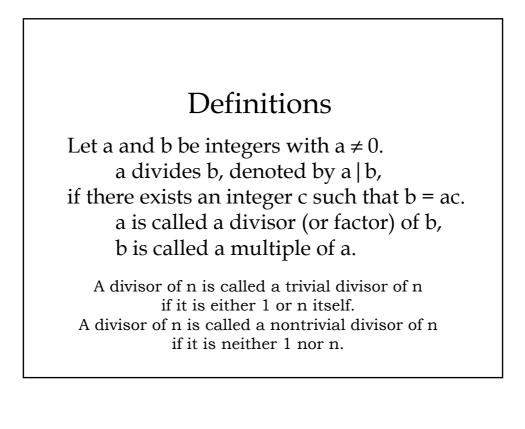
Theory of Divisibility

Divisibility has been studied for at least three thousand years. From before the time of Pythagoras, the Greeks considered questions about even and odd numbers, perfect and amicable numbers, and the primes, among many others; even today a few of these questions are still unanswered.



Example

The integer 200 has the following positive Divisors:

1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 200.

Thus, for example, we can write 4|200, 25|200, 12/200 49/200.

Theorem

Let a, b and c be integers. Then

- 1. if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$
- 2. if a | b then a | bc for all integers c.
- 3. if a | b and b | c then a | c.

Definition

A positive integer n greater than 1 is called prime if its only divisors are n and 1.

A positive integer n that is greater than 2 and is not prime is called composite.

Book of Elements IX

There are infinitely many primes.

SOME RESULTS

For all integers $n \ge 1$, there is a prime p such that n .

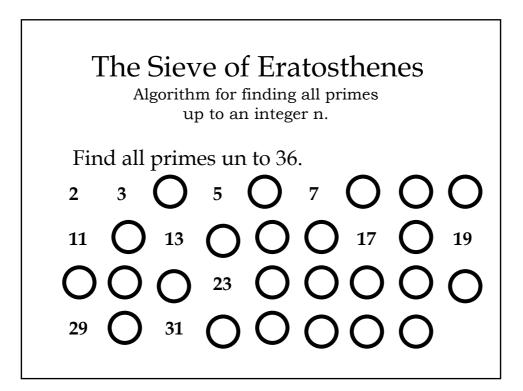
For a real number $x \ge 1$, there exists a prime between x and 2x.

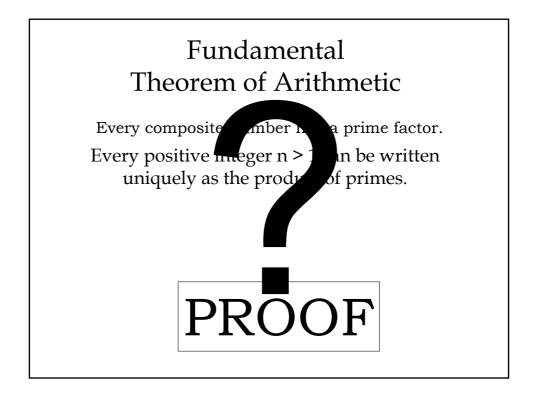
If n is a composite, n has a prime divisor p such that $p \le n^{1/2}$.

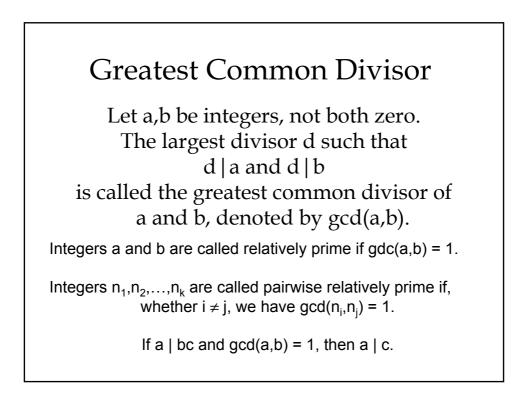
The Sieve of Eratosthenes

Algorithm for finding all primes up to an integer n.

- Create a list of integers from 2 to n.
- For prime p, from 2 up to $\lfloor n^{1/2} \rfloor$, delete all multiples p < pm \leq n.
- Print the integers remaining in the list.







