Primality Proofs

Geoffrey Exoo
Department of Mathematics and Computer Science
Indiana State University
Terre Haute, IN 47809
ge@cs.indstate.edu

July 30, 2013

Abstract

There is an web site [1] that lists the 5000 largest integers that are provably (as opposed to probably) prime. Each of these primes has a special form, in that each is very close to a large power of small integer, and this special form is essential to the proof of primality. The best known examples are the Mersenne primes, which have the form $2^n - 1$, and in fact the ten largest known primes are all Mersenne primes. For integers that cannot be expressed in one of these special forms, proving primality is much more difficult. In this note, we outline some basic methods that can be used to prove primality when no special form is assumed.

1 Introduction

We present a series of four related methods for proving that an integer n is prime. Each method works by factoring $n - 1$ into smaller known primes. The four methods are distinguished by the extent to which one is able to factor $n - 1$. The four methods are designed for the following situations.

Method 1: used if $n - 1$ can be completely factored into small primes,

Method 2: used if $n - 1$ can be completely factored into small primes and probable primes,

Method 3: used if $n - 1$ can be factored into two factors, AB such that the prime factorization of A is known and $A \geq B$, and

Method 4: used if $n - 1$ can be factored into two factors, AB such that the prime factorization of A is known and $A^2 \geq B > A$.

Before we begin detailing the methods, some background will be necessary.

Many of the elementary methods for factoring and primality proving make use of a theorem of Leonhard Euler. Euler's theorem is stated in terms of his *totient* function, ϕ, which is defined as follows.

Definition 1 *Let n be a positive integer, then $\phi(n)$ is the number of integers k such that $1 \leq k < n$ and $gcd(k, n) = 1$.*

There are a number of different proofs of this theorem. Most of them require some background in Number Theory or Abstract Algebra, so no proof is given here. However, the reader is encouraged to verify the theorem for a few specific numbers.

Theorem 1 *Let n be a positive integer, and $a \not\equiv 0 \bmod n$, then $a^{\phi(n)} \equiv 1 \bmod n$.*

Note that if n is a prime, $\phi(n) = n - 1$ and in this special case the Theorem was first proved by Fermat and is known as *Fermat's Little Theorem*.

Each of the methods discussed can be used to establish the primality of a (large) integer n by reducing the issue to the primality of a set of smaller integers. The idea is that the verification of the primality of any of the smaller integers can be done easily. So we need some guidelines as to what constitutes a small integer.

There are $78,498$ primes less than one million (10^6), so using a list of such primes one can quickly check whether or not an integer less than one trillion (10^{12}) is prime. If one were a little more ambitious, once could maintain a list of the $664,579$ primes less than 10^7 and use it to check the primality of integers less than 10^{14}.

2 The Basic Method: Lucas' Theorem

The method is based on the following theorem, due to Édouard Lucas (who also invented the *Towers of Hanoi* puzzle).

Theorem 2 *If a and $n > 1$ are integers and*

$$a^{n-1} \equiv 1 \bmod n$$

but for every prime q that divides $n-1$

$$a^{(n-1)/q} \not\equiv 1 \bmod n$$

then n is prime.

To apply the theorem and prove that a given integer n is prime, there are essentially two steps. First, the prime factorization of $n-1$ is needed. Second, one must find an integer a that satisfies the congruences. In general, the first will be considerably more difficult than the second step.

Example 0. As a simple illustration on the use of this theorem, we apply it to a trivial example. Our goal is to prove that 11 is prime. So, referring to the statement of the theorem, we have $n = 11$ and the prime factors of $n - 1 = 10$ are 2 and 5. If we can find an integer a $(1 \le a < 11)$ such that the following three statements hold, then we will have proved that 11 is prime (assuming that we know 2 and 5 to be prime).

$$a^{10} \equiv 1 \bmod 11$$
$$a^{10/2} = a^5 \not\equiv 1 \bmod 11$$
$$a^{10/5} = a^2 \not\equiv 1 \bmod 11$$

A little computation reveals that $a = 2$ works, since $a^{10} = 1024 = 1 + 93 \times 11 \equiv 1 \bmod 11$, $2^2 = 4 \not\equiv 1 \bmod 11$ and $2^5 = 32 \not\equiv 1 \bmod 11$. Therefore, 11 is prime. Let's try a more challenging example.

