Math 1560 - Notes 6

Ian Benway

17 February 2022

1 Special Integers

We start by observing that many small primes take the form $2^m \pm 1$ for some natural number m (e.g. 2, 3, 5, 17, 31).
We deal with the + and - cases separately.

Fermat Numbers

Lemma 1. *If $2^m + 1$ is prime, then $m = 2^n$ for some $n \geq 0$.*

Proof. We show the contrapositive. Suppose m is not a power of 2. Write $m = 2^n \cdot q$ for some odd $q > 1$.
The polynomial

$$f(t) = t^q + 1$$

has $t = -1$ as a root, so

$$f(t) = (t+1)g(t)$$

where $\deg f = q > 1$.

Thus,

$$\begin{aligned} x^m + 1 &= f(x^{2^n}) \\ &= (x^{2^n} + 1)g(x^{2^n}) \quad \text{where } m > 2^n. \end{aligned}$$

Plugging in $x = 2$ gives

$$2^{2^n} + 1 | 2^m + 1, \quad \text{and} \quad 2^{2^n} + 1 < 2^m + 1,$$

so $2^m + 1$ is not prime. □

Numbers of the form $2^{2^n} + 1$ are called **Fermat Numbers**. Those that are prime are called **Fermat Primes**. The first few Fermat Numbers are:

$$3, 5, 17, 257, 65537.$$

Fermat conjectured that all Fermat numbers are prime. He only calculated the first five. Years later, Euler found the next one: $2^{2^5}+1 = 641 \times 6700417$. It seems now that the ones Fermat calculated are the only Fermat Primes.

Mersenne Numbers

Lemma 2. *If $m > 1$ and $a^m - 1$ is prime, then $a = 2$ and m is prime.*

Proof. Suppose m is composite, so $m = nk$ for some $1 < k, n < m$. Then,

$$\begin{aligned} a^m - 1 &= (a^k)^n - 1 \\ &= (a^k - 1)(a^{k(n-1)} + \cdots + 1). \end{aligned}$$

This implies that $a^m - 1$ is composite. Hence m is prime.
Now $a^m - 1 = (a-1)(a^{m-1} + \cdots + 1)$, so we further have that $a = 2$. □

Integers of the form $2^p - 1$ for p a prime are called **Mersenne Numbers**. Mersenne numbers that are prime are called **Mersenne Primes**.

$$2^{82589933} - 1 \text{ is the biggest found yet.}$$

Mersenne primes are related to perfect numbers. An $n \in \mathbb{Z}_+$ is called **perfect** if

$$n = \sum_{\substack{d|n \\ d<n}} d.$$

Proposition. *If $n = 2^{p-1}(2^p - 1)$ where $p \in \mathbb{Z}_+$, and p and $2^p - 1$ are prime, then n is perfect.*

Proof. The function $\sigma(n) = \sum_{d|n} d$ is multiplicative. So if $n = 2^{p-1}(2^p - 1)$, then

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1).$$

Now,

$$\begin{aligned} \sigma(2^{p-1}) &= \frac{2^p - 1}{2 - 1} = 2^p - 1 \\ \sigma(2^p - 1) &= 1 + (2^p - 1) = 2^p. \end{aligned}$$

Hence $\sigma(n) = (2^p - 1)2^p = 2n$. So n is perfect. □

Proposition. *If $n \in \mathbb{Z}_+$ is even and perfect, then $n = 2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are both primes.*

Pseudoprimes & Carmichael Numbers

Theorem 1 (Wilson's Theorem)**.** *p is a prime if and only if* $(p-1)! \equiv -1 \mod p$

This is a rudimentary primality test, but it's not great, since it's very computationally expensive...

Recall Fermat's Little Theorem: If $p \in \mathbb{Z}_+$ is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$.

Thus if $a \in \mathbb{Z}_+$ and

$$a^n \not\equiv a \mod n$$

for some $a \in \mathbb{Z}_+$, then n is composite.

Does a converse hold?
Unfortunately not, e.g.

$$\begin{aligned} 2^{10} &= 1024 = 1 \mod 341 \\ \text{so} \quad 2^{341} &= (2^{10})^{34} \cdot 2 \equiv 2 \mod 341. \\ \text{But } 341 &= 11 \cdot 31, \text{ so 341 is composite.} \end{aligned}$$

We call n a **pseudoprime to the base** a if n is composite and satisfies

$$a^n \equiv a \mod n.$$

Thus 341 is a pseudoprime to the base 2.

Sadly again, it is not necessarily true that given a composite n, there exists an $a \in \mathbb{Z}_+$ such that n is not a pseudoprime to the base a.

$n \in \mathbb{Z}_+$ is called a **Carmichael Number** if n is composite and

$$a^n \equiv a \mod n \quad \forall a \in \mathbb{Z}.$$

The smallest Carmichael number is 561.

Proposition. *If a composite n is **not** a Carmichael number, then at least half of the congruence classes $a \in (\mathbb{Z}/n\mathbb{Z})^*$ are such that n is **not** a pseudoprime to the base a.*

Proof. Suppose n is a pseudoprime to the base $a_1, a_2, \ldots, a_r \in (\mathbb{Z}/n\mathbb{Z})^*$ and suppose

$$a^n \not\equiv a \mod n.$$

Then $\forall i$,

$$\begin{aligned} (a \cdot a_i)^{n-1} &= a^{n-1} \cdot a_i^{n-1} \\ &\equiv a^{n-1} \mod n \\ &\not\equiv 1 \mod n. \end{aligned}$$

Thus n is not a pseudoprime to the bases $a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_r$. □

This results in a probabilistic primality test.