Solved and unsolved problems in elementary number theory

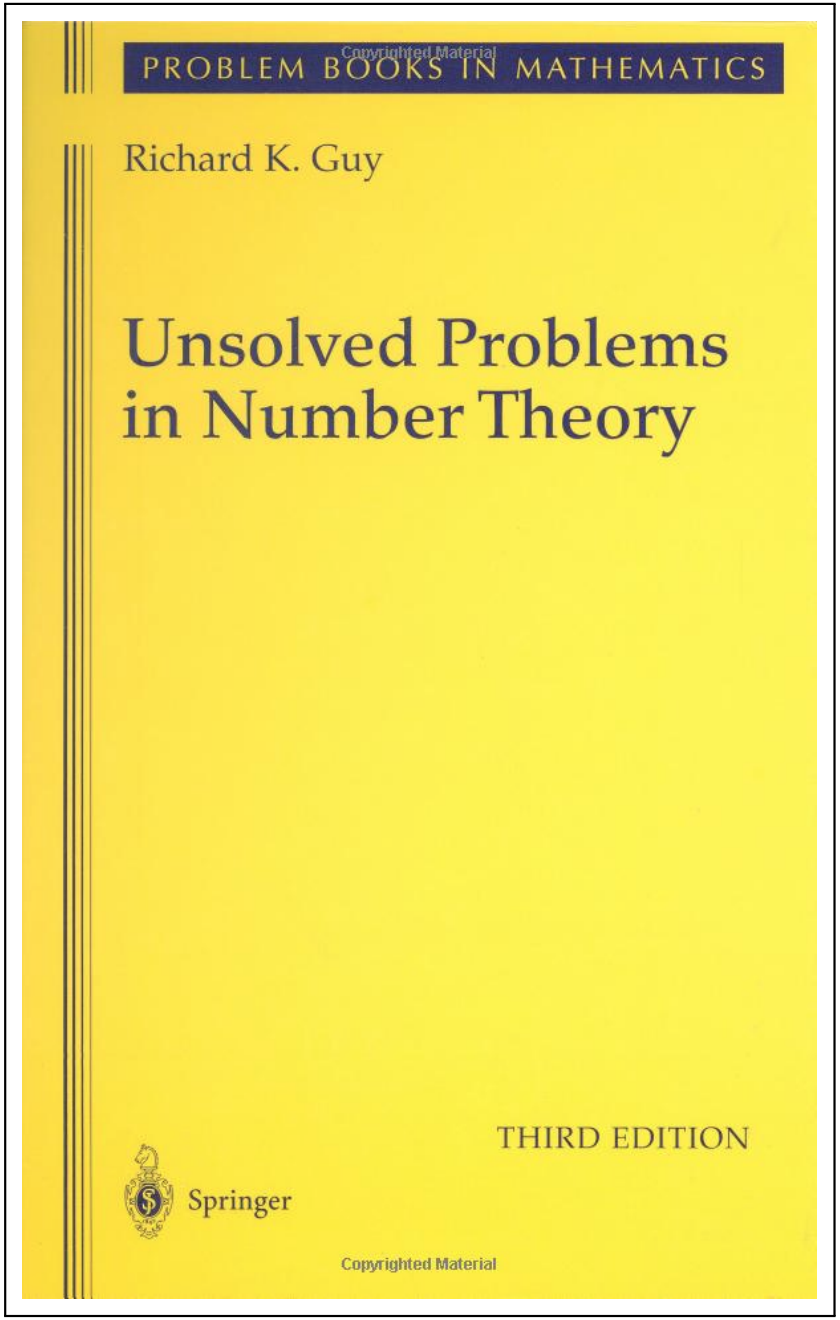
The University of Georgia

Paul Pollack

Athens/Atlanta Number Theory Seminar

February 25, 2014

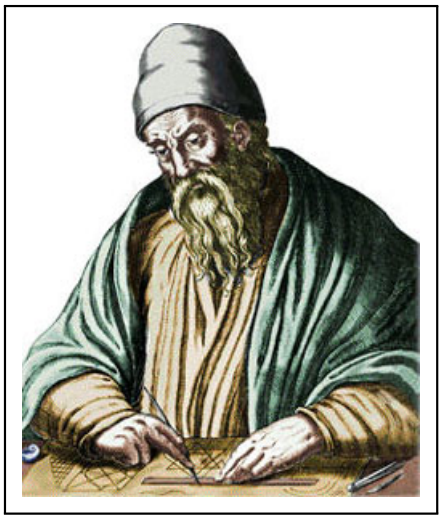
For a less *slanted* view of the subject, consider purchasing:



PART I: The simplest proof in number theory ?

Theorem (Euclid, ca. 300 BCE)

There are infinitely many primes.



Proof.

If $p_1, \ldots, p_n$ is any finite list of primes, let p_{n+1} be any prime divisor of $p_1 \cdots p_n + 1$. Then p_{n+1} is a new prime.

There are unsolved problems connected not just with the infinitude of primes but even with this proof of the infinitude of primes!

Answer the question and then question the answer

Two questions of A. A. Mullin (1963):

(i) Let $p_1 = 2$ and let p_{n+1} be the **smallest** prime factor of $p_1 \dots p_n + 1$.

(ii) Let $p_1 = 2$ and let p_{n+1} be the **largest** prime factor of $p_1 \dots p_n + 1$.

Call the sequence $\{p_n\}$ resulting from (i) the **first Euclid–Mullin sequence**, and (ii) the **second Euclid–Mullin sequence**.

'How many' of the infinitely many primes do we see in the resulting sequence $\{p_n\}$?

You can see a lot just by looking

First Euclid–Mullin sequence:
2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739, 23003, 30693651606209, 37, 1741, 1313797957, 887, 71, 7127, 109, 23, 97, 159227, 643679794963466223081509857, 103, 1079990819, 9539, 3143065813, 29, 3847, 89, 19, 577, 223, 139703, 457, 9649, 61, 4357, ...

You can see a lot just by looking

First Euclid–Mullin sequence:
2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739, 23003, 30693651606209, 37, 1741, 1313797957, 887, 71, 7127, 109, 23, 97, 159227, 643679794963466223081509857, 103, 1079990819, 9539, 3143065813, 29, 3847, 89, 19, 577, 223, 139703, 457, 9649, 61, 4357, ...

