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.

Definitions

Let a and b be integers with $a \neq 0$.

a divides b, denoted by $a \mid b$,

if there exists an integer c such that $b = ac$.

a is called a divisor (or factor) of b,

b is called a multiple of a.

A divisor of n is called a trivial divisor of n if it is either 1 or n itself.

A divisor of n is called a nontrivial divisor of n if it is neither 1 nor n.

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
$4|200$, $25|200$, $12\nmid 200$ $49\nmid 200$.

Theorem

Let a, b and c be integers. Then

1. if $a|b$ and $a|c$ then $a|(b+c)$
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

EUCLID

There are infinitely many primes.

SOME RESULTS

For all integers $n \geq 1$, there is a prime p such that $n < p \leq n!+1$.

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

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

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.

The Sieve of Eratosthenes

Algorithm for finding all primes
up to an integer n.

Find all primes un to 36.

2	3		5		7			
11		13				17		19
			23					
29		31						

Fundamental Theorem of Arithmetic

?

Every composite number has a prime factor.

Every positive integer n > 1 can be written uniquely as the product of primes.

PROOF

Greatest Common Divisor

Let a,b be integers, not both zero.
The largest divisor d such that
d|a and d|b
is called the greatest common divisor of a and b, denoted by gcd(a,b).

Integers a and b are called relatively prime if gdc(a,b) = 1.

Integers $n_1, n_2, \ldots, n_k$ are called pairwise relatively prime if, whether $i \neq j$, we have $\gcd(n_i, n_j) = 1$.

If a | bc and gcd(a,b) = 1, then a | c.

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 . 2 . 2 . 3 . 3 . 5 . 5
420 = 2 . 2 . 3 . 5 . 7

gcd(1800,420) = 2 . 2 . 3 . 5
= 60

That 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 . 2 . 2 . 3 . 3 . 5 . 5 . 7
= 12600.

That is 1800|12600 and 420|12600.
There is not any integer n < 12600 and
1800|n and 420|n.

SOME INTERESTING RESULTS

For any two positive integers, a and b,

$$\mathrm{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$$

Let $a = p_1^{\alpha 1}\, p_2^{\alpha 2} \ldots p_k^{\alpha k}$ and
$b = p_1^{\beta 1}\, p_2^{\beta 2} \ldots p_k^{\beta k}$.

Then

$\gcd(a,b) = p_1^{\min(\alpha 1,\beta 1)}\, p_2^{\min(\alpha 2,\beta 2)} \ldots p_k^{\min(\alpha k,\beta k)}$.

$\mathrm{lcm}(a,b) = p_1^{\max(\alpha 1,\beta 1)}\, p_2^{\max(\alpha 2,\beta 2)} \ldots p_k^{\max(\alpha k,\beta k)}$.

MERSENNE PRIMES

A number is call Mersenne number
if it is of the form $M_p = 2^p - 1$,
where p is a prime.

If Mersenne is a prime, it is called Mersenne prime.

Examples:

p = 2	$2^2 - 1 = 3$
p = 3	$2^3 - 1 = 7$
p = 5	$2^5 - 1 = 31$
p = 7	$2^7 - 1 = 127$
p = 11	$2^{11} - 1 = 2047$ $= 23 \times 89$
p = 13	$2^{13} - 1 = 8191$
p = 17	$2^{17} - 1 = 131071$.

MERSENNE PRIMES

A number is call Mersenne number
if it is of the form $M_p = 2^p - 1$,
where p is a prime.

If Mersenne is a prime, it is called Mersenne prime.

Until now, there are 37 known mersenne primes.

No.	p	Digits in M_p	discoverer
8	31	10	Euler, 1772
35	1398269	420921	Armengard & Woltman, 1996
36	2976221	895932	Spence & Woltman, 1997
37	3021377	909526	Clarkson, Woltman, Kurowski et al, 1998

MERSENNE PRIMES

There are some probabilistic estimates for the distribution of Mersenne primes:
In 1983, Wagstaff proposed the following conjecture:

1. Let $\pi_M(x)$ be the number of Mersenne primes less than x, then $\pi_M(x) \approx \frac{e^\gamma}{\ln 2} \log\log x = (2.5695...)\ln\ln x$,
where $\gamma = 0.5772$ is Euler's constant.
2. The expected number of Mersenne primes M_p with $x<q_n<2x$ is about $e^\gamma = 1.7806...$
3. The probability that Mp is a prime is about
$$\frac{e\gamma}{\ln 2} \cdot \frac{\text{Ln } aq}{\ln 2} = (2.5695...) \frac{\ln aq}{q},$$
where a $= 2$ if $q \equiv 3 \pmod 4$ or
$= 6$ if $q \equiv 1 \pmod 4$.

