Minimal Sets for Powers of 2

Bassam Abdul-Baki

November 12, 2010

Minimal Sets Theorem

Let x, y represent a string of digits (in base 10). x is defined to be a subsequence ($\triangleleft$) of y (denoted by x $\triangleleft$ y) if zero or more digits can be deleted from y, in any order, to get x (i.e., 24 $\triangleleft$ 1234).

A classical theorem of formal language theory states that every set of pairwise incomparable strings is finite.

Given any set of strings S, we define the minimal set M(S) as the set of minimal elements of S such that for each x $\ni$ S, y $\ni$ M(S), and x $\triangleleft$ y, then x = y. Since M(S) is obviously pairwise incomparable, M(S) is also finite.

In 2001, Jeffrey Shallit proved the following:

Theorem: If S = PRIMES = $\{2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\}$, then

M(S) = {2, 3, 5, 7, 11, 19, 41, 61, 89, 409, 449, 499, 881, 991, 6469, 6949, 9001, 9049, 9649, 9949, 60649, 666649, 946669, 60000049, 66000049, 66600049}.

His paper also gives the minimal set for all composite numbers with the (similar) proof left up to the reader. However, the minimal set for powers of two is stated without proof and we attempt to do so here.

In this paper, we make no differentiation between the string representation and the numerical representation of an integer.

Theorem: If S = POWERS-OF-2 = {1, 2, 4, 8, 16, 32, 64, ...}, then

M(S) = {1, 2, 4, 8, 65536}.

Proof

The powers-of-2 minimal set has proven difficult to prove. The method of testing it is relatively easy. Its implementation, on the other hand, is not.

For n = 0, $2^n = 1$.

For n = 4k+1, 4k+2, 4k+3, $2^n \equiv 2, 4, 8 \pmod{10}$.

Thus, we only need to look at 2^{4k} or 16^k powers.

Let H(n, k) = $\{16^n \bmod (10^k)\}$.

k	n	c	s	Min Period of Power of 16 (mod 10^k)
2	5	1	4	$16^6 \equiv 16^1 \equiv 16\,(mod\,10^2)$
3	25	1	12	$16^{26} \equiv 16^1 \equiv 16\,(mod\,10^3)$
4	125	1	36	$16^{126} \equiv 16^1 \equiv 16\,(mod\,10^4)$
5	625	2	108	$16^{627} \equiv 16^2 \equiv 256\,(mod\,10^5)$
6	3,125	2	324	$16^{3,127} \equiv 16^2 \equiv 256\,(mod\,10^6)$
7	15,625	2	972	$16^{15,627} \equiv 16^2 \equiv 256\,(mod\,10^7)$
8	78,125	2	2,916	$16^{78,127} \equiv 16^2 \equiv 256\,(mod\,10^8)$
k	5^{k-1}	$\lfloor\frac{k+3}{4}\rfloor$	$4 * 3^{k-2}$	$16^{5^{k-1}+\lfloor\frac{k+3}{4}\rfloor} \equiv 16^{\lfloor\frac{k+3}{4}\rfloor}(mod\,10^k)$

The column s represents the total number of powers of 16 that don't have any of $\{1, 2, 4, 8\}$ in the k^{th} decimal place. Searching for "$[0-9]*5[0-9]*5[0-9]*3[0-9]*6$" in each of the powers of length k, where "[0-9]*" represents zero or more digits, increases subsequent rows by a decreasing amount less than 3 times the previous.

