COMP8760 Lecture - 5

Primality Testing, Extended Euclidean Algorithm

Sanjay Bhattacherjee

University of Kent

2aw4s5

Study Material

Book 1	*Cryptography Made Simple*
Author	Nigel P. Smart.
	Link to eBook

Section 2.1.2 Trial Division
Section 2.1.3 Fermat's Test
Section 1.3.1 Greatest Common Divisors
Section 1.3.2 The Euclidean Algorithm
Section 1.3.3 The Extended Euclidean Algorithm

Primality Testing

Recap: The Prime Number Theorem (Gauss)

Let $\pi(X)$ be the function that counts the number of primes less than X.

$$\pi(X) \approx \frac{X}{\log_e X}.$$

Primes are quite common!

How do we test if a randomly generated number n
is prime or not?

Trial Division

Exhaustive search for factors of n till $\sqrt{n}$

- For each $2 \leq d \leq \sqrt{n}$
  - if $n \mod d = 0$, then n is not a prime;
    hence, break the loop
- if the above loop was not broken, then n is a prime

When p is not a prime, the value of d (the least factor) will be
the certificate of compositeness!

If n is prime, there is no certificate of primality!
To verify, one has to run the test once again!

Partial Trial Division

Search for factors of n till a bound $Y < \sqrt{n}$

- For each $2 \leq d \leq Y$
  - if $n \mod d = 0$, then n is not a prime;
    hence, break the loop
- if the above loop was not broken, then n is a prime with some probability

Eliminating Composites

Let $\{2, 3, \ldots, p_k\}$ be the set of all prime numbers less than Y.
Partial Trial Division will eliminate all but

$$\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

fraction of composites.

For all $p_i < 100$, we have $\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \approx 0.12$

Recall: Fermat's Little Theorem

Theorem

Let p be a prime number and a be an integer. Then,

$$a^p = a \mod p.$$

Proof Idea.

In Lagrange's Theorem, consider the group $\mathbb{Z}_p^\star = \{1, 2, \ldots, p-1\}$.
For any $a \in \mathbb{Z}_p^\star$,

$$a^{p-1} = 1 \mod p.$$

And hence,

$$a^p = a \mod p.$$

Fermat's Test: Is n a prime number?

For several randomly chosen $a \in \{2, \ldots, n-1\}$

$$\text{check if } a^{n-1} = 1 \mod n$$
$$\Longleftrightarrow \text{check if } a^{n} = a \mod n$$

- If $a^{n-1} \mod n$ is not 1, then n is composite.
- If $a^{n-1} \mod n$ is 1, then n is prime with "high probability".

Algorithm:

```
for i=1 to k do {
    Choose a ∈ [2,...,n−1] at random
    if a^(n−1) ≠ 1 mod n {
       return ("Composite", a)
    }
}
return ("Probably Prime", 1)
```

Exceptions: Carmichael Numbers

Composite numbers n for which $a^{n-1} \mod n = 1$, for every a mutually prime with n.
for every $a \in \{x : \gcd(x, n) = 1, 2 \leq x \leq n-1\}$.

Fermat's Test

The Test for n:

```
for i=1 to k do {
    Choose a ∈ [2, ..., n − 1] at random
    if a^(n−1) ≠ 1 mod n {
       return ("Composite", a)
    }
}
return ("Probably Prime", 1)
```

Properties:

- a is the "witness of compositeness"
- Very efficient (fast)
- No proof of primality
  As the value of k is increased, there is increased probability that n is indeed a prime.

Floor of $x \in \mathbb{R}$

Largest integer less than or equal to x

Notation: $\lfloor x \rfloor$

Examples:

- $\lfloor 0 \rfloor = 0$
- $\lfloor 0.5 \rfloor = 0$
- $\lfloor 0.999 \rfloor = 0$
- $\lfloor 1.001 \rfloor = 1$
- $\lfloor 1.999 \rfloor = 1$
- $\lfloor 786 \rfloor = 786$
- $\lfloor -0.2 \rfloor = -1$
- $\lfloor -0.999 \rfloor = -1$
- $\lfloor -1.001 \rfloor = -2$
- $\lfloor -1.999 \rfloor = -2$

How to find the Multiplicative Inverse of $a \in \mathbb{Z}_N^\star$?