Second Euclid–Mullin sequence:
2, 3, 7, 43, 139, 50207, 340999, 2365347734339, 468022564147112 9, 136884520658012 9, 889340324577880670089824574922371

You can see a lot just by looking

First Euclid–Mullin sequence:
2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739, 23003, 30693651606209, 37, 1741, 1313797957, 887, 71, 7127, 109, 23, 97, 159227, 643679794963466223081509857, 103, 1079990819, 9539, 3143065813, 29, 3847, 89, 19, 577, 223, 139703, 457, 9649, 61, 4357, ...

Second Euclid–Mullin sequence:
2, 3, 7, 43, 139, 50207, 340999, 2365347734339, 468022564147112 9, 136884520658012 9, 889340324577880670089824574922371

Conjecture (Shanks)

Every prime appears in the first Euclid–Mullin sequence.

Theorem

5 *never appears in the 2nd Euclid–Mullin sequence.*

Proof.

Suppose that 5 appears as p_{n+1}. Then 5 is the largest prime factor of $p_1 \cdots p_n + 1 = 6p_3 \cdots p_n + 1$, using $p_1 = 2$ and $p_2 = 3$. So

$$6p_3 \cdots p_n + 1 = 2^a 3^b 5^c$$

for some nonnegative integers a, b, c with $c \geq 1$.

Theorem

5 *never appears in the 2nd Euclid–Mullin sequence.*

Proof.

Suppose that 5 appears as p_{n+1}. Then 5 is the largest prime factor of $p_1 \cdots p_n + 1 = 6p_3 \cdots p_n + 1$, using $p_1 = 2$ and $p_2 = 3$. So

$$6p_3 \cdots p_n + 1 = 2^a 3^b 5^c$$

for some nonnegative integers a, b, c with $c \geq 1$.
In fact, $a = b = 0$, since LHS is prime to 6. So

$$6p_3 \cdots p_n + 1 = 5^c.$$

But LHS is 3 (mod 4) while RHS is 1 mod 4.

Cox and van der Poorten (1968) showed that all of

$$5, 11, 13, 17, 19, 23, 29, 31, 37, 41, \text{ and } 47$$

are missing from the second Euclid–Mullin sequence.

Cox and van der Poorten (1968) showed that all of

$$5, 11, 13, 17, 19, 23, 29, 31, 37, 41, \text{ and } 47$$

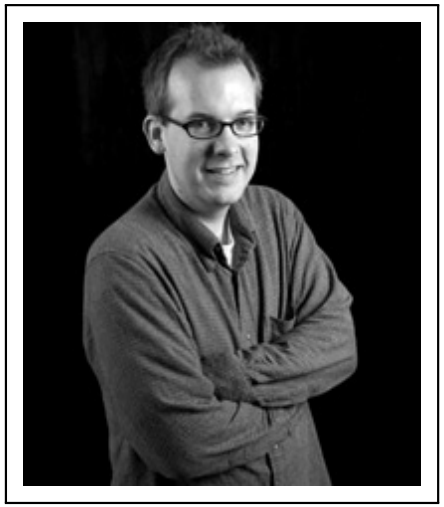
are missing from the second Euclid–Mullin sequence.

Conjecture

Infinitely many primes are missing.

Theorem (Booker, 2012)

The Cox–van der Poorten conjecture is true.



Simpler proof (P. and Treviño, 2014) to appear in the Amer. Math. Monthly. We use only quadratic reciprocity and elementary facts about the distribution of squares and nonsquares modulo p.

Conjecture

Only a density zero set of prime numbers appears in the second Euclid–Mullin sequence.

Even under GRH, Booker's proof only gives about $\sqrt{x}$ missing primes up to x.

Theorem (Booker)

Suppose that there is no algorithm to decide whether or not a prime belongs to the second Euclid–Mullin sequence. Then the conjecture is true!

In the beginning...

Inductively define a sequence of primes $p_1, p_2, \ldots$ by letting $p_1 = 2$ and then letting p_{k+1} be the least prime not already chosen that divides

$$\prod_{i \in \mathcal{S}} p_i + 1$$

for some subset $\mathcal{S}$ of $\{1, 2, \ldots, k\}$.
Does this sequence contain every prime?

In the beginning...

Inductively define a sequence of primes $p_1, p_2, \ldots$ by letting $p_1 = 2$ and then letting p_{k+1} be the least prime not already chosen that divides

$$\prod_{i \in \mathcal{S}} p_i + 1$$

for some subset $\mathcal{S}$ of $\{1, 2, \ldots, k\}$.
Does this sequence contain every prime?

Theorem (Pomerance, unpublished)

Yes! And in fact, p_i is the ith prime for every $i \geq 5$.

Pomerance has called this generating the primes "from nothing."

Filling a much-needed gap in the literature

Recall that the Möbius function is the arithmetic function which vanishes at nonsquarefree integers n and which satisfies

$$\mu(p_1 \cdots p_k) = (-1)^k$$

when $p_1 \cdots p_k$ is a product of distinct primes.

Lemma

The sum $\sum_{d|n} \mu(d)$ *takes the value* 1 *when* $n = 1$ *and the value* 0 *otherwise.*

Filling a much-needed gap in the literature

Recall that the Möbius function is the arithmetic function which vanishes at nonsquarefree integers n and which satisfies

$$\mu(p_1 \cdots p_k) = (-1)^k$$

when $p_1 \cdots p_k$ is a product of distinct primes.

Lemma

The sum $\sum_{d|n} \mu(d)$ takes the value 1 when $n = 1$ and the value 0 otherwise.

Let's suppose that there are only finitely many primes, and let's call their product D. Consider the power series

$$A(x) := \sum_{n=1}^{\infty} a_n x^n, \quad \text{where} \quad a_n = \sum_{\substack{d|n \\ d|D}} \mu(d).$$

Now μ is supported on the divisors of D, and so $A(x) = x$.

We can reverse the order of summation to get that

$$A(x) := \sum_{d|D} \mu(d) \sum_{n:\ d|n} x^d$$

$$= \sum_{d|D} \mu(d)(x^d + x^{2d} + \dots) = \sum_{d|D} \mu(d) x^d \frac{1}{1 - x^d}.$$

Now μ is supported on the divisors of D, and so $A(x) = x$.

We can reverse the order of summation to get that

$$A(x) := \sum_{d|D} \mu(d) \sum_{n:\ d|n} x^d$$
$$= \sum_{d|D} \mu(d)(x^d + x^{2d} + \dots) = \sum_{d|D} \mu(d) x^d \frac{1}{1-x^d}.$$

Multiplying by $1 - x^D$ to clear denominators gives

$$x(1-x^D) = A(x)(1-x^D)$$
$$= \sum_{d|D} \mu(d) x^d f_d(x), \quad \text{where} \quad f_d(x) = \frac{1-x^D}{1-x^d} \in \mathbb{C}[x].$$

OK, so ...

$$x(1-x^D) = A(x)(1-x^D)$$
$$= \sum_{d|D} \mu(d) x^d f_d(x), \quad \text{where} \quad f_d(x) = \frac{1-x^D}{1-x^d} \in \mathbb{C}[x].$$

Each $f_d(x)$ has degree $D-d$, so each $x^d f_d(x)$ has degree D.
So $\sum_{d|D} \mu(d) x^d f_d(x)$ has degree at most D.