Example 1. Using either the program `gp` or the extended precision arithmetic package `gmp`, one can check that the following 20-digit integer is a probable prime.

$$n = 2221222211221112111122111$$

To prove that this integer is prime using Lucas' theorem, we need to factor $n-1$. This example is small enough that one can find the prime factorization by trial division.

$$n - 1 = 2 \times 3^2 \times 5 \times 7 \times 11 \times 13 \times 37 \times 101 \times 271 \times 601 \times 967 \times 4231 \times 9901$$

In this case, we were lucky [1] since all of the prime factors of $n-1$ are relatively small.

To prove the primality of n, we need to find a value of a that meets the conditions of the theorem. It turns out that $a = 12$ is the smallest value that will work. Using an extended precision calculator (very carefully) one can verify the following congruence.

$$12^{2221222211221112111122110} \equiv 1 \bmod 2221222211221112111122111$$

Then for each prime factor q in the prime factorization of $n-1$ given above, one checks that $12^{(n-1)/q} \not\equiv 1 \bmod n$. The results of these computations are given in the following table.

[1] It took nearly 10,000 attempts to get this lucky.

q	2
$(n-1)/q$	1110611105610556055561055
$12^{(n-1)/q} \bmod n$	2221222211221112111122110
q	3
$(n-1)/q$	740407403740370703707370
$12^{(n-1)/q} \bmod n$	2182949738321903361431311
q	5
$(n-1)/q$	444244442244222422224422
$12^{(n-1)/q} \bmod n$	1961365065792481737175891
q	7
$(n-1)/q$	317317458745873158731730
$12^{(n-1)/q} \bmod n$	216088418235841707706948
q	11
$(n-1)/q$	201929291929192010102010
$12^{(n-1)/q} \bmod n$	1149404640467046734510464
q	13
$(n-1)/q$	170863247017008623932470
$12^{(n-1)/q} \bmod n$	1431748596055399543313771
q	37
$(n-1)/q$	60033032735705732733030
$12^{(n-1)/q} \bmod n$	2094226622050481435799357
q	101
$(n-1)/q$	21992299121001110011110
$12^{(n-1)/q} \bmod n$	1220581396132231768209210
q	271
$(n-1)/q$	8196391923325136941410
$12^{(n-1)/q} \bmod n$	1964432231292546731390102
q	601
$(n-1)/q$	3695877223329637456110
$12^{(n-1)/q} \bmod n$	370367282447852485652624
q	967
$(n-1)/q$	2297024003331036309330
$12^{(n-1)/q} \bmod n$	1688005164805213242843917
q	4231
$(n-1)/q$	524987523332808345810
$12^{(n-1)/q} \bmod n$	1066399149682614490143275
q	9901
$(n-1)/q$	224343218990113333110
$12^{(n-1)/q} \bmod n$	384146268175804518291995

3 Recursive Application of the Basic Method

In the examples above, we were able to find a complete factorization of $n-1$. This is not usually quite so easy. After factoring out the small prime factors, we might be left with a large factor whose primality is uncertain. In this case, one can apply the method recursively to the remaining factor. After the primality of the factor is established, one can complete the proof of the primality of the original integer.

