Годишник на ШУ „Епископ К. Преславски“
Факултет по математика и информатика, том XVIII С, 2017, стр. 15- 23

ON BIGGER PRIMES*

Ivo M. Michailov, Ivan S. Ivanov, Sintia A. Vladimirova, Fani M. Aleksandrova

ABSTRACT: *In this survey we discuss some classical problems about recognition of prime numbers. Various tests are studied that can be further programmed on a computer to find big primes.*

KEYWORDS: *primes, sieve of Eratosthenes*

1 Introduction

Prime numbers (or just primes) are natural numbers, like 2, 3, 5, 7, 11, . . . , which are not multiples of any smaller natural number (except 1). If a natural number is neither 1 nor a prime, it is called a composite number.

For example, among the numbers 1 through 6, the numbers 2, 3, and 5 are the prime numbers, while 1, 4, and 6 are not prime. 2 is a prime number, since the only natural numbers dividing it are 1 and 2. 3 is prime, as no numbers other than 1 and itself divide evenly into it. 4 is composite, since 2 is a number that divides evenly into it, in addition to 1 and itself. 5 is prime as only 1 and itself divide evenly into it. 6 is divisible by 2 and 3, therefore it is not prime.

No even number greater than 2 is prime because by definition, as any such even number n has at least three distinct divisors, namely 1, 2, and n. Accordingly, the term odd prime refers to any prime number greater than 2. Similarly, when written in the usual decimal system, all prime numbers larger than 5 would end in 1, 3, 7, or 9, since even numbers are multiples of 2, and numbers ending in 0 or 5 are multiples of 5.

Prime numbers are important, since the fundamental theorem in arithmetic states that every natural number greater than 1 is a product of prime numbers, and moreover, in an essentially unique way. Prime

*This work is partially supported by a project No RD-08-104/06.02.2017 of Shumen University.

numbers are like cousins, members of the same family, resembling one another, but not quite alike.

There are hints in the surviving records of the ancient Egyptians that they had some knowledge of prime numbers: the Egyptian fraction expansions in the Rhind papyrus, for instance, have quite different forms for primes and for composites. However, the earliest surviving records of the explicit study of prime numbers come from the Ancient Greeks. Euclid's Elements (circa 300 BC) contain important theorems about primes, including the infinitude of primes and the fundamental theorem of arithmetic. Euclid also showed how to construct a perfect number from a Mersenne prime. The Sieve of Eratosthenes, attributed to Eratosthenes, is a simple method to compute primes, although the large primes found today with computers are not generated this way.

It is quite natural, when studying the set of prime numbers, to ask the following questions, which we phrase informally as follows:

1. How many prime numbers are there?
2. How to recognize whether a natural number is a prime?
3. Are there functions defining prime numbers?
4. How are the prime numbers distributed?
5. Which special kinds of primes have been considered?

In this paper we will concentrate on the first two questions. For further information we refer the reader to the monograph [3].

2 How many prime numbers are there?

Firstly, let us note that any natural number $n > 1$ has a prime divisor. We can easily verify this claim using mathematical induction. Indeed, if n itself is not a prime, we can decompose it as a product of two numbers which are smaller than n, so we can apply the induction assumption on either of them. From this fact also follows the existence part of the main theorem in the arithmetic, namely every natural number $n > 1$ is a product of primes (see the beginning of the next section and for further reading [4]).

The answer to the question of how many prime numbers exist is given by the fundamental theorem:

Theorem 2.1. *There exist infinitely many prime numbers.*

There are at least 10 different proofs of the latter theorem (by Euclid, Kummer, Goldbach, Schorn, Thue, Perott, Auric, Métrod, Washington, and Furstenberg's). We shall give three of them below.

I Euclid's proof.

Suppose that $p_1 = 2 < p_2 = 3 < \cdots < p_r$ are all the primes. Let $P = p_1 p_2 \cdots p_r + 1$ and let p be a prime dividing P; then p cannot be any of $p_1, p_2, \ldots, p_r$, otherwise p would divide the difference $P - p_1 p_2 \cdots p_r = 1$, which is impossible. So this prime p is still another prime, and $p_1, p_2, ..., p_r$ would not be all the primes.

II Kummer's proof.

Suppose that there exist only finitely many primes $p_1 < p_2 < \cdots < p_r$. Let $N = p_1 p_2 \cdots p_r > 2$. The natural number $N - 1 > 1$ has a prime divisor p_i in common with N; so, p_i divides $N - (N - 1) = 1$, which is absurd!

III Furstenberg's proof.

This is an ingenious proof based on topological ideas. Since it is so short,we cannot do any better than transcribe it verbatim; it appeared in 1955:

In this note we would like to offer an elementary "topological" proof of the infinitude of the prime numbers. We introduce a topology into the space of integers S, by using the arithmetic progressions (from $-\infty$ to $+\infty$) as a basis. It is not difficult to verify that this actually yields a topological space. In fact, under this topology, S may be shown to be normal and hence metrizable. Each arithmetic progression is closed as well as open, since its complement is the union of other arithmetic progressions (having the same difference). As a result, the union of any finite number of arithmetic progressions is closed.

