Proving $a(n) = -1$

Robert Israel

February 18, 2024

If $a(n) > 0$, i.e. there exist $k > 0$, $m > 0$ and $d > 0$ such that $k^2 = (10^d + 1)m + n$ where $10^{d-1} \le m + n < 10^d$, then in principle we can find such k. m and d by a search: for each d we look at the solutions of $k^2 \equiv n \bmod (10^d + 1)$ with $0 < k \le 10^d$, and check the inequalities for $m = (k^2 - n)/(10^d + 1)$. If no such k, m, d exist, this search would go on forever, and in practice it will get bogged down fairly soon because finding square roots of n modulo $10^d + 1$ requires factoring $10^d + 1$, which becomes difficult for d greater than a few hundred. So how might we be able to prove $a(n) = -1$?

One way we might be able to do this would be to show that n is never a square modulo any $10^d + 1$. Some useful facts to consider:

1. n is a square mod $10^d + 1$ if and only if it is a square mod every prime power dividing $10^d + 1$.

2. Because $10^{ab} + 1$ is divisible by $10^a + 1$ if b is odd, the least d, if any, for which n is a square mod $10^d + 1$ is a power of 2.

3. If an odd prime p does not divide n, then n is a square mod p if and only if the Jacobi symbol $(n/(p \bmod 4n)) = 1$. The set $J(n)$ of natural numbers $k < 4n$ and coprime to $4n$ such that $(n/k) = 1$ form a group under multiplication mod $4n$.

4. Thus if n is a square mod some $10^d + 1$, there must be some j such that n is a square mod $10^{2^j} + 1$, and $((10^{2^j} + 1)/\gcd((10^{2^j} + 1, n) \bmod 4n$ is in $J(n)$.

5. Let $c_k = 10^{2^k} + 1 \bmod 4n$. Thus $c_0 = 11 \bmod 4n$ and $c_{k+1} = (c_k - 1)^2 + 1 \bmod 4n$. Of course this takes only a finite number of values, and as soon as $c_i = c_j$ with $i < j$, the sequence becomes periodic with $c_{i+r} = c_{j+r}$ for all $r \ge 0$.

Here are some examples.

- $n = 7$: $10^{2^j} + 1 \equiv 11 \bmod 28$ for $j = 0$ and alternates 17 and 5 for $j \ge 1$. Since $\{11, 17, 5\}$ is disjoint from $J(7) = \{1, 3, 9, 19, 25, 27\|$, this proves that $a(7) = -1$.

- $n = 10$:. $10^{2^j} + 1 \equiv 1 \bmod 40$ for $j \geq 2$, and $1 \in J(10)$, so it is possible that 10 is a square modulo some $10^d + 1$. In fact, if there is a generalized Fermat prime in base 10, i.e. some $10^{2^j} + 1$ is prime, then 10 would be a square modulo that prime. It seems that no generalized Fermat primes in base 10 are currently known, but there is no proof that they do not exist. 10 is not a square mod $10^{2^j} + 1$ for any $j \leq 12$: e.g. for $j = 0$ and 1, 10 is not a square mod the primes 11 and 101, for $j = 2$, 10 is not a square mod 73 or 137 which divide $10^{2^2} + 1$, and for $j = 3$, 10 is not a square mod 17 or 5882353 which divide $10^{2^3} + 1$. But the status of $j = 13$ is unknown. According to the database at `https://stdkmd.net/nrr/repunit/Phin10.txt`, $10^{8192} + 1$ has one known prime factor 3635898263938497962802538435084289, which $\equiv 9 \bmod 40$, and $(10/9) = 1$. Until more factors are found we don't know whether $j = 13$ works.

- $n = 12$: For $j = 0$, $10^{2^0} + 1 \equiv 11 \bmod 48$, and $(12/11) = 1$. Indeed, 12 is a square mod 11. However, $d = 1$ does not work, as since $12 > 10^1$ the condition $m + n < 10^d$ cannot be satisfied. So next we might look for cases where $10^d + 1 > 1$ is a multiple of 11. Note that $10^d + 1$ is a multiple of 11 if and only if d is odd. with $(10^{2x+1} + 1)/11 =$ A095372(x). For $x = 1$ we have $9091 \equiv 43 \bmod 48$, and $(12/43) = -1$; for $x \geq 2$, $A095372(x) \equiv 19 \bmod 48$, and $(12/19) = -1$. So multiples of 11 won't work. For $j = 1$, $10^{2^1} + 1 \equiv 5 \bmod 48$, and 5 is not in $J(12)$. For $j > 1$, $10^{2^j} + 1 \equiv 17 \bmod 48$, and $(12/17) = -1$. So we conclude that there are no $d > 1$ for which 12 is a square mod $10^d + 1$, and $a(12) = -1$.