Lucas-Lehmer, Miller-Rabin, and AKS Primality Test

Inho Ryu

Euler Circle

July 17, 2023

Background

- A primality test is an algorithm which determines whether an input number is prime.
  - Trial division
- Cryptography - Generating keys
- GIMPS: Great Internet Mersenne Prime Search
  - A collaborative project of people who use software on their PCs in order to find Mersenne primes
  - Fermat probable prime test, Lucas-Lehmer test

Repeated Squaring

There are two algorithms for the modular exponentiation problem: the naive algorithm and the repeated squaring algorithm.
The repeated squaring algorithm goes as follows:

1. Start with b and multiply it by itself ("squaring it") $\pmod m$
2. Square the new result $\pmod m$
3. etc. until power is equal or larger than original
4. Combine together some of these results, multiplying them together $\pmod m$

There are some steps we can take to make this easier, such as in $b^k \pmod m$ converting k to binary for the final step (see example).

Example

Say we wish to know the value $3^{200} \mod 50$.

1. $3^1 = 3 \mod 50 \to 3 \mod 50$
2. $3^2 = 9 \mod 50 \to 9 \mod 50$
3. $3^4 = 81 \mod 50 \to 31 \mod 50$
4. $3^8 = 961 \mod 50 \to 11 \mod 50$
5. $3^{16} = 121 \mod 50 \to 21 \mod 50$
6. $3^{32} = 441 \mod 50 \to 41 \mod 50$
7. $3^{64} = 1681 \mod 50 \to 31 \mod 50$
8. $3^{128} = 961 \mod 50 \to 11 \mod 50$
9. 3^{256}, but exponent is larger than initial, so halt.

Rewrite 200 in binary as 11001000. So, $200 = 128 + 64 + 8$. So $3^{200} \mod 50 = 3^{128+64+8} \mod 50 = 3^{128}3^{64}3^8 \mod 50$, and replace to get $(11)(31)(11) \mod 50 = 3751 \mod 50 = 1 \mod 50$.

Mersenne Primes

Definition (Mersenne Number)

$M_n = 2^n - 1$ where $n \in \mathbb{Z}^+$ and $n \geq 2$

- A Mersenne prime is a prime Mersenne number.
- There are only 51 Mersenne primes known
- Close relation to perfect numbers (Euclid-Euler Theorem)
  1. $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is a perfect number.
  2. All even perfect numbers are the product of a power of two and Mersenne prime

Rank	Number	Discovered	Digits	Form
1	$2^{82589933} - 1$	2018-12-07	24,862,048	Mersenne
2	$2^{77232917} - 1$	2017-12-26	23,249,425	Mersenne
3	$2^{74207281} - 1$	2016-01-07	22,338,618	Mersenne
4	$2^{57885161} - 1$	2013-01-25	17,425,170	Mersenne
5	$2^{43112609} - 1$	2008-08-23	12,978,189	Mersenne
6	$2^{42643801} - 1$	2009-06-04	12,837,064	Mersenne
7	$\Phi_3(-465859^{1048576})$	2023-05-31	11,887,192	Cyclotomic polynomial
8	$2^{37156667} - 1$	2008-09-06	11,185,272	Mersenne
9	$2^{32582657} - 1$	2006-09-04	9,808,358	Mersenne
10	$10223 \times 2^{31172165} + 1$	2016-10-31	9,383,761	Proth

Lucas-Lehmer Test

Define a sequence $\{s_i\}$ for all $i \geq 0$ by

$$s_i = \begin{cases} 4 & \text{if } i = 0; \\ s_{i-1}^2 - 2 & \text{otherwise.} \end{cases} \tag{0.1}$$

M_p is prime if and only if

$$s_{p-2} \equiv 0 \mod M_p \tag{0.2}$$

Example

$M_7 = 2^7 - 1 = 127$

1. $s_0 = 4 \pmod{127}$.
2. $s_1 = (4^2 - 2) \pmod{127} = 14 \pmod{127}$
3. $s_2 = (14^2 - 2) \pmod{127} = 67 \pmod{127}$
4. $s_3 = (67^2 - 2) \pmod{127} = 42 \pmod{127}$
5. $s_4 = (42^2 - 2) \pmod{127} = 111 \pmod{127}$
6. $s_5 = (111^2 - 2) \pmod{127} = 0 \pmod{127}$

Therefore, 127 is prime.

Alternative Starting Values

- Lucas-Lehmer residue calculated with these alternative starting values will still be zero if M_p is a Mersenne prime
- The terms of the sequence will be different and if M_p is not prime then the Lucas-Lehmer residue will be different from when calculated with $s_0 = 4$
- Universal starting values, as in they are valid for all (or nearly all) p, are 4, 10, and $(2 \mod M_p)(3 \mod M_p)^{-1}$, which is usually denoted by $2/3$ for short

Miller-Rabin Test

Given an integer $n \geq 5$, this algorithm outputs either true or false. If it outputs true, then n is probably prime, and if it outputs false, then n is definitely composite.