Consider now the set $A = \bigcup A_p$, where A_p consists of all multiples of p, and p runs through the set of primes ≥ 2. The only numbers not belonging to A are -1 and 1, and since the set $\{-1, 1\}$ is clearly not an open set, A cannot be closed. Hence A is not a finite union of closed sets which proves that there are an infinity of primes.

3 How to Recognize Whether a Natural Number is a Prime

In the article 329 of Disquisitiones Arithmeticae, Gauss (1801) wrote:

"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. . . . The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated."

The first observation concerning the problem of primality and factorization is clear: there is an algorithm for both problems. By this, we mean a procedure involving finitely many steps, which is applicable to every number N and which will indicate whether N is a prime, or, if N is composite, which are its prime factors. Namely, given the natural number N, try in succession every number $n = 2, 3, \ldots$ up to $[\sqrt{N}]$ (the largest integer not greater than $\sqrt{N}$) to see whether it divides N. If none does, then N is a prime. If, say, N_0 divides N, write $N = N_0 N_1$, so $N_1 < N$, and then repeat the same procedure with N_0 and with N_1. Eventually this gives the complete factorization into prime factors.

It should, however, be noted that for large numbers N, it may take a long time with this algorithm to decide whether N is prime or composite. This touches the most important practical aspect, the need to find an efficient algorithm - one which involves as few operations as possible, and therefore requires less time to be performed.

I The Sieve of Eratosthenes.

As we have already said, it is possible to find if N is a prime using trial division by every number n such that $n^2 \leq N$. Since multiplication is an easier operation than division, Eratosthenes (in the 3rd century BC) had the idea of organizing the computations in the form of the well-known sieve. It serves to determine all the prime numbers, as well as the factorizations of composite numbers, up to any given number N. This is illustrated now for $N = 40$.

Do as follows: write all the numbers up to 40; cross out all the multiples of 2, bigger than 2; in each subsequent step, cross out all the multiples of the smallest remaining number p, which are bigger than p.

It suffices to do it for $p^2 < 40$.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~

II Classical Primality Tests Based on Congruences.

Fermat's little theorem says that if p is a prime and a is any natural number not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$. However, we note right away that a crude converse of this theorem is not true – because there exist composite integers N, and $a \geq 2$, such that $a^{N-1} \equiv 1 \pmod{N}$.

Euler generalized Fermat's little theorem by introducing Euler's function. For every $n \geq 1$, let $\varphi(n)$ denote the number of integers $a, 1 \leq a < n$, such that $\gcd(a, n) = 1$ (the greatest common divisor of a and n is 1, or equivalently, a and n are relatively prime).

Euler proved the following:

Euler's Theorem. *If* $\gcd(a, n) = 1$, *then* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Nevertheless, a true converse of Fermat's little theorem was discovered by Lucas in 1876. It says:

Test 1. Let $N > 1$. Assume that there exists an integer $a > 1$ such that:

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $a^m \not\equiv 1 \pmod{N}$ for $m = 1, 2, \ldots, N-2$.

Then N is a prime.

Defect of this test: it might seem perfect, but it requires $N-2$ successive multiplications by a, and finding residues modulo N – too many operations.

Proof. It suffices to show that every integer $m, 1 \leq m < N$, is prime to N, that is, $\varphi(N) = N-1$. For this purpose, it suffices to show that there exists $a, 1 \leq a < N$, $\gcd(a, N) = 1$, such that the order of $a \pmod{N}$ is $N-1$. This is exactly spelled out in the hypothesis. □

In 1891, Lucas gave the following test:

Test 2. Let $N > 1$. Assume that there exists an integer $a > 1$ such that:

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $a^m \not\equiv 1 \pmod{N}$ for every $m < N$, such that m divides $N-1$.

Then N is a prime.

Defect of this test: it requires the knowledge of all factors of $N-1$, thus it is only easily applicable when $N-1$ can be factored, like $N = 2^n + 1$, or $N = 3 \times 2^n + 1$.

The proof of Test 2 is, of course, the same as that of Test 1.

In 1967, Brillhart & Selfridge [2] made Lucas' test more flexible:

Test 3. Let $N > 1$. Assume that for every prime factor q of $N-1$ there exists an integer $a = a(q) > 1$ such that

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $a^{(N-1)/q} \not\equiv 1 \pmod{N}$.

Then N is a prime.

Defect of this test: once again, it is necessary to know the prime factors of $N-1$, but fewer congruences have to be satisfied.