Least Common Multiple

Let a,b be integers, not both zero. The smallest multiple d such that d is a multiple of a and d is a multiple of b is called the least common multiple of a and b, denoted by lcm(a,b).

Theorem

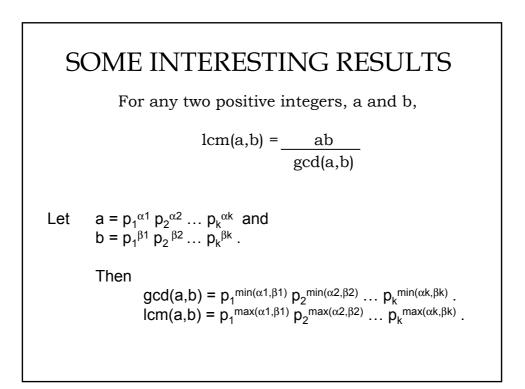
Let a, b be integers, not both zero. Let m = lcm(a, b). Suppose that x is a common multiple of a, b. Then m | x. (Every common multiple of a and b is a multiple of the least common multiple.)

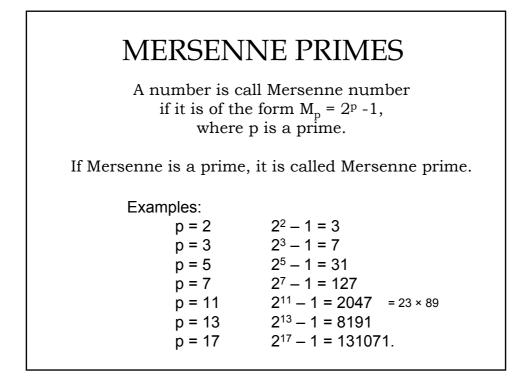
Example

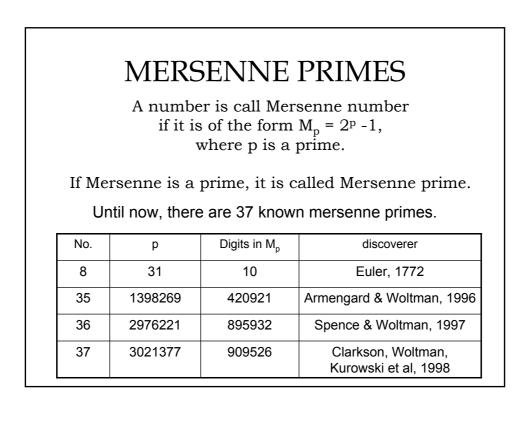
Find gcd(1800, 420)

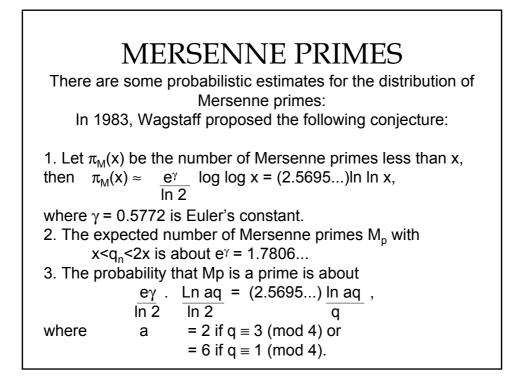
 $1800 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5$ $420 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7$ $gcd(1800,420) = 2 \cdot 2 \cdot 3 \cdot 5$ = 60That is 60 | 420 and 60 | 1800. There is not any integer m > 60 and m | 420 and m | 1800. Find lcm(1800,420). $lcm(1800,420) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7$ = 12600.That is 1800 | 12600 and 420 | 12600. There is not any integer n < 12600 and 1800 | n and 420 | n

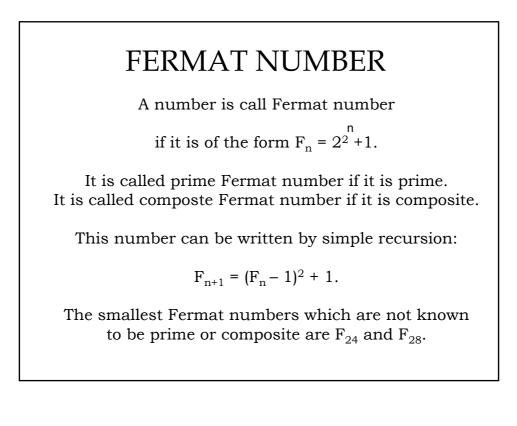
1800|n and 420|n.











