

# Popular values and popular subsets of Euler's $\varphi$ -function



Paul Pollack

AMS Special Session on  
Counting Methods in  
Number Theory

January 18, 2018

We let  $\varphi(n)$  denote Euler's totient function. That is,  $\varphi(n)$  is the number of integers in  $[1, n]$  that are relatively prime to  $n$ .

Equivalently,

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

The chief object of study in this talk is the arithmetic function

$$N(m) = \#\{n : \varphi(n) = m\}.$$

We let  $\varphi(n)$  denote Euler's totient function. That is,  $\varphi(n)$  is the number of integers in  $[1, n]$  that are relatively prime to  $n$ .

Equivalently,

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

The chief object of study in this talk is the arithmetic function

$$N(m) = \#\{n : \varphi(n) = m\}.$$

Here are its first several values:

$m$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$N(m)$	2	3	0	4	0	4	0	5	0	2	0	6	0	0

As an example,  $N(12) = 6$ , corresponding to  $\varphi^{-1}(12) = \{13, 21, 26, 28, 36, 42\}$ .

How large might we expect  $N(m)$  to be?

To get a feel for this, one might look at the first moment (or average) of  $N(m)$ . Note that

$$\sum_{m \leq x} N(m) = \#\{n : \varphi(n) \leq x\}.$$

Clearly,  $\varphi(n)$  is never larger than  $n$ . It is also not that much smaller: For all  $n \geq 3$ , we have  $\varphi(n) \gg n / \log \log n$ . Hence, any  $n$  with  $\varphi(n) \leq x$  satisfies  $n \ll x \log \log x$ , and so

$$\sum_{m \leq x} N(m) \ll x \log \log x.$$

The above argument is crude.

While  $\varphi(n)/n$  is occasionally as small as  $O(1/\log \log n)$ , such  $n$  are quite rare. Quantifying this, Erdős and Turán showed that there is a constant  $C > 0$  with

$$\sum_{m \leq x} N(m) \sim Cx, \quad x \rightarrow \infty.$$

It was later noticed that  $C$  could be given in closed form:  
 $C = \zeta(2)\zeta(3)/\zeta(6)$ .

### Proof sketch.

Apply the Wiener–Ikehara theorem to

$$\sum_{m=1}^{\infty} N(m)/m^s = \sum_{n=1}^{\infty} 1/\varphi(n)^s = \zeta(s) \prod_p (1 + (p-1)^{-s} - p^{-s}). \quad \blacksquare$$

So  $N(m)$  behaves like a constant, on average.

So  $N(m)$  behaves like a constant, on average.

### Question

*For how many  $m \leq x$  is  $N(m) > 0$ ? In other words, how does the count of  $\varphi$ -values up to  $x$  grow, as a function of  $x$ ?*

So  $N(m)$  behaves like a constant, on average.

### Question

*For how many  $m \leq x$  is  $N(m) > 0$ ? In other words, how does the count of  $\varphi$ -values up to  $x$  grow, as a function of  $x$ ?*

### Question

*How large can  $N(m)$  be as a function of  $m$ ? In other words, what is the maximal order of  $N(m)$ .*

Starting from about 1930, the 1st question was the subject of several papers, by Pillai, Erdős, Erdős–Hall, Pomerance, Maier–Pomerance, and most recently Ford (1998).

Ford obtains the correct order of the counting function. It behaves roughly like  $\frac{x}{\log x} \exp(C(\log \log \log x)^2)$ , where  $C \approx 0.82$ .



The first and second questions are, of course, related.

Since  $\varphi$  maps  $[1, x]$  into a subset of  $[1, x]$  of size  $x/(\log x)^{1+o(1)}$ , one sees immediately that

$$\max_{m \leq x} N(m) \geq (\log x)^{1+o(1)}.$$

The first and second questions are, of course, related.

Since  $\varphi$  maps  $[1, x]$  into a subset of  $[1, x]$  of size  $x/(\log x)^{1+o(1)}$ , one sees immediately that

$$\max_{m \leq x} N(m) \geq (\log x)^{1+o(1)}.$$

Erdős saw in 1935 how to do better. His idea was to construct a large  $\mathcal{N} \subset [1, x]$  such that  $\varphi(\mathcal{N})$  is entirely contained in the set of numbers that are  $(\log x)$ -smooth, meaning having no prime factors  $> \log x$ . Erdős knew that there were only  $x^{o(1)}$  numbers up to  $x$  that are  $(\log x)$ -smooth. Hence, by the Pigeonhole principle,

$$\max_{m \leq x} N(m) \geq \frac{\#\mathcal{N}}{\#\{(\log x)\text{-smooths } [1, x]\}} \geq x^{o(1)} \#\mathcal{N}.$$

If  $\varphi(n)$  is  $(\log x)$ -smooth, one needs  $p - 1$  to be  $(\log x)$ -smooth for all  $p \mid n$ . So to construct these  $n$ , one needs to know that there are primes  $p$  with  $p - 1$  having only small prime factors.

