Rabin's Probabilistic Algorithm for Compositeness

CSE 531: Computability and Complexity

December 4, 2001

1. Number-theoretic background

A *group* is $(H; \otimes, ^{-1}, e)$, where

1. H is a set closed under the operations $\otimes$, $^{-1}$, and e,
2. $\otimes$ is associative,
3. e is the identity: for all $x \in H$, $x \otimes e = e \otimes x = x$, and
4. x^{-1} is the inverse of x: for all $x \in H$, $x^{-1} \otimes x = x \otimes x^{-1} = e$.

Let H be a finite group and $G \subseteq H$. G is a *subgroup* of H (denoted $G \leq H$) iff $x \in G$ and $y \in G$ implies $x \otimes y \in G$. G is a *proper subgroup* of H iff $G \leq H$ and $G \neq H$.

Theorem 1: (Lagrange) If H is a finite group and $G \leq H$, then $|G|$ divides $|H|$.

The *order* of x in H (denoted $o(x)$) is the least positive integer k (if it exists) such that $x^k = e$, where x^k is shorthand for $\underbrace{x \otimes x \otimes \cdots \otimes x}_{k \text{ factors of } x}$.

Theorem 2: If $x \in H$ and k is a positive integer, $x^k = e$ iff $o(x) \mid k$.

$Z_m = \{0, 1, \ldots, m-1\}$.

$Z_m^* = \{a \in Z_m \mid \gcd(a, m) = 1\}$.

Theorem 3: Z_m^* is a group under multiplication mod m.

Theorem 4: (Fermat's "Little") If p is prime and $a \in Z_p^*$, then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 5: If $\gcd(a, m) \neq 1$, then $a^{m-1} \not\equiv 1 \pmod{m}$.

Theorem 6: If $m = p^e$ for a prime p and integer $e > 1$, then $\{a \mid a^{m-1} \equiv 1 \pmod{m}\}$ is a proper subgroup of Z_m^*.

Theorem 7: Given a, k, and m in binary, $a^k \bmod m$ can be computed in polynomial time.

Theorem 8: (Chinese remainder) Suppose $\gcd(p, q) = 1$. Then $\phi : Z_{pq} \rightarrow Z_p \times Z_q$ defined as $\phi(r) = (r \bmod p, r \bmod q)$ is a bijection.

2. Rabin's algorithm to test if $m > 1$ is composite (1980)

1. **if** $m = 2$ **then return** "prime";
2. **if** m is even **then return** "composite";
3. **choose** $a \in Z_m - \{0\}$ randomly and uniformly;
4. **if** $a^{m-1} \not\equiv 1 \pmod{m}$ **then return** "composite";
5. let $m - 1 = 2^k u$, where u is odd;
6. **for** h **from** 0 **to** $k - 1$ **do**
   if $a^{2^h u} \not\equiv \pm 1 \pmod{m}$ **and** $(a^{2^h u})^2 \equiv 1 \pmod{m}$ **then return** "composite";
7. **return** "probably prime".

3. Correctness properties

If m is prime, Pr(Rabin's algorithm returns "composite") $= 0$.
If m is composite, Pr(Rabin's algorithm returns "composite") $\geq 1/2$.