But $x(1-x^D)$ has degree $D+1$, and this is a contradiction.

OK, so ...

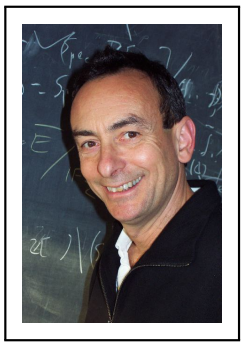
$$x(1-x^D) = A(x)(1-x^D)$$
$$= \sum_{d|D} \mu(d) x^d f_d(x), \quad \text{where} \quad f_d(x) = \frac{1-x^D}{1-x^d} \in \mathbb{C}[x].$$

Each $f_d(x)$ has degree $D-d$, so each $x^d f_d(x)$ has degree D.
So $\sum_{d|D} \mu(d) x^d f_d(x)$ has degree at most D.

But $x(1-x^D)$ has degree $D+1$, and this is a contradiction.

Remark

This is a version, due to Ken Ribet, of a proof published by P. in Elem. Math., 2011. Ribet's version comes from a MATH 115 HW assignment: Students were asked to decide whether or not the proof was correct.



PART II: Messing with perfection

Let $s(n) := \sum_{d|n, d<n} d$ denote the sum of the proper divisors of n.
So if $\sigma(n) = \sum_{d|n} d$ is the usual sum-of-divisors function, then

$$s(n) = \sigma(n) - n.$$

For example,

$$s(4) = 1 + 2 = 3, \qquad \sigma(4) = 1 + 2 + 4 = 7.$$

The ancient Greeks said that n was ...
deficient if $s(n) < n$, for instance $n = 5$;
abundant if $s(n) > n$, for instance $n = 12$;
perfect if $s(n) = n$, for example $n = 6$.

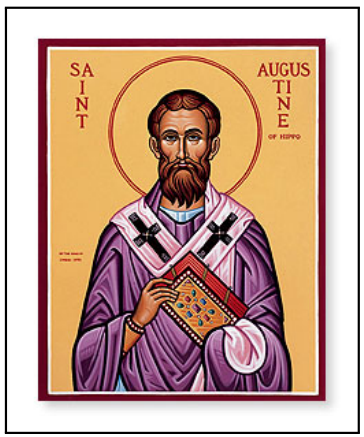
Nicomachus (60-120 AD) and the Goldilox theory

The superabundant number is . . . as if an adult animal was formed from too many parts or members, having "ten tongues", as the poet says, and ten mouths, or nine lips, and provided with three lines of teeth; or with a hundred arms, or having too many fingers on one of its hands. . . . The deficient number is . . . as if an animal lacked members or natural parts . . . if he does not have a tongue or something like that.

. . . In the case of those that are found between the too much and the too little, that is in equality, is produced virtue, just measure, propriety, beauty and things of that sort — of which the most exemplary form is that type of number which is called perfect.

Iamblichus (245-325) and St. Augustine (354-430) on perfect numbers

The number Six .... which is said to be perfect ... was called Marriage by the Pythagoreans, because it is produced from the intermixing of the first meeting of male and female; and for the same reason this number is called Holy and represents Beauty, because of the richness of its proportions.



Six is a number perfect in itself, and not because God created all things in six days; rather, the converse is true. God created all things in six days because the number is perfect.

A deep thought

We tend to scoff at the beliefs of the ancients.

A deep thought

We tend to scoff at the beliefs of the ancients.
But we can't scoff at them personally, to their faces, and this is what annoys me.

– Jack Handey

From numerology to number theory

Perfect numbers are solutions to the equation $\sigma(N) = 2N$. What do these solutions look like?

Theorem (Euclid)

If $2^n - 1$ is a prime number, then $N := 2^{n-1}(2^n - 1)$ is a perfect number.

For example, $2^2 - 1$ is prime, so $N = 2 \cdot (2^2 - 1) = 6$ is perfect.
A slightly larger example ($\approx$ 35 million digits) corresponds to $n = 57885161$.

From numerology to number theory

Perfect numbers are solutions to the equation $\sigma(N) = 2N$. What do these solutions look like?

Theorem (Euclid)

If $2^n - 1$ is a prime number, then $N := 2^{n-1}(2^n - 1)$ is a perfect number.

For example, $2^2 - 1$ is prime, so $N = 2 \cdot (2^2 - 1) = 6$ is perfect.
A slightly larger example ($\approx$ 35 million digits) corresponds to $n = 57885161$.

Theorem (Euler)

If N is an **even** *perfect number, then N comes from Euclid's rule.*

From numerology to number theory

Perfect numbers are solutions to the equation $\sigma(N) = 2N$. What do these solutions look like?

Theorem (Euclid)

If $2^n - 1$ is a prime number, then $N := 2^{n-1}(2^n - 1)$ is a perfect number.

For example, $2^2 - 1$ is prime, so $N = 2 \cdot (2^2 - 1) = 6$ is perfect.
A slightly larger example ($\approx$ 35 million digits) corresponds to $n = 57885161$.

Theorem (Euler)

If N is an **even** *perfect number, then N comes from Euclid's rule.*

Problem

Are there any **odd** *perfect numbers?*

Anatomy of an odd perfect integer

. . . a prolonged meditation has satisfied me that the existence of [an odd perfect number] - its escape, so to say, from the complex web of conditions which hem it in on all sides - would be little short of a miracle.

– J. J. Sylvester

Anatomy of an odd perfect integer

> *. . . a prolonged meditation has satisfied me that the existence of [an odd perfect number] - its escape, so to say, from the complex web of conditions which hem it in on all sides - would be little short of a miracle.*
>
> – J. J. Sylvester

If N is an odd perfect number, then:

1. N has the form $p^e M^2$, where $p \equiv e \equiv 1 \pmod 4$ (Euler),
2. N has at least 10 distinct prime factors (Nielsen, 2014) and at least 101 prime factors counted with multiplicity (Ochem and Rao, 2012),
3. $N > 10^{1500}$ (Ochem and Rao, 2012).

Conjecture

There are no odd perfect numbers.