### Theorem (Baker–Harman 1998)

*For large  $T$ , there are “many” primes  $p \leq T$  with  $p - 1$  having all prime factors at most  $T^{0.2961}$ .*

Erdős in 1935 had a much weaker version of the theorem, with 0.2961 replaced by an exponent slightly smaller than 1.

Using B–H, Erdős’s construction produces  $\mathcal{S}$  with  $\#\mathcal{N} \geq x^{0.7039 - o(1)}$ , each member of  $\varphi(\mathcal{N})$  being  $(\log x)$ -smooth; hence,

$$\max_{m \leq x} N(m) \geq x^{0.7038}.$$

Erdős had this result with 0.7038 replaced by some positive constant.

Probably the exponent 0.2961 can be replaced with any exponent  $> 0$ . This would show that for any  $\epsilon > 0$  and all large  $x$ ,

$$\max_{m \leq x} N(m) \geq x^{1-\epsilon}.$$

This is already beyond reach, but we can be bold and see what happens if we assume something like the Baker–Harman theorem for still smaller values of  $T$ , of the size  $T^{o(1)}$ . The “right” conjecture can be guessed based on assuming that smooth  $p-1$ 's are distributed similarly to smooth  $n$ 's of the same size. This suggests:

### Conjecture

Let  $L(x) = \exp(\log x \cdot \frac{\log \log \log x}{\log \log x})$ . Then

$$\max_{m \leq x} N(m) \geq x/L(x)^{1+o(1)}, \quad (\text{as } x \rightarrow \infty).$$

This conjecture was first proposed by Pomerance (1980).

In the same paper, Pomerance **proved** (unconditionally) that

$$\max_{m \leq x} N(m) \leq x/L(x)^{1+o(1)} \quad (\text{as } x \rightarrow \infty).$$

Thus, subject to plausible conjectures on the distribution of smooth shifted primes, we understand the upper order of  $N(m)$ .

## From popular values to popular subsets

---

Recently I considered the following question: Suppose  $\mathcal{S}$  is a subset of  $[1, x]$  with  $\#\mathcal{S} \approx x^\alpha$ ? What can one say about  $\#\varphi^{-1}(\mathcal{S})$ ? In other words, how large is

$$\sum_{m \in \mathcal{S}} N(m) \quad ?$$

Of course, one can put in Pomerance's pointwise upper bound for  $N(m)$ , but the result is worse than trivial if  $\alpha > 0$ . Remember that the sum is certainly  $\ll x$ , and we cannot bound the size of single term by anything smaller than  $x/L(x)^{1+o(1)}$ .

## Theorem (P., 2018)

Fix  $\alpha \in (0, 1)$ . Then as  $x \rightarrow \infty$ ,

$$\#\varphi^{-1}(\mathcal{S}) \leq x/L(x)^{1-\alpha+o(1)},$$

uniformly in the choice of subsets  $\mathcal{S} \subset [1, x]$  with  $\#\mathcal{S} \leq x^\alpha$ .

Choosing  $\alpha \approx 0$  recovers Pomerance's pointwise bound on  $N(m)$ .

The result is probably best possible for every  $\alpha$ . Let  $\mathcal{S}$  be the set of  $(\log x)^{1/(1-\alpha)}$ -smooths in  $[1, x]$ . Then  $\#\mathcal{S} = x^{\alpha+o(1)}$ . Banks, Friedlander, Pomerance, Shparlinski have shown — conditional on the same conjectures alluded to before — that  $\#\varphi^{-1}(\mathcal{S}) = x/L(x)^{1-\alpha+o(1)}$ .

## One idea

---

The proof uses several estimates from probabilistic number theory/anatomy of integers. It becomes particularly important to understand the frequency of large values of the additive function

$$W(n) := \sum_{p^e \parallel n} \omega(\varphi(p^e)).$$

We do this by estimating a large exponential moment of  $W(n)$ . The proof uses Rankin's trick and is modeled on an earlier argument of Luca and Pomerance bounding

$$\sum_{n \leq x} \tau(\varphi(n)),$$

with  $\tau$  the usual divisor function.



