ENTRY NUMBER THEORY

[ENTRY NUMBER THEORY] Authors: Oliver Knill: 2003 Literature: Hua, introduction to number theory

ABC conjecture

[ABC conjecture] If a,b,c are positive integers, let N(a,b,c) be the product of the prime divisors of a,b,c, with each divisor counted only once. The conjecture claims that for every $\epsilon > 0$, there is a constant mu¿1 such that for all coprime a,b and c=a+b, then $max(|a|,|b|,|c|) \leq muN(a,b,c)^(1+epsilon)$.

irreducible polynomial

A root of an [irreducible polynomial] with integer coefficients is called an [algebraic number].

amicable

Two integers are called [amicable] if each is the sum of the distinct proper factors of the other. For example: 220 and 284 are amicable. Amicable numbers are 2-periodic orbits of the sigma function $\sigma(n)$ which is the sum of the divisors of n.

Apery's theorem

[Apery's theorem]: the value of the zeta function at z=3 is irrational.

arithmetic function

An [arithmetic function] is a function $f(n)$ whose domain is the set of positive integers. An important class of arithmetic functions are multiplicative functions $f(nm) = f(n)f(m)$. An example is the Möbius function $\mu(n)$ defined by $\mu(1) = 1$, $\mu(n) = (-1)^r$ if n is the product of r distinct primes and $\mu(n) = 0$ otherwise.

Artinian conjecture

[Artinian conjecture]: a quantitative form of the conjecture that every non-square integer is a primitive root of infinitely many primes. [Beal's conjecture] If $a^x + b^y = c^z$, where a,b,c,x,y,z are positive integers and $x, y, z > 2$, then a, b, c must have a common factor. It is known that for every x, y, z, there are only finitely many solutions. The Beal conjecture is a ageneralization of Fermat's last theorem. The conjecture was announced in December 1997. The prize is now 100'000 Dollars for either a proof or a counterexample. The conjecture was discovered by the Texan number theory enthusiast and banker Andrew Beal.

Bertrands postulate

[Bertrands postulate] tells that for any integer n greater than 3, there is a prime between n and $2n-2$. The postulate is a theorem, proven by Tchebychef in 1850.

Bezout's lemma

[Bezout's lemma] tells that if f and g are polynomials over a field K and d is the greatest common divisor of f and g, then $d = af + bg$, where a,b are two other polynomials. This generalizes Euclid's theorem for integers.

Brun's constant

The [Brun's constant] is the sum of the reciprocals of all the prime twins. It is estimated to be about 1.9021605824. While one does not know, whether infinitely many prime twins exist, the sum of their reciprocals is known to be finite. This has been proven by the Norwegian Mathematician Viggo Brun (1885-1978) in 1919.

Carmichael numbers

[Carmichael numbers] are natural numbers which are Fermat pseudoprime to any base. Named after R.D. Carmichael who discoved them in 1909. It is known that there are infinitely many Carmichael numbers. The Carmichael numbers under 100'000 are 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, and 75361.

Chineese reminder problem

The [Chineese reminder problem] tells that if $n_1, \ldots, n_k$ are natural numbers which are pairwise relatively prime and if $a_1, \ldots, a_k$ are any integers, then there exists an integer x which solves simultaneously the congruences $x == a_1(modn_1), \ldots, x == a_k(modn_k)$. All solutions are congruent to a given solution modulo $\prod_{j=1}^{k} n_j$. The theorem was established by Qin Jiushao in 1247.

coprime

Two numbers a,b are called [coprime] if their greatest common divisor is 1.

ElGamal

[ElGamal] The ElGamal cryptosystem is based on the difficulty to solve the discrete logarithm problem modulo a large number $n = p^r$, where p is a prime and and r is a positive integer: solving $g^x = b \mathrm{mod} n$ for x is computationally hard. Suppose you want to send a message encoded as an integer m to Alice. A large integer n and a base g are chosen and public. Alice who has a secrete integer a has published the integer $c = g^k \mathrm{mod}(n)$ as her public key. Everybody knows n, g, c. To send Alice a message m, we chose an integer k at random and send Alice the pair $(A, B) = (g^m, kg^{am})$ modulo n. (We can compute $g^{am} = (g^a)^m = c^m$ using the publically availble information only.) Alice can recover from this the secret message $m = A^a/B$. However, somebody intercepting the message is not able to recover m without knowing a. He would have to find the discrete logarithm of g^m with base g to do so but this is believed to be a computationally difficult problem.

