Lecture 17 : Primality Testing

Our first attempt

I/p : an odd integer $n \geq 3$

1. Pick an $a \in \{1, \dots, n-1\}$ uniformly at random.
2. Compute $a^{n-1} \bmod n$.
   - if this is not 1 then return "composite" else return "prime"

Every prime number is called "prime" by the above algorithm. We need to bound the probability that a composite number is called "prime".

Suppose the converse of the little theorem is true. That is, if n is composite then $\exists\, a \in \mathbb{Z}_n^*$ such that $a^{n-1} \not\equiv 1 \pmod n$.
- Recall that $\mathbb{Z}_n^*$ is the set of elements in $\{0, 1, \dots, n-1\}$ that are relatively prime to n.
- when n is prime, $\mathbb{Z}_n^* = \{1, 2, \dots, n-1\}$.

For composite n, how do we find witnesses of compositeness?
- pick an a unif. at random from $\{1, \dots, n-1\}$.
- if $\gcd(a, n) \neq 1$ then fine — we have found a divisor of n.

  else $a \in \mathbb{Z}_n^*$.

Claim. If the converse of the little theorem is true, then for at least half the elements $a \in \mathbb{Z}_n^*$, we have $a^{n-1} \not\equiv 1 \pmod n$.

Proof. The set of elements $x \in \mathbb{Z}_n^*$ such that $x^{n-1} = 1 \pmod n$ forms a subgroup of $G = \mathbb{Z}_n^*$. This subgroup is not the entire group $\mathbb{Z}_n^*$ since $\exists\, a \in \mathbb{Z}_n^*$ such that $a^{n-1} \not\equiv 1 \pmod n$. Thus the size of this subgroup $\leq \frac{|\mathbb{Z}_n^*|}{2}$ (by Lagrange's theorem)

So among the elements in $\{1, \ldots, n-1\}$, at least half the elements witness the "compositeness" of n. (why?)

- either $a \notin \mathbb{Z}_n^*$, in which case we have $a^{n-1} \not\equiv 1 \pmod{n}$

or $a \in \mathbb{Z}_n^*$ and it is outside the subgroup $\mathcal{H}$ which is $\{x \in \mathbb{Z}_n^* : x^{n-1} = 1 \pmod{n}\}$

or $a \in \mathcal{H}$.

Our claim showed that $|\mathcal{H}| \leq \frac{|\mathbb{Z}_n^*|}{2}$.
Thus all elements in $\{1, \ldots, n-1\} \setminus \mathcal{H}$ witness a's compositeness and these are at least half the elements in $\{1, \ldots, n-1\}$.

Unfortunately, the converse of the little theorem is false. There are composite numbers called "Carmichael numbers" such that n is composite and for all $a \in \mathbb{Z}_n^*$, we have $a^{n-1} = 1 \pmod{n}$.

Ex. 561. Note that $561 = 3 \times 11 \times 17$.

Another idea: $\underbrace{\text{Square roots of } 1}$

We will see that any composite number n that is not a prime power has non-trivial square roots of 1 in the "mod n" world.

Chinese Remainder Theorem. Let n be a composite number that is not a prime power. So $n = \alpha \cdot \beta$ where $\gcd(\alpha, \beta) = 1$. There is a bijection $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_\alpha \times \mathbb{Z}_\beta$ defined as $f(a) = (a \bmod \alpha, a \bmod \beta)$.

Note that $\mathbb{Z}_n = \underbrace{\{0, 1, \ldots, n-1\}}_{\text{all possible remainders when we divide a number by } n}$

In the first place, $\underbrace{|\mathbb{Z}_n|}_{=n} = \underbrace{|\mathbb{Z}_\alpha|}_{=\alpha} \cdot \underbrace{|\mathbb{Z}_\beta|}_{=\beta}$

$\boxed{\text{So if } f \text{ is onto, then } f \text{ has to be 1-1.}}$

How do we show that f is onto?
- take any $r_1 \in \{0, 1, \ldots, \alpha-1\}$ and $r_2 \in \{0, 1, \ldots, \beta-1\}$.

We claim $\exists\, r \in \{0, 1, \ldots, n-1\}$ such that $\boxed{f(r) = (r_1, r_2)}$
We need to come up with x & y
such that $r = x\alpha + y\beta \pmod n$
where $y\beta \bmod \alpha = r_1$ and $x\alpha \bmod \beta = r_2$.

We know that $\gcd(\alpha, \beta) = 1$. So $\beta \in \mathbb{Z}_\alpha^*$.
Hence $\exists\, b$ such that $b\beta = 1 \pmod \alpha$.
So $r_1 b\beta = r_1 \pmod \alpha$.

Similarly $\alpha \in \mathbb{Z}_\beta^*$. Hence $\exists\, a$ such that
$a\alpha = 1 \pmod \beta$. So $r_2 a\alpha = r_2 \pmod \beta$.

Let $r = r_1 b\beta + r_2 a\alpha \pmod n$.
$r \bmod \alpha = (r_1 b\beta + r_2 a\alpha + kn) \bmod \alpha = r_1$
$r \bmod \beta = (r_1 b\beta + r_2 a\alpha + kn) \bmod \beta = r_2$

- Moreover f restricted to $\mathbb{Z}_n^*$ maps onto $\mathbb{Z}_\alpha^* \times \mathbb{Z}_\beta^*$. Let $r \in \mathbb{Z}_n^*$. Suppose $f(r) = (a, b)$.
That is, $r = k_1\alpha + a$ and $r = k_2\beta + b$.

