# Numbers that become composite after changing one or two digits

Sergei Konyagin

## Summary

- Introduction
- Sketch of the proof of Theorem 1
- Sketch of the proof of Theorem 2
- Open questions

## Introduction

It is easy to see that $N = 200$ possesses the following property: if we replace any digit in the decimal expansion of $N$ with $d \in \{0, \ldots, 9\}$, then the number created by this replacement is composite. Moreover, $N$ shares this property with all numbers $10M$ where $M$ runs over a subset of $\mathbb{N}$ of density $1$. A question if there exist numbers $N$ possessing this property, coprime to $10$, is more difficult. P. Erdős (1950) showed that there exists an infinite arithmetic progression of odd integers $N$ with the property that $|N - 2^i|$ is composite for every $i$.

Modifying this method F. Cohen and J.L. Selfridge (1975) exhibited an arithmetic progression of odd integers $N$ such that $|N - 2^i|$ and $N + 2^i$ are both composite for every $i$. Therefore, if we replace any digit in the binary expansion of $N$, then the number created by this replacement is composite. A similar problem for decimal expansions was studied by M. Filaseta, M. Kozek, Ch. Nicol, and J. Selfridge (2011).

They proved that there are infinitely many composite natural numbers $N$, coprime to $10$, with the property that if we replace any digit in the decimal expansion of $N$ with $d \in \{0, \ldots, 9\}$, then the number created by this replacement is composite. The aim of the talk is to give answers to two questions posed in their paper.

**Theorem 1.** *For any base $b > 1$ there are infinitely many primes $p$ that are composite for every replacement of a digit*.

**Theorem 2.** *For any base $b > 1$ the set of composite natural numbers $N$ that remain composite when any one or two digits base $b$ are changed has a positive lower density*.

After giving the talk I have learned that Theorem 1 was proved by T. Tao (2011). moreover, he established the existence of the set of primes of related positive density possessing this property. However, for completeness I have preserved the sketch of the proof of Theorem 1 in this revision of my talk.

## Sketch of the proof of Theorem 1

We take a large positive integer $n$, and we will seek for primes $N < b^n$ that become composite after changing one digit. We consider only $N$ with

$$N \equiv 1 (\operatorname{mod} b). \qquad (1)$$

It suffices to check that $N$ is a prime and that all positive integers of the form

$$N' = N + ab^j$$

with $1 \leqslant |a| < b$, $0 \leqslant j < n$, are composite.

We take a small number $\varepsilon > 0$ depending on $b$. Let $m = [n^{\varepsilon}]$. For any $a$ with $1 \leqslant |a| < b$, we consider an interval $I_a = [K_a, mK_a)$ so that these intervals split an interval $[7, M)$ for some $M$,

$$M < 7 \times n^{2b\varepsilon}. \tag{2}$$

Fix $a$ . For a vector $\mathbf{u} = (u_k)_{k \in I_a}$ with $u_k = u_k^{(a)} \in \mathbb{Z}$ we denote

$$J(a, \mathbf{u}) = \{j < n : \exists k \in I_a : j \equiv u_k (\mathrm{mod} k)\},$$

$$J'(a, \mathbf{u}) = [0, n) \setminus J(a, \mathbf{u}).$$

By averaging arguments, there exists a vector $\mathbf{u}$ with $|J'(a, \mathbf{u})| \leqslant n/m$. Denote $J(a) = J(a, \mathbf{u})$, $J'(a) = J(a', \mathbf{u})$. So, we have

$$|J'(a)| \leqslant n/m. \tag{3}$$

We observe that the numbers $u_k$ have been chosen for all $k \in [7, M)$.

Let $q(k)$ be any prime divisor of $b^k - 1$ such that $q(k)$ does not divide any $b^{k'} - 1$ with $0 < k' < k$. For any $k \geqslant 7$ such $q(k)$ does exist by Bang's theorem (moreover, it exists for any $k \geqslant 3$ if $b > 2$). We require the following congruences for $N$

$$\forall a \forall k \in I_a \ N + ab^{u_k} \equiv 0 (\operatorname{mod} q(k)). \tag{4}$$

Thus, we have that for all $a$ and $j \in J(a)$ the number $N' = N + ab^j$ is composite provided that $N' \neq q(k)$ for $7 \leqslant k < M$. Observe that

$$\prod_{7 \leqslant k < M} q(k) < q^{M^2} < q^{n^{5b\varepsilon}}. \tag{5}$$

We choose $\varepsilon$ so small that $5b\varepsilon < 0.9$.

We take $L$ so that

$$\pi(L) = [2bn/m] + b + M \tag{6}$$

and associate with any $a$ and $j \in J'(a)$ a prime $q(a,j) \in (b, L]$ distinct from all primes $q(k), 7 \leqslant k < M$. By (6) the numbers $q(a,j)$ can be chosen distinct. Now we require the following congruences for $N$

$$\forall a \forall j \in J'(a)\ N + ab^j \equiv 0 (\operatorname{mod} q(a,j)). \tag{7}$$

So, the number $N' = N + ab^j$ is composite provided that $N' > L$.

