# Primality Tests

## Reading

Sections 12.1, 12.2, 12.3, 12.7

## Practice Problems

**12.1** 3, 4, 7, 13
**Challenge 12.1** (optional) 14, 17, 18
**12.3** 1-5, 8, 9
**12.7** 1, 2

## Notes

### Fermat's Test

In these sections we explore a number of results related to primality and compositeness testing, starting with Fermat's test for compositeness.

> **Fermat's Test for Compositeness**
>
> Suppose there is a $\bar{a} \in \mathbb{Z}_n$ such that:
>
> $$a^{n-1} \neq 1 \bmod n$$
>
> Then $n$ must be a composite number. We call $a$ a *Fermat witness* for the compositeness of $n$.

This is a good start for a strategy for determining if a number is composite or not. If a number $n$ was prime, then raising anything to the $n-1$ would always result in $1$. So we can try computing some $a^{n-1}$ and seeing if any of them is not equal to $1$.

This raises an important question though, namely whether it is possible for a composite number to always produce a $1$ when we compute $a^{n-1}$. In fact it is possible. These numbers have a name:

> A composite number $n$ is called a **Carmichael Number** if for every integer $a$ with $\gcd(a, n) = 1$ we have:
>
> $$a^{n-1} = 1 \bmod n$$
>
> Carmichael numbers tend to "fool" Fermat's test. You cannot use the test to show a number is composite.

Carmichael numbers are relatively rare occurences. The smallest Carmichael number is $561$. Until recently we did not even know if there were infinitely many Carmichael numbers. This was settled positively in 1994.

> The composite number $n$ is a Carmichael number if and only if:
>
> 1. For every prime $p$ dividing $n$ we also have that $p-1$ divides $n-1$.
> 2. $n$ is the product of distict primes (i.e. square-free).

As you can tell, determining if a number is a Carmichael number is easy. Finding one that is however is considerably harder.

We will not prove this very interesting result, but the book devotes two sections on it.

### Miller-Rabin Test

The Miller-Rabin test is an improvement on Fermat's test:

> **Miller-Rabin Test for Compositeness**
>
> Suppose $n \in \mathbb{N}$, $n-1 = 2^k q$ where $q$ is odd. Let $a$ be an integer in the range $1, 2, \dots, n-1$, and consider the congruences:
>
> $$a^q = 1 \bmod n$$
> $$a^q = -1 \bmod n$$
> $$a^{2q} = -1 \bmod n$$
> $$a^{4q} = -1 \bmod n$$
>
> and so on till
>
> $$a^{2^{k-1}q} = -1 \bmod n$$
>
> If none of these congruences holds, then $n$ is composite. $a$ is then called a *Miller-Rabin witness.*

We will now prove this result.

- We will instead show the contrapositive: If $n$ is a prime, then one of those congruences must hold.
- To see that, consider $a^{n-1} - 1$.
- By difference of squares formula: $a^{n-1} - 1 = a^{2^k q} - 1 = (a^{2^{k-1}q} + 1)(a^{2^{k-1}q} - 1)$.
- Repeating it we get:

$$a^{n-1} - 1 = a^{2^k q} - 1 = (a^{2^{k-1}q} + 1)(a^{2^{k-1}q} - 1) = (a^{2^{k-1}q} + 1)(a^{2^{k-2}q} + 1) \cdots (a^q + 1)(a^q - 1)$$

- Since the left-hand-side is equal to $0$ for a prime, the right-hand-side must also. And since $n$ is prime it must mean that one of the factors in the right-hand-side must equal $0$. This is exactly what the test calls for.

Let us demonstrate the use of the Miller-Rabin test for the Carmichael number $561 = 3 \cdot 11 \cdot 17$. Then $561 - 1 = 560 = 2 \cdot 280 = 2^2 \cdot 70 = 2^3 \cdot 5$. So $k = 3$ and $q = 35$.

So according to the test we need to:

- Compute $a^q = 2^{35}$ and compare it to $\pm 1$.
- Compute $a^{2q}$ and compare it to $-1$.
- Compute $a^{4q}$ and compare it to $-1$.

We have $2^{35} = 2^{32}2^3 = 103 \cdot 8 = 824 = 263 \bmod 561$ which is not equal to $\pm 1$.

Next up we need to compute $(a^q)^2 = 263^2 = 166$ which is not equal to $-1$ either.

Next we need $a^{4q} = (a^{2q})^2 = 166^2 = 67$ which is also not equal to $-1$.

Since none of the 4 congruences is true, we conclude that $561$ is a composite.

A question still remains, how many different numbers $a$ we would have to try. A useful theorem in that regard is the following:

> Suppose $n$ is odd and composite. Then the number of Miller-Rabin witnesses for $n$ is at least $\frac{3}{4}(n - 1)$.

In other words, if $n$ is indeed composite and we pick an $a$ at random, we have a $\frac{3}{4}$ chance that this $a$ will be a witness. Three quarters of all the $a$'s we could pick are witnesses for the Miller-Rabin test.

This provides us an excellent practical test for primality:

> **Miller-Rabin Probabilistic Primality Test**
>
> Let $n$ be an odd number, and run the Miller-Rabin test many times, say $100$, with randomly selected inputs $a$ in the range $1, 2, \ldots, n - 1$.
>
> 1. If any of those values is a Miller-Rabin witness to the compositeness of $n$, then $n$ is in fact definitely composite.
> 2. If all those values are not Miller-Rabin witnesses, then $n$ is prime with very high probability.

### The AKS test for primality

In 2002 a wonderful event occured. Manindra Agrawal, Neeraj Kayal and Nitin Saxena devised an algorithm that can run efficiently and can deterministically prove that a number is prime. Kayal and Saxena were undergraduates at the time.

