Lecture 03

Jose Capco (jcapco@risc.jku.at)

Recall the Miller-Rabin Test:

The Miller-Rabin Test. Let $n \in 2\mathbb{N}+9$ and suppose that $n-1 = 2^t q$ for some $t \in \mathbb{N}$ and $q \in 2\mathbb{N}+1$. Then n is prime iff for all $a \in \mathbb{N}$ relatively prime to n either of the following holds

$$\begin{array}{ll} a^q = \pm 1 \bmod n & \text{or} \\ a^{2^s q} = -1 \bmod n & \text{for some } s = 1, \ldots, t-1 \end{array} \tag{*}$$

Furthermore, only at most $1/4$ of the $a \bmod n \in (\mathbb{Z}/n)^*$ will satisfy (*) if n is not a prime.

For proving the above theorem we will make use of the following Lemma (also in the last lecture, proof is an exercise)

Lemma 1. Let X be an indeterminate, p be an odd prime and $m \in \mathbb{N}$ such that $p \nmid m$ and suppose $e \in \mathbb{N}$, then the number of solutions for $X^m = 1 \bmod p^e$ in the ring $\mathbb{Z}/p^e$ is given by

$$\gcd(m, \phi(p^e)) = \gcd(m, p^{e-1}(p-1))$$

There is an immediate corollary to the Lemma that will also be useful in proving the Theorem ...

Corollary 2. Let $p \in \mathbb{P}$ be an odd prime and $a, e \in \mathbb{N}$. Then $a^m = -1 \bmod p^e$ iff $a^m \neq 1 \bmod p$ and $a^{2m} = 1 \bmod p$

Proof. One direction is clear, so we prove "$\Leftarrow$". From the above Lemma we immediately see that $X^2 = 1 \bmod p^e$ has exactly two solutions namely $\{1, -1\} \bmod p^e$. Since a^m is a solution of $X^2 = 1 \bmod p^e$ and $a^m \neq 1 \bmod p^e$ we can conclude that $a^m = -1 \bmod p^e$.

□

Now we continue the proof of what we left in the last lecture

Continuation Proof of Miller-Rabin Test. In the last lecture, we assumed $n \in 2\mathbb{N}+9$ to be an odd composite and the prime factorization of n was written as $n = \prod_{i=1} p_i^{e_i}$ (so k distinct prime numbers divide n). We also defined

$$m := \max\{l \,:\, 2^l \mid p_i - 1 \quad \forall i = 1, \ldots, k\}$$

and the set

$$A(n) := \{a \bmod n \,:\, a^{2^{m-1}q} = \pm 1 \bmod n\}$$

We have already shown

Step 1: $A(n) \supset \{a \bmod n \,:\, a \text{ satisfies (*)}\}$

For the next step we will count $A(n)$

Step 2: We will show that

$$\#A(n) = 2^{k(m-1)+1} \prod_{i=1}^{k} \gcd(q, p_i - 1)$$

For each prime $p \in \mathbb{P}$ such that $p^e \,||\, n$, the number of solutions mod p^e for $x^{2^{m-1}q} = 1 \bmod p^e$ is (by Lemma 1)

$$\gcd(2^{m-1}q, p-1) = 2^{m-1} \gcd(q, p-1)$$

By the Chinese Remainder Theorem, to solve for the same problem modulo n, we just multiply these numbers for each p dividing n, i.e.

$$\#\{x \bmod n : x^{2^{m-1}q} = 1 \bmod n\} = \prod_{i=1}^{k} 2^{m-1} \gcd(q, p_i - 1) = 2^{k(m-1)} \prod_{i=1}^{k} \gcd(q, p_i - 1)$$

To get $\#A(n)$ we need to also count all $x \bmod n$ such that $x^{2^{m-1}q} = -1 \bmod n$. Again we look at $p \in \mathbb{P}$ such that $p^e \,||\, n$ and count all the $x \bmod n$ such that $x^{2^{m-1}q} = -1 \bmod p^e$. By the above Corollary, this is just all those $x \bmod p^e$ such that $x^{2^m q} = 1 \bmod p^e$ and $x^{2^{m-1}q} \neq 1 \bmod p^e$ i.e. the count for such x is

$$\#\{x \bmod n : x^{2^{m-1}q} = -1 \bmod p^e\} = (2^m - 2^{m-1}) \gcd(q, p) = 2^{m-1} \gcd(q, p_i - 1)$$

By the Chinese Remainder Theorem, we obtain

$$\#\{x \bmod n : x^{2^{m-1}q} = -1 \bmod n\} = 2^{k(m-1)} \prod_{i=1}^{k} \gcd(q, p_i - 1)$$

and adding these two numbers leads to our wanted result.

Step 3: We will show that $\frac{\#A(n)}{\phi(n)} \leq \frac{1}{4}$, and thus complete the proof of the Theorem.

By the previous step we have

$$\frac{\#A(n)}{\phi(n)} = 2 \prod_{p^e || n} \frac{2^{m-1} \gcd(q, p-1)}{p^{e-1}(p-1)} = 2 \prod_{p^e || n} \frac{1}{k_p p^{e-1}}$$

where $k_p := \dfrac{p-1}{\gcd(q, p-1) 2^{m-1}}$ for each $p \in \mathbb{P}$ dividing n. Notice that for all $p \in \mathbb{P}$ dividing n, $k_p \in \mathbb{N}$ and $2 \mid k_p$ so $k_p \geq 2$. In fact, by analysing k_p and only including Case 3 below, we have already proven the Theorem but with a ratio $\frac{\#A(n)}{\phi(n)} \leq \frac{1}{2}$. But we want to show the better ratio, so we proceed ...

