Search for Primes

Karim El Shenawy

March 2021

Introduction

This course notebook is the collection of theorem proofs, exercises and answers from Unit 10 of the Number Theory Through Inquiry (Mathematical Association of America Textbooks).

Theorems from Search for Primes

10.1 Exercise

If n is a d-digit number, explain why the trial division primality test requires roughly $10^{\frac{d}{2}}$ *trials.*

Solution. By the trial division primality test a number n is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divide n. The proof is the following

Proof. Suppose natural number p has no prime divisor less than or equal to $\sqrt{p}$. This implies that p is prime. Now, by contradiction, let's assume that p is composite and each prime divisor p_i of p satisfies $p_i > \sqrt{p}, i \in \mathbf{Z}$. Thus, by the Fundamental Theorem of Arithmetic, $p = p_1 p_2 ... p_k, \exists k \in \mathbf{Z}$. However,

$$p = p_1 p_2 ... p_k > \sqrt{p}\sqrt{p} p_3 ... p_k = p p_3 ... p_k \geq p.$$

This shows that $p > p$ which is an obvious contraction. Thus, p must be prime.

Conversely, suppose p is prime. Then the only divisor of p is itself which implies that $p > \sqrt{p}$ since $p > 1$. Thus, p has no prime divisor less than or equal to $\sqrt{p}$. □

Now back to the question, to test the primality of n, we would need to perform trial divisions by primes that are less or equal to $\sqrt{n}$ if any one of these primes divide n, n is composite. Otherwise, n is prime.

Suppose n has d-digits. Then $n < 10^d$. By Prime Number Theorem,

$$\begin{aligned}
\pi(\sqrt{n}) &\approx \frac{\sqrt{n}}{\ln\sqrt{n}} \\
\pi(\sqrt{n}) &< \frac{c\cdot\sqrt{n}}{\ln\sqrt{n}} && (c = \text{ constant}) \\
&< \sqrt{n} && \text{where n is large} \\
n &< 10^d && \text{n has d-digits} \\
\sqrt{n} &< 10^{\frac{d}{2}}
\end{aligned}$$

Therefore, the trial division primality test requires roughly $10^{\frac{d}{2}}$ trials.

10.2 Exercise

If n is a d-digit number, explain why the Wilson's Theorem primality test requires roughly 10^d *multiplications.*

Solution. By Wilson's Theorem, an natural number n, $n > 1$ is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$. Therefore, to test the primality of a natural number n as a d-digit number, we would have to compute $(n-1)!$ which is $n-1$ number multiplications computed. We know that $n < 10^d$. Thus, the number of multiplications will be roughly 10^d.

10.3 Question

Suppose that Algorithm A requires d^2 *steps and Algorithm B requires* 2^d *steps, where d is the number of digits in the number to be tested. Suppose our computer can carry out one million steps per second. How long would it take for our computer to carry out each algorithm when the number to be tested has 200 digits?*

Solution.

- Algorithm A requires d^2. Then $d = 200 \Longrightarrow 200^2 = 40000$ steps.
- Algorithm B requires 2^d. Then $d = 200 \Longrightarrow 2^200 = 1,6069 \times 10^{60}$ steps.

If our computer carries $1 \times 10^6 steps/second$. Then Algorithm A will take less time on our computer.

- Algorithm A takes $\Longrightarrow \frac{40000}{1\times10^6}$ seconds.
- Algorithm B takes $\Longrightarrow \frac{1,6069\times10^{60}}{1\times10^6}$ seconds.

