Square values of Euler’s function

Carl Pomerance, Dartmouth College

based on joint work with

P. Pollack
Euler’s function: \( \varphi(n) \) is the cardinality of \( (\mathbb{Z}/n\mathbb{Z})^\times \).

It is ubiquitous in number theory.

Just one very cool result about \( \varphi \):
Computing \( \varphi(n) \) is random polynomial time equivalent to factoring \( n \). (No randomness needed for \( n = pq \).)
Here are some questions about \( \varphi \):

- What is the minimal order of \( \varphi \), the maximal order, the average order, the normal order?

- Is \( \varphi \) ever 1-to-1, that is, is there some number \( n \) such that \( \varphi(m) = n \) has exactly one solution \( m \)? At the other extreme, how popular can values \( n \) be?

- How many values of \( \varphi \) are in \([1, x]\)?
On the first bullet we know quite a lot.

After Mertens we know that $\varphi(n) \geq (1 + o(1))n/(e^\gamma \log \log n)$ as $n \to \infty$ and that this is best possible.

The maximal order of $\varphi(n)$ is $n - 1$, achieved at the primes.

On average, $\varphi(n)$ behaves like $\frac{6}{\pi^2}n$ as $n \to \infty$. (The best error term in this average order is not known.)

Schoenberg (1928) showed that $\varphi(n)/n$ has a continuous distribution function, the forerunner of many similar results.
Carmichael (1922) conjectured that \( \varphi \) is never 1-to-1, that is, if \( \varphi(m) = n \), then there is a number \( m' \neq m \) with \( \varphi(m') = n \). This is known to be true for all \( n \leq 10^{10^{10}} \), a result of Ford, who also showed that if there is one counterexample, then a positive proportion of \( \varphi \)-values are counterexamples!

Erdős (1935) proved that there are infinitely many \( n \) such that \( \varphi(m) = n \) has more than \( n^c \) solutions and he conjectured that this holds for each \( c < 1 \). The best result to date here is by Baker & Harman who have shown there are infinitely many values \( n \) where there are more than \( n^{0.7} \) pre-images under \( \varphi \). It’s known that the Erdős conjecture follows from the Elliott–Halberstam conjecture (Granville).
The set of values of \( \varphi \) was first considered by Pillai (1929):

*The number \( V_\varphi(x) \) of \( \varphi \)-values in \([1, x]\) is \( O(x/(\log x)^c) \), where \( c = \frac{1}{e} \log 2 = 0.254\ldots \).*

**Pillai’s idea:** There are not many values \( \varphi(n) \) when \( n \) has few
prime factors, and if \( n \) has more than a few prime factors, then
\( \varphi(n) \) is divisible by a high power of 2.

Since \( \varphi(p) = p - 1 \), we have \( V_\varphi(x) \geq \pi(x + 1) \gg x/\log x \).

**Erdős (1935):** \( V_\varphi(x) = x/(\log x)^{1+o(1)} \).

**Erdős’s idea:** Deal with \( \Omega(\varphi(n)) \) (the total number of prime
factors of \( \varphi(n) \), with multiplicity). This paper, already
mentioned in connection with popular \( \varphi \)-values, was seminal for
the various ideas introduced. For example, the proof of the
infinitude of **Carmichael** numbers owes much to this paper.
Again: \( V_\varphi(x) = x/(\log x)^{1+o(1)} \).
But: What’s lurking in that “\( o(1) \)”?

After work of Erdős & Hall, Maier & P, and Ford, we now know that \( V_\varphi(x) \) is of magnitude

\[
\frac{x}{\log x} \exp \left( A(\log_3 x - \log_4 x)^2 + B \log_3 x + C \log_4 x \right),
\]

where \( \log_k \) is the \( k \)-fold iterated log, and \( A, B, C \) are explicit constants.

Unsolved: Is there an asymptotic formula for \( V_\varphi(x) \)?
Do we have \( V_\varphi(2x) \sim 2V_\varphi(x) \)?
The same results and unsolved problem pertain as well for the image of $\sigma$, the sum-of-divisors function.