Counting perfects

Let $V'(x)$ denote the number of odd perfect numbers $n \leq x$.

Theorem (Hornfeck)

We have $V'(x) \leq x^{1/2}$.

Counting perfects

Let $V'(x)$ denote the number of odd perfect numbers $n \leq x$.

Theorem (Hornfeck)

We have $V'(x) \leq x^{1/2}$.

Proof.

Each odd perfect N has the form $p^e M^2$. If $N \leq x$, then $M \leq \sqrt{x}$.
We will show that each M corresponds to at most one N.
In fact, since $\sigma(p^e)\sigma(M^2) = \sigma(N) = 2N = 2p^e M^2$, we get

$$\frac{\sigma(p^e)}{p^e} = \frac{2M^2}{\sigma(M^2)}.$$

The right-hand fraction depends only on M.
The left-hand side is already a reduced fraction, since
$p \nmid 1 + p + \cdots + p^e = \sigma(p^e)$. Thus, p^e depends only on M.

Counting perfects

Let $V(x)$ denote the number of perfect numbers $n \leq x$.

Theorem

We have the following estimates for $V(x)$:

Counting perfects

Let $V(x)$ denote the number of perfect numbers $n \leq x$.

Theorem

We have the following estimates for $V(x)$:

$$\textit{Volkmann, 1955} \qquad V(x) = O(x^{5/6})$$

Counting perfects

Let $V(x)$ denote the number of perfect numbers $n \leq x$.

Theorem

We have the following estimates for $V(x)$:

$$\begin{aligned} \textit{Volkmann, 1955} \qquad & V(x) = O(x^{5/6}) \\ \textit{Hornfeck, 1955} \qquad & V(x) = O(x^{1/2}) \end{aligned}$$

Counting perfects

Let $V(x)$ denote the number of perfect numbers $n \leq x$.

Theorem

We have the following estimates for $V(x)$:

$$\begin{aligned} \textit{Volkmann, 1955} \qquad & V(x) = O(x^{5/6}) \\ \textit{Hornfeck, 1955} \qquad & V(x) = O(x^{1/2}) \\ \textit{Kanold, 1956} \qquad & V(x) = o(x^{1/2}) \end{aligned}$$

Counting perfects

Let $V(x)$ denote the number of perfect numbers $n \leq x$.

Theorem

We have the following estimates for $V(x)$:

$$\begin{aligned} \textit{Volkmann, 1955} \quad & V(x) = O(x^{5/6}) \\ \textit{Hornfeck, 1955} \quad & V(x) = O(x^{1/2}) \\ \textit{Kanold, 1956} \quad & V(x) = o(x^{1/2}) \\ \textit{Erdős, 1956} \quad & V(x) = O(x^{1/2-\delta}) \end{aligned}$$

Counting perfects

Let $V(x)$ denote the number of perfect numbers $n \leq x$.

Theorem

We have the following estimates for $V(x)$:

$$\begin{aligned}
\textit{Volkmann, 1955} \quad & V(x) = O(x^{5/6}) \\
\textit{Hornfeck, 1955} \quad & V(x) = O(x^{1/2}) \\
\textit{Kanold, 1956} \quad & V(x) = o(x^{1/2}) \\
\textit{Erdős, 1956} \quad & V(x) = O(x^{1/2-\delta}) \\
\textit{Kanold, 1957} \quad & V(x) = O(x^{1/4}\frac{\log x}{\log\log x})
\end{aligned}$$

Counting perfects

Let $V(x)$ denote the number of perfect numbers $n \leq x$.

Theorem

We have the following estimates for $V(x)$:

$$\begin{aligned}
\textit{Volkmann, 1955} \quad & V(x) = O(x^{5/6}) \\
\textit{Hornfeck, 1955} \quad & V(x) = O(x^{1/2}) \\
\textit{Kanold, 1956} \quad & V(x) = o(x^{1/2}) \\
\textit{Erdős, 1956} \quad & V(x) = O(x^{1/2-\delta}) \\
\textit{Kanold, 1957} \quad & V(x) = O(x^{1/4}\frac{\log x}{\log\log x}) \\
\textit{Hornfeck \& Wirsing, 1957} \quad & V(x) = O(x^{\epsilon})
\end{aligned}$$

This is the end of the story (so far), but it shouldn't be!
If there are no odd perfect numbers, and if plausible seeming conjectures on the distribution of Mersenne primes hold, then

$$V(x) \sim \frac{e^{\gamma}}{\log 2} \log\log x.$$

Here γ is the Euler–Mascheroni constant.

The best known version of the Hornfeck–Wirsing method, due to Wirsing (1959), gives an upper bound

$$V(x) \leq x^{C/\log\log x},$$

where C is an absolute, positive constant.

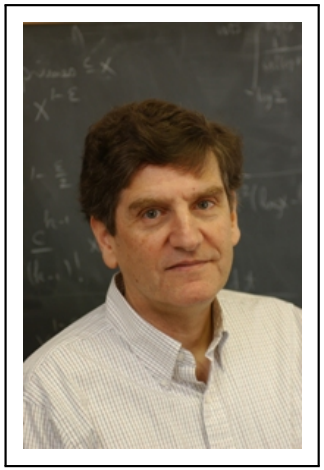
Approximating perfection

There are countless variations on the theme of perfect numbers, some of which seem just as intractable — maybe even moreso.

Definition (Cattaneo, 1951)

We say n is **quasiperfect** if $\sigma(n) = 2n + 1$.

We have no examples!



Theorem (Pomerance–P., 2013)

The number of quasiperfect $n \leq x$ is $O_\epsilon(x^{\frac{1}{4}+\epsilon})$.

Prime-perfect numbers

Pomerance suggested calling a number **prime-perfect** if n and $\sigma(n)$ have the same set of distinct prime factors. For example, if $n = 270$, then

$$n = 2 \cdot 3^3 \cdot 5, \quad \textit{and} \quad \sigma(n) = 2^4 \cdot 3^2 \cdot 5,$$

so n is prime-perfect.

Prime-perfect numbers

Pomerance suggested calling a number **prime-perfect** if n and $\sigma(n)$ have the same set of distinct prime factors. For example, if $n = 270$, then

$$n = 2 \cdot 3^3 \cdot 5, \quad \textit{and} \quad \sigma(n) = 2^4 \cdot 3^2 \cdot 5,$$

so n is prime-perfect.

