CSEP 521: Applied Algorithms
Lecture 6 Randomized Primality Testing

Richard Anderson

January 21, 2021

Announcements

- Today is the 21[st] day of the 21[st] year of the 21[st] century

Primality Testing

- Miller-Rabin test demonstrated importance of randomized algorithm
  - Break through result in 1980
- Depends on number theory (maybe a senior ugrad class)
  - But much of the algorithm can be appreciated without the theory
- The key concept is that of a witness
  - If something is true, a witness always says TRUE
  - If something is false, a witness says TRUE with probability less than ½

Primality testing

Is the number:
38,448,590,786,041,766,459,732,220,363,801,744,241,896,763,259,493,887,920,989,231,800,007,262,253,532,084,767,190,
284,597,690,724,762,898,279,841,570,128,623,506,757,165,008,658,334,072,162,989,430,299,242,002,399,263,948,157,60
7,441,618,354,889,045,484,455,604,450,713,181,265,743,757,650,808,578,235,094,058,535,442,090,523,274,067,570,229,4
06,671,451,796,017,542,179,880,527,768,546,296,447,905,493,082,191
prime?

- A number p is prime if its only proper divisors are 1 and p, and is composite otherwise
- Small primes {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, . . .}
- Simple primality testing algorithms
  - Trial division
  - Sieve of Eratosthenes

Why prime testing is important: cryptography

- RSA public key encryption
  - Relies on factoring "being hard", N = pq where p and q are prime
  - Recommendation is that N is 2048 bits with p and q roughly 1024 bits
  - 1024 bits is roughly 300 digits
- Need a way to generate "random primes"
  - Guess and check

Complexity of number problems

- Run time based on size of input
- Input N has size $\log_2 N$
- Polynomial time corresponds to polynomial in the size of the number
- Runtime polynomial in N is exponential in the number of bits

Bignum computation

- Arithmetic computation on large numbers – hundreds or thousands or millions of digits
- Run time expressed as a function of the number of digits
- Addition of two n-bit numbers: O(n)
- Multiplication of two n-bit numbers: $O(n^2)$ or $O(n^{3/2})$ or O(n log n loglog n)
- Bignum arithmetic implemented by storing numbers in an array of ints
  - 1024 bit number would require an array of 32 ints

Exponentiation: Compute A^N

- Do the computation mod M
  - $129038105814095380935^{843098142309124380\,9}$ MOD 10000000000000000000000
- Compute by repeated squaring
- A raised to 2^K can be computed in K multiplications

Greatest Common Divisor

- GCD(A, B) = D, where D is the largest number that divides both A and B
- Runs in $O(n^2)$ time for n bit numbers

```
function gcd(a, b)
   while b ≠ 0
      t := b
      b := a mod b
      a := t
   return a
```

A: 33707, B: 15207
A: 15207, B: 3293
A: 3293, B: 2035
A: 2035, B: 1258
A: 1258, B: 777
A: 777, B: 481
A: 481, B: 296
A: 296, B: 185
A: 185, B: 111
A: 111, B: 74
A: 74, B: 37
A: 37, B: 0

Prime testing – Idea: Modular arithmetic

- Let P be prime
- Consider the set of integers {1, 2, 3, . . ., P-1} with the operation *, where multiplication is done mod P
- Can the structure of modular multiplication be used to show P is prime?
- Set with multiplication mod P referred to as Z^*_P

1	2	3	4	5	6
2	4	6	1	3	5
3	6	2	5	1	4
4	1	5	2	6	3
5	3	1	6	4	2
6	5	4	3	2	1

Modular multiplication

1	2	3	4	5	6	7	8	9	10	11	12
2	4	6	8	10	12	1	3	5	7	9	11
3	6	9	12	2	5	8	11	1	4	7	10
4	8	12	3	7	11	2	6	10	1	5	9
5	10	2	7	12	4	9	1	6	11	3	8
6	12	5	11	4	10	3	9	2	8	1	7
7	1	8	2	9	3	10	4	11	5	12	6
8	3	11	6	1	9	4	12	7	2	10	5
9	5	1	10	6	2	11	7	3	12	8	4
10	7	4	1	11	8	5	2	12	9	6	3
11	9	7	5	3	1	12	10	8	6	4	2
12	11	10	9	8	7	6	5	4	3	2	1

1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	13	12	11	10	9	8	7	6	5	4	3	2	1

Zero divisors for integers mod N

- X is a zero divisor if AX = 0 mod N for some A != 0
- Fact: X is a zero divisor if and only if GCD(X, N) > 1
- Z^*_N = { y in [1 .. N-1] | GCD(y, N) = 1 }
- $|Z^*_N| = \Phi(N)$