Now the proof for $\frac{\#A(n)}{\phi(n)} \leq \frac{1}{4}$ is divided into three cases

Case 1: $k \geq 3$

This is the easiest case because 2 divides k_p for each $p \in \mathbb{P}$ dividing n, which implies that $\frac{\#A(n)}{\phi(n)} \leq \frac{1}{4}$.

Case 2: $k = 2$ and $e_i > 1$ for some $i = 1, 2$

We still have 2 dividing k_p for each $p \in \mathbb{P}$ dividing n, which gives us at most $1/2$ for $\#A(n)/\phi(n)$. Furthermore we have one odd prime power (at least 3) appearing in the denominator i.e.

$$\frac{\#A(n)}{\phi(n)} \leq \frac{1}{6} < \frac{1}{4}$$

Case 3: $k = 1$, so there is one prime $p \in \mathbb{P}$ and a number $e > 1$ such that $n = p^e$.

Here is the only place where we make use of the fact that $n > 9$. We have (one "easily" shows that $k_p = 2$)

$$\frac{\#A(n)}{\phi(n)} = 1/p^{e-1} \leq 1/5 < 1/4$$

The second inequality is because $p > 3$ if $e = 2$ (since $n > 9$). And if $p = 3$ then $e > 2$ and we still have the inequality above.

Case 4: $k = 2$ and n is square free
Suppose $p_1, p_2 \in \mathbb{P}$ be two distinct primes such that $n = p_1 p_2$.
If $2^{m+1} \mid p_2 - 1$ then we have

$$k_{p_2} = \frac{p_2 - 1}{\gcd(q, p_2 - 1)2^{m-1}} \geq \frac{2^{m+1}(p_2 - 1)}{2^{m-1}(p_2 - 1)} = 4$$

and thus $\frac{\#A(n)}{\phi(n)} \leq 1/4$. We obtain the same result if $2^{m+1} \mid p_1 - 1$
Suppose now that $2^m \mid\mid p_i - 1$ for $i = 1, 2$. Notice now that $n - 1 = p_1 - 1 \bmod (p_2 - 1)$ and so $p_2 - 1 \nmid n - 1$. In particular, there is an odd prime p_3 dividing $p_2 - 1$ by a higher power than it dividies $n - 1$. So we have

$$k_{p_2} = \frac{p_2 - 1}{\gcd(q, p_2 - 1)2^{m-1}} \geq \frac{2p_3(p_2 - 1)}{p_2 - 1} = 2p_3 \geq 6$$

and so

$$S(n)/\phi(n) \leq 1/6 < 1/4$$

□

We now switched to a different primality proving algorithm. Our aim to prove the correctness of the AKS algorithm (the letters represent the name of the creator of this algorithm: Agrawal, Kayal and Saxena). The motivation for this primality test is in fact a very old theorm that characterizes prime numbers but is rather inefficient to use for checking primality

Wilson's Theorem. $p \in \mathbb{N}$ is a prime iff $(p-1)! = -1 \bmod p$

Proof. "⇒" If $p \in \mathbb{N}$ is a prime number then $(p-1)! = \prod_{x \in \mathbb{F}_p^*} x$. For $p = 2$ the result is clear and for an odd prime we see that except for 1 and -1, every number in $\mathbb{F}_p$ and its multiplicative inverse are distinct. Therefore the above product is the product of pairs of numbers with their inverses and of 1 and of -1 and this amounts to $-1 \bmod p$.
"⇐" If $p \notin \mathbb{P}$ then there is a $q \in \mathbb{P}$ such that $q \mid p$ and $2 \leq q < p$. Suppose that $(p-1)! = -1 \bmod p$, then $q \mid (p-1)!$ which means that $(p-1)!$ and p are not coprime while $-1 = p - 1 \bmod p$ is associated to a number that is coprime to p (i.e. invertible in $\mathbb{F}_p^*$) and this is a contradiction. □

Exercise 1. Use Wilson's to show

1. p and $p + 2$ are two primes (i.e. twin-primes) iff $4(p-1)! = -4 - p \bmod p(p+2)$
2. A number $p \in 2\mathbb{N} + 1$ is a prime iff $\left(\left(\frac{p-1}{2}\right)!\right)^2 = (-1)^{(p+1)/2} \bmod p$

So theoretically one can test for a prime using the above theorem, but the above is just as bad as testing by trial division (where you test each numbers from 2 to $\lceil \sqrt{p} \rceil$ and see if they can divide p). But the above theorem is complementary to another characterization of prime numbers (that is also inefficient when directly used for testing primes)

Proposition 3. Let X be an indeterminate, $n \in 2\mathbb{N} + 1$ and $a \in \mathbb{N}$ be such that $(a, n) = 1$ then n is a prime number iff $(X + a)^n = X^n + a \bmod n$ (so we are looking at an equality in $(\mathbb{Z}/n\mathbb{Z})[X]$).

Proof. We will prove this in the next lecture. □