Since $r \in \mathbb{Z}_n^*$, $r \in \mathbb{Z}_\alpha^*$ and $r \in \mathbb{Z}_\beta^*$.
Thus $a \in \mathbb{Z}_\alpha^*$ and $b \in \mathbb{Z}_\beta^*$. In fact, it is easy to show that $|\mathbb{Z}_n^*| = |\mathbb{Z}_\alpha^*| \cdot |\mathbb{Z}_\beta^*|$.
Thus f is a bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_\alpha^* \times \mathbb{Z}_\beta^*$.

Exercise. Suppose $f(r) = (r_1, r_2)$ and $f(s) = (s_1, s_2)$. Show that $f(rs) = (r_1 s_1, r_2 s_2)$.
$= f(r) \cdot f(s)$
coordinatewise multiplication

So f is an isomorphism between $\mathbb{Z}_n^*$ and $\mathbb{Z}_\alpha^* \times \mathbb{Z}_\beta^*$.

Example. Let $n = 15$. So there is an isomorphism f between $\mathbb{Z}_{15}^*$ and $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$.

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, $\mathbb{Z}_3^* = \{1, 2\}$, $\mathbb{Z}_5^* = \{1,2,3,4\}$.
$f(1) = (1,1)$, $f(2) = (2,2)$, $f(4) = (1,4)$,
$f(7) = (1,2)$, $f(8) = (2,3)$, $f(11) = (2,1)$,
$f(13) = (1,3)$, $f(14) = (2,4)$.

What are the square roots of 1 in the "mod 15" world? 1 and 14 are the trivial square roots of 1: these are $\pm 1 \pmod{15}$.
- observe that there are 2 non-trivial square roots of 1 in the "mod 15" world. These are 4 and 11: $4^2 = 16 = 1 \pmod{15}$ and $11^2 = 121 = 1 \pmod{15}$.
- what are $f(4)$ and $f(11)$? Does this give us a clue on the non-trivial square roots of 1 in the "mod n" world?

Observation. If n is an odd composite number that is not a prime power then $x^2 = 1 \pmod n$ is satisfied by at least 4 elements in $\mathbb{Z}_n^*$
(why?)

Let us now write down the algorithm.

Miller-Rabin Primality Testing Algorithm

Step 0. Check if $n = a^b$ for integers $a, b \geq 2$.
If so then return "composite".

Step 1. Select $a \in \{1, \ldots, n-1\}$ uniformly at random and compute $a^{n-1} \bmod n$. If this is not 1 then return "composite".

Step 2. (Algorithm reaches this step $\Rightarrow a^{n-1} = 1 \pmod n$)
~~Compute~~ Let $n-1 = 2^k \cdot t$ where t is odd.

Compute $\underbrace{a^t, a^{2t}, a^{4t}, a^{8t}, \ldots}_{\bmod n}$ till a 1 is seen. If the number before 1 is not -1 then return "composite".

Else return "prime".

Claim. If n is prime then the algorithm always returns "prime".

Proof. We have $a^{n-1} = 1 \pmod n$ $\forall a \in \{1, \ldots, n-1\}$ by the little theorem. So the algorithm cannot return "composite" in Step 1.

If $x^2 = 1 \pmod n$ then $(x+1)(x-1) = 0 \pmod n$. That is, either $x+1 = 0 \pmod n$ or $x-1 = 0 \pmod n$. This is because n is prime: if a prime number n divides $(x+1)(x-1)$ then n has to divide either $(x+1)$ or $(x-1)$. So the algorithm cannot return "composite" in Step 2.

The algorithm obviously cannot return "composite" in Step 0.

$\square$

Suppose n is composite. In case $\gcd(a, n) \neq 1$ then $a^{n-1} \not\equiv 1 \pmod n$ and so the algorithm returns "composite". Henceforth we can assume $\gcd(a, n) = 1$, i.e., $a \in \mathbb{Z}_n^*$.

Case 1. n is not Carmichael. That is, $\exists\, a \in \mathbb{Z}_n^*$ such that $a^{n-1} \not\equiv 1 \pmod{n}$. In this case for at least $\frac{|\mathbb{Z}_n^*|}{2}$ elements x in $\mathbb{Z}_n^*$ we have $x^{n-1} \not\equiv 1 \pmod{n}$.

So the test in Step 1 succeeds with probability $\geqslant 1/2$

Case 2. n is Carmichael. So we have

$$a^{n-1} \equiv 1 \pmod{n} \quad \forall\, a \in \mathbb{Z}_n^*.$$

We need to show that Step 2 succeeds with probability $\geqslant 1/2$

Let us build the following table. Let $\mathbb{Z}_n^* = \{a_1, \dots, a_r\}$

	t	$2t$	$4t$		$2^h.t$	$2^{h+1}.t$		$2^k t$
a_1						1		1
a_2						1		1
								$\vdots$
a_r						1		1

$\boxed{\text{not all 1's}}$ all these columns are all 1's.

- The rows are indexed by the elements of $\mathbb{Z}_n^*$.
- The columns are indexed by $t, 2t, \dots, 2^k.t$ where $n-1 = 2^k.t$ (t is odd).
- Since n is Carmichael, the last column is all 1's. Consider the ~~first~~ last column in this table that is not all 1's. There always exists such a column since the first column is not all 1's. (why?)

Claim. At least half the elements in the last column in this table that is not all 1's are neither 1 nor $-1 \pmod{n}$. That is,

$$x^{2^h.t} \not\equiv \pm 1 \pmod{n} \text{ for at least}$$

half the elements in $\{a_1, a_2, \dots, a_r\}$.