10.4 Exercise

Show that the algorithm described in Question 3.6 for computing $a^r \pmod{n}$ *is a polynomial time algorithm in the number of digits in r.*

Solution. Let a, n, r and k be natural numbers where k is $0 \leq k \leq n-1$, then we can proceed with the following;

$$\begin{aligned} k_1 &\equiv a^2 \pmod{n} && 0 \leq k_1 \leq n-1 \\ k_1 \cdot a &\equiv a^3 \pmod{n} && \\ k_2 &\equiv a^3 \pmod{n} && \text{Where } k_2 = k_1 * a \text{ and } 0 \leq k_2 \leq n-1 \\ k_3 &\equiv a^4 \pmod{n} && \text{Where } k_3 = k_2 * a \text{ and } 0 \leq k_3 \leq n-1 \\ &... && \\ k_r \times a &\equiv a^{r+2} \pmod{n} && \text{Where } k_r = k_{r-1} * a \text{ and } 0 \leq k_r \leq n-1 \\ k_{r-1} &\equiv a^r \pmod{n} && \end{aligned}$$

Thus, you never multiply numbers larger than n. We compute $k_r \times a \equiv a^{r+2} \pmod{n}$ and we recompute the new k with a until a^r. Thus, this is a polynomial time algorithm in the number of digits in r.

10.5 Exercise

State the contrapositive of Fermat's Little Theorem.

Solution. The contrapositive of Fermat's Little Theorem is
If there exists a natural number n and some number a for which $a^n - a$ is not divisible by n. Then n is not a prime number.

10.6 Exercise

Use Fermat's Little Theorem to show that $n = 737$ is composite.

Solution. Let $n = 737$, then we need to find an integer a such that $a^{737} \equiv$ or $\not\equiv a \pmod{737}$. Let's try $a = 2$,

$$\frac{a^{737} - a}{737} = \frac{2^{737} - 2}{737}$$

Thus, there is some integer a such that $737 \nmid a^{737} - a$. Therefore, 737 is composite.

10.7 Question

State the converse to Fermat's Little Theorem. Do you think the converse to Fermat's Little Theorem is true?

Solution. The converse to Fermat's Little Theorem is as follows
If $a^n \equiv a \pmod{n}$ for all integers a, then n is prime.
The converse part of the Theorem is not true. Let's try an example. with composite number $561 = 3 \cdot 11 \cdot 17$. However, $a^{561} \equiv a \pmod{561}$ for all integers a. This is known as the Carmichael Number which is a composite number n such that $b^n \equiv b \pmod{n}$ for all integers b.

10.8 Theorem

Let n be a natural number greater than 1. Then n is prime if and only if $a^{n-1} \equiv 1 \pmod{n}$ *for all natural numbers a less than n.*

Proof. Suppose natural number n, $n > 1$, is prime. Then by Fermat's Little Theorem $a^{n-1} \equiv 1 \pmod{n}$ for all integers a, $a < n$.

Conversely, suppose n is not prime. Then by Fundamental Theorem of Arithmetics, $n = p_1 p_2 ... p_k, \exists k \in \mathbf{Z}$ and p is prime. Suppose that $n = n_1 \cdot n_2$ and $n > n_1, n_2$. Thus,

$$\begin{aligned} \implies n_1^{n-1} &\equiv 1 \pmod{n} \\ \implies n_1^{n-1} - 1 &\equiv 0 \pmod{n} \end{aligned}$$

Similarly,

$$\begin{aligned} \implies n_2^{n-1} &\equiv 1 \pmod{n} \\ \implies n_2^{n-1} - 1 &\equiv 0 \pmod{n} \end{aligned}$$

Then, by $n = n_1 \cdot n_2$,

$$\begin{aligned} n^{n-1} - 1 &\equiv 0 \pmod{n} \\ (n_1^{n-1} - 1)(n_2^{n-1} - 1) &\equiv 1 \pmod{n} \\ n_1^{n-1} n_2^{n-1} - n_1^{n-1} - n_2^{n-1} + 1 &\equiv 1 \pmod{n} \\ n^{n-1} - n_1^{n-1} - n_2^{n-1} + 1 &\equiv 1 \pmod{n} \\ 0 - 1 - 1 + 1 &\equiv 1 \pmod{n} \\ -1 &\equiv 1 \pmod{n} \end{aligned}$$