## A problem of Davenport–Heilbronn

---

According to Erdős (1958), Davenport and Heilbronn corresponded about the second moment of  $N(m)$ , i.e., the behavior of

$$\frac{1}{x} \sum_{m \leq x} N(m)^2. \quad (*)$$

Note that the sum counts the number of pairs  $n, n'$  with  $\varphi(n) = \varphi(n') \leq x$ .

Heilbronn proved that  $(*)$  tends to infinity as  $x \rightarrow \infty$ .

## A problem of Davenport–Heilbronn

---

According to Erdős (1958), Davenport and Heilbronn corresponded about the second moment of  $N(m)$ , i.e., the behavior of

$$\frac{1}{x} \sum_{m \leq x} N(m)^2. \quad (*)$$

Note that the sum counts the number of pairs  $n, n'$  with  $\varphi(n) = \varphi(n') \leq x$ .

Heilbronn proved that  $(*)$  tends to infinity as  $x \rightarrow \infty$ .

Taking a single term is enough to show unconditionally that

$$(*) > (x^{0.7038})^2/x > x^{0.4}$$

for large  $x$  and, conjecturally, that

$$(*) > x/L(x)^{2+o(1)}, \quad \text{as } x \rightarrow \infty.$$

There's also a fairly easy upper bound. Let  $A = \max_{m \leq x} N(m)$ . Then

$$\sum_{m \leq x} N(m)^2 \leq A \sum_{m \leq x} N(m) \ll Ax.$$

Since  $A \leq x/L(x)^{1+o(1)}$ , we get that

$$(*) \leq x/L(x)^{1+o(1)}, \quad \text{as } x \rightarrow \infty.$$

Q: What is the correct exponent on  $L(x)$ ? Is it 1, 2 or something inbetween?

There's also a fairly easy upper bound. Let  $A = \max_{m \leq x} N(m)$ . Then

$$\sum_{m \leq x} N(m)^2 \leq A \sum_{m \leq x} N(m) \ll Ax.$$

Since  $A \leq x/L(x)^{1+o(1)}$ , we get that

$$(*) \leq x/L(x)^{1+o(1)}, \quad \text{as } x \rightarrow \infty.$$

**Q:** What is the correct exponent on  $L(x)$ ? Is it 1, 2 or something inbetween?

**Theorem (P., 2018)**

As  $x \rightarrow \infty$ ,

$$(*) \leq x/L(x)^{2+o(1)}.$$

## The number of solutions to $\varphi(n') = \varphi(n)$ , with $n$ given

Let  $C(n) = N(\varphi(n))$ . In other words,  $C(n)$  is the number of  $n'$  with  $\varphi(n') = \varphi(n)$ . Clearly,  $C(n) \geq 1$  for all  $n$ .

### Conjecture (Carmichael, 1907)

$C(n) > 1$  for all  $n$ .

Carmichael's conjecture remains open.

### Theorem (Ford, 1999)

$C(n)$  assumes each integer value  $> 1$  infinitely often.

One could also consider the average and typical values of  $C(n)$ . Studying the average of  $C(n)$  is more or less equivalent to understanding the second moment of  $N(m)$  (the Davenport–Heilbronn question).

What about the typical size of  $C(n)$ ? Erdős and Pomerance showed that for asymptotically 100% of  $n \leq x$  (as  $x \rightarrow \infty$ ), the number  $\varphi(n)$  has  $(\frac{1}{2} + o(1))(\log \log x)^2$  prime factors.

Now the number of integers up to  $x$  with more than  $(\frac{1}{2} + o(1))(\log \log x)^2$  prime factors has size

$$x / \exp((1/2 + o(1))(\log \log x)^2 \log \log \log x).$$

Using this, one can show — as Florian Luca and I did in 2011 — that for 100% of  $n \leq x$  (as  $x \rightarrow \infty$ ), we have

$$C(n) > \exp((1/2 + o(1))(\log \log x)^2 \log \log \log x).$$

Theorem (P., 2018)

*For 100% of  $n \leq x$  (as  $x \rightarrow \infty$ ), we have*

$$C(n) < \exp((1/2 + o(1))(\log \log x)^2 \log \log \log x).$$

## Power values of Euler's function

---

**Question:** Is  $\varphi(n)$  a square for infinitely many  $n$ ?



## Power values of Euler's function

---

**Question:** Is  $\varphi(n)$  a square for infinitely many  $n$ ?

**YES**, since  $\varphi(2^{2k+1}) = (2^k)^2$ , or  $\varphi(5^{2k+1}) = (2 \cdot 5^k)^2$ .

OK, but what if we restrict to **squarefree**  $n$ ? The answer is still yes.