Theorem (Pomerance–P., 2011)

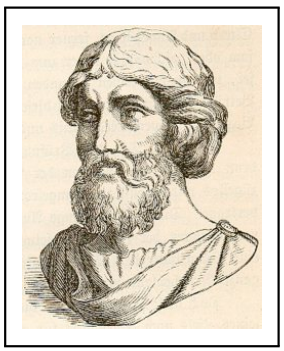
The number of prime-perfect $n \le x$ is at most $x^{1/3+\epsilon}$ for all large x. Moreover, there **are** *infinitely many prime-perfect numbers n. In fact, for each k, there are more than $(\log x)^k$ examples $n \le x$ once x is large.*

Did Pythagoras invent arithmetic dynamics?

Consider the map $s\colon \mathbb{N} \cup \{0\} \to \mathbb{N} \cup \{0\}$, extended to have $s(0) = 0$. A perfect number is nothing other than a positive integer fixed point.

We say n is **amicable** if n generates a two-cycle: in other words, $s(n) \neq n$ and $s(s(n)) = n$. For example,

$$s(220) = 284, \quad \text{and} \quad s(284) = 220.$$



Pythagoras, when asked what a friend was, replied:

One who is the other I, such are 220 and 284.

The distribution of amicable numbers

There are over ten million amicable pairs known, but we have no proof that there are infinitely many.
But we can still guess!

Let $A(x)$ be the number of pairs with smaller member $\leq x$.

Conjecture (Bratley–Lunnon–McKay, 1970)

$A(x) = o(\sqrt{x})$.

They based this on a complete list of amicable pairs to 10^7.

A voice of dissent

Here is data up to 10^{13} from a more recent survey of Garcia, Pedersen, and te Riele (2004):

x	$A(x)$	$A(x)\ln(x)/\sqrt{x}$	$A(x)\ln^2(x)/\sqrt{x}$	$A(x)\ln^3(x)/\sqrt{x}$	$A(x)\ln^4(x)/\sqrt{x}$
10^5	13	0.473	5.45	62.7	722
10^6	42	0.580	8.02	111	1530
10^7	108	0.550	8.87	143	2305
10^8	236	0.435	8.01	148	2717
10^9	586	0.384	7.96	165	3418
10^{10}	1427	0.329	7.57	174	4011
10^{11}	3340	0.268	6.78	172	4347
10^{12}	7642	0.211	5.83	161	4454
10^{13}	17519	0.166	4.96	149	4448

In contrast with B-L-McK, Erdős suggests that for each $\epsilon > 0$ and each positive integer K, one has

$$x^{1-\epsilon} < A(x) < x/(\log x)^K.$$

Upper bounds

Let $V_2(x)$ denote the number of $n \leq x$ belonging to some amicable pair. (Thus, $A(x) \leq V(x) \leq 2A(x)$.)

Theorem

We have the following estimates for $V_2(x)$:

Upper bounds

Let $V_2(x)$ denote the number of $n \leq x$ belonging to some amicable pair. (Thus, $A(x) \leq V(x) \leq 2A(x)$.)

Theorem

We have the following estimates for $V_2(x)$:

Erdős, 1955 $\qquad V_2(x) = o(x)$

Upper bounds

Let $V_2(x)$ denote the number of $n \leq x$ belonging to some amicable pair. (Thus, $A(x) \leq V(x) \leq 2A(x)$.)

Theorem

We have the following estimates for $V_2(x)$:

Erdős, 1955	$V_2(x) = o(x)$
Rieger, 1973	$V_2(x) = O(x/(\log_4 x)^{1/2-\epsilon})$

Upper bounds

Let $V_2(x)$ denote the number of $n \leq x$ belonging to some amicable pair. (Thus, $A(x) \leq V(x) \leq 2A(x)$.)

Theorem

We have the following estimates for $V_2(x)$:

Erdős, 1955	$V_2(x) = o(x)$
Rieger, 1973	$V_2(x) = O(x/(\log_4 x)^{1/2-\epsilon})$
Erdős & Rieger, 1975	$V_3(x) = O(x/\log_3 x)$

Upper bounds

Let $V_2(x)$ denote the number of $n \leq x$ belonging to some amicable pair. (Thus, $A(x) \leq V(x) \leq 2A(x)$.)

Theorem

We have the following estimates for $V_2(x)$:

Erdős, 1955	$V_2(x) = o(x)$
Rieger, 1973	$V_2(x) = O(x/(\log_4 x)^{1/2-\epsilon})$
Erdős & Rieger, 1975	$V_3(x) = O(x/\log_3 x)$
Pomerance, 1977	$V(x) = O(x/\exp(c\sqrt{\log_3 x \log_4 x}))$

Upper bounds

Let $V_2(x)$ denote the number of $n \leq x$ belonging to some amicable pair. (Thus, $A(x) \leq V(x) \leq 2A(x)$.)

Theorem

We have the following estimates for $V_2(x)$:

Erdős, 1955	$V_2(x) = o(x)$
Rieger, 1973	$V_2(x) = O(x/(\log_4 x)^{1/2-\epsilon})$
Erdős & Rieger, 1975	$V_3(x) = O(x/\log_3 x)$
Pomerance, 1977	$V(x) = O(x/\exp(c\sqrt{\log_3 x \log_4 x}))$
Pomerance, 1981	$V_2(x) = O(x/\exp((\log x)^{1/3}))$

Upper bounds

Let $V_2(x)$ denote the number of $n \leq x$ belonging to some amicable pair. (Thus, $A(x) \leq V(x) \leq 2A(x)$.)

Theorem

We have the following estimates for $V_2(x)$:

Erdős, 1955	$V_2(x) = o(x)$
Rieger, 1973	$V_2(x) = O(x/(\log_4 x)^{1/2-\epsilon})$
Erdős & Rieger, 1975	$V_3(x) = O(x/\log_3 x)$
Pomerance, 1977	$V(x) = O(x/\exp(c\sqrt{\log_3 x \log_4 x}))$
Pomerance, 1981	$V_2(x) = O(x/\exp((\log x)^{1/3}))$
Pomerance, 2014	$V_2(x) = O(x/\exp((\log x)^{1/2}))$

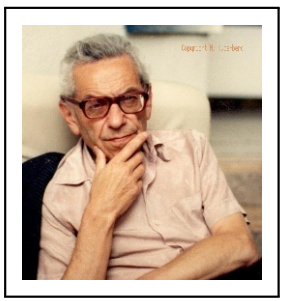
Sociable numbers

More generally, we call n a k-**sociable number** if n starts a cycle of length k. (So perfect corresponds to $k = 1$, amicable to $k = 2$.) For example,

$$2115324 \mapsto 3317740 \mapsto 3649556 \mapsto 2797612 \mapsto 2115324 \mapsto \ldots$$

is a sociable 4-cycle. We know 221 cycles of order > 2.