Multiplicative inverse of $a \in \mathbb{Z}_N^\star$ is the solution $x \in \mathbb{Z}_N^\star$ to the equation:

$$a \cdot x = 1 \pmod{N}$$

Note:

The inverse x exists only for $a \in \mathbb{Z}_N^\star$ for which

$$\gcd(a, N) = 1$$

and not for the other $a \in \mathbb{Z}_N$.

Algorithm:

Find $d = \gcd(a, N)$ using the Extended Euclidean Algorithm (EEA).

Precursor: All EA remainders take the form: $r_i = s_i \cdot a + t_i \cdot b$

$$\begin{aligned} a &= q \cdot b + r \\ r &= 1 \cdot a - q \cdot b \end{aligned}$$

Compute $\gcd(50, 9)$ using the Euclidean algorithm

$$\begin{aligned} \gcd(50,9) &= \gcd(9, 50 \mod 9) \\ &= \gcd(9,5) \\ &= \gcd(5, 9 \mod 5) \\ &= \gcd(5,4) \\ &= \gcd(4, 5 \mod 4) \\ &= \gcd(4,1) \\ &= \gcd(1, 4 \mod 1) \\ &= \gcd(1,0) \\ &= 1 \end{aligned}$$

$$\begin{aligned} r_0 = 50 \quad &= 1 \cdot 50 + 0 \cdot 9 \\ r_1 = 9 \quad &= 0 \cdot 50 + 1 \cdot 9 \\ r_2 = 5 \quad &= 1 \cdot 50 - 5 \cdot 9 \\ r_3 = 4 \quad &= 9 - 1 \cdot 5 \\ &= 1 \cdot 9 - 1 \cdot (50 - 5 \cdot 9) \\ &= (-1 \cdot 50) + (6 \cdot 9) \\ r_4 = 1 \quad &= 5 - 1 \cdot 4 \\ &= 1 \cdot (50 - 5 \cdot 9) - 1 \cdot ((6 \cdot 9) + (-1 \cdot 50)) \\ &= 50 - 5 \cdot 9 - 6 \cdot 9 + \cdot 50 \\ &= 2 \cdot 50 - 11 \cdot 9 \end{aligned}$$

Note that the remainders at each step can be expressed as:

$$r_i = s_i \cdot a + t_i \cdot b$$

EEA: Example 1 - $\gcd(20, 12)$

$$r_i = s_i \cdot 20 + t_i \cdot 12$$

r'	$=$	s'	$\cdot$	20	$+$	t'	$\cdot$	12	
r	$=$	s	$\cdot$	20	$+$	t	$\cdot$	12	
									Operations with $q \leftarrow \lfloor r'/r \rfloor$
20	$=$	1	$\cdot$	20	$+$	0	$\cdot$	12	
12	$=$	0	$\cdot$	20	$+$	1	$\cdot$	12	
									$q = 1 \leftarrow \lfloor 20/12 \rfloor$ $r = r' - qr = 20 - 1 \cdot 12 = 8$ $s = s' - qs = 1 - 1 \cdot 0 = 1$ $t = t' - qt = 0 - 1 \cdot 1 = -1$
12	$=$	0	$\cdot$	20	$+$	1	$\cdot$	12	
8	$=$	1	$\cdot$	20	$+$	-1	$\cdot$	12	
									$q = 1 \leftarrow \lfloor 12/8 \rfloor$ $r = r' - qr = 12 - 1 \cdot 8 = 4$ $s = s' - qs = 0 - 1 \cdot 1 = -1$ $t = t' - qt = 1 - (1 \cdot -1) = 2$
8	$=$	1	$\cdot$	20	$+$	-1	$\cdot$	12	
4	$=$	-1	$\cdot$	20	$+$	2	$\cdot$	12	
									$q = 2 \leftarrow \lfloor 8/4 \rfloor$ $r = r' - qr = 8 - 2 \cdot 4 = 0$ $s = s' - qs = 1 - (2 \cdot -1) = 3$ $t = t' - qt = -1 - (2 \cdot 2) = -5$
4	$=$	-1	$\cdot$	20	$+$	2	$\cdot$	12	
0	$=$	3	$\cdot$	20	$+$	-5	$\cdot$	12	
									Since $r = 0$, we stop and output (r', s', t')

