Escola Politècnica Superior **Universitat de Lleida**
Grau en Enginyeria Informàtica

Computational tools for problem solving

Lab list 2

Fermat and Miller-Rabin primality tests.
The following are two compositeness tests which use binary exponentiation all the time.

Problem 1. Fermat's Little Theorem says: if n is prime and a is any integer not divisible by n then

$$a^{n-1} \equiv 1 \pmod{n}.$$

This is not an "if and only if" statement, and counterexamples n exist and are called Carmichael numbers.
Nevertheless, Fermat's little Theorem allows for a simple test to detect compositeness: if for some $1 < a < n$ we find $a^{n-1} \not\equiv 1 \pmod{n}$ then n is not a prime number.

i) Show Fermat's little Theorem for $n = 17$ and any a in $\{1, 2, \ldots, 16\}$.

ii) Show what happens if $n = 124$ and $a = 3$. And if $n = 124$ and $a = 5$? We say 124 is a Fermat pseudoprime in base 5.

iii) Show what happens for $n = 561$ and any $a \in \{1, \cdots, 560\}$ such that $gcd(a, 561) = 1$. We say 561 is a pseudoprime in any base, or a *Carmichael number*.

iv) Find the first (composite) n which is a Fermat pseudoprime in base $a = 2$.

v) Find the first (composite) n which is a Fermat pseudoprime in base $a = 3$.

vi) Find all Carmichael numbers less than 10000.

vii) Show $323, 90.751$ are not prime numbers using Fermat's little Theorem.

Another well known test for compositeness is Miller-Rabin test. This is based on the fact that there are just 2 square roots of 1 modulo a prime p:

$$x^2 \equiv 1 \pmod{p} \Longleftrightarrow x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p} \Longleftrightarrow p \mid (x-1) \text{ or } p \mid (x+1)$$

$$\Longleftrightarrow x \equiv 1, -1 \pmod{p}$$

Using this, Miller-Rabin takes the reciprocal of a further implication of n being a prime. Take $n - 1$ and write it as

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

where s is the largest possible. Notice that the square root of 2^s is 2^{s-1}. The implication is the following. Assume n is prime and take $1 < a < n$. Then by Fermat's little theorem we have

$$a^{2^s d} \equiv 1 \pmod{n}$$

and the procedure is to take repeated square roots modulo n at each side of the equivalence. Two exclusive options may happen:

a) there is some $0 \leq r \leq s-1$ such that $a^{2^r d} \equiv -1 \pmod{n}$.

b) $a^{2^r d} \equiv 1 \pmod{n}$ for all $0 \leq r \leq s-1$. This implies $a^d \equiv 1 \pmod{n}$.

The reciprocal of this implication is Miller-Rabin test.

Miller-Rabin test (probabilistic). Choose some integer $1 < a < n$. Let $2^s d = n-1$ where d is odd. If $a^d \not\equiv 1 \pmod{n}$ and $a^{2^r d} \not\equiv -1 \pmod{n}$ for all $1 \leq r \leq s-1$ then n is composite.

Notice the direct implication is not true for composite n, so in these cases the hypotheses of the test might not hold for some a. If this is the case, one changes a and repeats the test. Because the amount of good a is known to be at least $\frac{3}{4}$, the probability that we hit a liar in k repeats of the test is about 4^{-k}, so if we repeat the test k times for diferent a's and the hypotheses of the test do not allow to comclude compositeness, then probably n is prime.

Example 1: let $n = 221$ and take $a = 137$. We have $n-1 = 220 = 2^2 55$, so $s = 2, d = 55$. Then

$$a^d \pmod{n} = 137^{55} \pmod{221} \equiv 188 \not\equiv 1 \pmod{221}$$

$$a^{2^0 d} \pmod{n} = 137^{55} \pmod{221} \equiv 188 \not\equiv -1 \pmod{221}$$

$$a^{2^1 d} \pmod{n} = 137^{110} \pmod{221} \equiv 205 \not\equiv -1 \pmod{221}$$

So 137 is a witness that 221 is a composite number.

Example 2: let $n = 221$ and take $a = 174$. We have $n-1 = 220 = 2^2 55$, so $s = 2, d = 5$. Then

$$a^d \pmod{n} = 174^{55} \pmod{221} \equiv 47 \not\equiv 1 \pmod{221}$$

$$a^{2^0 d} \pmod{n} = 174^{55} \pmod{221} \equiv 47 \not\equiv -1 \pmod{221}$$

$$a^{2^1 d} \pmod{n} = 174^{110} \pmod{221} \equiv 220 \equiv -1 \pmod{221}$$

So 174 is a liar.

Example 3: let $n = 1973$ and take $a = 51$. We have $n - 1 = 1972 = 2^2 * 493$, so $s = 2, d = 493$. Then

$$a^d \pmod n = 51^{493} \pmod{1973} \equiv 1714 \not\equiv 1 \pmod{1973}$$
$$a^{2^0 d} \pmod n = 51^{493} \pmod{1973} \equiv 1714 \not\equiv -1 \pmod{1973}$$
$$a^{2^1 d} \pmod n = 51^{2*493} \pmod{1973} \equiv 1972 \equiv -1 \pmod{1973}$$

So 51 is a liar or 1973 is a prime. We would take another a and repeat.

Problem 2.

i) Write a program for the Miller - Rabin test. Try it for $1.000.009, 15.772.929$ and the Mersenne numbers $M_{19} = 2^{19} - 1, M_{31} = 2^{31} - 1$.