Example 2. Let's prove that the 40-digit integer

$$n = 21122212111122111211112212121122221222111$$

is prime. A search through small primes gives the following, perhaps incomplete, factorization.

$$n - 1 = 2 \times 5 \times 285355717 \times 740206375859016387294673378183$$

This leaves us with a new problem - an uncertainly about the primality of the last factor. However, leaving that aside for the moment, we find that using $a = 37$ is the smallest value that satisfies the conditions of the theorem.

q	2
$(n-1)/q$	1056110605556105560556106060561110611055
$37^{(n-1)/q} \bmod n$	2112221211112211121111221212112222122110
q	5
$(n-1)/q$	422444242222244222422224424242224444244422
$37^{(n-1)/q} \bmod n$	1209999676948245787739440995657254072740
q	285355717
$(n-1)/q$	7402063758590163872946733781830
$37^{(n-1)/q} \bmod n$	1245810415581446524363882348882550750038
q	740206375859016387294673378183
$(n-1)/q$	2853557170
$37^{(n-1)/q} \bmod n$	868884182377049806585573408165439359793

It remains to prove that the final factor is prime. Verifying this requires another application of the method. We need to prove that

$$n_2 = 740206375859016387294673378183$$

is prime. We find that $n_2 - 1$ factors as follows.

$$n_2 - 1 = 2 \times 3 \times 7 \times 10613 \times 13577 \times 2645479 \times 6234737 \times 7415477$$

Since (by our working definition) these are all small primes, we need only find a value of a that meets the requirement of the theorem. It happens that $a = 13$ is the smallest value that works, since

$$13^{n_2-1} \equiv 1 \bmod n_2$$

and no smaller power of 13 is congruent to one modulo n_2. The other details are given in the table below.

q	2
$(n-1)/q$	370103187929508193647336689091
$13^{(n-1)/q} \bmod n$	740206375859016387294673378182
q	3
$(n-1)/q$	246735458619672129098224459394
$13^{(n-1)/q} \bmod n$	155252787556456678999909851854
q	7
$(n-1)/q$	105743767979859483899239054026
$13^{(n-1)/q} \bmod n$	283075596468830260344585016817
q	10613
$(n-1)/q$	69745253543674398124439214
$13^{(n-1)/q} \bmod n$	37411016732304939115468925392
q	13577
$(n-1)/q$	54519140889667554488817366
$13^{(n-1)/q} \bmod n$	2352151787472608168741011521
q	2645479
$(n-1)/q$	279800510931674901707658
$13^{(n-1)/q} \bmod n$	7117520496080548503983024733
q	6234737
$(n-1)/q$	118722951081820514208486
$13^{(n-1)/q} \bmod n$	300489223308558754989268633781
q	7415477
$(n-1)/q$	99819118292594850917166
$13^{(n-1)/q} \bmod n$	211673824333939603919414981909

This shows that n_2 is prime, which in turn implies that all the factors given for the original n are prime, thereby completing the proof that n itself is prime.

4 A More Powerful Method: Pocklington's Theorem

Recursive application of the basic method is not always enough. It might happen that we are left with a large factor that is not prime, as verified by a compositeness test such as Miller-Rabin, but which we are unable to factor. The next two methods enable us to prove primality with only a partial factorization of $n - 1$.

Theorem 3 *Let a and $n > 1$ be integers. Suppose that $n-1 = A \times B$, such that $A \geq B$ and that the prime factorization of A is known. If $a^{n-1} \equiv 1 \bmod n$ and $gcd(a^{(n-1)/q} - 1, n) = 1$ for each prime factor q of A, then n is prime.*

Example 3. This method will be used to prove that the 60-digit integer

$$n = 112221212122221122121112121221212221212122121122122111211121$$

is prime. First we find that $n-1$ factors as follows.

$$n - 1 = 2 \times 3 \times 5 \times 163243 \times 5614681 \times 6814061 \times 353973481 \times n_0$$

where

$$n_0 = 783363895481958941836183117 3$$

and just to illustrate the method, let us suppose that we are unable to determine whether or not n_0 is prime (actually you should be able to make this determination). Since $n_0^2 < n$, we can apply the theorem, and find that when $a = 7$

$$gcd(7^{(n-1)/q} - 1, n) = 1$$

for each of the first seven prime divisors of n. The table below gives the values needed to verify the proof.

