Number Theory 2, 2017: Squares in the Fibonacci sequence.

We define the Fibonacci sequence (u_m) to be the following sequence: $u_1 = u_2 = 1$, and $u_m = u_{m-1} + u_{m-2}$ for $m \geq 3$. We can also define u_m for $m \leq 0$ so that the formula $u_m = u_{m-1} + u_{m-2}$ remains true. The way I remember the standard normalisation for the Fibonacci sequence is that $u_5 = 5$ and $u_{12} = 12^2 = 144$. Note in particular that u_{12} is a square Fibonacci number. But it's the last square Fibonacci number:

Theorem. 1 and 144 are the only squares in the Fibonacci sequence.

Before we embark on a proof, we need two preliminaries about squares modulo a prime number, one of which I will not prove.

1) Prove that if p is a prime number which is 3 mod 4, then p does not divide any integer of the form $n^2 + 1$ (hint on my number theory 1 sheet).

2) Believe me when I tell you, if p is a prime number which is 5 or 7 mod 8, then p does not divide any integer of the form $n^2 + 2$. [I do know an elementary proof of this for $p \equiv 5 \bmod 8$, but for $p \equiv 7 \bmod 8$ the only proofs I know at the time of writing use university-level mathematics].

We also need some basics about the Fibonacci sequence, and a related sequence, the Lucas sequence. Define the Lucas sequence (v_m) by $v_1 = 1$, $v_2 = 3$ and $v_m = v_{m-1} + v_{m-2}$ for $m \geq 3$ (and also for $m \leq 0$). Let $\alpha > \beta$ be the two real roots of $x^2 - x - 1 = 0$.

3) Prove that $u_m = (\alpha^m - \beta^m)/\sqrt{5}$ and that $v_m = \alpha^m + \beta^m$.

4) Prove that if m is an integer then $v_m = 2u_m + u_{m-3}$. If (x, y) denotes the highest common factor of the integers x and y, prove that $(u_m, u_{m-1}) = 1$. Deduce that $(u_m, v_m) = (2u_{m-2}, u_{m-3})$ is either 1 or 2.

5) Let m now be a positive integer. Prove that v_m is odd if m is not a multiple of 3. Prove that v_m is not a multiple of 3 if 4 divides m. Prove that $v_m \equiv 7 \bmod 8$ if $m \equiv 4 \bmod 12$ or $m \equiv 8 \bmod 12$. Deduce that if $m \equiv 4 \bmod 12$ or $m \equiv 8 \bmod 12$ then v_m has a prime factor $p > 3$ which is 3 mod 4, and also that v_m has a prime factor which is either 5 or 7 mod 8.

6) Prove that if m, n are integers then $2u_{m+n} = u_m v_n + u_n v_m$ and $v_{4n} = v_{2n}^2 - 2$. Deduce that $u_{2m} = u_m v_m$. Deduce also that v_{2n} divides $2(u_{m+4n} + u_m)$. Deduce that if n is not a multiple of 3 then $u_{m+4n} \equiv -u_m \bmod v_{2n}$.

Now we embark on the proof proper, which is a delicate mixture of easy congruence arguments and more global results about squares modulo primes.

7) By looking at the Fibonacci sequence mod 16, prove that if u_m is a square then m is congruent to one of $-1, 0, 1, 2 \bmod 12$.

8) Now say $m = 4t + q$ with $q \in \{-1, 1, 2\}$ and $t > 0$. Write $t = 2^r s$ with s odd and $r \geq 0$. Set $n = 2^r$, so $m = 4ns + q$. Prove that $u_m \equiv -u_q \equiv -1 \bmod v_{2n}$. Prove that there exists a prime $p \equiv 3 \bmod 4$ such that $u_m \equiv -1 \bmod p$. Deduce that u_m is not a square.

9) Deduce that if $m > 2$ and u_m is a square, then m is a multiple of 12.

The most delicate part of the argument is eliminating u_m with m a multiple of 12 and $m > 12$. This is where we use the fact that I have not proved, namely that if $p \equiv 5$ or 7 mod 8 then -2 is not a square mod p. In fact we prove a little more in this case: we prove that if $m > 12$ is a multiple of 12 then u_m is neither a square nor twice a square.

10) Say $m = 8t + 12$ with $t > 0$. Write $t = 2^r s$ with s odd and $r \geq 0$. Set $n = 2^{r+1}$, so $m = 4ns + 12$. Prove that $u_m \equiv -u_{12} \equiv -144 \bmod v_{2n}$. Deduce that there is a prime number $p \equiv 3 \bmod 4$ with $p > 3$ such that $u_m \equiv -144 \bmod p$. Deduce that u_m is not a square. Deduce furthermore that there is a prime number $p \equiv 5$ or 7 mod 8 such that $2u_m \equiv -288 \bmod p$. Conclude that $2u_m$ is not a square either.

11) Conclude that if $m = 12j$ with j odd and $j > 1$ then neither u_m nor $2u_m$ is a square.

We are nearly there—we only have to deal with u_m for m a multiple of 24 now. Here is the last clever trick: let S be the set of integers $t > 1$ such that u_{12t} is either a square or twice a square. We want to prove that S is empty and we do this by checking that it has no least element.

12) Assume S is non-empty. Let M be the smallest element of S. Prove that $M = 2N$ is even. One checks that $u_{24} = u_{12}v_{12} = 144 \times 322$ is not a square, and hence $M \geq 4$. Now $u_M = u_{2N} = u_N v_N$. Check that this implies $N \in S$. But $N < M$. Contradiction!

Done. This proof is due to J. H. E. Cohn, in 1963.

Kevin Buzzard, Department of Mathematics, Imperial College, London SW7 2AZ.
`buzzard@imperial.ac.uk`