A PROBLEM

STEPHEN ZHOU

1. Introduction

Consider this problem, which was first solved in [1]: What numbers (in base 10) are there such that appending 1 to both ends of the number is the same as multiplication by 99? This is equivalent to asking when

$$10^{k+2} + 10x + 1 = 99x \tag{1.1}$$

where $k = \lfloor \log(x) \rfloor$. This is in fact the only k that has a chance of working, so the condition is unnecessary.

Thus we can rearrange the problem as follows: Find x, k such that

$$\frac{10^{k+2} + 1}{89} = x \tag{1.2}$$

As long as

$$10^{k+2} = -1 \pmod{89} \tag{1.3}$$

we can determine x from k, so we just need to solve this. It turns out that $\text{ord}_{89} 10 = 44$, so $10^{22+44i} = -1 \pmod{89}$. Thus

$$x = \frac{10^{22+44i} + 1}{89}. \tag{1.4}$$

2. A Generalization

We can generalize this problem to any base b: find x such that

$$b^{k+2} + bx + 1 = (b^2 - 1)x, k = \lfloor \log(x) \rfloor. \tag{2.1}$$

or

$$x = \frac{b^{k+2} + 1}{b^2 - b - 1}, k = \lfloor \log(x) \rfloor. \tag{2.2}$$

For any $b > 3$, we see that

$$b^k < \frac{b^{k+2} + 1}{b^2 - b - 1} < b^{k+1}, \tag{2.3}$$

so the condition on k is unnecessary.

As before, this reduces to solving

$$g^{k+2} = -1 \pmod{b^2 - b - 1}. \tag{2.4}$$

Let $m = b^2 - b - 1$. For (8) to have a solution $t = k + 2$, $\text{ord}_m(b)$ must be even and $t = \text{ord}_m(b)/2$. For any prime $p | m$, let p^{s_p} be the highest power dividing m. Then $g^t \equiv -1 \pmod{p^{s_p}}$. Notice that $b^2 - b - 1$ is always odd, so $2 \nmid m$. Notice that $b^2 - b - 1$ is

Date: June 4, 2024.

always odd, so $2 \nmid m$. For there to exist solutions $\pmod{p^{s_p}}$, $\text{ord}_{p^{s_p}}(b)$ must be even. Since $\text{ord}_{p^{s_p}}(b)$ is a power of p times $\text{ord}_p(b)$, this is equivalent to $\text{ord}_p(b)$ being even. Since $\text{ord}_m(b) = \text{lcm}\{\text{ord}_{p^{s_p}}(b)\}$, we can write $t = \text{ord}_m(b) = \text{ord}_{p^{s_p}}(b)c$ for some c. In order for (8) to hold $\pmod{p^{s_p}}$, we need c to be odd for there to be a solution. Thus a solution exists if and only if the highest powers of 2 dividing $\text{ord}_p(b)$ are the same for every $p|m$. We have just proven the following theorem.

Theorem 2.1. *The generalized problem has a solution in base b if and only if there exists an X such that*

$$v_p(\text{ord}_p(b)) = X \tag{2.5}$$

for every $p|b$.

An interesting problem is to find the probability that for a randomly chosen b the problem has a solution in base b. Let the set of all bases b such that the generalized problem does have a solution be B. Then we want to find the density of B.

Surely, $b \notin B$ if for some $p|b^2 - b - 1$, $\text{ord}_p(b)$ is odd. Let $p \equiv 3 \pmod 4$ be a prime for which which $x^2 - x - 1$ splits in F_p. Let u, v be the roots of $x^2 - x - 1 \pmod p$, so that $uv = -1$. Since

$$\left(\frac{-1}{p}\right) = -1 \tag{2.6}$$

one of u, v must be a residue modulo p. Let that residue be a_p. Then for *any* $b \equiv a_p \pmod p$, we have that $p|b^2 - b - 1$. Since

$$b^{\frac{p-1}{2}} = \left(\frac{a_p}{p}\right) = 1 \tag{2.7}$$

and $\frac{p-1}{2}$ is odd, $\text{ord}_p b$ is odd, so $b \notin B$. Basically, each prime p for which $x^2 - x - 1 \pmod p$ splits removes a whole residue class from b.

Now we need to find which primes p for which $f(x) = x^2 - x - 1$ splits in F_p. Let the set of these primes be C. We can easily see that the density of B is

$$1 - \prod_{p \in C} \left(1 - \frac{1}{p}\right). \tag{2.8}$$

Now we need a lemma.

Lemma 2.2. *Let $\{a_i\}$ be a sequence of numbers in $[0, 1]$. Then*

$$\prod_{i=1}^{\infty} (1 - a_i) = 0 \tag{2.9}$$

if and only if

$$\sum_{i=1}^{\infty} a_i = \infty \tag{2.10}$$

Proof. Taking logarithms, the (13) is equivalent to

$$\sum_{i=1}^{\infty} \ln(1 - a_i) \tag{2.11}$$

diverging. Taking the Taylor series for $\ln(1-x)$, we see that

$$\sum_{i=1}^{\infty} \ln(1-a_i) = \sum_{i=1}^{\infty} a_i + \frac{a_i^2}{2} + \frac{a_i^3}{3} \dots \tag{2.12}$$

so

$$\sum_{i=1}^{\infty} a_i + \frac{a_i^2}{2} + \frac{a_i^3}{2^2} \dots \leq \sum_{i=1}^{\infty} \ln(1-a_i) \leq \sum_{i=1}^{\infty} a_i + a_i^2 + a_i^3 \dots \tag{2.13}$$

or

$$\sum_{i=1}^{\infty} \frac{a_i}{1-\frac{a_i}{2}} \leq \sum_{i=1}^{\infty} \ln(1-a_i) \sum_{i=1}^{\infty} \sum_{i=1}^{\infty} \frac{a_i}{1-a_i}. \tag{2.14}$$