EEA: Example 2 - $\gcd(50, 9)$

$$r_i = s_i \cdot 50 + t_i \cdot 9$$

r'	$=$	s'	$\cdot$	50	$+$	t'	$\cdot$	9	
r	$=$	s	$\cdot$	50	$+$	t	$\cdot$	9	
									Operations with $q \leftarrow \lfloor r'/r \rfloor$
50	$=$	1	$\cdot$	50	$+$	0	$\cdot$	9	
9	$=$	0	$\cdot$	50	$+$	1	$\cdot$	9	
									$q = 5 \leftarrow \lfloor 50/9 \rfloor$
									$r = r' - qr = 50 - 5 \cdot 9 = 5$
									$s = s' - qs = 1 - 5 \cdot 0 = 1$
									$t = t' - qt = 0 - 5 \cdot 1 = -5$
9	$=$	0	$\cdot$	50	$+$	1	$\cdot$	9	
5	$=$	1	$\cdot$	50	$+$	-5	$\cdot$	9	
									$q = 1 \leftarrow \lfloor 9/5 \rfloor$
									$r = r' - qr = 9 - 1 \cdot 5 = 4$
									$s = s' - qs = 0 - 1 \cdot 1 = -1$
									$t = t' - qt = 1 - (1 \cdot -5) = 6$
5	$=$	1	$\cdot$	50	$+$	-5	$\cdot$	9	
4	$=$	-1	$\cdot$	50	$+$	6	$\cdot$	9	
									$q = 1 \leftarrow \lfloor 5/4 \rfloor$
									$r = r' - qr = 5 - 1 \cdot 4 = 1$
									$s = s' - qs = 1 - (1 \cdot -1) = 2$
									$t = t' - qt = -5 - (1 \cdot 6) = -11$
4	$=$	-1	$\cdot$	50	$+$	6	$\cdot$	9	
1	$=$	2	$\cdot$	50	$+$	-11	$\cdot$	9	
									When $r = 0$, we can stop and output (r', s', t')

The Extended Euclidean Algorithm (EEA)

$$r_i = s_i \cdot a + t_i \cdot b$$

Input: a, b
Output: r_m, s_m, t_m

Initialisation:

$r' \leftarrow a$, $r \leftarrow b$
$s' \leftarrow 1$, $s \leftarrow 0$
$t' \leftarrow 0$, $t \leftarrow 1$

Iteration: `while` $r \neq 0$ `do:`

$q \leftarrow \lfloor r'/r \rfloor$
$(r', r) \leftarrow (r, r' - q \cdot r)$
$(s', s) \leftarrow (s, s' - q \cdot s)$
$(t', t) \leftarrow (t, t' - q \cdot t)$

Final: $d \leftarrow r', x \leftarrow s', y \leftarrow t'$
`return` d, x, y

Multiplicative Inverse

$$d = \gcd(a, N) = x \cdot a + y \cdot N \pmod{N}$$

We know that the multiplicative inverse of $a \pmod N$ exists if and only if

$$d = \gcd(a, N) = 1$$

Hence, we can find x such that

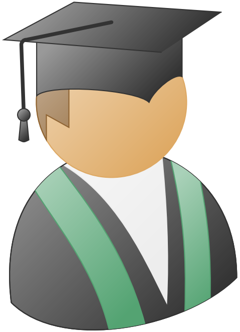
$$1 = x \cdot a \pmod{N}$$

Output of the Extended Euclidean Algorithm:

$1 = 2 \cdot 50 - 11 \cdot 9$

- $1 = 2 \cdot 50 \pmod 9 = 2 \cdot 5 \pmod 9$
  Hence, 2 and 5 are multiplicative inverses of each other $\pmod 9$
- $1 = -11 \cdot 9 \pmod{50} = 39 \cdot 9 \pmod{50}$
  Hence, 39 and 9 are multiplicative inverses of each other $\pmod{50}$

Note: $-11 \pmod{50} = 39 \pmod{50}$, because $39 + 11 = 0 \pmod{50}$.



Thank you for your kind attention!