Let $\mathcal{N}$ be the set of all positive integers $N < b^n$ satisfying (1), (4), and (7). Clearly, $\mathcal{N}$ is an arithmetic progression with the difference

$$D = b \prod_{7 \leqslant k < M} q(k) \prod_{a} \prod_{j \in J'(a)} q(a, j).$$

Taking $\varepsilon = 1/(8b)$ and recalling (2) and (5) we conclude

$$D \leqslant \exp\left(n^{1-\varepsilon/2}\right). \tag{8}$$

For all $N \in \mathcal{N}$, with a few exceptions, all positive numbers $N' = N + ab^j$ with $1 \leqslant |a| < b$, $0 \leqslant j < n$, are composite. One can take a subprogression $\mathcal{N}' \subset \mathcal{N}$ with the difference $D^2$ without exceptions. By (8) and Linnik's theorem, $\mathcal{N}' \cap [1, b^n)$ contains a prime, and we are done.

## Sketch of the proof of Theorem 2

We take a large positive integer $n$, and we will seek for many positive integers $N < b^n$ that remain composite when any two digits base $b$ are changed. We consider only $N$ with

$$N \equiv 0 (\mathrm{mod}\, b). \tag{9}$$

It suffices to check that all positive integers of the form

$$N' = N + a_1 + a_2 b^j$$

with $0 \leqslant a_1 < b$, $|a_2| < b$, $0 \leqslant j < n$, are composite.

We take a small number $\varepsilon > 0$ depending on $b$. Let $L = [(1/\varepsilon)^{2b^2}]$. For any $a_1$ and $a_2$ with $0 \leqslant a_1 < b$, $|a_2| < b$ we consider an interval $I_{a_1,a_2} = [K_{a_1,a_2}, K_{a_1,a_2}/\varepsilon)$ so that these intervals split an interval $[L, M)$ for some

$$M \leqslant L^2. \tag{10}$$

Fix $a_1$ and $a_2$. Denote

$$J(a_1, a_2) = \{j < n : \exists k \in I_{a_1,a_2} : j \equiv u_k (\operatorname{mod} k)\}$$

for appropriate (randomly chosen) $u_k$,

$$J'(a_1, a_2) = [0, n) \setminus J(a_1, a_2).$$

We have

$$|J'(a_1, a_2)| \ll \varepsilon n. \tag{11}$$

Let $q(k)$ be any prime divisor of $b^k - 1$ such that $q(k)$ does not divide any $b^{k'} - 1$ with $0 < k' < k$. We get from standard arguments

$$\sum_{L \leqslant k \leqslant L^2} \frac{1}{q(k)} \ll 1. \tag{12}$$

Let $N$ satisfy

$$\forall a_1, a_2 \forall k \in I_{a_1,a_2} \;\; N + a_1 + a_2 q^{u_k} \equiv 0 (\mathrm{mod}\, q(k)). \tag{13}$$

Thus, for all $a_1, a_2$ and $j \in J(a_1, a_2)$ the number $N' = N + a_1 + a_2 b^j$ is composite provided that $N' > \max_k q(k)$. Let $\mathcal{N}$ be the set of all positive integers $N < b^n$ satisfying (9) and (13). Clearly, $\mathcal{N}$ is an arithmetic progression with difference

$$D = b \prod_{L \leqslant k < M} q(k).$$

By Brun – Titcmarsh theorem and (12), for any fixed $a_1, a_2$ and $j \in J'(a_1, a_2)$ the number of primes of the form $N + a_1 + a_2 b^j, N \in \mathcal{N}$, is

$$\ll S := \frac{b^n}{\varphi(D) \log(b^n/D)} \ll \frac{b^n}{nD}.$$

Now we can estimate, by (11), the number $T$ of such $N \in \mathcal{N}$ that $N + a_1 + a_2 b^j$ is prime for at least one $a_1, a_2$ and $j \in J'(a_1, a_2)$:

$$T \ll 2b^2 \varepsilon n S \ll 2b^2 \varepsilon \frac{b^n}{D}.$$

Taking $\varepsilon = cb^{-2}$ for sufficiently small $c > 0$, we get $T \leqslant \frac{b^n}{2D}$. Thus, at least $\frac{b^n}{3D}$ values of $N$ are desirable.

The above arguments give a double exponential estimate for the density $\delta$ of the set of numbers $N$ satisfying the theorem

$$\delta \gg \exp(-\exp(Cb^2 \log b)).$$

## Open questions

By heuristic arguments, we can expect that Theorems 1 and 2 are sharp in the following sense.

**Conjecture 1.** *For any base $b > 1$ there are finitely many natural numbers $N$, $(N, b) = 1$ that are composite for every replacement of one or two digits*.

It looks that it is very hard to prove it even if we allow to replace a bounded number of digits. Maybe, a local version of the conjecture is more feasible.

**Conjecture 2.** *There is an absolute constant $C$ such that for any base $b > 1$, any natural number $M$ and any sufficiently large natural number $N$ one can get after replacement at most $C$ digits of $N$ a number coprime to $M$.*

M. Filaseta has informed me about the following challenging question.

**Conjecture 3.** *For any natural number $M$ there is a natural number $n$ such that $5 \times 2^n + 1$ is coprime to $M$.*

If we replace $5$ by $3$ or $7$, there is nothing to prove. Say, for any odd $M$

$$3 \times 2^{M!} + 1 \equiv 4 (\bmod M).$$