Theorem: Let $x_0 = 5\, and\, x_{i+1} = 5 * x_i - 4$, $\forall i \geq 0$, $i \in \mathbb{N}$, then

$$16^{5^i + \lfloor \frac{i+3}{4} \rfloor} \cong 16^{\lfloor \frac{i+3}{4} \rfloor}\, (mod\, 10^{i+1}). \tag{1}$$

Proof

$$\begin{aligned}
x_0 &= 5 \\
x_1 &= 5^2 - 4 \\
x_2 &= 5^3 - 4 \times 5 - 4 \\
x_{i+1} &= 5 \times x_i - 4 \\
&= 5^{i+2} - 4 \times \sum_{j=0}^{i} 5^j \\
&= 5^{i+2} - 5^{i+1} + 1 \\
&= 4 \times 5^{i+1} + 1 \qquad (2) \\
&\cong 1\, (mod\, 4) \\
2^{x_{i+1}} - 2 &= 2^{5x_i - 4} - 2 \\
&= 2 \times (2^{5x_i - 5} - 1) \\
&= 2 \times (2^{5(x_i - 1)} - 1) \\
&= 2 \times (2^{x_i - 1} - 1) \times (2^{4(x_i-1)} + 2^{3(x_i-1)} + 2^{2(x_i-1)} + 2^{x_i - 1} + 1) \qquad (3) \\
2^{x_i - 1} &= 2^{4 \times 5^{i-1}} \\
&= 16^{5^{i-1}} \\
&\cong 1\, (mod\, 5) \\
\Rightarrow 2^{n(x_i - 1)} &\cong 1\, (mod\, 5)
\end{aligned}$$

$$\Rightarrow 2^{4(x_i-1)} + 2^{3(x_i-1)} + 2^{2(x_i-1)} + 2^{x_i - 1} + 1 \cong 0\, (mod 5) \tag{4}$$

$$\therefore By\, (3)\, and\, (4), 2^{x_{i+1}} - 2 = 5k \times (2^{x_i} - 2) \tag{5}$$

By the Fermat-Euler Theorem,

$$2^4 \cong 1\, (mod\, 5) \tag{6}$$

$$and\, 2^5 \cong 2\, (mod\, 5). \tag{7}$$

$\therefore$ By induction on (3) using (5) and (7),

$$\begin{aligned}
2^{x_{i+1}} - 2 &= 2 \times (2^{x_i - 1} - 1) \times (2^{4(x_i-1)} + 2^{3(x_i-1)} + 2^{2(x_i-1)} + 2^{x_i-1} + 1) \\
&\cong 0 \, (mod \, 5(2^{x_i} - 2)) \\
&\cong 0 \, (mod \, 5^{i+2}).
\end{aligned}$$

Since $2||(2^{x_i} - 2)$, and $(2,\, 5) = 1$, then

$$\begin{aligned}
2^i \times 2^{4\times 5^i + 1} &\cong 2^{i+1} \, (mod \, 10^{i+1}) \\
2^{4\times 5^i + i + 1} &\cong 2^{i+1} \, (mod \, 10^{i+1})
\end{aligned}$$

Let j$\in \mathbb{N}$, $\ni i + 1 + j \cong 0$ (mod 4) for min j ≥ 0.

i	j	i+1+j
0	3	4
1	2	4
2	1	4
3	0	4
4	3	8
5	2	8
6	1	8
7	0	8
i	$-(i+1)(mod 4)$	$4 \times \lfloor \frac{i+4}{4} \rfloor$

$$\begin{aligned}
2^{4\times 5^i + i + 1} &\cong 2^{i+1} (mod 10^{i+1}) \\
2^{4\times 5^i + i + 1 + j} &\cong 2^{i+1+j} (mod 10^{i+1}) \\
2^{4\times 5^i + 4\times \lfloor \frac{i+4}{4} \rfloor} &\cong 2^{4\times \lfloor \frac{i+4}{4} \rfloor} (mod 10^{i+1}) \\
16^{5^i + \lfloor \frac{i+4}{4} \rfloor} &\cong 16^{\lfloor \frac{i+4}{4} \rfloor} (mod 10^{i+1})
\end{aligned}$$

Replacing i with i - 1 gives (1). $\blacksquare$

References

1. Jeffrey O. Shallit - "Minimal Primes", *J. Recreational Mathematics* **30** (2) (1999-2000), 113-117 - http://www.cs.uwaterloo.ca/ shallit/Papers/minimal5.ps.

2. Microsoft Corporation -"Microsoft .NET Framework" - http://www.microsoft.com/net/