1	2	4	7	8	11	13	14
2	4	8	14	1	7	11	13
4	8	1	13	2	14	7	11
7	14	13	4	11	2	1	8
8	1	2	11	4	13	14	7
11	7	14	2	13	1	8	4
13	11	7	1	14	8	4	2
14	13	11	8	7	4	2	1

Powers of elements

P = 7, 11, 13

- Compute $A^1, A^2, A^3, \ldots, A^{P-1}$

1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	3	6	12	11	9	5	10	7	1
3	9	1	3	9	1	3	9	1	3	9	1
4	3	12	9	10	1	4	3	12	9	10	1
5	12	8	1	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	1
7	10	5	9	11	12	6	3	8	4	2	1
8	12	5	1	8	12	5	1	8	12	5	1
9	3	1	9	3	1	9	3	1	9	3	1
10	9	12	3	4	1	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	1
12	1	12	1	12	1	12	1	12	1	12	1

P = 17, 19, 23

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	9	18	13	3	6	12	1	2	4	8	16	9	18	13	3	6	12	1
3	9	4	12	13	16	2	6	18	8	1	3	9	4	12	13	16	2	6	18	8	1
4	16	18	3	12	2	8	9	13	6	1	4	16	18	3	12	2	8	9	13	6	1
5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1
6	13	9	8	2	12	3	18	16	4	1	6	13	9	8	2	12	3	18	16	4	1
7	3	21	9	17	4	5	12	15	13	22	16	20	2	14	6	19	18	11	8	10	1
8	18	6	2	16	13	12	4	9	3	1	8	18	6	2	16	13	12	4	9	3	1
9	12	16	6	8	3	4	13	2	18	1	9	12	16	6	8	3	4	13	2	18	1
10	8	11	18	19	6	14	2	20	16	22	13	15	12	5	4	17	9	21	3	7	1
11	6	20	13	5	9	7	8	19	2	22	12	17	3	10	18	14	16	15	4	21	1
12	6	3	13	18	9	16	8	4	2	1	12	6	3	13	18	9	16	8	4	2	1
13	8	12	18	4	6	9	2	3	16	1	13	8	12	18	4	6	9	2	3	16	1
14	12	7	6	15	3	19	13	21	18	22	9	11	16	17	8	20	4	10	2	5	1
15	18	17	2	7	13	11	4	14	3	22	8	5	6	21	16	10	12	19	9	20	1
16	3	2	9	6	4	18	12	8	13	1	16	3	2	9	6	4	18	12	8	13	1
17	13	14	8	21	12	20	18	7	4	22	6	10	9	15	2	11	3	5	16	19	1
18	2	13	4	3	8	6	16	12	9	1	18	2	13	4	3	8	6	16	12	9	1
19	16	5	3	11	2	15	9	10	6	22	4	7	18	20	12	21	8	14	13	17	1
20	9	19	12	10	16	21	6	5	8	22	3	14	4	11	13	7	2	17	18	15	1
21	4	15	16	14	18	10	3	17	12	22	2	19	8	7	9	5	13	20	6	11	1
22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1	22	1

P = 9, 12, 15, 21

1	1	1	1	1	1	1	1
2	4	8	7	5	1	2	4
3	0	0	0	0	0	0	0
4	7	1	4	7	1	4	7
5	7	8	4	2	1	5	7
6	0	0	0	0	0	0	0
7	4	1	7	4	1	7	4
8	1	8	1	8	1	8	1

1	1	1	1	1	1	1	1	1	1	1
2	4	8	4	8	4	8	4	8	4	8
3	9	3	9	3	9	3	9	3	9	3
4	4	4	4	4	4	4	4	4	4	4
5	1	5	1	5	1	5	1	5	1	5
6	0	0	0	0	0	0	0	0	0	0
7	1	7	1	7	1	7	1	7	1	7
8	4	8	4	8	4	8	4	8	4	8
9	9	9	9	9	9	9	9	9	9	9
10	4	4	4	4	4	4	4	4	4	4
11	1	11	1	11	1	11	1	11	1	11

1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	1	2	4	8	1	2	4	8	1	2	4
3	9	12	6	3	9	12	6	3	9	12	6	3	9
4	1	4	1	4	1	4	1	4	1	4	1	4	1
5	10	5	10	5	10	5	10	5	10	5	10	5	10
6	6	6	6	6	6	6	6	6	6	6	6	6	6
7	4	13	1	7	4	13	1	7	4	13	1	7	4
8	4	2	1	8	4	2	1	8	4	2	1	8	4
9	6	9	6	9	6	9	6	9	6	9	6	9	6
10	10	10	10	10	10	10	10	10	10	10	10	10	10
11	1	11	1	11	1	11	1	11	1	11	1	11	1
12	9	3	6	12	9	3	6	12	9	3	6	12	9
13	4	7	1	13	4	7	1	13	4	7	1	13	4
14	1	14	1	14	1	14	1	14	1	14	1	14	1

