18.781 Problem Set 2: Due Wednesday, February 29.

1. Let $M_m = 2^m - 1$ for $m \in \mathbb{N}$; this is a *Mersenne number.*

(a) Show that M_m is composite if m is composite.

A number n is a *pseudoprime* if it satisfies Fermat's theorem to the base 2—that is,

$$2^n \equiv 2 \pmod{n} \tag{1}$$

—but nevertheless is not prime.

(b) Show that if m satisfies (**??**) then so does M_m.

Combining (a) and (b), we see that if m is pseudoprime then so is M_m. Mersenne believed that M_m was prime whenever m was, at least for $m < 256$. But in a letter to his friend Frenicle, Fermat explains that M_{37} is composite. He restricted the potential prime divisors of M_{37} by applying his theorem.

(c) Carry out Fermat's argument: Show that if p is a prime divisor of M_{37} then p must be of the form $37t+1$. Then find the first few primes of this form (using the list of primes!), and check whether they divide M_{37}. (This can be done easily by computing $2, 4, 8, \ldots, 2^{32} \bmod p$ and then $2^{37} = 2^{32} \cdot 2^4 \cdot 2 \bmod p$.)

Thus $M_{37}, M_{M_{37}}, M_{M_{M_{37}}}, \ldots,$ is an infinite sequence of pseudoprimes. Since 341 is also pseudoprime, we get infinitely many others as well: $M_{341}, M_{M_{341}}, \ldots$.

2. This problem reveals a thumb-smudge on Fermat's crystal ball.

(a) Show that if $m \in \mathbb{N}$ has an odd divisor (other than ± 1!), then $2^m + 1$ is not prime.

$F_m = 2^{2^m} + 1$ is the mth *Fermat number.* Fermat believed them all to be prime.

(b) Show that F_m does satisfy (**??**), so it is either prime or pseudoprime. Fermat probably knew this.

(c) Use arguments like those of 2(c) to show that if p is a prime divisor of F_5 then p is of the form $64t + 1$. Find the primes $p < 1000$ of this form, and check them till you find one which does divide F_5.

Euler carried out exactly this program almost a century after Fermat's death. This is a classic example of how a scientist can be blinded by belief.

3. (Korselt, 1899) Show that $n \in \mathbb{N}$ satisfies $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$ if and only if n satisfies both of the following conditions:

(i) n is square-free (i.e., no prime occurs more than once in its prime factorization).

(ii) If p is a prime divisor of n, then $p-1$ divides $n-1$.

Composite numbers satisfying these conditions are now called *Carmichael numbers*, rather than Korselt numbers. Carmichael's contribution was simply to give some examples (including the smallest, $561 = 3 \times 11 \times 17$). Let this be a lesson: always give examples!

4. Let $n \in \mathbb{N}$, and suppose that the decimal expansion of $1/n$ is

$$\frac{1}{n} = .a_1 a_2 \ldots .$$

(a) Show that n is prime to 10 if and only if its decimal expansion is purely periodic (like $1/3 = .333\ldots$ but unlike $1/6 = .1666\ldots$).

(b) Part (a) shows that 10 is a unit in $\mathbb{Z}_n^*$ if and only if n is prime to 10. Show further that in that case the order of 10 in $\mathbb{Z}_n^*$ equals the minimal period of its decimal expansion.

You have shown in particular that if $n = p$ is prime then 10 is a primitive root mod p if and only if the decimal expansion of $1/p$ has minimal period equal to $p-1$. Gauss was very interested in this, and made a table of the decimal expansions of the reciprocals of all primes less than 1000.

The true definition of science is that it is the study of the beauty of the world—Simone Weil

(Simone Weil was a well-known writer and mystic before World War II, and was the sister of André Weil, one of the century's greatest number theorists.)