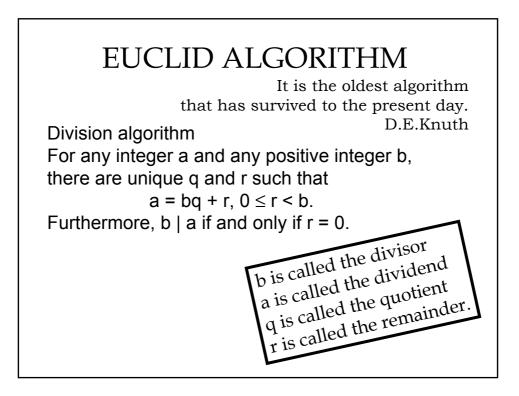
FERMAT NUMBER

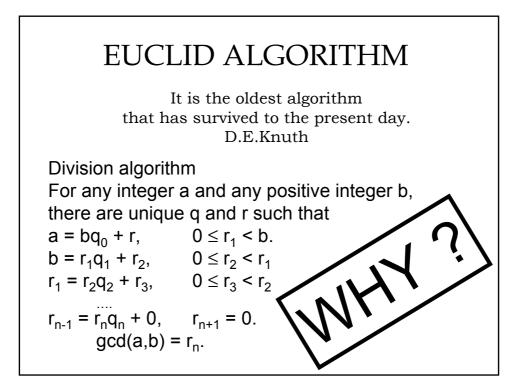
Fermat in 1640 conjectured, all Fermat numbers were primes after he had verified it up to n=4, but Euler in 1732 found that the fifth Fermat number is not a prime, since $F_5 = 641 \times 6700417$ is a product of two primes. Fermat was wrong !

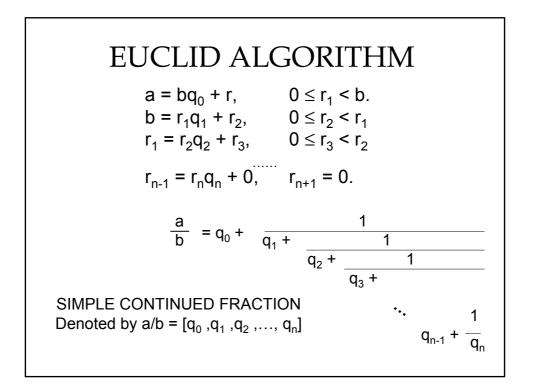
To date, the Fermat numbers F_6 , F_7 , ..., F_{11} have been completely factored.

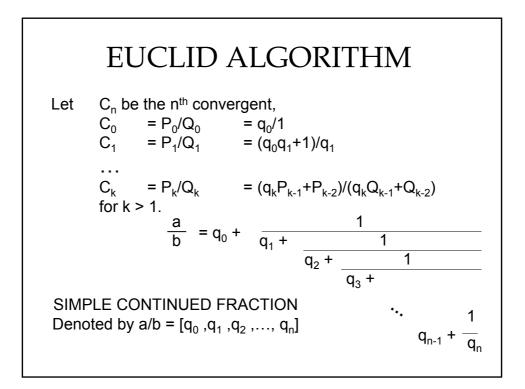
Many open problems:

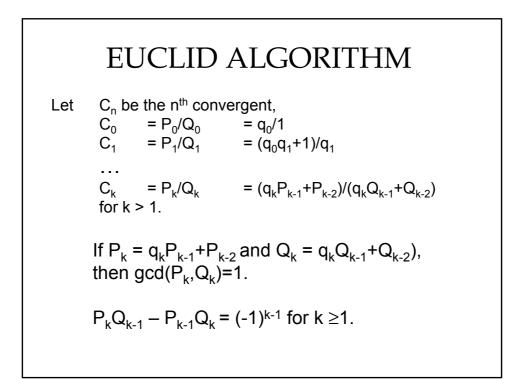
- Are there infinitely many prime (composite) Fermat numbers?
- Is every Fermat number square-free?











EUCLID ALGORITHM

SOME RESULTS

THEOREM

•Any finite simple continued fraction represents a rational number.