In 1959, Erdős conjectured that the image of $\sigma$ and the image of $\varphi$ has an infinite intersection; that is, there are infinitely many pairs $m, n$ with

$$\sigma(m) = \varphi(n).$$

It is amazing how many famous conjectures imply that the answer is yes!
Yes, if there are infinitely many twin primes:

If \( p, p + 2 \) are both prime, then
\[
\varphi(p + 2) = p + 1 = \sigma(p).
\]

Yes, if there are infinitely many Mersenne primes:

If \( 2^p - 1 \) is prime, then
\[
\varphi(2^p + 1) = 2^p = \sigma(2^p - 1).
\]

Yes, if the Extended Riemann Hypothesis holds.
It would seem a promising strategy to prove that there are at most finitely many solutions to $\sigma(m) = \varphi(n)$; it has some fantastic and unexpected corollaries!

However, Ford, Luca, & P (2010): There are indeed infinitely many solutions to $\sigma(m) = \varphi(n)$.

We gave several proofs, but one proof uses a conditional result of Heath-Brown: If there are infinitely many Siegel zeros, then there are infinitely many twin primes.
Some further results:

**Garaev** (2011): For each fixed number $a$, the number $V_{\varphi, \sigma}(x)$ of common values of $\varphi$ and $\sigma$ in $[1, x]$ exceeds $\exp((\log \log x)^a)$ for $x$ sufficiently large.

**Ford & Pollack** (2011): Assuming a strong form of the prime $k$-tuples conjecture, $V_{\varphi, \sigma}(x) = x/(\log x)^{1+o(1)}$.

**Ford & Pollack** (2012): Most values of $\varphi$ are not values of $\sigma$ and vice versa.
Square values

Banks, Friedlander, P, & Shparlinski (2004): There are more than $x^{0.7}$ integers $n \leq x$ with $\varphi(n)$ a square.

Remark. There are only $x^{0.5}$ squares below $x$. (!)
Here is an outline of the proof: Let $Q$ denote the product of the primes to $B := \log x / \log \log x$. Consider primes $B < p \leq (\log x)^3$ with $p - 1$ having all prime factors at most $B$. There are a lot of these primes (Baker & Harman). Form squarefree numbers $Qm$, where $m$ is composed of some of these primes and $Qm \leq x/Q$. Since $Q = x^{o(1)}$, we find there are more than $x^{2/3-\epsilon}$ numbers $Qm$. Note that $\varphi(Qm)$ has all prime factors at most $B$.

For each number $Qm$ so constructed, consider the exponent vector mod 2 for $\varphi(Qm)$ and let $d \mid Q$ be that divisor with the same exponent vector. Then $dQm \leq x$ and $\varphi(dQm) = d\varphi(Qm)$ is a square.

Optimizing the exponent “3” at the start of the proof gets the result.
We have just considered the number of $n \leq x$ that $\varphi$ maps to a square. But how many squares are $\varphi$-values?

Consider the function $V_{\Box}(x)$, the number of integers $n \leq x$ with $n^2$ a $\varphi$-value.

In the same paper with Banks, Friedlander, & Shparlinski we showed that $V_{\Box}(x) > x^{0.234}$ for all sufficiently large $x$.

This was considerably improved by Banks & Luca (2011) who showed that $V_{\Box}(x) \gg x/(\log x)^4$. A similar result was obtained by a different method by Freiberg (2012).

But what of upper bounds?
Surely we must have $V\Box(x) = o(x)$ as $x \to \infty$, right?

That is, surely it must be that most squares are not $\varphi$-values. Right off the top, except for 1, we can eliminate all odd numbers, so the upper density of numbers $n$ with $n^2$ a $\varphi$-value is at most $\frac{1}{2}$.

Let’s look at an actual count. To $10^8$ there are exactly 26,094,797 numbers $n$ with $n^2$ a $\varphi$-value. That is, more than half of the even numbers to 100 million work.

Are you still sure that $V\Box(x) = o(x)$?
Might there be a positive proportion of integers $n$ with $n^2$ a value of $\varphi$?

Pollack & P (2013): No, the number of $n \leq x$ with $n^2$ a $\varphi$-value is $O(x/(\log x)^{0.0063})$. The same goes for $\sigma$.