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	11	1	2	4	8	16	11	1	2	4	8	16	11	1	2	4
3	9	6	18	12	15	3	9	6	18	12	15	3	9	6	18	12	15	3	9
4	16	1	4	16	1	4	16	1	4	16	1	4	16	1	4	16	1	4	16
5	4	20	16	17	1	5	4	20	16	17	1	5	4	20	16	17	1	5	4
6	15	6	15	6	15	6	15	6	15	6	15	6	15	6	15	6	15	6	15
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1
9	18	15	9	18	15	9	18	15	9	18	15	9	18	15	9	18	15	9	18
10	16	13	4	19	1	10	16	13	4	19	1	10	16	13	4	19	1	10	16
11	16	8	4	2	1	11	16	8	4	2	1	11	16	8	4	2	1	11	16
12	18	6	9	3	15	12	18	6	9	3	15	12	18	6	9	3	15	12	18
13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1
14	7	14	7	14	7	14	7	14	7	14	7	14	7	14	7	14	7	14	7
15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15
16	4	1	16	4	1	16	4	1	16	4	1	16	4	1	16	4	1	16	4
17	16	20	4	5	1	17	16	20	4	5	1	17	16	20	4	5	1	17	16
18	9	15	18	9	15	18	9	15	18	9	15	18	9	15	18	9	15	18	9
19	4	13	16	10	1	19	4	13	16	10	1	19	4	13	16	10	1	19	4
20	1	20	1	20	1	20	1	20	1	20	1	20	1	20	1	20	1	20	1

P = 9, 12, 15, 21 for Z^*_N

1	1	1	1	1	1	1	1
2	4	8	7	5	1	2	4
4	7	1	4	7	1	4	7
5	7	8	4	2	1	5	7
7	4	1	7	4	1	7	4
8	1	8	1	8	1	8	1

1	1	1	1	1	1	1	1	1	1	1
5	1	5	1	5	1	5	1	5	1	5
7	1	7	1	7	1	7	1	7	1	7
11	1	11	1	11	1	11	1	11	1	11

1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	1	2	4	8	1	2	4	8	1	2	4
4	1	4	1	4	1	4	1	4	1	4	1	4	1
7	4	13	1	7	4	13	1	7	4	13	1	7	4
8	4	2	1	8	4	2	1	8	4	2	1	8	4
11	1	11	1	11	1	11	1	11	1	11	1	11	1
13	4	7	1	13	4	7	1	13	4	7	1	13	4
14	1	14	1	14	1	14	1	14	1	14	1	14	1

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	11	1	2	4	8	16	11	1	2	4	8	16	11	1	2	4
4	16	1	4	16	1	4	16	1	4	16	1	4	16	1	4	16	1	4	16
5	4	20	16	17	1	5	4	20	16	17	1	5	4	20	16	17	1	5	4
8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1
10	16	13	4	19	1	10	16	13	4	19	1	10	16	13	4	19	1	10	16
11	16	8	4	2	1	11	16	8	4	2	1	11	16	8	4	2	1	11	16
13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1
16	4	1	16	4	1	16	4	1	16	4	1	16	4	1	16	4	1	16	4
17	16	20	4	5	1	17	16	20	4	5	1	17	16	20	4	5	1	17	16
19	4	13	16	10	1	19	4	13	16	10	1	19	4	13	16	10	1	19	4
20	1	20	1	20	1	20	1	20	1	20	1	20	1	20	1	20	1	20	1

Idea (that doesn't quite work)

- Theorem: if P is prime, $A^{P-1} = 1 \pmod P$
- Pick a bunch of numbers at random from [1 .. P-1]
  - Compute $X^{P-1} \bmod P$ for each one
  - If all results are 1, then say Prime
  - If at least one of them is not 1, then say Composite

Carmichael Numbers
What about 561 = 3*11*17

- $2^{560} = 1 \bmod 561$
- $4^{560} = 1 \bmod 561$
- $5^{560} = 1 \bmod 561$
- $7^{560} = 1 \bmod 561$
- $8^{560} = 1 \bmod 561$
- $10^{560} = 1 \bmod 561$
- $14^{560} = 1 \bmod 561$
- . . . . .