The AKS test is based on the following theorem:

> Let $a$ be such that $\gcd(a, n) = 1$. Then $n$ is prime if and only if:
>
> $$(x + \bar{a})^n = x^n + \bar{a}$$
>
> As polynomials over $\mathbb{Z}_n$.

Let us discuss the proof of this theorem:

- First, assume $n = p$ is prime.
  - By the binomial theorem, we have:

    $$(x + \bar{a})^p = \sum_{k=0}^{p} \binom{p}{k} x^k \bar{a}^{n-k}$$

    where we have used the binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$.
  - When $0 < k < p$ this binomial coefficient has to be a multiple of $p$, as none of the denominator terms can cancel it out.
  - So all the terms of the polynomial other than the first and last must be equal to $0$.
  - All that is left is to compare the constant terms, $\bar{a}^p$ and $\bar{a}$. Fermat's theorem guarantees that those two are indeed equal.
- Conversely, if the two polynomials are equal to each other then that means that all the intermediate coefficients must vanish, so $\frac{n!}{k!(n-k)!} = 0 \bmod n$ for all $0 < k < n$. We show that this would mean $n$ must be prime.
  - Suppose $n$ was composite, so that there is some prime $q$ that divides $n$. Then we consider $\binom{n}{q} = \frac{n!}{q!(n-q)!}$.
  - We can write this as:

    $$\frac{n(n-1)(n-2)\cdots(n-q+1)}{q(q-1)(q-2)\cdots 1}$$
  - If this is to be equal to $0$ modulo $n$, then it must be the case that $n$ divides it.
  - But that means that the quantity $\frac{(n-1)(n-2)\cdots(n-q+1)}{q(q-1)(q-2)\cdots 1}$ must be an integer, i.e. that $q$ must divide the numerator.
  - Since $q$ divides $n$, it cannot divide any of those factors in the numerator (they are not equal to $0$ modulo $q$).
  - So we get a contradiction. Therefore $n$ must be prime.

While this proves our theorem, it does not yet provide an efficient way to determine if a number is prime, as the number of coefficients that need to be examined are numerous.

What AKS were able to do is show that in fact you don't need to compute the polynomial $(x + \bar{a})^n$ itself, but rather its reduction modulo $x^r - 1$ for an appropriately chosen relatively small $r$.

> The remainder of the polynomial division of $(x+\bar{a})^n$ by $x^r-1$ can be computed in reasonable time based on $r$ and $\log_2(n)$.
>
> The method is essentially that of fast exponentiation.

As an example, consider $n = 43$, which is a prime. And suppose for now that $r = 3$ and $\bar{a} = 2$. Then we would be looking for:

$$(x+2)^{43} = \left(a_1x^2 + a_2x + a_3\right) \bmod (x^3-1, 43)$$

We can do this by fast exponentiation. For example:

$$\begin{gathered}
(x+2)^2 = x^2 + 4x + 4 \\
(x+2)^4 = (x^2+4x+4)^2 = 24x^2 + 33x + 24 \bmod (x^3-1, 43) \\
(x+2)^8 = (24x^2+33x+24)^2 = 5x^2 + 10x + 10 \bmod (x^3-1, 43) \\
(x+2)^{16} = (5x^2+10x+10)^2 = 28x^2 + 10x + 28 \bmod (x^3-1, 43) \\
(x+2)^{32} = (28x^2+10x+28)^2 = 34x^2 + 11x + 11 \bmod (x^3-1, 43) \\
(x+2)^{11} = (x+2)^8(x+2)^2(x+2) = (27x^2+42x+27)(x+2) = 10x^2 + 25x + 38 \bmod (x^3-1, 43) \\
(x+2)^{43} = (x+2)^{32}(x+2)^{11} = x + 2 \bmod (x^3-1, 43)
\end{gathered}$$

And of course computing $x^{43} + 2$ is even simpler, since modulo the polynomial $x^3 - 1$ we can treat every third power of $x$ as a $1$, therefore $x^{43} = x \bmod (x^3-1, 43)$.

So in this case we observe that we get the same resulting polynomial from both computations.

We can now describe the AKS algorithm, but first the main theorem:

> **AKS Theorem**
>
> Let $n > 1$ be a natural number. Suppose $r$ be such that:
>
> - $ord_r(n) > (\log_2(n))^2$,
> - $n$ is not a perfect power
> - $n$ has no prime factor less than or equal to $r$.
>
> Then $n$ is prime if and only if
>
> $$(x+a)^n = x^n + a \bmod (x^r-1, n)$$
>
> for all $a \leq \sqrt{r}\log_2(n)$.

We can turn this theorem into an algorithm:

> **AKS Algorithm for Primality**

1. Determine if $n$ is a perfect power. If so then $n$ is composite. End.
2. Determine a number $r$ such that $ord_r(n) > (\log_2(n))^2$.
3. Check whether $a$ has a prime factor $\leq r$. If so, $n$ composite. End.
4. Check $(x + a)^n = x^n + a \bmod (x^r - 1, n)$ for all $a \leq \sqrt{r}\log_2(n)$. If it holds for all those numbers, $n$ is prime. Otherwise $n$ is composite. End.

Let us see how all these can be done fast.

1. If $n = a^b$ with $a \geq 2$, then we must have that $b \leq \log_2(n)$. All we have to do then is compute the $b$-th root of $n$ for each $b = 2, \ldots, \log_2(n)$ and see if any of them is an integer. That is relatively easy and fast to do.
2. This part is complicated, but it turns out that such an $r$ can be found of size approximately $\log_2(n)^3$, which is very small compared to $n$.
3. For this part we just need to do one division for each number up to $r$. There are not all that many of those.
4. Again there are not all that many numbers to test, and testing each of them does not take all that much time, as we discussed earlier.