Primality

CIS002-2 Computational Alegrba and Number Theory

David Goodwin

david.goodwin@perisic.com

University of Bedfordshire

09:00, Friday 4th November 2011

Contents

Prime numbers

Definition

An integer $p > 1$ is said to be **prime** if the only positive divisors of p are 1 and p itself.

Prime numbers

Lemma (2.3)

Let p be prime, and let a and b be any integers

A *either $p \mid a$, or a and p are coprime.*

B *if $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Corollary (2.4)

If p is prime and p divides $a_1 \dots a_k$ then p divides a_i for some integer i.

Prime-Power Factorisation

The next result, known as the **fundamental theorem of arithmetic**, explains why prime numbers are so important: they are the basic building blocks out of which all integers can be constructed.

Theorem (2.5)

Each integer $n > 1$ has a prime-power factorisation

$$n = p_1^{e_1} \dots p_k^{e_k}$$

where $p_1, \dots, p_k$ are distinct primes and $e_1, \dots, e_k$ are positive integers; this factorisation is unique, apart from permutations of the factors.

Prime-Power Factorisation

Example

200 has the prime-power factorisation $2^3 \times 5^2$, or alternatively $5^2 \times 2^3$ if we permute the factors, but it has no other prime-power factorisations.

Example

1200 has the prime-power factorisation $2^4 \times 3^1 \times 5^2$.

Prime numbers < 100

2, 3, 5, 7,

11, 13, 17, 19,

23, 29,

31, 37,

41, 43, 47,

53, 59,

61, 67,

71, 73, 79,

83, 89,

97.

Prime numbers < 1000

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,
101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199,
211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293,
307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397,
401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499,
503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599,
601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691
701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797,
809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887,
907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997.

Euclid's Theorem

Theorem (2.6)

There are infinitely many primes

A Proof of Euclid's Theorem

Proof.

The proof is by contradiction: we assume that there are only finitely many primes, and then we obtain a contradiction from this, so it follows that there must be infinitely many primes.

Suppose then that the only primes are $p_1, p_2, \ldots, p_k$. Let

$$m = p_1 p_2 \ldots p_k + 1$$

Since n is an integer greater than 1, theorem (2.5) implies that it is divisible by some prime p (this includes the possibility that $m = p$). By our assumption, this prime p must be one of $p_1, p_2, \ldots, p_k$, so p divides their product $p_1 p_2 \ldots p_k$. Since p divides both m and the product $p_1 p_2 \ldots p_k$ it divides $m - p_1 p_2 \ldots p_k = 1$, which is impossible. □

Prove the fundamental theorem of arithmatic to be true.

Lemma (2.7)

If $2^m + 1$ is prime then $m = 2^n$ for some integer $n \geqslant 0$.

Fermat Primes

Numbers in the form $F_n = 2^{2^n} + 1$ are called fermat numbers, and those which are prime are called fermat primes.

The first 5 Fermat numbers are prime, and they are they only known Fermat numbers that are prime. 65537, the largest known Fermat prime, is commonly used as a public exponent in the RSA cryptosystem.

Mersenne Primes

Integers in the form $M_p = 2^p - 1$ are called Mersenne numbers, and those which are prime are called Mersenne primes.

According to wikipedia, there are currently 47 known Mersenne primes.

2,147,483,647 - the 8th Mersenne prime

"The number 2,147,483,647 is also the maximum value for a 32-bit signed integer in computing. It is therefore the maximum value for variables declared as int in many programming languages running on popular CPUs, and the maximum possible score (or amount of money) for many video games. The appearance of the number often reflects an error, overflow condition, or missing value. Similarly, (214) 748-3647 is the sequence of digits represented as a United States phone number and is the most common phone number listed on web pages."

Primality

- How do we determine whether a given integer n is prime?
- How do we find the prime-power factorisation of a given integer n?

Primality testing

Lemma (2.8)

An integer $n > 1$ is composite if and only if it is divisible by some prime $p \leqslant \sqrt{n}$.

Proof.

If n is divisible by such a prime p, then since $1 < p \leqslant \sqrt{n} < n$ it follows that n is composite. Conversely, if n is composite then $n = ab$ where $1 < a < n$ and $1 < b < n$; at least one of a and b is less than or equal to $\sqrt{n}$ (if not $ab > n$), and this factor will be divisible by a prime $p \leqslant \sqrt{n}$, which then divides n □

University of Bedfordshire

Primality testing

In decimal notation, we write a positive integer n in the form $a_k a_{k-1} \dots a_1 a_0$ meaning that

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

where $a_0 \dots a_k$ are integers with $0 \leqslant a_i \leqslant 9$ for all i, and $a_k \neq 0$.

Primality testing

We see that n is divisible by 2 if and only if a_0 is divisible by 2. Similarly we see that n is divisible by 5 if and only if a_0 is 0 or 5. It can be shown (by use of the binomial theorem) that an integer n is divisible by 3 if and only if the sum of its digits is divisible by 3. Some integer n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

$$n = a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots - a_1 + a_0$$

Primality testing

This method of primality testing is effective for small integers n, since there are not too many primes p to consider, but when n becomes large it is very time consuming. In cryptography, one

regularly uses integers with several hundred decimal digits (if n is in the order of 10^{100} there would be about 8×10^{47} primes to test - the fastest supercomputers (in 1998) would take far longer than the estimated age of the universe (15 billion years) to complete the task). Factorisation of large numbers must be more difficult than

primality testing, since the prime-power factorisation of an integer immediately tells us whether or not it is prime.

RSA public key system

A very effective cryptographic system (known as the RSA public key system, after its inventors Rivest, Shamir and Adlemann, 1978) is based on the fact that it is very easy to calculate the product $n = pq$ of two large primes p and q, while it is extremely difficult to reverse this process and obtain factors p and q from n

University of Bedfordshire

Questions

1. is 8703585473 divisible by 3? Is it divisible by 11?
2. Are 157, 221, 641 or 1103 prime?
3. Evaluate the mersenne number $M_{13} = 2^{13} - 1$. Is it prime?
4. Factorise 247, 6887 and 3992003.
5. For which primes p is $p^2 + 2$ also prime?
6. Show that if $p > 1$ and $p \mid (p-1)! + 1$, then p is prime.

Questions (II)

7. Show that $F_0 F_1 \ldots F_{n-1} = F_n - 2$ for all $n \geqslant 1$
8. Find the prime-power factorisations of 132
9. Find the prime-power factorisations of 400
10. Find the prime-power factorisations of 1995
11. Find $gcd(132, 400)$.
12. Find $gcd(132, 1995)$.
13. Find $gcd(132, 400, 1995)$.

University of Bedfordshire

Questions (III)

14. Show that if $a \geqslant 2$ and $a^m - 1$ is prime, then a is even and m is a power of 2.