Scribe Notes for *Algorithmic Number Theory*
Class 26—June 23, 1998

Scribes: Lynn W. Jones and Hussein Suleman

Abstract

In today's class, we completed our discussion of recognizing prime numbers. The source of today's lecture is a reading from the Handbook of Applied Cryptography [3] . In addition, we began discussing about elliptic curves.

1 Primality Testing

The Miller-Rabin Test

We have already looked at algorithms that use nondeterminism and randomness to give an answer to an instance of the PRIMES problem. The Miller-Rabin algorithm relies on properties of the multiplicative group $(\mathbb{Z}/(n))^*$ and randomness to determine whether its input is composite or prime.

If n is an odd integer, write $n-1$ as $2^s d$ where $s \geq 1$ and d is odd. We define the set of *strong liars* as

$$\mathrm{S}(n) \quad = \quad \{a \in (\mathbb{Z}/(n))^* : a^d \equiv 1 (\mathrm{mod}\ n) \text{ or } a^{2^r d} \equiv -1 (\mathrm{mod}\ n) \text{ for some } r \text{ with } 0 \leq r < s\}.$$

If n is prime, the order of every a in $(\mathbb{Z}/(n))^*$ is $2^t d'$ where $t > 0$ and $d' \mid d$. Hence when n is prime, $(\mathbb{Z}/(n))^* = \mathrm{S}(n)$.

Example 1.1. We are given $n = 13$, so we write $n - 1 = 2^2 3$. Then $s = 2$ and $d = 3$. We know that the possible values for a are those in $\mathbb{Z}/(13)$. We can build a table for $a^{2^0 d} (\mathrm{mod}\ 13)$ and $a^{2^1 d} (\mathrm{mod}\ 13)$.

The first test, $a^3 \equiv 1 (\mathrm{mod}\ 13)$, qualifies 1, 3, and 9 as strong liars. The second test, with $r = 0$, is $a^3 \equiv -1 (\mathrm{mod}\ 13) \equiv 12 (\mathrm{mod}\ 13)$ and qualifies 4, 10, and 12 as strong liars. The second test, with $r = 1$, is $a^6 \equiv -1 (\mathrm{mod}\ 13) \equiv 12 (\mathrm{mod}\ 13)$; it qualifies the remaining elements. This is as we expect, since n is prime.

Lemma 1.2. *(Lemma 9.4.4 in the text)*

Let n be an odd integer greater than or equal to 3. Then n is prime if and only if $S(n) = (\mathbb{Z}/(n))^*$. If n is composite, then $|S(n)| \leq (n-1)/4$. An element of $(\mathbb{Z}/(n))^* - S(n)$ is a strong witness to the fact that n is composite.

a	$a^3 \pmod{13}$	$a^6 \pmod{13}$
1	1	1
2	8	12
3	1	1
4	12	1
5	8	12
6	8	12
7	5	12
8	5	12
9	1	1
10	12	1
11	5	12
12	12	1

Table 1: Table of elements for Miller-Rabin test.

Miller-Rabin(n)

Write $n-1 = 2^s d$ where d is odd.
Choose $a \in \{1, 2, \ldots, n-1\}$ uniformly at random.
$a_0 \leftarrow a^d \bmod n$.
If $a_0 = 1$, then return "prime".
If $a_0 = -1$, then return "prime".
For $i \leftarrow 1$ to s do:
    $a_i \leftarrow a_{i-1}^2 \bmod n$.
    If $a_i = -1$ then return "prime".
Return "composite".

Miller-Rabin provides a Monte Carlo algorithm that correctly identifies composites with probability at least 3/4. The time complexity is $O((\lg n)^3)$ bit operations. When Miller-Rabin returns that n is a prime, we repeat the algorithm to gain confidence in the result.

