Math 580/780I Notes 6

Fermat's Little Theorem:

- **Theorem 11.** *For any prime p and any integer a, $a^p - a$ is divisible by p.*

- **Comments:** In other words, with p and a as above, $a^p \equiv a \pmod{p}$. The theorem is equivalent to: if p is a prime and a is an integer with $(a, p) = 1$ (in other words, with p not dividing a), then $a^{p-1} \equiv 1 \pmod{p}$.

- **Proof 1:** Use induction. The theorem holds with $a = 1$. If it holds for a, then

$$(a+1)^p = \sum_{j=0}^{p} \binom{p}{j} a^j \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$

This proves the theorem for positive integers. Since every integer is congruent to a positive integer modulo p, the result follows.

- **Proof 2:** Again, we may suppose $a > 0$. Fix a colors. The number of necklaces with p beads, each bead colored with one of the a colors (allowing repetitions), having at least two beads colored differently is $(a^p - a)/p$. Here, we count necklaces as distinct if one cannot be obtained from the other by a rotation (we don't allow flipping necklaces over). Thus, $(a^p - a)/p \in \mathbb{Z}$, and the result follows.

- Fermat's Little Theorem can be used for determining that a given integer N is composite as follows:

(i) Check N for small prime factors (this step isn't necessary but is reasonable).

(ii) Write N in base 2 as $N = \sum_{j=0}^{k} \epsilon_j 2^j$ with $\epsilon_j \in \{0, 1\}$ for each j and $k = \lfloor \log N / \log 2 \rfloor + 1$.

(iii) Compute $2^{2^j} \pmod{N}$ by squaring.

(iv) Calculate $m \in \{0, 1, \ldots, N-1\}$ such that

$$m \equiv \prod_{j=0}^{k} 2^{\epsilon_j 2^j} \equiv 2^N \pmod{N}.$$

(v) If $m \neq 2$, then N is composite. Otherwise the test is inconclusive.

- **Comments:** The algorithm works for establishing that "most" composite numbers are composite (i.e., for most composite numbers, $m \neq 2$). If $m = 2$, then one can check if $3^N \equiv 3 \pmod{N}$. Note that the algorithm takes on the order of $\log N$ steps so that the algorithm is a polynomial time algorithm (it runs in time that is polynomial in the length of the input - elaborate on this). There are no polynomial time algorithms that determine conclusively whether an arbitrary integer is composite.

- Definitions. A *pseudoprime* is a composite number $n > 1$ satisfying $2^n \equiv 2 \pmod{n}$. A *probable prime* is an integer $n > 1$ satisfying $2^n \equiv 2 \pmod{n}$. (Explain the reasons behind these definitions.)

- **Examples.** Explain why $341 = 11 \times 31$ is a pseudoprime. As indicated by the second Challenge Problem below, one can show that $F_n = 2^{2^n} + 1$ is a probable prime. (Note that for $n > 5$, F_n is really probably not a prime.)

- Definition. An *absolute pseudoprime* (or a *Carmichael number*) is a composite number $n > 1$ such that $a^n \equiv a \pmod{n}$ for every integer a.
- **Example.** Explain why $561 = 3 \times 11 \times 17$ is an absolute pseudoprime.
- **Comment:** Alford, Granville, and Pomerance have shown that there exist infinitely many absolute pseudoprimes. The easier result that there exist infinitely many pseudoprimes is the Challenge Problem below.

Homework:

(1) Prove that 645 is a pseudoprime.

(2) Prove that 2010 is not a pseudoprime. In other words, explain why

$$2^{2010} \not\equiv 2 \pmod{2010}.$$

(3) Justify that

$$201^{2010} \equiv 201 \pmod{2010}.$$

(4) Show that if k is an integer, then one of the two consecutive numbers $k^{2010} - 1$ and k^{2010} is divisible by 31.

(5) Prove that 1105 is an absolute pseudoprime.

(6) Prove that 1729 is an absolute pseudoprime. (As a side note, this number is interesting in another way. Observe that $1729 = 1^3 + 12^3 = 9^3 + 10^3$. The number 1729 is the smallest positive integer that is the sum of two cubes in two different ways.)

Challenge Problem 1:

Prove that if n is a pseudoprime, then $2^n - 1$ is a pseudoprime. (Note that this implies that there are infinitely many pseudoprimes.)

Challenge Problem 2:

Prove that, for every positive integer n, $F_n = 2^{2^n} + 1$ is a probable prime.