

**Math 104A, Number Theory, Fall 2002.**  
**Summary of Lecture 17.**

**Example 3.1.9.** We considered an application of modular arithmetic to shuffling a deck of cards. With the riffle shuffle, the position of the  $i$ th card after  $k$  shuffles is  $2^k i \pmod{53}$ , and we return to the original position after 52 shuffles.

**Theorem 4.1.1.** (The little Fermat theorem). Let  $p$  be a prime. Then  $a^p \equiv 1 \pmod{p}$  for all integers  $a$ . In particular if  $p \nmid a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .

We gave the two proofs in the book.

**Proposition 4.1.5.** If  $a^r \equiv 1 \pmod{p}$  and  $p$  is prime, define  $d = (r, p-1)$ , then  $a^d \equiv 1 \pmod{p}$ .

We proved this.

We did examples 4.1.2, 4.1.3, 4.1.6 and 4.1.7.