Example 1.3. Given $n = 21$, we can write $n - 1 = 2^2 5$. Then $s = 2$ and $d = 5$. Choose $a \in [1, 20]$ at random; in class, we chose $a = 6$. Compute $a_0 = a^5 \bmod 21 = 6$. Since $a_0 \not\equiv 1 \pmod{21}$ and $a_0 \not\equiv -1 \pmod{21}$, then compute $a_1 = a_0^2 \bmod 21 = 6^2 \bmod 21 \equiv -6 \pmod{21}$. Return "composite".

Certificates of Primality

We have discussed algorithms that recognize primes and composites. We may also want to construct an output that certifies that an input n is prime. One such output relies on the following property of prime numbers.

Theorem 1.4. *(see Kilian [2]) Suppose that for some $a \in (\mathbb{Z}/(n))^*$ and some integer $q > \sqrt{n}$, we have $\gcd(a-1, n) = 1$ and $a^q \equiv 1 (mod\ n)$. If q is prime, then n is prime.*

Proof. By contradiction. Suppose that q is prime and n is not prime. Then there is a prime $p < \sqrt{n}$ that divides n. Consequently, $a^q \equiv 1 (\text{mod } p)$. Let r be the order of a in $(\mathbb{Z}/(n))^*$. We know that r must divide q. Also, we know that $r \leq p-1$. So $r < p < q$. Since q is prime, r must be 1. Hence $a \equiv 1 (\text{mod } p)$. So $p \mid (a-1)$ and $p \mid n$. But, $\gcd(a-1, n) = 1$. This is a contradiction, so such a p cannot exist. Therefore, n is prime. □

The *certificate* we want is a sequence $(q_i, a_i), (q_{i-1}, a_{i-1}), \ldots, (q_1, a_1), q_0$ where $q_0 = n$. This certifies that n is prime if:

1. q_i is a "small" prime (relative to what can be proven deterministically in polynomial time), and
2. (q_j, a_j) must constitute a proof that q_{j-1} is prime, $1 \leq j \leq i$, by Theorem 1.4.

Example 1.5. Let $n = q_0 = 179$. Then guess $q_1 = 89$ and $a_1 = 9$. Check that $89 > \sqrt{179}$, then use Theorem 1.4 to verify that q_1 is prime: $9^{89} \equiv 1 (\text{mod } 179)$ and $\gcd(9-1, 179) = 1$. Next, guess $q_2 = 11$ and $a_2 = 45$. Check that $11 > \sqrt{89}$, and use Theorem 1.4 to verify that q_2 is prime: $45^{11} \equiv 1 (\text{mod } 89)$ and $\gcd(45-1, 89) = 1$. Since 11 is a small prime, we stop and produce the certificate: (11,45),(89,9),179.

Guessing q and a is one method of obtaining these values. If q is guessed, then we can use the previously discussed algorithms to gain some confidence that q is prime before proceeding.

2 Elliptic Curves

Definition 2.1. Let $\mathbb{F}$ be a field of characteristic not 2 or 3. An *elliptic curve* is a pair $(A, B) \in \mathbb{F} \times \mathbb{F}$ such that $4A^3 + 27B^2 \neq 0$. It defines a set of points $E_{A,B}(\mathbb{F}) = \{(x, y) : y^2 = x^3 + Ax + B\} \cup \{I\}$.

In this definition, we can think of I as being equivalent to infinity.

Example 2.2. Consider the field $\mathbb{R}$. The graph in Figure 1 represents the elliptic curve generated by $A = -5$ and $B = 1$ in this field.

Note that the graph is symmetric about the x-axis.

In order to make $E_{A,B}$ into a group, we need to define an addition operation. Define $s + t$ to be the reflection about the x-axis of the third point of the graph cut by the straight line passing through s and t.

It can be seen that every line passing through two points will intersect with the graph at one other point, except for the points tangential to the ovoid portion of the graph. An example of such a point is u. In that case $u + u = -v$. Alternatively, we could write $u = (-u) + (-v)$, which indicates that points tangential to the curve still conform to the definition of addition.

Example 2.3. Consider the field $\mathbb{F} = \mathbb{Z}/(5)$ with $A = \overline{2}$ and $B = \overline{4}$.