Let $V_k(x)$ denote the number of k-sociable numbers $n \leq x$.



Theorem (Erdős, 1976)

Fix k. The set of k-sociable numbers has asymptotic density zero. In other words, $V_k(x)/x \to 0$ as $x \to \infty$.

Counting sociables

How fast does $V_k(x)/x \to 0$? Erdős's proof gives ...

Counting sociables

How fast does $V_k(x)/x \to 0$? Erdős's proof gives ...

$$V_k(x)/x \leq 1/\overbrace{\log\log\cdots\log}^{3k \text{ times}} x.$$

In joint work with Mits Kobayashi and Carl Pomerance, we obtain more reasonable bounds. A further improvement is possible for odd k.

Theorem (P., 2010)

Suppose k is odd, and let $\epsilon > 0$. Then

$$V_k(x) \leq x/(\log x)^{1-\epsilon}$$

for all large x.

Counting sociables

What if we count all sociable numbers at once? Put

$$V(x) := V_1(x) + V_2(x) + V_3(x) + \dots$$

Is it still true that most numbers are not sociable numbers?

Counting sociables

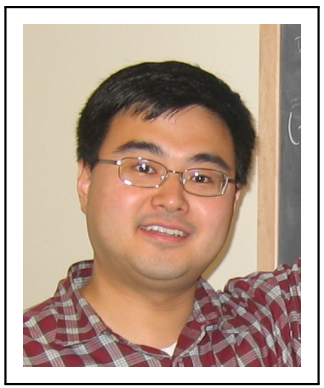
What if we count all sociable numbers at once? Put

$$V(x) := V_1(x) + V_2(x) + V_3(x) + \dots$$

Is it still true that most numbers are not sociable numbers?

Theorem (K.–P.–P., 2009)

$$\limsup V(x)/x \leq 0.0021.$$



Theorem (K.–P.–P., 2009)

The number of $n \leq x$ which belong to a cycle entirely contained in $[1, x]$ is $o(x)$, as $x \to \infty$.

Here 0.0021 is standing in for the density of **odd abundant numbers**, odd numbers n for which $s(n) > n$ (e.g., $n = 945$).

A parting shot: Perfect polynomials

A function field analogue of perfect numbers was proposed by E. F. Canaday, the first doctoral student of L. Carlitz.

Definition

We say a polynomial $A(T)$ in one variable over $\mathbb{F}_2$ is **perfect** if $A = \sum_{D|A} D$, where D runs over all divisors of A in $\mathbb{F}_2[T]$.

A parting shot: Perfect polynomials

A function field analogue of perfect numbers was proposed by E. F. Canaday, the first doctoral student of L. Carlitz.

Definition

We say a polynomial $A(T)$ in one variable over $\mathbb{F}_2$ is **perfect** if $A = \sum_{D|A} D$, where D runs over all divisors of A in $\mathbb{F}_2[T]$.

Canaday originally called these 'one-rings'.

A parting shot: Perfect polynomials

A function field analogue of perfect numbers was proposed by E. F. Canaday, the first doctoral student of L. Carlitz.

Definition

We say a polynomial $A(T)$ in one variable over $\mathbb{F}_2$ is **perfect** if $A = \sum_{D|A} D$, where D runs over all divisors of A in $\mathbb{F}_2[T]$.

Canaday originally called these 'one-rings'.

Theorem (Canaday, 1941)

The perfect polynomials that split completely over $\mathbb{F}_2$ are exactly those of the form $A = (T(T+1))^{2^n-1}$.

Canaday found several other sporadic examples:

Degree	Factorization into Irreducibles
5	$T(T+1)^2(T^2+T+1)$
	$T^2(T+1)(T^2+T+1)$
11	$T(T+1)^2(T^2+T+1)^2(T^4+T+1)$
	$T^2(T+1)(T^2+T+1)^2(T^4+T+1)$
	$T^3(T+1)^4(T^4+T^3+1)$
	$T^4(T+1)^3(T^4+T^3+T^2+T+1)$
15	$T^3(T+1)^6(T^3+T+1)(T^3+T^2+1)$
	$T^6(T+1)^3(T^3+T+1)(T^3+T^2+1)$
16	$T^4(T+1)^4(T^4+T^3+1)(T^4+T^3+T^2+T+1)$
20	$T^4(T+1)^6(T^3+T+1)(T^3+T^2+1)(T^4+T^3+T^2+T+1)$
	$T^6(T+1)^4(T^3+T+1)(T^3+T^2+1)(T^4+T^3+1)$

Motivated by this list, Canaday made the following conjecture:

Conjecture

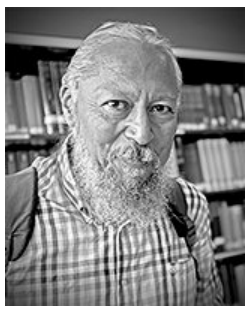
There are no **odd** *perfect polynomials. Here "odd" means divisible by neither* T *nor* $T + 1$*.*

Motivated by this list, Canaday made the following conjecture:

Conjecture

There are no **odd** *perfect polynomials. Here "odd" means divisible by neither T nor $T+1$.*

Not hard to show that if T is a factor of a perfect polynomial, then so is $T+1$, and that any odd perfect polynomial is a square. Very little is known towards the conjecture; the sharpest results we have is:



Theorem (Gallardo and Rahavandrainy, 2009)

Any odd perfect A has at least 5 *distinct irreducible factors.*

The analogous conjecture over $\mathbb{F}_q$ fails quite often, e.g., whenever q is a proper prime power (Gallardo–P.–Rahavandrainy, 2008).

Part III: An Euler ϕ-for-all

(this pun brought to you by L. Thompson )

As usual, we let $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. Its most famous appearance is in **Euler's theorem**: $a^{\phi(n)} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$.

Part III: An Euler ϕ-for-all

(this pun brought to you by L. Thompson )

As usual, we let $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. Its most famous appearance is in **Euler's theorem**: $a^{\phi(n)} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$.
Many other appearances throughout mathematics:

Theorem (Szele, 1947)

Every group of order n is cyclic if and only if $\gcd(n, \phi(n)) = 1$.

Erdős (1948) showed that this condition cuts out a set with counting function $\sim e^{-\gamma} x / \log_3 x$ as $x \to \infty$.

How do we understand the Euler function?

The same way we understand anything else – by asking and answering insightful questions!

- How many numbers up to x belong to the range of the Euler function?
- What is the multiplicative structure of numbers that appear in the range?

How do we understand the Euler function?

The same way we understand anything else – by asking and answering insightful questions!

