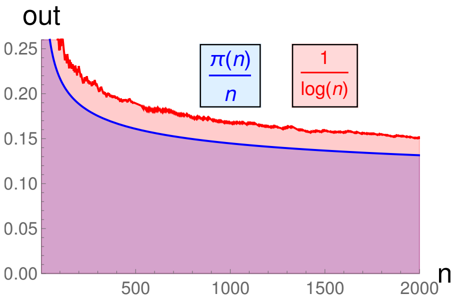
What is...Frobenius' density theorem?

Or: Does it factor?

The prime number theorem $\pi(n) \sim n/\log(n)$





The probability of n being prime is (roughly) $1/\log(n)$

Any hope to compute factors modulo p?

$$f(X) = X^4 + X^3 + 1$$

2	$X^4 + X^3 + 1$	(4)
3	$(X^3 + 2X^2 + 2X + 2)(X + 2)$	$(3, 1)$
5	$(X^3 + 3X^2 + X + 2)(X + 3)$	$(3, 1)$
7	$X^4 + X^3 + 1$	(4)
11	$(X^3 + 9X^2 + 6X + 4)(X + 3)$	$(3, 1)$
13	$X^4 + X^3 + 1$	(4)
17	$(X^3 + 7X^2 + 8X + 14)(X + 11)$	$(3, 1)$
19	$(X^3 + 11X^2 + 15X + 17)(X + 9)$	$(3, 1)$
23	$(X^2 + 4X + 20)(X + 6)(X + 14)$	$(2, 1, 1)$
29	$(X^2 + 12X + 26)(X + 7)(X + 11)$	$(2, 1, 1)$

For example $(-3)^4 + (-3)^3 + 1 = 55 = 0 \bmod 5$ or 11

The prime number theorem for factorizations

\# of appearances of types for the first 10000 primes for $f(X) = X^4 + X^3 + 1$:

(4)	$(3,1)$	$(2,2)$	$(2,1,1)$	$(1,1,1,1)$
2479	3367	1250	2489	414
$\approx 1/4$	$\approx 1/3$	$\approx 1/8$	$\approx 1/4$	$\approx 1/24$

\# of appearances of types for the first 10000 primes for $g(X) = X^4 - 12X^3 + 1$:

(4)	$(3,1)$	$(2,2)$	$(2,1,1)$	$(1,1,1,1)$
2500	3319	1233	2516	430
$\approx 1/4$	$\approx 1/3$	$\approx 1/8$	$\approx 1/4$	$\approx 1/24$

Side node. Finitely many exceptional cases of higher multiplicities, *e.g.* $g(X) = X^4 - 12X^3 + 1 \equiv (X+1)^4 \bmod 2$, are not counted!

Enter, the theorem!

For each $f \in \mathbb{Z}[X]$ of degree n there exists a group $G \subset S_n$ such that the density of primes p for which f has decomposition type c is

$$d(c) = \frac{\#\{g \in G \mid \text{cycle type is } c\}}{\#G}$$

G is the Galois group associated to f

Consequences.

(a) $d(c)$ is the probability of a random prime having factorization type c

(b) Average number of zeros modulo p is the number of factors of f over $\mathbb{Z}$

(c) For a given n there exist only finitely many classes of irreducible polynomials with the same probability type

(d) For $G = S_n$ we have $d(c)^{-1} \in \mathbb{N}$

Only five patterns for degree 4

f	G	(4)	$(3,1)$	$(2,2)$	$(2,1,1)$	$(1,1,1,1)$
X^4+X^3+1	S_4	$1/4$	$1/3$	$1/8$	$1/4$	$1/24$
X^4+3X^2+7X+4	A_4	0	$2/3$	$1/4$	0	$1/12$
X^4-X^2-1	D_4	$1/4$	0	$3/8$	$1/4$	$1/8$
X^4-X^2+1	$(\mathbb{Z}/2\mathbb{Z})^2$	0	0	$3/4$	0	$1/4$
$X^4+X^3+X^2+X+1$	$\mathbb{Z}/4\mathbb{Z}$	$1/2$	0	$1/4$	0	$1/4$

Thank you for your attention!

I hope that was of some help.