Proof. It is enough to show that $\varphi(N) = N-1$, and since $\varphi(N) \leq N-1$, it suffices to show that $N-1$ divides $\varphi(N)$. If this is false, there exists a prime q and $r \geq 1$ such that q^r divides $N-1$, but q^r does not divide $\varphi(N)$. Let $a = a(q)$ and let e be the order of a mod N. Thus e divides $N-1$ and e does not divide $(N-1)/q$, so q^r divides e. Since $a^{\varphi(N)} \equiv 1 \pmod{N}$, then e divides $\varphi(N)$, so $q^r | \varphi(N)$, which is a contradiction, and concludes the proof. □

To make the primality tests more efficient, it is desirable to avoid the need to find all prime factors of $N-1$. So there are tests that only require a partial factorization of $N-1$. The basic result was proved by Pocklington in 1914, and it is indeed very simple:

Theorem 3.1. *Let $N-1 = q^n R$, where q is a prime, $n \geq 1$, and q does not divide R. Assume that there exists an integer $a > 1$ such that:*

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $gcd(a^{(N-1)/q} - 1, N) = 1$.

Then each prime factor of N *is of the form* $mq^n + 1$, *with* $m \geq 1$.

Proof. Let p be a prime factor of N, and let e be the order of a mod p, so e divides $p-1$; by condition (ii), e cannot divide $(N-1)/q$, because p divides N; hence, q does not divide $(N-1)/e$; so q^n divides e, and a fortiori, q^n divides $p-1$. □

The above statement looks more like a result on factors than a primality test. However, if it may be verified that each prime factor $p = mq^n + 1$ is greater than $\sqrt{N}$, then N is a prime. When q^n is fairly large, this verification is not too time consuming.

Pocklington gave also the following refinement of his result above:

Theorem 3.2. *Let* $N - 1 = FR$, *where* $gcd(F, R) = 1$ *and the factorization of* F *is known. Assume that for every prime* q *dividing* F *there exists an integer* $a = a(q) > 1$ *such that:*

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $gcd(a^{(N-1)/q} - 1, N) = 1$.

Then each prime factor of N *is of the form* $mF + 1$, *with* $m \geq 1$.

The same comments apply here. So, if $F > \sqrt{N}$, then N is a prime. This result is very useful to prove the primality of numbers of certain special form. The old criterion of Proth (1878) is easily deduced:

Test 4. Let $N = 2^n h + 1$ with h odd and $2^n > h$. Assume that there exists an integer $a > 1$ such that $a^{(N-1)/2} \equiv -1 \pmod{N}$. Then N is prime.

Proof. $N - 1 = 2^n h$, with h odd and $a^{N-1} \equiv 1 \pmod{N}$. Since N is odd, then $\gcd(a^{(N-1)/2} - 1, N) = 1$. By the above result, each prime factor p of N is of the form $p = 2^n m + 1 > 2^n$. But $N = 2^n h + 1 < 2^{2n}$, hence $\sqrt{N} < 2^n < p$ and so N is prime. □

In the following test (using the same notation) it is required to know that R (the nonfactored part of $N-1$) has no prime factor less than a given bound B. Precisely:

Test 5. Let $N-1=FR$, where $\gcd(F,R)=1$, the factorization of F is known, B is such that $FB>\sqrt{N}$, and R has no prime factors less than B. Assume:

(i) For each prime q dividing F there exists an integer $a=a(q)>1$ such that $a^{N-1}\equiv 1 \pmod N$ and $\gcd(a^{(N-1)/q}-1,N)=1$.

(ii) There exists an integer $b>1$ such that $b^{N-1}\equiv 1 \pmod N$ and $\gcd(b^F-1,N)=1$.

Then N is a prime.

Proof. Let p be any prime factor of N, let e be the order of b modulo N, so e divides $p-1$ and also e divides $N-1=FR$. Since e does not divide F, then $\gcd(e,R)\neq 1$, so there exists a prime q such that $q|e$ and $q|R$; hence, $q|p-1$. However, by the previous result of Pocklington, F divides $p-1$; since $\gcd(F,R)=1$, then qF divides $p-1$. So $p-1\geq qF\geq BF>\sqrt{N}$. This implies that $p=N$, so N is a prime. □

The paper of Brillhart, Lehmer & Selfridge [1] contains other variants of these tests, which have been put to good use to determine the primality of numbers of the form $2^r+1, 2^{2r}\pm 2^r+1, 2^{2r-1}\pm 2^r+1$.

We have already said enough and will make only one further comment: these tests require prime factors of $N-1$.

REFERENCES:

1. Brillhart, J., Lehmer, D.H. & Selfridge, J.L. New primality criteria and factorizations of $2^m\pm 1$. *Math. Comp.* **29** (1975), 620–647.

2. Brillhart, J. & Selfridge, J.L. Some factorizations of $2^n\pm 1$ and related results. *Math. Comp.* **21** (1967), 87–96 and p. 751.

3. Paulo Ribenboim, "The Little Book of Bigger Primes", Second Edition, Springer-Verlag, New York, 2004.

4. Н. Зяпков, Н. Янков, И. Михайлов, „Елементарна теория на числата“, Фабер, Велико Търново, 2008.

Ivo M. Michailov
Faculty of Mathematics and Informatics, Shumen University,
Universitetska str. 115, 9700 Shumen, Bulgaria
e-mail: ivo_michailov@yahoo.com

Ivan S. Ivanov
Faculty of Mathematics and Informatics, Shumen University,
Universitetska str. 115, 9700 Shumen, Bulgaria
e-mail: slaveicov@abv.bg