- How many numbers up to x belong to the range of the Euler function?
- What is the multiplicative structure of numbers that appear in the range?

Theorem (I. M. Trivial)

From the prime number theorem,

$$\begin{aligned} \#\{\phi(n) \leq x\} &\geq \#\{p \leq x\} \\ &\approx x/\log x, \quad \textit{for large } x. \end{aligned}$$

A matching upper bound?

Put $V(x) := \#\{\phi(n) \leq x\}$.

Theorem (Pillai, 1929)

$V(x) \ll x/(\log x)^{\log 2/e}$.

Proof sketch.

"Most" $n \leq x$ are divisible by a large number of odd primes, say at least K such. If n is divisible by K odd primes, then $2^K \mid \phi(n)$. But there are only $x/2^K$ integers $n \leq x$ divisible by 2^K. Now optimize on K; we end up with $K = \frac{\log_2 x}{e}$.

By looking at the total number of prime factors of $\phi(n)$ (with multiplicity), this was improved by Erdős.

Theorem (Erdős, 1934)

For each $\epsilon > 0$, *we have* $V(x) \ll x/(\log x)^{1-\epsilon}$.

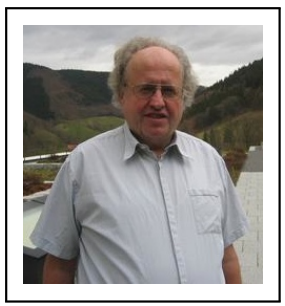
OK, so $V(x) = x/(\log x)^{1+o(1)}$, as $x \to \infty$.
A lot can hide in a $o(1)$ term.

By looking at the total number of prime factors of $\phi(n)$ (with multiplicity), this was improved by Erdős.

Theorem (Erdős, 1934)

For each $\epsilon > 0$, we have $V(x) \ll x/(\log x)^{1-\epsilon}$.

OK, so $V(x) = x/(\log x)^{1+o(1)}$, as $x \to \infty$.
A lot can hide in a $o(1)$ term.



Theorem (Maier and Pomerance, 1988)

For a certain constant $C \approx 0.8178\cdots$ (given implicitly), the following holds: As $x \to \infty$,

$$V(x) = \frac{x}{\log x} \exp((C + o(1))(\log\log\log x)^2).$$

Theorem (Ford, 1998)

For certain constants $C \approx 0.8178\ldots$ *and* $D \approx 2.176\ldots$, *we have*

$$V(x) \asymp \frac{x}{\log x} \exp\Big((C(\log_3 x - \log_4 x)^2 + D\log_3 x - (D + \frac{1}{2} - 2C)\log_4 x\Big).$$

Theorem (Ford, 1998)

For certain constants $C \approx 0.8178\ldots$ *and* $D \approx 2.176\ldots$, *we have*

$$V(x) \asymp \frac{x}{\log x} \exp((C(\log_3 x - \log_4 x)^2 + D\log_3 x - (D + \frac{1}{2} - 2C)\log_4 x).$$

Open problem

Get an asymptotic formula for $V(x)$, as $x \to \infty$.

Open problem

Short of answering the last question, at least decide whether $V(2x)/V(x) \to 2$ as $x \to \infty$.

Theorem (Ford, 1998)

For certain constants $C \approx 0.8178\ldots$ *and* $D \approx 2.176\ldots$, *we have*

$$V(x) \asymp \frac{x}{\log x} \exp\bigl(C(\log_3 x - \log_4 x)^2 + D\log_3 x - (D + \frac{1}{2} - 2C)\log_4 x\bigr).$$

One taste of the underlying structure theory:
Typical "preimages" have about $2C\log_3 x$ prime factors.
For an absolute constant $\rho = 0.54259\ldots$, the ith largest prime factor $q_i(n)$ satisfies

$$\log_2 q_i \approx \rho^{i-1}\log_2 x$$

for small values of i.

Open problem (Erdős, $\leq$ 1959)

Show that there are infinitely many numbers m in the range of both the Euler ϕ-function and the sum-of-divisors function σ.

This is entirely believable:

Open problem (Erdős, $\leq$ 1959)

Show that there are infinitely many numbers m in the range of both the Euler ϕ-function and the sum-of-divisors function σ.

This is entirely believable:

(i) follows from the twin prime conjecture; if $p, p+2$ is a twin prime pair, then $\phi(p+2) = p+1 = \sigma(p)$.

Open problem (Erdős, $\leq$ 1959)

Show that there are infinitely many numbers m in the range of both the Euler ϕ-function and the sum-of-divisors function σ.

This is entirely believable:

(i) follows from the twin prime conjecture; if $p, p+2$ is a twin prime pair, then $\phi(p+2) = p+1 = \sigma(p)$.

(ii) true if there are infinitely many Mersenne primes $2^n - 1$; then $\sigma(2^n - 1) = 2^n = \phi(2^{n+1})$

Open problem (Erdős, $\leq$ 1959)

Show that there are infinitely many numbers m in the range of both the Euler ϕ-function and the sum-of-divisors function σ.

This is entirely believable:

(i) follows from the twin prime conjecture; if $p, p+2$ is a twin prime pair, then $\phi(p+2) = p+1 = \sigma(p)$.

(ii) true if there are infinitely many Mersenne primes $2^n - 1$; then $\sigma(2^n - 1) = 2^n = \phi(2^{n+1})$

(iii) true under GRH (Pomerance, unpublished)

Open problem (Erdős, $\leq$ 1959)

Show that there are infinitely many numbers m in the range of both the Euler ϕ-function and the sum-of-divisors function σ.

This is entirely believable:

(i) follows from the twin prime conjecture; if $p, p+2$ is a twin prime pair, then $\phi(p+2) = p+1 = \sigma(p)$.

(ii) true if there are infinitely many Mersenne primes $2^n - 1$; then $\sigma(2^n - 1) = 2^n = \phi(2^{n+1})$

(iii) true under GRH (Pomerance, unpublished)

(iv) common values are ... pretty common, from the data!

Let $V_\phi(N) = \#\{\phi(n) \leq N\}$, $V_\sigma(N) = \#\{\sigma(n) \leq N\}$, and $V_{\phi,\sigma}(N) = \#\{m \leq N : m \text{ is in the range of both } \phi, \sigma\}$.

