Math 406 Section 6.2: Fermat Pseudoprimes and Carmichael Numbers

1. **Introduction:** Given a number n it is incredibly useful to know if n is prime. This can of course be determined by checking factors but this can be long and difficult. Instead it's often that we develop tests for primality and if a number passes a series of tests we might call it a pseudoprime, indicating that it's "almost" prime, meaning it passed our tests. Pseudoprimes are useful wherever primes are because if they pass (many) tests for primality then they may be used as subsitutes for primes.

2. **Fermat Pseudoprimes:**

   (a) **Introduction:** Fermat's Little Theorem tells us that if p is prime and $a \in \mathbb{Z}$ with $p \nmid b$ then $b^{p-1} \equiv 1 \bmod p$. Consequently if n is a number then if we can find an $b \in \mathbb{Z}$ with $n \nmid b$ and with $b^{n-1} \not\equiv 1 \bmod n$ then n is not prime.

   Example: Given the number $n = 63$ observe that if we choose $b = 2$ then we observe that:

   $$2^{62} \equiv 4 \not\equiv 1 \bmod 63$$

   so we can conclude that 63 is not prime using the base $b = 2$ to check.

   Of course given a number n we might try some b and find that $b^{n-1} \equiv 1 \bmod n$ in which case we cannot conclude that n is not prime nor can we conclude that it is prime. However we could say that it passed a test of primality using $b = 2$.

   Example: Given the number $n = 341$ observe that if we choose $b = 2$ then we observe that:

   $$2^{340} \equiv 1 \bmod 341$$

   so 341 passes our primality test using $b = 2$. Note that $341 = 11 \cdot 31$ is not prime.

   (b) **Definition:** Let n be a positive composite integer. If $b \in \mathbb{Z}^+$ is such that $b^{n-1} \equiv 1 \bmod n$ then we say that n *is a Fermat pseudoprime to the base* b.

   Example: The number $n = 645$ is a Fermat pseudoprime to the base $b = 2$ since $2^{644} \equiv 1 \bmod 645$, as can be shown using methods from class. Note that $645 = 3 \cdot 5 \cdot 43$ is not prime.

   We might then wonder that if we were checking some composite n using a variety of b are we guaranteed to find a base b with $b^{n-1} \not\equiv 1 \bmod b$, thereby proving n not prime? In other words could some composite n pass our primality test with every possible b?

3. **Absolute Fermat Pseudoprimes (Carmichael Numbers):**

   (a) **Definition:** A composite integer n which satisfies $b^{n-1} \equiv 1 \bmod n$ for all b with $\gcd(n, b) = 1$ is called an *Absolute Fermat Pseudoprime* or a *Carmichael number*.

   Example: Consider $n = 561 = 3 \cdot 11 \cdot 17$. Suppose $\gcd(561, b) = 1$, which then tells us that $\gcd(3, b) = \gcd(11, b) = \gcd(17, b) = 1$. By Fermat's Little Theorem we then have $b^2 \equiv 1 \bmod 3$, $b^{10} \equiv 1 \bmod 11$, and $b^{16} \equiv 1 \bmod 17$. It follows that $b^{560} \equiv (b^2)^{280} \equiv 1 \bmod 3$, $b^{560} \equiv (b^{10})^{56} \equiv 1 \bmod 11$, and $b^{560} \equiv (b^{16})^{35} \equiv 1 \bmod 17$. Therefore $b^{560} \equiv 1 \bmod 561$.

   Note: This last fact follows from the general fact that since each of the three primes $3, 11, 17$ appear in the PF of $b^{560} - 1$ that the product must divide $b^{560} - 1$.

   Examples: The first few Carmichael numbers are: 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341. These are even more rare than primes!

   Note: There are infinitely many Carmichael numbers. This was only proven in 1994.

   (b) **Theorem:** If $n = p_1 p_2 ... p_r$ with $r \geq 3$ and with all distinct primes p_i satisfying $(p_i - 1) \mid (n - 1)$ for all i then n is a Carmichael number.

   Proof: Suppose $\gcd(n, b) = 1$, when then tells us that $\gcd(p_i, b) = 1$ for all i. By Fermat's Little Theorem we then have $b^{p_i - 1} \equiv 1 \bmod p_i$ for all i. Since for all i there is some d_i with $n - 1 = (p_i - 1)d_i$ it follows that $b^{n-1} \equiv (b^{p_i - 1})^{d_i} \equiv 1 \bmod p_i$ for all i. Therefore $b^{n-1} \equiv 1 \bmod n$. $\mathcal{QED}$

   Note: The proof doesn't look like it uses the fact that $r \geq 3$. In fact, it turns out that if $n = pq$ for distinct primes p and q then it is impossibe to have $(p - 1) \mid (n - 1)$ and $(q - 1) \mid (n - 1)$. Thus $r = 2$ is excluded in the sense that the remaining hypotheses cannot be true.

   Korselt's Criterion (1899): The above theorem is an iff. The proof of the reverse direction requires primitive roots (which we don't have yet) and the Chinese Remainder Theorem (which we do).

4. **Future:** Another common class of pseudoprimes are the Euler Pseudoprimes. We'll encounter these later.