Thus, n must be a prime. □

10.9 Question

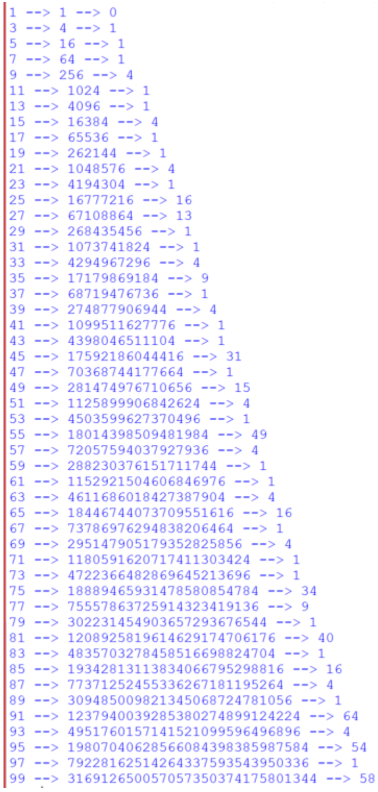
Does the previous theorem give a polynomial or exponential time primality test?

Solution. The previous theorem must be an polynomial time primality test since we are computing all possible integers a where $a < n$.

10.10 Exercise

Compute $2^{n-1} \pmod{n}$ *for all odd numbers n less than 100. If you have access to a computer, and some computing software, keep going. Test any conjecture you make along the way. State a probably prime test based on your observations.*

Solution.



```
1 --> 1 --> 0
3 --> 4 --> 1
5 --> 16 --> 1
7 --> 64 --> 1
9 --> 256 --> 4
11 --> 1024 --> 1
13 --> 4096 --> 1
15 --> 16384 --> 4
17 --> 65536 --> 1
19 --> 262144 --> 1
21 --> 1048576 --> 4
23 --> 4194304 --> 1
25 --> 16777216 --> 16
27 --> 67108864 --> 13
29 --> 268435456 --> 1
31 --> 1073741824 --> 1
33 --> 4294967296 --> 4
35 --> 17179869184 --> 9
37 --> 68719476736 --> 1
39 --> 274877906944 --> 4
41 --> 1099511627776 --> 1
43 --> 4398046511104 --> 1
45 --> 17592186044416 --> 31
47 --> 70368744177664 --> 1
49 --> 281474976710656 --> 15
51 --> 1125899906842624 --> 4
53 --> 4503599627370496 --> 1
55 --> 18014398509481984 --> 49
57 --> 72057594037927936 --> 4
59 --> 288230376151711744 --> 1
61 --> 1152921504606846976 --> 1
63 --> 4611686018427387904 --> 4
65 --> 18446744073709551616 --> 16
67 --> 73786976294838206464 --> 1
69 --> 295147905179352825856 --> 4
71 --> 1180591620717411303424 --> 1
73 --> 4722366482869645213696 --> 1
75 --> 18889465931478580854784 --> 34
77 --> 75557863725914323419136 --> 9
79 --> 302231454903657293676544 --> 1
81 --> 1208925819614629174706176 --> 40
83 --> 4835703278458516698824704 --> 1
85 --> 19342813113834066795298816 --> 16
87 --> 77371252455336267181195264 --> 4
89 --> 309485009821345068724781056 --> 1
91 --> 1237940039285380274899124224 --> 64
93 --> 4951760157141521099596496896 --> 4
95 --> 19807040628566084398385987584 --> 54
97 --> 79228162514264337593543950336 --> 1
99 --> 316912650057057350374175801344 --> 58
```

We can observe that all prime odd values n are congruent to 1 modulo n.
Conjecture. *For all odd natural numbers n, if* $2^{n-1} \equiv 1 \pmod{n}$ *then n is prime.*

10.11 Theorem

Let a and n be relatively prime natural numbers. Then n is prime if and only if $(x+a)^n \equiv x^n + a \pmod{n}$ *for every integer x.*

Proof. Let a and n be relatively prime natural numbers and n is prime. Suppose $(x+a)^n \equiv x^n + a \pmod{n}$ for every integer x. By Fermat's Little Theorem, $a^n \equiv a \pmod{n}$. Then, by direct proof,

$$(x+a)^n = x^n + nx^{n-1}a + \frac{n(n-1)}{2!}x^{n-2}a^2 + ... + nx^1a^{n-1} + a^n$$
$$(x+a)^n \equiv (x^n + a^n) \pmod{n}$$
$$(x+a)^n \equiv (x^n + a) \pmod{n}$$