Any rational number can be expressed as a finite simple continued fraction in exactly two ways, one with an odd number of terms and one with an even number of terms.
Any irrational number can be written uniquely as an infinite simple continued fraction.

•If x is an infinite simple continued fraction, then x is irrational.

EUCLID ALGORITHM DEFINITIONS Any irrational number which is the root of a quadratic equation ax²+bx+c=0 with integer coefficients is called guadratic irrational.

Any infinite simple continued fractional is said to be periodic if there exists integers k and m such that

 $q_{i+m} = q_i$, for $i \ge k$.

The periodic simple continued fraction is usually denoted by

 $[q_1, q_2, q_3, \dots, q_k, \overline{q_{k+1}, q_{k+2}, \dots, q_{k+m}}].$

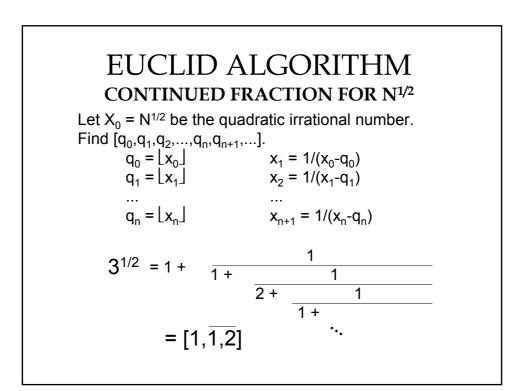
If it is of the form $[q_1,q_2,q_3,...,q_{m-1}]$, then it is called purely periodic.

The smallest positive integer m satisfying the above relationship is called the period of the expansion.

EUCLID ALGORITHM

QUADRATIC IRRATIONAL

Any periodic simple continued fraction is a quadratic irrational. Conversely, any quadratic irrational has a periodic expansion as a simple continued fraction.



DIOPHANTINE EQUATIONS

Diophantus of Alexandria (250 AD.)

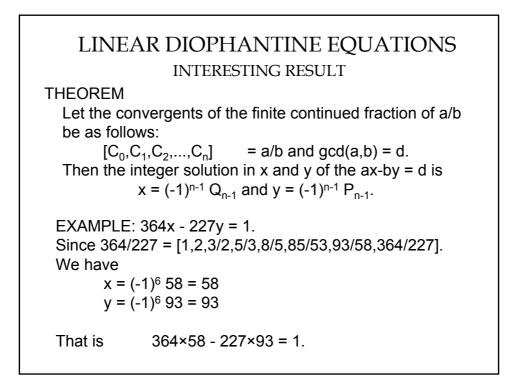
Problem:

Determination of whether or not a polynomial equation f(x,y,z,...)=0 in variables x,y,z,..., with integral coefficients, has integral solutions, or in some cases rational solutions.

The integral solutions of a Diophantine equation f(x,y)=0represents the points with integral coordinates on the curve f(x,y)=0.

EXAMPLE: $x^2-2y^2=0$, the only integral solution is (x,y)=(0,0).

	-
LINEAR DIOPHANTINE EQUATIONS Definition: The algebraic equation with two variables, ax + by = c is called a linear Diophantine equation, for which we wish to find integer solutions in x and y.	
we wish to find integer solutions in x and y.	
Theorems: Not both a and b equal to 0, and d = gcd(a,b). The linear Diophantine equation ax+by=c has integer solutions In x and y if and only if d c. (if not, this has no integer solution.)	
If (x_0, y_0) is a particular integral solution of ax+by=c, then all other solutions of this equation are given by $(x,y) = (x_0 + (b/d)t, y_0 - (a/d)t)$ with t an integral parameter.	



LINEAR DIOPHANTINE EQUATIONS INTERESTING RESULT EXAMPLE: 20719x - 13871y = 1. Since 20719/13871 = [1,3/2,118/79,829/555,1776/1189,2723/1823,4499/3012,20719/13871]. $x = (-1)^7 3012 = -3012$ We have $y = (-1)^7 4499 = -4499$ 20719×(-3012) - 13871×(-4499) = 1. That is For linear Diophantine equation: axy + bx + cy = d. This equation can be reduced as (ax + c) (ay + b) = ad + bc.If mn is a factorization of ad + bc and a|(n-c) and a|(m-b), an integer solution is x = (n-c)/ay = (m-b)/a