Farey Sequence

The [Farey Sequence] of order n is the finite sequence of rational numbers a/b, with $0 \leq a \leq b \leq n$ such that a, b have no common divisor different from 1 and which are arranged in increasing order.

$F_1 =$	$(0/1, 1/1)$
$F_2 =$	$(0/1, 1/2, 1)$
$F_3 =$	$(0/1, 1/3, 1/2, 2/3, 1/1)$
$F_4 =$	$(0/1, 1/4, 1/3, 1/2, 2/3, 3/4)$
$F_5 =$	$(0/1, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4/4/5)$

Number

[Number]:

N:	natural numbers	e.g. $1, 2, 3, 4, ...$
Z:	integers	e.g. $-1, 0, 1, 2, ...$
Q:	rational numbers	e.g. $5/6, 5, -8/10$
R:	real numbers	e.g. $1, \pi, e, \sqrt(2), 5/4$
C:	complex numbers	e.g. $i, 2, e + i\pi/2, 4\pi/e$

natural numbers

The numbers $1, 2, 3, ...$ are called the [natural numbers].

Fermats last theorem

[Fermats last theorem]. For any ineger n bigger than 2, the equation $x^n + y^n = z^n$ has no solutions in positive integers. This theorem was proven in 1995 by Andrew Wiles with the assistance of Richard Taylor. The theorem has a long history: in an annotation of his copy "Diophantus", Fermat wrote a note: "On the other hand, it is impossible to seperate a cube into two cubes, or a biquadrate into two biquadrates, or generally any power except a squre into two powers with the same exponent. I have discovered a truely marvelous proof of this which however the margin is not large enough to contain."

Fermat-Catalan Conjecture

[Fermat-Catalan Conjecture] There are only finitely many triples of coprime integer powers x^q, y^q, z^r for which $x^p + y^q = z^r$ with $1/p + 1/q + 1/r < 1$.

Fermats little theorem

[Fermats little theorem] If p is prime and a is an integer which is not a multiple of p, then $a^(p-1) = 1 mod p$. Example: $2^4 = 16 = 1 \pmod 5$. Fermats little theorem is a consequence of the Lagrange theorem in algebra, which says that for finite groups, the order of a subgroup divides the order of the group. Fermats theorem is the special case, when the finite group is the cyclic group with $p-1$ elements. Fermats little theorem is somtimes also stated in the form: for every integer a and prime number p, the number $a^p - a$ is a multiple of p.

Fermat numbers

Numbers $F_n = 2^(2^n) + 1$ are called [Fermat numbers]. Examples are

$F_0 = 3$	prime
$F_1 = 5$	prime
$F_2 = 17$	prime
$F_3 = 257$	prime
$F_4 = 65537$	prime
$F_5 = 641 \cdot 6700417$	composite

No other prime Fermat number beside the first 5 had been found so far.

fundamental theorem of arithmetic

The [fundamental theorem of arithmetic] assures that every natural number n has a unique prime factorization. In other words, there is only one way in which one can write a number as a product of prime numbers if the order of the product does not matter. For example, $84 = 2237$ is the prime factorization of 84.

Goldbach's conjecture

[Goldbach's conjecture]: Every even integer n greater than two is the sum of two primes. For example: $8 = 5+3$ or $20 = 13 + 7$. The conjecture has not been proven yet.

greatest common divisor

The [greatest common divisor] of two integers n and m is the largest integer d such that d divides n and d divides m. One writes $d = gcd(n, m)$. For example, $gcd(6, 9) = 3$. There are few recursive algorithms for gcd: one of them is the Euclidean algorithm: $gcd(m, n) = \{k = m \ mod \ n; if \ (k == 0) \ return(n); else \ return(gcd(n, k))\}$.

prime number or prime

A positive integer n is called a [prime number] or [prime], if it is divisible by 1 and n only. The first prime numbers are $2, 3, 5, 7, 11, 13, 17$. An example of a non prime number is 12 because it is divisible by 3. There are infinitely many primes. Every natural number n can be factorized uniquely into primes: for example $42 = 237$.

prime factorization

The [prime factorization] of a positive integer n is a sequence of primes whose product is n. For example: $18 = 3 \cdot 3 \cdot 2$ or $100 = 2 \cdot 2 \cdot 5 \cdot 5$ or $17 = 17$. Every integer has a unique prime factorization.