Conversely, suppose $(x+a)^n \equiv (x^n+a) \pmod{n}$ then by direct proof,

$$\begin{aligned}
(x+a)^n &= x^n + nx^{n-1}a + \frac{n(n-1)}{2!}x^{n-2}a^2 + ... + nx^1a^{n-1} + a^n \\
(x+a)^n &\equiv (x^n+a^n) \pmod{n} \\
(x+a)^n &\equiv (x^n+a) \pmod{n} \\
(x^n+a^n) &\equiv (x^n+a) \pmod{n} \\
a^n &\equiv a \pmod{n}
\end{aligned}$$

Thus, n must be prime, by Fermat's Little Theorem. □

10.12 Blank Paper Exercise

- Trial division primality test
- Wilson's primality test
- Fermat's Little Theorem and it's converse
- AKS primality test
- Pepin's test
- Proth's test
- Lucas-Lehmer test

Supplementary from Finding Prime Numbers

10.1.1 Conjecture

Let p be an odd natural number. Then, if any two of the following three conditions hold, so does the third.

a. $p = 2^k \pm 1$ *or* $p = 4^k \pm 3$

a. $2^p - 1$ *is prime*

a. $\frac{2^p+1}{3}$ *is prime*

10.1.2 Theorem

If $a_1 \equiv a_2 \pmod{n}$ *then*

$$(\tfrac{a_1}{n}) = (\tfrac{a_2}{n}).$$

Proof. By direct proof,

$$\begin{aligned} a_1 &\equiv a_2 \pmod{n} \\ a_1 \cdot \frac{1}{n} &\equiv a_2 \cdot \frac{1}{n} \pmod{n} \\ (\frac{a_1}{n}) &\equiv (\frac{a_2}{n}) \pmod{n} \end{aligned}$$

Then,

$$(\tfrac{a_1}{n}) = (\tfrac{a_2}{n}).$$

□

10.1.3 Theorem

The Jacobi symbol is multiplicative. That is

$$(\tfrac{a_1 a_2}{n}) = (\tfrac{a_1}{n})(\tfrac{a_2}{n}).$$

Proof. Suppose that $a_1 \equiv a_2 \pmod{n}$ then by direct proof,

$$\begin{aligned} (\frac{a_1 a_2}{n}) &= (\frac{a_1}{n})(\frac{a_2}{n}) \\ a_2(\frac{a_2}{n}) &= (\frac{a_2}{n})(\frac{a_2}{n}) && \text{By Theorem 10.1.2} \\ a_2 &= (\frac{a_2}{n}) \end{aligned}$$

Now, if $a_2 \pmod{n}$ is a quadratic residue then $(\frac{a_2}{n}) = 1$. Similarly, if $a_2 \pmod{n}$ is not a quadratic residue then $(\frac{a_2}{n}) = -1$. Either or, since $n \mid a$, then $(\frac{a_2}{n}) = 0$ which would suggest that $a_2 = 0$ as well. □

10.1.4 Theorem

$$(\frac{2}{n}) = \begin{cases} 1 & n = \pm 1 \pmod{8} \\ -1 & n = \pm 3 \pmod{8} \end{cases}$$

Proof. Identifying two cases:

- Case 1: $n = \pm 1 \pmod{8}$ then $2 \pmod{n}$ is a quadratic residue thus $(\frac{2}{n}) = 1$.
- Case 2: $n = \pm 3 \pmod{8}$ then $2 \pmod{n}$ is not a quadratic residue thus $(\frac{2}{n}) = -1$.

