Lecture 37, Nov. 16

37.1 Algorithm (Fermat Test)**.** *Input n.*

Each step randomly choose $a \in [1, n-1]$ with $gcd(a, n) = 1$. If $a^{n-1} \neq 1 \mod n$ then n is composite. Otherwise repeat. After repeating $k-$times, output n is probably prime.

37.2 Definition. Let n be composite and $gcd(a, n) = 1$. We call a is a Fermat witness if $a^{n-1} \neq 1 \mod n$, otherwise we call a a Fermat Liar.

37.3 Example. 1 is always a Fermat Liar.

37.4 Proposition. *If there exists a Fermat Witness, then at least half of $a \in [1, n-1]$ ($gcd(a, n) = 1$) are Fermat Witness.*

Proof. Let $a_1, a_2, \cdots, a_r$ are all Fermat Liars. Let a be a Fermat Witness. Then we have aa_i with $i \in [1, r]$ are Fermat Witness. $\square$

37.5 Definition (Carmichael Number)**.** A composite n is called Carmichael number if for all a with $gcd(a, n)$ we have $a^{n-1} = 1 \mod n$.

37.6 Lemma. *Let n be prime. The solution to $x^2 = 1 \mod n$ are exactly $x = \pm 1 \mod n$.*

Proof. Since $x^2 = 1 \mod n$, then $n \mid (x^2 - 1)$ and then $n \mid (x+1)(x-1)$. Since n is prime, then either $n \mid (x+1)$ or $n \mid (x-1)$. $\square$

37.7 Proposition. *Let n be prime with $gcd(a, n) = 1$.*

$$n - 1 = 2^r d$$

then either $a^d = 1 \mod n$ or at least one of

$$a^d, a^{2d}, a^{2^2 d}, a^{2^3 d}, \cdots, 2^{2^{r-1} d} = -1 \mod n$$

37.8 Algorithm (Miller-Rabin Test)**.** *Input odd n. Then $n - 1 = 2^r d$ where d is odd. Each step randomly pick $a \in [1, n-1]$ with $gcd(a, n) = 1$.*

Compute

$$a^d \mod n$$
$$a^{2d} \mod n$$
$$a^{2^2 d} \mod n$$
$$\cdots$$
$$a^{2^{r-1} d} \mod n$$

If $a^d \neq 1 \mod n$ and all the remainders above $\neq -1$, then output n is composite. After $k-$time, output n is probably prime.

37.9 Definition. Let n be composite and $gcd(a, n) = 1$. We call a a strong lair if a lies to you in Miller-Rabin test. Otherwise we call it a strong witness.

37.10 Proposition. *Let n be composite. At least $3/4$ of $a \in [1, n-1]$ with $gcd(a, n) = 1$ are strong witness.*