We also improved the lower bound of Banks & Luca, getting $V\Box(x) \gg x/(\log^2 x \log \log x)$. 
An idea of the proofs:

The lower bound is fairly straightforward. Let \( y = \log^2 x \) and consider primes \( q \leq x \) with \( q \equiv 1 \pmod{p^2} \) for some prime \( p \in [y, 2y] \) and with \( (q - 1)/p^2 \) not divisible by any prime in \( [y, 2y] \). There are a lot of these primes \( q \) and via Cauchy–Schwarz one can get lots of pairs of these primes \( q_1, q_2 \) corresponding to \( p_1^2, p_2^2 \), respectively, and with \( (q_1 - 1)/p_1^2 = (q_2 - 1)/p_2^2 \). Then \( \varphi(q_1 q_2) \) is a square.

This gets \( \gg x / (\log x \log \log x)^2 \) distinct choices of integers \( \sqrt{\varphi(q_1 q_2)} \leq x \), and to gain an additional factor of \( \log \log x \) one can consider more dyadic intervals up to \( y^{1+\epsilon} \).
The upper bound $V_{\square}(x) \leq x/(\log x)^{0.0063}$ is considerably more difficult.

Say $\varphi(m) = n^2$ with $n \leq x$. Let $p$ denote the largest prime factor of $n$. Then one of the following 4 possibilities must occur:

- $p^3 \mid m$,
- $p^2 \mid m$ and $\exists$ some prime $q \mid m$, $q \equiv 1 \pmod{p}$,
- $\exists$ two primes $q_1, q_2 \mid m$, $q_1 \equiv q_2 \equiv 1 \pmod{p}$,
- $\exists$ some prime $q \mid m$, $q \equiv 1 \pmod{p^2}$.

The first two cases do not contribute much, so most of the work is in the 3rd and 4th cases.
The 3rd case: $q_1, q_2 \mid m$, $q_1 \equiv q_2 \equiv 1 \pmod{p}$.

Write $q - 1 = apb^2$ with $ap$ squarefree. Since $(q_1 - 1)(q_2 - 1) \mid n^2$, we have

$$n = ua_1a_2a_3b_1b_2p,$$

with $a_1a_2a_3p$ squarefree and

$$a_1a_3pb_1^2 + 1 \text{ prime, } a_2a_3pb_2^2 + 1 \text{ prime}.$$

By the sieve and using $p > x^{1/\log \log x}$, the number of $n$ is

$$\ll \sum_{u,a_1,a_2,a_3,b_1,b_2} \frac{x(\log \log x)^6}{ua_1a_2a_3b_1b_2(\log x)^3}.$$
You can see we’re in a spot of trouble here! But using that we may assume that $\Omega(n) \leq \alpha \log \log x$, with $\alpha$ fixed and a tad larger than 1, we can use Rankin’s trick to estimate the contribution here and see that it is

$$x(\log \log x)^6 \ll \frac{x(\log \log x)^6}{(\log x)^{3-\alpha-\alpha \log(\alpha/6)}}.$$ 

We win for $\alpha$ small enough (but greater than 1), since $1 + \log 6 < 3$.

The last case when $q \mid m$, $q \equiv 1 \pmod{p^2}$: Here we have $n = uabp$, with $a(bp)^2 + 1$ prime. The sieve is trickier here and we need to consider sub-cases depending on the size of the largest prime factor of $ua$. But in the end it (barely) works.
We get the same result for numbers $n$ for which $n^2$ is a $\sigma$-value. We also get the same for the number of squarefull numbers $n \leq x^2$ with $n$ a $\varphi$-value (and probably too for $\sigma$-values).

What about $\lambda$ (Carmichael’s universal exponent function)?

Note that the range of $\lambda$ has density 0 (Erdős, P, Schmutz) and there are finer results, but we’re asking about squares in the range. We have not proved anything, but I have a heuristic argument that the set of numbers $n$ with $n^2$ a $\lambda$-value has asymptotic density $\frac{1}{2}$. That is, for almost all even $n$, $n^2 = \lambda(m)$ is solvable.
Happy birthday Ram!