1. Compute the unique integers m and k such that m is odd and $n - 1 = 2^k \cdot m$.
2. Choose a random integer a with $1 < a < n$.
3. Set $b = a^m \pmod{n}$. If $b \equiv \pm 1 \pmod{n}$ output true and terminate.
4. If $b^{2^r} \equiv -1 \pmod{n}$ for any r with $1 \leq r \leq k - 1$, output true and terminate. Otherwise output false.

Example

$n = 11$

1. Compute the unique integers m and k such that m is odd and $n - 1 = 2^k \cdot m$.
    1. We set $n = 11$, $k = 1$, and $m = 5$. The values for k and m are the only ones possible. $11 - 1 = 2^1 \cdot 5$
2. Choose a random integer a with $1 < a < n$.
    1. Set $a = 6$, as it falls under $1 < a < 11$.
3. Set $b = a^m \mod n$. If $b \equiv \pm 1 \mod n$ output true and terminate.
    1. $b = 6^5 \mod 11$. $b \equiv -1 \mod 11$. Therefore, 11 is probably prime and terminate the process.

Choice of Bases

- No composite number is a strong pseudoprime to all bases at the same time
- One way is to try all possible bases, which would be deterministic, but this is inefficient and the Miller test would be a better variant for this task
- Another solution is to pick a base at random as is established in the Miller-Rabin test.
  - When n is composite, most bases are witnesses
  - We can reduce the chance of a false positive by testing more base
    - If n is a pseudoprime to some base, then it seems more likely to be a pseudoprime to another base.

Acurracy

- Probability that a composite number is declared to be probably prime
- The more bases a that are tried, the better the accuracy of the test
- At most $1/4$ of the bases a are strong liars for n.
  - If n is composite, then running the Miller-Rabin test k times would result in n being declared probably prime with a probability at most 4^{-k}
- 4^{-k} is the worst case scenario, so for larger values of n, the probability for a composite number to be declared probably prime is often significantly smaller than 4^{-k}
  - For most numbers n, the probability is bounded by 8^{-k}, as the probability gets extremely impossible as we consider larger values of n
- This improved error rate should not be relied on to verify primes, as there could be a carefully chosen pseudoprime in order to defeat the primality test

AKS Test

Important because it can:

1. Verify the primality of any general number given
2. Have the maximum running time be bounded by a polynomial over the number of digits in the target number
3. Deterministically distinguish whether the number is prime or composite
4. Not conditional on any subsidiary unproven hypothesis

AKS Test (Basic Idea)

Suppose n is a natural number, and a an integer coprime to n. The number n is prime if and only if the relation

$$(x+a)^n = x^n + a \quad in \ (\mathbb{Z}/n\mathbb{Z})[x] \tag{0.3}$$

holds

Basic Idea (Continued)

Suppose that $n = p$ is a prime. Observe that $\binom{p}{i} = p!/(i!(p-i)!)$ is a multiple of p for all $1 \leq i \leq p-1$. Therefore, using the binomial theorem, in $(\mathbb{Z}/p\mathbb{Z})[x]$, we have

$$(x+a)^p = x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^{p-i} a^i + a^p = x^p + a^p = x^p + a \quad (0.4)$$

where the last relation holds because $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$ by Fermat.

If n is not prime, then there is some $1 \leq i \leq n-1$ with $\binom{n}{i}$ not being a multiple of n. Therefore in this case the binomial theorem shows that the coefficients of x^{n-1} (or x^i) on both sides of the identity of the lemma do not match mod n.

AKS Test Algorithm

1. Check that n is not a perfect power
2. Check that n has no prime factor smaller than $100(\log n)^5$
3. Find the smallest integer r such that the order of $n \mod r$ is $\geq 9(\log n)^2$
4. Check the key identity:

$$(x+a)^n \equiv x^n + a \mod (n, x^r - 1) \tag{0.5}$$

for various values of $a \in \mathbb{Z}$. But it is enough to check for all $1 \leq a \leq r \leq 100(\log n)^5$

Example

$n = 3, a = 1$
$(x-1)^3 - (x^3 - 1) = (x^3 - 3x^2 + 3x - 1) - (x^3 - 1) = -3x^2 + 3x$
All the coefficients are divisible by 3, so 3 is prime.

Conclusion

- Lucas-Lehmer Test - Mersenne Numbers
- Miller-Rabin Test - Probalistic test
- AKS Test - Deterministic test for all numbers

Thanks for listening