CS 681: Computational Number Theory and Algebra Lecture 12: Primality testing
Lecturer: Manindra Agrawal **Notes by: Shashi Mittal**

August 12, 2005.

1 Introduction

The primality testing problem is : Given a number $n \in \mathbb{Z}$, is n a prime number ? We want to perform this operation as efficiently as possible.

In this lecture, we will discuss a few algorithms and ideas for solving this problem using the properties of finite fields.

2 Using properties of $\mathbb{Z}_n$ for primality testing

For any number n, consider the ring $R = \mathbb{Z}_n$. Recall the following two facts related to $\mathbb{Z}_n$.

Fact 2.1 *If n is prime, then $\mathbb{Z}_n$ is a field. The only automorphism of this field is the trivial automorphism, and for $a \in \mathbb{Z}_n$, $a^n = a$.*

Fact 2.2 *If n is composite, square free number divisible by at least two distinct primes, then R is not a field. R has only one automorphism, that is the trivial automorphism.*

Further, in the case where n is composite, a^n may not be necessarily equal to a (unlike the case where n is a prime number). For example, if we take $n = 6$, then for $2 \in \mathbb{Z}_6$, $2^6 = 4$. This gives us a clue for primality testing : Take any $a \leq n$, and check if a^n is a in $\mathbb{Z}_n$ or not. If not, then n is necessarily composite, otherwise n may or may not be prime (this depends on our choice of a, for example, if we choose for $\mathbb{Z}_6$ $a = 3$, then $3^6 = 3$, even though 6 is not a prime number).

Therefore we have the following algorithm for primality testing:

Algorithm-1(n)

1. Select a few $a \in \mathbb{Z}_n$
2. If $a^n = a$ in $\mathbb{Z}_n$ for all a selected above, then print "Prime"
3. else print "Composite"

Note that we can perform the test that $a^n \equiv a(mod\ n)$ in $O(\log n)$ time, by the method of repeated squaring. Hence the above algorithm has a running time which is polynomial in $\log n$.

Unfortunately, Algorithm-1 does not always work correctly, because of existence of special kind of numbers, called *Carmichael numbers.*

Definition 2.1 *A composite number n is a* Carmichael number, *if $p-1|n-1$ for all primes $p|n$.*

Theorem 2.1 *If n is a carmichael number, then $a^n \equiv a(mod\ n)$ for all a.*

Proof: Suppose $p|n$, consider $a^n(mod\ p)$. Since $p-1|n-1$, therefore $a^{p-1} \equiv a(mod\ p)$ in $\mathbb{Z}_p$, and hence $a^n(mod\ p) = a.a^{n-1}(mod\ p) = a(mod\ p)$. Hence, $a^n \equiv a(mod\ p)$ for all $p|n$, and hence by Chinese remaindering theorem, $a^n \equiv a(mod\ n)$ for all a. ∎

The smallest carmichael number is 561 (since $561 = 3 \times 11 \times 13$, and 2|3601, 10|560 and 16|560). It has been shown that there are infinitely many carmichael numbers [1].

Clearly our previous algorithm fails on all carmichael numbers. Therefore, we need to extend our method so that carmichael numbers can also be handled.

3 Generalizing the previous approach

Consider the ring

$$R = \mathbb{Z}_n[X]/(X^r - 1)$$

Suppose n is prime. Then, by Chinese remaindering theorem, we have

$$R = \mathbb{Z}_n \oplus \sum_{i=1}^{k} \mathbb{Z}_n/(h_i(x))$$

where $h_i(x)$ is irreducible over $\mathbb{Z}_n$.

Fact 3.1 *All $h_i(x)$ have the same degree, and R has $(\frac{r-1}{k})^k$ automorphisms*

In particular, $\psi(e(X)) = e^n(X)$ for $e(X) \in R$ is an automorphism. Therefore $\psi, \psi^2, \ldots, \psi^{\frac{r-1}{k}}$ are distinct automorphisms.

However, if n is composite, then ψ may not be an automorphism. This gives us a clue for another potential algorithm for primality testing.

Algorithm-2(n)

1. Choose an appropriately small r.
2. Test if ψ is an automorphism in $R = \mathbb{Z}_n[x]/(x^r - 1)$
3. If yes, then print "Prime"
4. else print "Composite"

3.1 Testing if ψ is an automorphism in R

1. From the definition of ψ, it is easy to see that the property $\psi(e_1(X)e_2(X)) = \psi(e_1(X))\psi(e_2(X))$ holds for all $e_1(X), e_2(X) \in R$.
2. We need to have $\psi(e_1(X) + e_2(X)) = \psi(e_1(X)) + \psi(e_2(X))$. One possible method is to try out all possible $e_1(X)$ and $e_2(X)$ in this equation. Since there are n^r elements in R, this will require n^{2r} such equality testings. However, using the following lemma, this can be verified in n^r checks only :

   Lemma 3.1 *$\psi(e(X)) = e(\psi(X))$ for all $e(X) \in R$ iff ψ is a homomorphism under addition.*

3. We also need to verify whether ψ is a one-one mapping or not. If ψ is a one-one mapping, then

$$\begin{aligned} \psi(e_1(X)) &= \psi(e_2(X)) \\ \psi(e_1(X) - e_2(X)) &= 0 \\ \psi(e_1(X) - e_2(X))^n &= 0 \end{aligned}$$

   Problem : Find the exact condition when $(e_1(X) - e_2(X))^n = 0$, i.e. characterize the conditions on n and $X^r - 1$ that make $e^n(X) = 0$ for non zero $e(X)$.

References

[1] Alford, W.L., Granville, A. and Pomerance, C (1994). There are infinitely many Carmichael numbers. *Annals of Mathematics*