Pells equation

Fermat claimed first that [Pells equation] $dy^2 + 1 = x^2$, where d is an integer has always integer solutions x and y. The name "Pell equation" was given by Euler evenso Pell seems nothing have to do with the equation. Lagrange was the first to prove the existence of solutions. One can find solutions by performing the Continued fraction expansion of the square root of d.

Fermat number

A [Fermat number] is an integer of the form $F_k = 2^(2^k) + 1$. The first Fermat numbers are $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. They are all primes and called Fermat primes. Fermat had claimed that all F_k are primes. Euler disproved that showing that 641 divides F_5. The Fermat numbers F_5 until F_9 are known to be not prime and also have been factored. Fermat numbers play a role in constructing regular polygons with ruler and compass. The factorization of Fermat numbers serves as a challenge to factorization algorithms.

Fermat prime

A [Fermat prime] is a Fermat number which is prime.

Mersenne number

An integer $2^n - 1$ is called a [Mersenne number]. If a Mersenne number is prime, it is called a Mersenne prime.

Mersenne number

If a Mersenne number $2^n - 1$ is prime, it is called a [Mersenne prime]. In that case, n must be prime. Known examples are n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377,24036583 It is not known whether there are infinitely many Mersenne primes.

perfect number

An integer n is called a [perfect number] if it is equal to the sum of its proper divisors. For example $6 = 1+2+3$ or $28 = 1+2+4+7+14$ are perfect numbers. Also, if $2^n - 1$ is prime then $2^{n-1}(2^n - 1)$ is perfect because $1+2+4+...+2^(n-1) = 2^n - 1$. This was known already to Euclid. Every even perfect number is of the form $p(p+1)/2$, where $p = 2^n - 1$ is a Mersenne prime. It is not known whether there is an odd perfect number, nor whether there are infinitely many Mersenne primes.

partition

The [partition] of a number n is a decomposition of n into a sum of integers. Examples are $5 = 1+2+2$. The number of partitions of a number n is denoted by $p(n)$ and plays a role in the theory of representations of finite groups. For example: $p(4) = 5$ because of the following partitions $4 = 3+1 = 2+2 = 1+1+2 = 1+1+1+1$ Euler introduced the Power series $f(x) = \sum p(n)x^n$ which is $(1-x)^{-1}(1-x^2)^{-1}....$ The algebra of formal power series leads to powerful identites like $(1+x)^{-1}(1+x^2)^{-1}(1+x^3)^{-1}... = (1+x)(1-x)(1+x^2)(1-x^2).../(1-x)(1-x^2)... = (1-x^2)(1-x^4).../(1-x)(1-x^2)... = (1-x)^{-1}(1-x^3)^{-1}(1-x^5)^{-1}....$ The left hand side is the generating function for $a(n)$, the number of partitions of n into distinct numbers. The right hand side is the generating function of $b(n)$, the number of partitions of n into an odd number of summands. The algebraic identity has shown that $a(n) = b(n)$. For example, for $n = 5$, one has $a(5) = 3$ decomposition $5 = 5 = 4+1 = 3+2$ into different summands and also $b(5) = 3$ decompositions into an odd number of summands $5 = 5 = 2+2+1 = 1+1+1+1+1$.

prime number

A [prime number] is an positive integer which is divisible only by 1 or itself. For example, 12 is not a prime number because it is divisible by 3 but the integer 13 is a prime number. The first prime numbers are $2, 3, 5, 7, 11, 13, 17, 23....$ There are infinitely many prime numbers because if there were only finitely many, their product $p_1p_2...p_k = n$ has the property that $n+1$ is not divisible by any p_i. Therefore, $n+1$ would either be a new prime number of be divisible by a new prime number. This contradicts the assumption that there are only finitely many.

prime twin

[prime twin] Two positive integers $p, p+2$ are called prime twins if both p and $p+2$ are prime numbers. For example $(3, 5)$, $(11, 13)$ and $17, 19$ are prime twins. It is unknown, whether there are infinitely many prime twins. One knows that $\sum_i 1/p_i$, where $(p_i, p_i + 2)$ are prime times is finite. In 2004, R. F. Arenstorf from Vanderbilt University has presented a 38-page possible proof of the twin-prime conjecture using methods from classical analytic number theory.

