Algorithm Analysis and Design (CS1.301)

Monsoon 2021, IIIT Hyderabad
13 October, Wednesday (Lecture 14)

Number Theoretic Algorithms (contd.)

Rabin-Miller Primality Testing Algorithm

The algorithm proceeds as follows. On input p,

1. If p is even, accept if $p = 2$; else reject.
2. Select $a_1, \dots, a_k \in \mathcal{Z}_p^+$ randomly.
3. For each i from 1 to k:
    4. Compute $a_i^{p-1} \mod p$ and reject if different from 1.
    5. Let $p - 1 = st$ where $t = 2^h$ and s is odd.
    6. Compute $a_i^{s \cdot 2^0}, a_i^{s \cdot 2^1}, \dots, a_i^{s \cdot 2^h} \mod p$.
    7. If some element of this sequence is not 1, find the last element that is not 1 and reject if it is not -1.
4. Accept.

Correctness

If p is an odd prime number, the algorithm will definitely accept it. This can be proved as follows.
If the algorithm rejects in stage 4, we know that $a^{p-1} \not\equiv 1 \mod p$, which implies that p is composite by Fermat's little theorem.
If the algorithm rejects in stage 7, there is a $b \in \mathcal{Z}_p^+$, such that $b \equiv \pm 1 \mod p$ and $b^2 \equiv 1 \mod p$. This means that $(b-1)(b+1) \equiv 0 \mod p$, which means that p is composite.
Therefore, if the algorithm rejects, p is composite. This means that if p is prime, then the algorithm must accept it.

If p is an odd composite number, it will be accepted with a chance of at most 2^{-k}. To prove this, we will show that the probability of $a \in \mathcal{Z}_p^+$ is a witness for it is at least $\frac{1}{2}$. This can be shown by finding a unique witness for each nonwitness.
For every nonwitness, the sequence of stage 6 is either all 1s or contains -1 at some position followed by 1s. Among all nonwitnesses of the second kind, let h

be that for which -1 appears at the largest position in the sequence, and let j be that position. Therefore we know that $h^{s\cdot 2^j} \equiv -1 \mod p$.
Suppose $p = qr$ for relatively prime q, r. By the Chinese Remainder Theorem, there exists a $t \in \mathcal{Z}_p^h$ such that $t \equiv h(\mod q)$ and $t \equiv 1(\mod r)$. Therefore, $t^{s\cdot 2^j} \equiv -1(\mod q)$, and $t^{s\cdot 2^j} \equiv 1(\mod r)$. Therefore t is a witness.
Now, we can show that $dt \mod p$ is a unique witness for each nonwitness d. First, $d^{s\cdot 2^j} \equiv \pm 1 \mod p$ and $d^{s\cdot 2^{j-1}} \equiv 1 \mod p$ because of how j was chosen; therefore dt is a witness. It is straightforward that it is unique.
For the second case of p being composite (p is a prime power), let $p = q^e$. Let $t = 1 + q^{e-1}$. Expanding t^p, we see that $t^p \equiv 1 \mod p$. Therefore t is a stage 4 witness. Now we can proceed as in the other case, showing that dt is a unique witness for each nonwitness d.