# 01204211 Discrete Mathematics
# Lecture 18: Primality testing (3)

Jittat Fakcharoenphol

October 6, 2015

# The first algorithm

This lecture presents the primality testing algorithm based on the Fermat test.

To perform the test if $q$ is a prime, we pick an integer $a$ from the range $\{2, 3, \ldots, q-1\}$ and check that the condition specified by the Fermat's Little Theorem is satisfied.

**PROCEDURE** FermatTest($q$,$a$)
1. **if** $GCD(q, a) \neq 1$ **then return** "COMPOSITE" **endif**
2. Find $y = a^{q-1} \bmod q$
3. **if** $y \neq 1$ **then**
4. **return** "COMPOSITE"
5. **else**
6. **return** "PRIME"
7. **endif**

# Guarantees

Let's consider all input/output possibilities. Let $y =$FermatTest($q$,$a$).

| | $y$=PRIME | $y$=COMPOSITE |
|---|---|---|
| $q$ is prime | Correct | Incorrect |
| $q$ is composite | Incorrect | Correct |

However, from the Fermat's Little Theorem, we know that if $q$ is prime, the test always return "PRIME"; thus the test is always correct.

# Guarantees

Let's consider all input/output possibilities. Let $y$ =FermatTest($q$,$a$).

| | $y$=PRIME | $y$=COMPOSITE |
|---|---|---|
| $q$ is prime | Correct | |
| $q$ is composite | Incorrect | Correct |

However, from the Fermat's Little Theorem, we know that if $q$ is prime, the test always return "PRIME"; thus the test is always correct.
We then need to consider the case when $q$ is composite. In this case, the Fermat's Little Theorem does not provide any guarantee. However, we hope that if $q$ is not a prime, we may be able to find $a$ such that FermatTest($q$,$a$) reveals the truth, i.e., it returns COMPOSITE.

# Witness

- Let's try to be precise. For a composite $q$, if $a$ is an integer such that FermatTest($q$,$a$) returns COMPOSITE, we say that $a$ is a **witness** for $q$.
- It would be great if, for any composite $q$, we can quickly find its witness. But unfortunately, there exists a composite $q$ with very few witnesses. I.e., every witness $a$ for $q$ shares its factor (i.e., it is such that $gcd(a, q) \neq 1$). They are called **Carmichael numbers**.

> A **Carmichael** number is a composite number $q$ such that
> $$b^{q-1} \bmod q = 1,$$
> for all integers $1 < b < n$ which are relatively prime to $q$.

- The first Carmichael number is 561. The next ones are 1105, 1729, and 2465.

# Witnesses for non-Carmichael numbers (1)

Let's focus on the bright side. Suppose that $q$ is not Carmichael, can we say anything about its witnesses? Can we say that there are plenty of them?

# Witnesses for non-Carmichael numbers (2)

Let $a$ be $q$'s witness such that $gcd(a, q) = 1$, i.e., we also have that

$$a^{q-1} \bmod q \neq 1.$$

Let's consider a non-witness $b$, i.e., $b$ is an integer such that $gcd(b, q) = 1$ and

$$b^{q-1} \bmod q = 1.$$

Now, consider $ab$. We have that

$$\begin{aligned}
(ab)^{q-1} \bmod q &= (a^{q-1}b^{q-1}) \bmod q \\
&= (a^{q-1} \bmod q)(b^{q-1} \bmod q) \\
&= a^{q-1} \bmod q \\
&\neq 1
\end{aligned}$$

Can we use this to say that there are a lot of witnesses?

# A lot of witnesses

Since we can show that given a witness $a$ and a non-witness $b$, $ab$ is also witness, we might be able to construct a lot of witnesses from non-witnesses.
Let $A \subseteq \{2, 3, \ldots, q-1\}$. Let $B$ be the set of non-witnesses which are relatively prime to $q$, i.e.,

$$B = \{b \in A : (gcd(b, q) = 1) \wedge (b^{q-1} \mod q = 1)\}.$$

Let $C = \{ab \mod q : b \in A\}$. We know that every $c \in C$ is a witness.
If we know that $|C| = |B|$, can you show that the probability of choosing a witness from the set $A$ is large (i.e, at least $1/2$).
Now, is it obvious that $|C| = |B|$? What is missing?

# The missing argument

To show that $|C| = |B|$, we need to argue that when we multiply every element of $B$, we do not get duplicate elements. I.e., we need to prove that for $x \in B$ and $y \in B$ such that $x \neq y$,

$$ax \mod q \neq ay \mod q,$$

when $gcd(a, q) = 1$.
**Quick check:** prove this statement.
(Note: From the definitions of $a$ and $B$, you may assume that $gcd(q, a) = gcd(q, x) = gcd(q, y) = 1$.)

# Conclusions

From the previous discussion, we know that for non-Carmichael numbers, the Fermat test succeeds with probability at least $1/2$.
Further developments:

- In 1976, Miller and Rabin show that one can deal with Carmichael numbers, providing the first randomized algorithm for testing primes.
- In 2002, Agrawal, Kayal, and Saxena devise an $O(m^{12})$-time deterministic algorithm for primality testing.