Pythagorean triple

Three integers x, y, z form a [Pythagorean triple] if $x^2 + y^2 = z^2$. An example is $3^2 + 4^2 = 5^2$. Pythagorean triples define triangles with a right angle and integer side lengths x, y, z. They were known and useful already by the Babylonians and used to triangulate rectangular regions. The Pythagorean triples with even x can be parameterized with $p > q$ and $x = 2pq, y = p^2 - q^2$, $z = p^2 + q^2$. Each Pythagrean triple corresponds to rational points on the unit circle: $X^2 + Y^2 = 1$, where $X = x/z, Y = y/z$.

relatively prime

Two integers n and m are [relatively prime] if their greatest common divisor $gcd(n, m)$ is 1. In other words, one does not find a common factor of n and m other than 1.

Sieve of Eratosthenes

The [Sieve of Eratosthenes] allows to construct prime numbers. By sieving away all multiplies of $2, 3, ..., N$ and listing what is left, one obtains a list of all the prime numbers smaller than N^2. For example:

multiples of 2:	4,6,8,10,12,14,16,18,20,22,24,26,...
multiplis of 3:	6,9,12,15,18,21,24,...
multiples of 5:	10,15,20,25,...

The numbers $2, 3, 5, 7, 11, 13, 17, 19, 23$ do not appear in this list and are all the prime numbers smaller or equal than 5^2. To list all the prime number up to N^2, one would have to list all the multiples of k for $k \leq N$.

quadratic residue

A square modulo m, then n is called a A [quadratic residue] modulo m is an integer n which is a square modulo m. That is one can find an integer x such that $n = x^2$ (modm). If m is not a quadratic residue, it is called a quadratic non-residue modulo n. Examples:

- 2 is a quadratic residue modulo 7 because $3^2 = 2$ modulo 7.
- If p is an odd prime, then there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues modulo p.

Legendre symbol

The [Legendre symbol] encodes, whether n is a quadratic residue modulo a prime number p or not: $Legendre(n, p) = 1$ if n is a quadratic residue and $Legendre(n, p) = -1$ if n is not a quadratic residue. If p is a prime number, then $Legendre(-1, p) = (-1)^(p-1)/2)$ and $Legendre(2, p) = (-1)^(p^2-1)/8)$.

law of quadratic reciprocity

The [law of quadratic reciprocity] tells that if p, q are distinct odd prime numbers, then $Legendre(p, q) \cdot Legendre(q, p) = (-1)^n$, where $n = (p-1)(q-1)/4$. Gauss called this result the "queen of number theory". The theorem implies that if $p = 3$ (mod4) and $q = 3$ (mod4), then exactly one of the two congruences $x^2 = p$ (modq) or $x^2 = q$ (modp) is solvable. Otherwise, either both or none is solvable.

Jacobi symbol

[Jacobi symbol] If $m = p_1...p_k$ is the prime factorization of m, define $Jacobi(n, m)$ as the product of $Legendre(n, p_i)$, where $Legendre(n, p)$ denotes the Legendre symbol of n and p and $m = p_1 \cdots p_k$ is the prime factorization of m.

Jacobi symbol

A positive integer a which generates the multiplicative group modulo a prime number p is called a [primitive root of p]. Examples:

- $a = 2$ is a primitive root modulo $p = 5$, because $1 = a^0, 2 = a^1, 4 = a^2, 3 = a^3$ is already the list of elements in the multiplicative group of 5.
- $a = 4$ is not a primitive root modulo $p - 5$ because $4^2 = 1$ mod5.

Liouville

An irrational number a is called [Liouville] if there exists for every integer m a sequence p_n/q_n of irreducible fractions such that $\lim_{n\to\infty} q_n^m |a - p_n/q_n| = 0$. Liouville numbers form a class of irrational numbers which can be approximated well by rational numbers. An example of a Liouville number is 0.10100100001000000001... ,where the number of zeros between the 1's grows exponentially.

Möbius function

The [Möbius function] μ is an example of multiplicative arithmetic function. It is defined as

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^r & n = p_1 \cdot .. \cdot p_r, p_i < p_{i+1} \\ 0 & \text{otherwise} \end{cases} .$$

sigma function

Orbits of the [sigma function] $\sigma(n)$ giving the sum of the divisors of n is called an [aliquot sequence]. One starts with a number n and forms $\sigma(n), \sigma(\sigma(n))$ etc. Example: $12, 16, 15, 9, 4, 3, 1$. Perfect numbers are fixed points, amicable numbers are periodic orbits. Higher periodic orbits are called sociable chains. The Catalan conjecture states that every aliquot sequence

This file is part of the Sofia project sponsored by the Provost's fund for teaching and learning at Harvard university. There are 45 entries in this file.

Index