Because $0 \leq a_i < 1$, both the terms of left and right sums are $O(a_i)$, so the terms of the middle sum are $O(a_i)$ as well. Thus (14) diverges alongside (13). ■

If we can prove S contains a residue class of primes, then (14) is true by Dirichlet's theorem. Recall the quadratic formula in $\mathbb{R}$: the solutions to x^2+px+q are given by $\frac{-p\pm\sqrt{p^2-4q}}{2}$. The proof works for any field F where $1+1\neq 0$ or $\text{char}(F)\neq 2$, which includes F_p.

Thus the quadratic $x^2-x-1 \pmod p$ splits if and only if $(\frac{\text{disc}(f)}{p})=1$, or $(\frac{5}{p})$, i.e., $p\equiv \pm 1 \pmod 5$. Thus, if $p\equiv 3 \pmod 4$ and $p\equiv \pm 1 \pmod 5$, then $p\in C$, so C contains the primes equivalent to $p\equiv 11, 19 \pmod{20}$. Thus the density of B is 0 by lemma 2.2.

Theorem 2.3. *The probability a randomly chosen base has a solution to the generalized problem is* 0.

3. Another Generalization

This problem has several obvious generalizations. The rest of this paper will be focused on solutions to these generalizations.

The most general generalization is to find when

$$b^t \equiv -1 \pmod{f(b)} \tag{3.1}$$

has a solution. This is far too broad to have a general solution, so we will have to be satisfied with some special cases.

If we add 1 to both ends of a base b integer, n times, we get the equation

$$\frac{b^n-1}{b-1}(b^t+1) = 0 \pmod{b^{2n}-b^n-1}, \tag{3.2}$$

Where $t=k+3$. Since $\gcd(\frac{b^n-1}{b-1}, b^{2n}-b^n-1)=1$ we really need to solve

$$b^t+1\equiv 0 \pmod{b^{2n}-b^n-1}. \tag{3.3}$$

So we have just gotten a special case of the first generalization! Let B_n be the set of all bases b such that this has a solution. $b\in B$ if and only if $\text{ord}_{f(b^n)}(b)$ is even. For fixed b, let $m=b^{2n}-b^n-1$, and let $\text{ord}_m(b)=x$ and $\text{ord}_m(b^n)=y$. Then $x|yn$. Thus y being odd implies that x is odd as long as n is odd. Thus, when n is odd, $b\in B_n$ only if $b^n\in B$, so the density of B_n in $\mathbb{N}$ is B's density in $\mathbb{N}^n$.

Unfortunately, this doesn't help us find the density of B_n, since its possible that B's density in $\mathbb{N}^n$ is greater than B's density in $\mathbb{N}$ since the n^{th} powers have 0 density in $\mathbb{N}$. For example, if $B=\mathbb{N}^3$, then its density in $\mathbb{N}^3$ is obviously 1, but the cubes have density 0 in

$\mathbb{N}$. And we also have no way to determine if a n^{th} power is in B, since that depends on its residue $\pmod p$, and there's no nice way to find the n^{th} powers $\pmod p$.

However, we can get quite close to solving this using a special case of Frobenius' density theorem [2].

Theorem 3.1. *Let f be a polynomial of degree n. Then the set of primes for which f splits completely has density as* $\frac{1}{|\text{Gal}(f)|} \geq \frac{1}{n!}$.

This is actually a special case of the more general Chebotarev's density theorem. We will also need a second theorem. The following definition will make the statement more convenient.

Definition 3.2. A set $A \in \mathbb{N}$ is said to be *large* if

$$\sum_{a \in A} \frac{1}{a} = \infty. \tag{3.4}$$

Theorem 3.3. *Let $A \in \mathbb{N}$ be a large set, and let B have positive density in A. Then B is large.*

Now let's see what these theorems have to do with the density of B_n. Let the set of all primes $p \equiv 3 \pmod 4$ for which $f(b^n) \pmod p$ splits completely be C_n. Then we basically just do the same thing as in the case $n = 1$ to see that the density of B is

$$1 - \prod_{p \in C_n} \left(1 - \frac{1}{c}\right) \tag{3.5}$$

which is equal to 0 if and only if

$$\sum_{c \in C} \frac{1}{c} = \infty, \tag{3.6}$$

that is, if C is a large set. If we could apply the Frobenius density theorem on B_n, then this would be true, since B_n would be a subset of $\mathbb{P}$ with positive density and thus a large set by theorem 3.2. However, we can't do that because we restricted B_n to the primes $p \equiv 3 \pmod 4$. So even though we know that $f(b^n)$ splits completely in F_p for a decent fraction of p, it's possible that nearly all of these primes are $1 \pmod 4$, so we can't use the Frobenius density theorem.

References

[1] "Carl Pomerance" "J.L. Hunsucker". "On An Interesting Property Of 112359550561797752809". In: *Fibonnacci Quarterly* 13.4 (1975), pp. 331–333.

[2] "H.W. Lenstra Jr. "P. Stevenhagen". "Chebotarev and his Density Theorem". In: ().