Here is a sketch of a proof. Consider the numbers  $\varphi(p) = p - 1$  for odd primes  $p \leq x$ . Each  $p - 1$  is even and smaller than  $x$ , we can write

$$p - 1 = \prod_{\ell \leq x/2} \ell^{v_\ell(p-1)}.$$

To each  $p$ , we assign the *exponent vector*  $(v_\ell(p - 1) \bmod 2)_{\ell \leq x/2}$ . This lives vector in  $\mathbb{F}_2^k$ , where  $k = \pi(x/2)$ .

To each  $p$ , we assign the *exponent vector*  $(v_\ell(p-1) \bmod 2)_{\ell \leq x/2}$ . This lives vector in  $\mathbb{F}_2^k$ , where  $k = \pi(x/2)$ .

Suppose that some subset of our  $p$ 's is such that the corresponding collection of exponent vectors sums to 0 in  $\mathbb{F}_2^k$ . Then the product of those  $p$ 's — call this  $n$  — has  $\varphi(n)$  a square.

How do we know we can find such a subset? Linear algebra to the rescue! The number of vectors is  $\pi(x) - 1$ , while the dimension of  $\mathbb{F}_2^k$  is  $k = \pi(x/2)$ . So a dependence relation is forced.

So there is at least **one** squarefree  $n$  with  $\varphi(n) = \square$ . But we can re-do the construction after removing the finitely many  $p$ 's dividing  $n$  to produce a new  $n$ , etc.

**Question:** Can we count the number of  $n \leq x$  for which  $\varphi(n)$  is a square? Call this  $V_{\square}(x)$ .

To produce many  $n$  by the above construction, one can restrict the primes  $p$  in the construction to ones for which  $p - 1$  is smooth. Note that this puts the exponent vector in an  $\mathbb{F}_2$ -vector space of small dimension.

Using the Baker–Harman theorem on smooth  $p - 1$ 's, Banks–Friedlander–Pomerance–Shparlinski showed that

$$V_{\square}(x) > x^{0.7038}$$

for large  $x$ .

## Theorem (Banks–Friedlander–Pomerance–Shparlinski)

*Assuming the aforementioned conjectures on smooth shifted primes,*

$$V_{\square}(x) \geq x/L(x)^{1+o(1)}, \quad (x \rightarrow \infty).$$

*In fact, the same lower bound holds for the number of  $n \leq x$  for which  $\varphi(n)$  is a  $k$ th power, for any fixed  $k$ .*

## Theorem (Banks–Friedlander–Pomerance–Shparlinski)

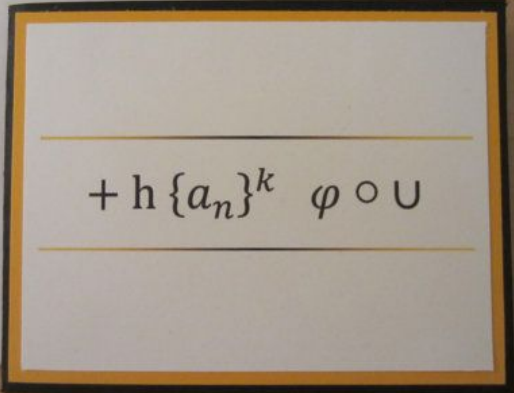
*Assuming the aforementioned conjectures on smooth shifted primes,*

$$V_{\square}(x) \geq x/L(x)^{1+o(1)}, \quad (x \rightarrow \infty).$$

*In fact, the same lower bound holds for the number of  $n \leq x$  for which  $\varphi(n)$  is a  $k$ th power, for any fixed  $k$ .*

## Theorem (P., 2018)

*The number of  $n \leq x$  for which  $\varphi(n)$  is squarefull is at most  $x/L(x)^{1+o(1)}$ , as  $x \rightarrow \infty$ .*

A photograph of a white card with a black border and a yellow inner border, placed on a wooden surface. The card has two horizontal yellow lines. Between these lines, the mathematical expression  $+h \{a_n\}^k \varphi \circ U$  is handwritten in black ink. The card is slightly offset to the right and top from a larger white sheet of paper behind it.
$$+h \{a_n\}^k \varphi \circ U$$