□

10.1.5 Theorem

If a and n are odd, then

$$(\frac{a}{n}) = \begin{cases} -\frac{n}{a} & a \equiv n \equiv 2 \pmod 4 \\ \frac{n}{a} & \text{otherwise} \end{cases}$$

Proof. Incomplete. □

10.1.6 Exercise

Use Theorems 10.1.2-10.1.5 to compute $\frac{122}{329}$ *and* $\frac{1240}{3003}$.
Solution

- $(\frac{122}{329})$

$$\begin{aligned}(\frac{122}{329}) &= (\frac{61 \times 2}{329}) \\ &= (\frac{61}{329})(\frac{2}{329}) \\ &= (\frac{24}{61})(1) \\ &= (\frac{-12}{61})(1) \\ &= (\frac{6}{61})(1) \\ &= (\frac{-3}{61})(1) \\ &= (-\frac{1}{3})(1) \\ &= -1(1) \\ &= -1\end{aligned}$$

- $(\frac{1240}{3003})$

$$\begin{aligned}
(\frac{1240}{3003}) &= (\frac{620\times 2}{3003}) \\
&= (\frac{620}{3003})(\frac{2}{3003}) \\
&= (\frac{310}{3003})(\frac{2}{3003})(-1) \\
&= (\frac{155}{3003})(\frac{2}{3003})(-1)(-1) \\
&= (\frac{58}{155})(-1)(-1)(-1)(-1) \\
&= (\frac{29}{155})(\frac{2}{155}) \\
&= (\frac{29}{155})(-1) \\
&= -(\frac{10}{29}) \\
&= -(\frac{5}{29})(\frac{2}{29}) \\
&= -(\frac{4}{5})(-1) \\
&= (\frac{2}{5})(\frac{2}{5})(-1) \\
&= (\frac{1}{5})(\frac{2}{5}) \\
&= (-1)(-1) \\
&= 1
\end{aligned}$$

10.1.7 Theorem

Let n be prime. Then

$$(\tfrac{a}{n}) \equiv a^{\frac{n-1}{2}} \pmod{n}.$$

Proof. Incomplete. □

10.1.8 Exercise

Make use of Theorem 10.1.7 to devise a probabilistic primality test, and state with what probability a number will be certified as prime.

Solution. If n is prime then

$$(\tfrac{a}{n}) \equiv a^{\frac{n-1}{2}} \pmod{n}.$$

Tested on a computer and gotten the result of 91% correct.

10.1.9 Lemma

Let p be prime and write $p-1 = 2^s m$ where $m \geq 1$ is odd. Then for all numbers a, $1 \leq a \leq p-1$, either $a^m \equiv 1 \pmod{p}$, or there is an r, $1 \leq r \leq s-1$ such that $a^{2^r m} \equiv -1 \pmod{p}$.

10.1.10 Exercise

State the contrapositive form of Lemma 10.1.9.

Solution. Suppose that for all numbers a, $1 \leq a \leq p-1$, either $a^m \equiv 1 \pmod{p}$, or there is an r, $1 \leq r \leq s-1$ such that $a^{2^r m} \equiv -1 \pmod{p}$. If we can write $p-1 = 2^s m$ where $m \geq 1$ is odd then p is prime.

10.1.11 Theorem

Let p be an odd natural number and let A be the set of strong liars for p. The number of elements in A is not greater than $\frac{\phi(p)}{4}$.

10.1.12 Exercise

Devise a probabilistic primality test based on Lemma 10.1.9 and use it to check if 221 is prime, using values of 174 and 137 for a.

Solution. Suppose that 221 is prime. Then by Lemma 10.1.9,

1. $p-1 = 220 = 2^s m = 2^2 \cdot 55$ where $m = 55 \geq 1$ and odd
2. Then, suppose a is 174:

$$\begin{aligned} a^m &\equiv 1 \pmod{p} \\ 174^{55} &\equiv 1 \pmod{221} \\ 47 &\not\equiv 1 \pmod{221} \end{aligned}$$

3. Then, suppose a is 137:

$$\begin{aligned} a^m &\equiv 1 \pmod{p} \\ 137^{55} &\equiv 1 \pmod{221} \\ 188 &\not\equiv 1 \pmod{221} \end{aligned}$$

Thus, 221 is not prime.