Miller-Rabin: Theory and Background

Scot Anderson, Ph.D.

February 16, 2009

1 Introduction

This lecture series gives an introduction to the theory used in the Miller-Rabin algorithm. We assume a knowlege of prime number concepts and factoring in general, however we do not cover nor do we assume a background in abstract algebra. This lecture is take from Sections 8.1 and 4.3 of (Stallings)

2 Prime Numbers

We start with a definition of prime numbers.

Definition 1 *A prime number is a number $p \in \mathbb{Z}^+$ which has only two natural numbers that divide p evenly, p and 1. We denote the set of all prime numbers $\mathcal{P}$.*

Any positive integer a can be written as a product of prime numbers. When we write this product down we have factored a and the multiplication expression is unique.

$$a = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t} \tag{1}$$

where $p_1 < p_2 < \ldots < p_t$. We can write down a shorthand notation of (1) as follows

$$a = \prod_{p \in \mathcal{P}} p^{a_p} \tag{2}$$

Multiplying two numbers becomes the process of adding the exponents of the primes shared in common and including the other unique terms. If $k = a \cdot b$, then using the notation from (2)

$$k = \prod_{p \in \mathcal{P}} p^{k_p}$$

where $k_p = a_p + b_p$.

For example

$$\begin{aligned} 9 \times 12 &= (3^2)(3 \cdot 2^2) \\ &= 3^3 \cdot 2^2 \end{aligned}$$

What does it mean in terms of factors if we say that a divides b? Simply put the factors of a must be contained in the factors of b. Suppose we let $a = 15$ and $b = 165$. Does 15 divide 165? Lets look at the factors.

$$\begin{aligned} 15 &= 3 \cdot 5 \\ 165 &= 3 \cdot 5 \cdot 11 \end{aligned}$$

We see that the factors of 15 are indeed contained in 165. This amounts to simplifying a division problems.

$$\frac{3 \cdot 5 \cdot 11}{3 \cdot 5} = 11$$

where crossing off the 3's and the 5's leaves 11.

This leads to another interesting mathematical problem. That of finding a $\gcd(a, b)$. But the $\gcd(a, b)$ is just the factors in common.

Definition 2 *The greatest common divisor of two natural numbers a, b denoted,* $\gcd(a, b)$ *is the largest natural number that divides both a and b. Mathematically this can be stated as*

$$k = \gcd(a, b)$$

where $k_p = \min(a_p, b_p)$.

Factoring a large number is no easy task, so the preceeding information is useful for definition, but does not directly lead to a practical method of calculating the greatest common divisor.

3 Euclidean Algorithm

Section 2 talked about gcd of two numbers and the Euclidean algorithm is all about finding the gcd of two numbers. Let's start by considering a few special cases and definitions. First

$$\gcd(a, b) = \gcd(|a|, |b|) \tag{3}$$

which just means that the gcd will always be positive and we can ignore the sign of the integers a and b.

We also have the obvious relation

$$\gcd(p_1, p_2) = 1$$

where $p_1, p_2 \in \mathcal{P}$. But do p_1 and p_2 have to be prime? No,

$$\gcd(9, 4) = 1$$

and neither of these numbers is prime. But they are *relatively prime.*

Definition 3 *Two numbers $a, b \in \mathbb{Z}^+$ are relatively prime if* $\gcd(a, b) = 1$.

Euclid's algorithm is based on the following theorem.

Theorem 4 *For any nonnegative integer a and any positive integer b and $a \geq b$,*

$$\gcd(a, b) = \gcd(b, a \bmod b) \tag{4}$$

Proof. Let $d = \gcd(a, b)$ where a, b satisfy the above conditions. Then by the definition of gcd,

$$\begin{gathered} d|a \\ d|b \end{gathered}$$

For any positive integer b, a can be expressed in the form

$$\begin{aligned} a &= kb + r \equiv r (\bmod b) \qquad (5) \\ a \bmod b &= r \qquad (6) \end{aligned}$$

This form is just equivalence modulo b and is an easy way to see the meaning of the equavalence relation symbol $\equiv$.

Now

$$d|a \Rightarrow d|\left[kb + r\right]$$

We know that

$$\begin{aligned} d|b &\Rightarrow d|kb \\ d|a &\Rightarrow d|kb + d|r \\ &\Rightarrow d|(a \bmod b) \end{aligned}$$

hence the set of common divisor of a and b are equivalent to the set of divisors of b and $a \bmod b$. From this we get the Euclidean algorithm: ■

EUCLID(a, b)

Proof.

1. $A \leftarrow a; B \leftarrow b$
2. if $B = 0$ return A
3. $R = A \bmod B$
4. $A \leftarrow B$
5. $B \leftarrow R$
6. goto 2

■

See also Extended Euclid(m, b) on page 111.

Finish up with a discussion of pages 242 and 243 ending in the miller rabin algorithm