q	2
$(n-1)/q$	56110606061111056106055606061060611060606106056106105560556 0
$7^{(n-1)/q} - 1 \bmod n$	112221212122221122121112121221212221212122121122122111211120
q	3
$(n-1)/q$	374070707074070407070373737404040737373740403740407037370 40
$7^{(n-1)/q} - 1 \bmod n$	904572726011627962682864807767611923159172151362228523623 52
q	5
$(n-1)/q$	224442424244442244242224242442424442424244424224424422242224
$7^{(n-1)/q} - 1 \bmod n$	758805088301236510607160130696478276845377153902618945883 28
q	163243
$(n-1)/q$	687448846947318550388758606624554934742207145924309840
$7^{(n-1)/q} - 1 \bmod n$	803626155967726391465562017740413842789732016856641358876 30
q	5614681
$(n-1)/q$	19987103830515237129431239498951449104966447982017520
$7^{(n-1)/q} - 1 \bmod n$	1069785952343576016491289412114218446874080252629395756346 20
q	6814061
$(n-1)/q$	16469064794433322818963921987374668529107990245775920
$7^{(n-1)/q} - 1 \bmod n$	820614243941513967618792001597058395829781719844105689665 17
q	353973481
$(n-1)/q$	317032823490585505531450027526814137842495949921520
$7^{(n-1)/q} - 1 \bmod n$	120010773335984533709520445174489529465766139956086128537 27

5 An Even More Powerful Method: Brillhart, Lehmer and Selfridge

As the integers under consideration become larger, factoring $n-1$ becomes more difficult. Our final method requires that the portion of $n-1$ that can be factored into primes is at least as great as the cube root of n.

Theorem 4 *Let n be an integer, where $n-1 = A \times B$ and where the complete factorization of A is known, and satisfy the inequality $n^{1/3} \leq A < n^{1/2}$. Let a be an integer such that $a^{n-1} \equiv 1 \bmod n$ and suppose for each prime factor q of A we have $gcd(a^{(n-1)/q} - 1, n) = 1$. Let $c_2 A^2 + c_1 A + 1$ be the base A represenation of n. Then n is prime if and only if $c_1^2 - 4c_2$ is not a square.*

Example 4. We apply this theorem to prove that the 80-digit integer

$$21211212112211112112212211111212212211221221211212222112111222212212121211112211$$

is prime. A little effort reveals the following factorization of $n-1$.

$$n - 1 = 2 \times 3 \times 5 \times 649981 \times 60178589057 \times 1036760601625393 \times n_0$$

where

$$n_0 = 581168182413917485045400796216336922986370 6849.$$

The product of all factors of $n-1$, except for n_0, is

$$A = \frac{n-1}{n_0} = 36497545381973681273169361157742 90$$

and so

$$A^2 = 1332070818909228388070205288328721092665454204559175415456622500 4100.$$

Since $A^2 > n_0$, we have $A > n^{1/3}$, and one can check that $A < n^{1/2}$. So the requirements of the theorem are met. Using a value of $a = 3$, we find that the condition

$$a^{n-1} \equiv 1 \bmod n$$

and the condition

$$a^{(n-1)/q} \not\equiv 1 \bmod n$$

are satisfied for $q \in \{2, 3, 5, 649981, 60178589057, 1036760601625393\}$. The verification of these conditions, and the verification that 1036760601625393 is prime, are left as exercises. It remains to show that the final condition of the theorem is satisfied. In the base A representation of n we find that

$$c_2 = 1592348680799$$

and

$$c_1 = 4322574271156628396194139228491 39.$$

The reader should check that

$$n = c_2 A^2 + c_1 A + 1$$

and that

$$c_1^2 - 4c_2 = 18684648329665257192018093554631693366009637871060111497795831 8125$$

and is not a square, completing the proof that n is prime.

References

[1] The List of Largest Known Primes Home Page, `http://primes.utm.edu/primes/`.