Math 6a - Problem Set 1

1. Show that there are infinitely many primes of the form $4k + 3$.

2. In lectures, we saw that division was transitive, that is, if $a|b$ and $b|c$, then $a|c$. Below, I give several possible meanings for $a \sim b$ where a and b are integers. Which of these are transitive, in the sense that $a \sim b$ and $b \sim c$ implies $a \sim c$? Give proofs or counterexamples.

   (a) $a \sim b$ iff a does not divide b

   (b) $a \sim b$ iff $a < b + 2019$

   (c) $a \sim b$ iff $a^2 \equiv b^2 \pmod{2019}$

   (d) $a \sim b$ iff $\gcd(a, b) > 2019$

3. Prove that a number $a_n a_{n-1} \ldots a_2 a_1 a_0$ written in base 10 is divisible by 9 if and only if $a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0$ is.

4. (a) The last digits of the Fibonacci numbers are $0, 1, 1, 2, 3, 5, 8, 3, 1, 4, 5, \ldots$. Show that the sequence consists of the same cycle repeated infinitely often.

   (b) For a fixed natural number m, consider now the sequence $F_n \pmod{m}$. Show again that the sequence consists of the same cycle repeated infinitely often and this cycle has length less than or equal to $m^2 - 1$.

   (c) Show that if r divides n, then F_r divides F_n (where we start with $F_0 = 0$ and $F_1 = 1$).

5. A message has been encrypted using RSA and the encoding $01 \leftrightarrow A$, $02 \leftrightarrow B$, ..., $26 \leftrightarrow Z$ with exponent $e = 5$ and modulus $n = 2881$. The encrypted message is

   0559 0752 0915 0849 0405 0002 1702 1373.

   What is the decrypted message? (You may use an online modular exponentiation calculator.)