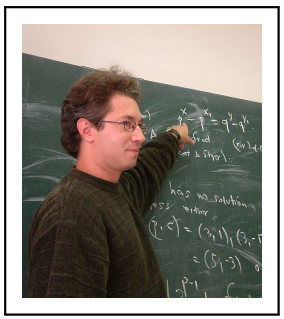
N	$V_\phi(N)$	$V_\sigma(N)$	$V_{\phi,\sigma}(N)$	$V_{\phi,\sigma}(N)/V_\phi(N)$	$V_{\phi,\sigma}(N)/V_\sigma(N)$
10000	2374	2503	1368	0.5762426	0.5465441
100000	20254	21399	11116	0.5488299	0.5194635
1000000	180184	189511	95145	0.5280436	0.5020553
10000000	1634372	1717659	841541	0.5149017	0.4899348
100000000	15037909	15784779	7570480	0.5034264	0.4796063
1000000000	139847903	146622886	69091721	0.4940490	0.4712206

So at 10^9, we see that the proportion of ϕ values that are also σ-values is about 49.4%.

Let $V_\phi(N) = \#\{\phi(n) \le N\}$, $V_\sigma(N) = \#\{\sigma(n) \le N\}$, and $V_{\phi,\sigma}(N) = \#\{m \le N : m \text{ is in the range of both } \phi, \sigma\}$.

N	$V_\phi(N)$	$V_\sigma(N)$	$V_{\phi,\sigma}(N)$	$V_{\phi,\sigma}(N)/V_\phi(N)$	$V_{\phi,\sigma}(N)/V_\sigma(N)$
10000	2374	2503	1368	0.5762426	0.5465441
100000	20254	21399	11116	0.5488299	0.5194635
1000000	180184	189511	95145	0.5280436	0.5020553
10000000	1634372	1717659	841541	0.5149017	0.4899348
100000000	15037909	15784779	7570480	0.5034264	0.4796063
1000000000	139847903	146622886	69091721	0.4940490	0.4712206

So at 10^9, we see that the proportion of ϕ values that are also σ-values is about 49.4%.



Theorem (Ford, Luca, Pomerance, 2010)

Erdős's conjecture is true. In fact, $V_{\phi,\sigma}(x) \ge \exp((\log\log x)^c)$ *for a certain constant* $c > 0$.

What is the true order of $V_{\phi,\sigma}(x)$?
In particular, could it be that a positive proportion of ϕ-values are actually also σ-values?

What is the true order of $V_{\phi,\sigma}(x)$?
In particular, could it be that a positive proportion of ϕ-values are actually also σ-values?

NO!

Theorem (Ford, P., 2012)

We have $V_{\phi,\sigma}(x) \leq V_{\phi}(x)/(\log\log x)^{1/2+o(1)}$.

What is the true order of $V_{\phi,\sigma}(x)$?
In particular, could it be that a positive proportion of ϕ-values are actually also σ-values?

NO!

Theorem (Ford, P., 2012)

We have $V_{\phi,\sigma}(x) \le V_\phi(x)/(\log\log x)^{1/2+o(1)}$.

Both $V_\phi(x)$ and $V_\sigma(x)$ have the shape $x/(\log x)^{1+o(1)}$. So independence might suggest $V_{\phi,\sigma}(x) = x/(\log x)^{2+o(1)}$. Is this right?

What is the true order of $V_{\phi,\sigma}(x)$?
In particular, could it be that a positive proportion of ϕ-values are actually also σ-values?

NO!

Theorem (Ford, P., 2012)

We have $V_{\phi,\sigma}(x) \le V_\phi(x)/(\log\log x)^{1/2+o(1)}$.

Both $V_\phi(x)$ and $V_\sigma(x)$ have the shape $x/(\log x)^{1+o(1)}$. So independence might suggest $V_{\phi,\sigma}(x) = x/(\log x)^{2+o(1)}$. Is this right?

AGAIN, NO! (well, probably...)

Theorem (Ford, P., 2011)

Assuming a strong, quantitative form of the prime k-tuples conjecture, we have $V_{\phi,\sigma}(x) = x/(\log x)^{1+o(1)}$, *as* $x \to \infty$.

In both proofs, the fine structure theory of ϕ and σ-values developed by Ford plays an essential role.

Many other questions could be mentioned.

We know most integers are missing from the range of the Euler function. Are most **squares** missing?

Theorem (Banks, Friedlander, Pomerance, Shparlinski)

$\#\{n \leq x : \phi(n) = \square\} \geq x^{0.7038}$ *for large* x*; conjecturally the exponent can be taken to be* $1 - o(1)$*.*

We know most integers are missing from the range of the Euler function. Are most **squares** missing?

Theorem (Banks, Friedlander, Pomerance, Shparlinski)

$\#\{n \leq x : \phi(n) = \square\} \geq x^{0.7038}$ *for large* x*; conjecturally the exponent can be taken to be* $1 - o(1)$*.*

Up to 10^8, there are 26094797 values of n for which n^2 belongs to the range of the ϕ-function.
Thus, more than half of the even $n \leq 10^8$ have n^2 in the range of ϕ.

We know most integers are missing from the range of the Euler function. Are most **squares** missing?

Theorem (Banks, Friedlander, Pomerance, Shparlinski)

$\#\{n \le x : \phi(n) = \square\} \ge x^{0.7038}$ *for large* x*; conjecturally the exponent can be taken to be* $1 - o(1)$*.*

Up to 10^8, there are 26094797 values of n for which n^2 belongs to the range of the ϕ-function.
Thus, more than half of the even $n \le 10^8$ have n^2 in the range of ϕ.

Theorem (P. and Pomerance, 2013)

Asymptotically 0% *of squares are in the range of* ϕ*.*

We know most integers are missing from the range of the Euler function. Are most **squares** missing?

Theorem (Banks, Friedlander, Pomerance, Shparlinski)

$\#\{n \le x : \phi(n) = \square\} \ge x^{0.7038}$ *for large* x*; conjecturally the exponent can be taken to be* $1 - o(1)$*.*

Up to 10^8, there are 26094797 values of n for which n^2 belongs to the range of the ϕ-function.
Thus, more than half of the even $n \le 10^8$ have n^2 in the range of ϕ.

Theorem (P. and Pomerance, 2013)

Asymptotically 0% *of squares are in the range of* ϕ*.*

Problem

What about cubes?


NANDRI
Danke
ARIGAT
thanks
MAULIATE
TERIMA
MAKASIH
OBRIGADU
KOMAPSUMNIDA
KAMSAHAMNIDA
XIÈXIE
TANGKIU
THANKS
ARIGATŌ
GRAZIAS
URUURU
KASIH
DANKE
RAHMAT
xièxie
dōmo
GRAZIAS
TERIMA
TACK
MAULIATE
Merci
SHUKRAN
MAKASIH
THANKS
RAHMAT
Merci
KASIH