$\overline{4}A^3 + \overline{27}B^2 = (\overline{-1})(\overline{8}) + (\overline{2})(\overline{16}) = \overline{-3} + \overline{2} = \overline{4} \neq 0$

Therefore (A, B) represents an elliptic curve.

In Table 2, the entries with corresponding values in the second columns represent elements of the set $E_{A,B}$. Thus,

$$E_{A,B} = \{(0,2), (0,3), (2,1), (2,4), (4,1), (4,4), I\}$$

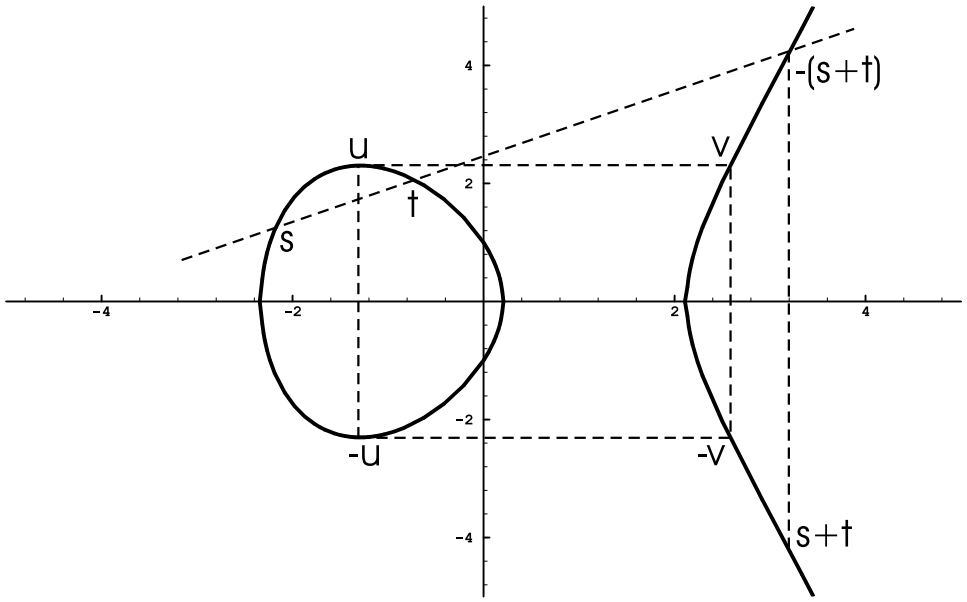

Figure 1: Visualization of elliptic curve in $\mathbb{R} \times \mathbb{R}$

X	$X^3 + \overline{2}X + \overline{4}$
$\overline{0}$	$\overline{4}$
$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{1}$
$\overline{3}$	$\overline{2}$
$\overline{4}$	$\overline{1}$

Y	Y^2
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{4}$
$\overline{4}$	$\overline{1}$

Table 2: Table of possible x and y values used to generate $E_{A,B}$

We can test pairs of elements to verify that addition works. Consider $(\overline{4},\overline{1})+(\overline{0}+\overline{3})$. The slope is $\frac{\overline{3}-\overline{1}}{\overline{0}-\overline{4}}=\overline{2}$ so the direction of the line is $(\overline{1},\overline{2})$. Thus, the equation of the line is $(\overline{4},\overline{1})+\lambda(\overline{1},\overline{2})$.

Choosing $\lambda=\overline{4}$, we will get the point $(\overline{4},\overline{1})+(\overline{4},\overline{3})=(\overline{3},\overline{4})$. The reflection of this point is $(\overline{2},\overline{1})$, which is contained in the group. Similarly, we can verify that addition is closed for all possible operand combinations.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory*, The MIT Press, Cambridge, Massachusetts, 1996.

[2] J. Kilian, *Uses of randomness in algorithms and protocols*, The MIT Press, Cambridge, Massachusetts, 1990.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, eds., *Handbook of Applied Cryptography*, CRC Press, Boca, Raton, 1997.