- Carmichael numbers are rare (but there are an infinite number)
- Either all numbers in Z^*_N satisfy $X^{N-1} = 1 \bmod N$ or at most half the numbers in Z^*_N satisfy $X^{N-1} = 1 \bmod N$

Witnesses and Certificates

- Certificate C that can be used to prove a property
  - To show N is composite, find a number A such that 1 < GCD(A, N) < N
  - 178 is a Certificate that 11481 is composite
- Is there a certificate for primality?
- Prime Witness
  - A property that always holds for primes
  - A property that only sometimes holds for composites

Euler Test

- N – 1 mod N = -1 mod N, so we can think of N-1 as -1 in Z^*_N
- For P prime, $a^{(p-1)/2} = 1$ or $a^{(p-1)/2} = -1$
  - Half of the values of a have $a^{(p-1)/2} = 1$ and half have $a^{(p-1)/2} = -1$
- But there are composite numbers that fool the Euler Test
  - 1729 = 7 * 13 * 19
  - 2^{864} = 1 mod 1729, 3^{864} = 1 mod 1729, 4^{864} = 1 mod 1729, . . .

Lemma 14.32 (Motwani-Raghavan)

- Let N an odd composite that is not a power of a prime and suppose that for some a in Z^*_N, $a^{(N-1)/2} = -1$ mod N
- Let S be the set of numbers a in Z^*_N where $a^{(N-1)/2} = -1$ mod N or $a^{(N-1)/2} = 1$ mod N
- Then $|S| <= ½ |Z^*_N|$
- Or in English: if the Euler Test passes with a -1, then at most half the values fool the test

Prime Testing Algorithm

1. If N is perfect power return Composite
2. Choose a bunch of random values $b_1, b_2, \ldots, b_t$ from [1..n-1]
3. If GCD(b_j,N) return Composite
4. $r_j = b_j^{(N-1)/2}$
5. If r_j != 1 and r_j != -1 return Composite
6. If r_j = 1 for all j return Composite
7. Return prime

What could go wrong

- Composite number could fail line 5 and fail line 6 and be called prime
- Prime could be reported as composite on line 6
- Double sided error with failure probability 2^{-t}

Miller-Rabin test

- Determine if n is prime
- Given an integer a, 1 < a < n,
  - Miller(n, a) returns either "maybe prime" or "definitely composite"
  - For n prime, Miller(n, a) always says "maybe prime"
  - For n composite, Miller(n, a) says "maybe prime" with probability at most ¼ for a random a
- By running the Miller test repeatedly, we can make it arbitrary high probability

Fermat Test

- Fermat's little theorem
  - For prime n, $a^{(n-1)} = 1 \pmod{n}$ for all a
- For most composite numbers, this fails most of the time
- Unfortunately, there are set of composite numbers (Carmichael numbers) that satisfy this
  - {561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, 101101, 115921, 126217, 162401, 172081, 188461, 252601, 278545, 294409, 314821, 334153, ...}

Miller-Rabin test

- For a prime number n, the only square roots of 1 modulo n, are 1 and -1
- For $n = 2^s d + 1$, $a^d = 1 \pmod{n}$ or $a^{(2^r)d} = -1 \pmod{n}$ for some $0 <= r < s$
- For a composite number at most ¼ of values a satisfy these conditions

Pseudo-code

```
Input #1: n > 3, an odd integer to be tested for primality
Input #2: k, the number of rounds of testing to perform
Output: "composite" if n is found to be composite, "probably prime" otherwise

write n as 2^r·d + 1 with d odd (by factoring out powers of 2 from n − 1)
WitnessLoop: repeat k times:
   pick a random integer a in the range [2, n − 2]
   x ← a^d mod n
   if x = 1 or x = n − 1 then
      continue WitnessLoop
   repeat r − 1 times:
      x ← x^2 mod n
      if x = n − 1 then
         continue WitnessLoop
   return "composite"
return "probably prime"
```

Other facts on Prime Testing

- Miller-Rabin test is deterministic if Extended Riemann Hypothesis is true
- 2002 a deterministic polynomial time test based on Cyclotomic Polynomials was discovered
  - Agrawal-Kayal-Saxena, IIT Kanpur
  - Not practical (termed galactic algorithm – see Wikipedia)
- Factoring is thought to be harder then primality testing
  - In practice, numbers of about 100 decimal digits are factorable in a few hours on a PC
  - 250 decimal digit (829 bit) RSA keys have been factored (2700 CPU Years)
  - Recommendation for RSA is 2048 bit keys

RSA

- RSA key is a number n=pq, where p and q are prime
- How do you generate random primes of 300 digits?
- Generate random number of 300 digits and test if they are prime
  - Of course, there are simple tricks to avoid small divisors
- Prime number theorem: Probability of a random number less than N is prime is about 1/log N (Natural logarithm)
- For 300 digits, this is about 1 in 690