FERMAT NUMBER

A number is call Fermat number

if it is of the form $F_n = 2^{2^n} + 1$.

It is called prime Fermat number if it is prime.
It is called composte Fermat number if it is composite.

This number can be written by simple recursion:

$$F_{n+1} = (F_n - 1)^2 + 1.$$

The smallest Fermat numbers which are not known to be prime or composite are F_{24} and F_{28}.

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 $F_6, F_7, \ldots, F_{11}$
have been completely factored.

Many open problems:

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

EUCLID ALGORITHM

It is the oldest algorithm
that has survived to the present day.
D.E.Knuth

Division algorithm
For any integer a and any positive integer b,
there are unique q and r such that

$$a = bq + r, \ 0 \le r < b.$$

Furthermore, b | a if and only if r = 0.

b is called the divisor
a is called the dividend
q is called the quotient
r is called the remainder.

EUCLID ALGORITHM

It is the oldest algorithm
that has survived to the present day.
D.E.Knuth

Division algorithm
For any integer a and any positive integer b,
there are unique q and r such that

$a = bq_0 + r, \qquad 0 \le r_1 < b.$
$b = r_1q_1 + r_2, \qquad 0 \le r_2 < r_1$
$r_1 = r_2q_2 + r_3, \qquad 0 \le r_3 < r_2$
....
$r_{n-1} = r_nq_n + 0, \qquad r_{n+1} = 0.$
$\gcd(a,b) = r_n.$

WHY ?

EUCLID ALGORITHM

$a = bq_0 + r, \qquad 0 \le r_1 < b.$
$b = r_1q_1 + r_2, \qquad 0 \le r_2 < r_1$
$r_1 = r_2q_2 + r_3, \qquad 0 \le r_3 < r_2$
......
$r_{n-1} = r_nq_n + 0, \qquad r_{n+1} = 0.$

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{\ddots}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

SIMPLE CONTINUED FRACTION
Denoted by $a/b = [q_0, q_1, q_2, \ldots, q_n]$

EUCLID ALGORITHM

Let C_n be the n^{th} convergent,

$C_0 = P_0/Q_0 = q_0/1$

$C_1 = P_1/Q_1 = (q_0 q_1+1)/q_1$

…

$C_k = P_k/Q_k = (q_k P_{k-1}+P_{k-2})/(q_k Q_{k-1}+Q_{k-2})$

for k > 1.

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{}{\ddots \, q_{n-1} + \cfrac{1}{q_n}}}}}$$

SIMPLE CONTINUED FRACTION

Denoted by $a/b = [q_0, q_1, q_2, \ldots, q_n]$

EUCLID ALGORITHM

Let C_n be the n^{th} convergent,

$C_0 = P_0/Q_0 = q_0/1$

$C_1 = P_1/Q_1 = (q_0 q_1+1)/q_1$

…

$C_k = P_k/Q_k = (q_k P_{k-1}+P_{k-2})/(q_k Q_{k-1}+Q_{k-2})$

for k > 1.

If $P_k = q_k P_{k-1}+P_{k-2}$ and $Q_k = q_k Q_{k-1}+Q_{k-2}$), then $\gcd(P_k,Q_k)=1$.

$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}$ for $k \geq 1$.

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 $ax^2+bx+c=0$ with integer coefficients is called quadratic irrational.

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

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

The periodic simple continued fraction is usually denoted by

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

If it is of the form $[\overline{q_1,q_2,q_3,\ldots,q_{m-1}}]$, 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.

EUCLID ALGORITHM

CONTINUED FRACTION FOR $N^{1/2}$

Let $X_0 = N^{1/2}$ be the quadratic irrational number.
Find $[q_0,q_1,q_2,\ldots,q_n,q_{n+1},\ldots]$.

$$\begin{array}{ll}
q_0 = \lfloor x_0 \rfloor & x_1 = 1/(x_0-q_0) \\
q_1 = \lfloor x_1 \rfloor & x_2 = 1/(x_1-q_1) \\
\ldots & \ldots \\
q_n = \lfloor x_n \rfloor & x_{n+1} = 1/(x_n-q_n)
\end{array}$$

$$3^{1/2} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \ddots}}}$$

$$= [1,\overline{1,2}]$$

DI0PHANTINE EQUATIONS

Diophantus of Alexandria (250 AD.)

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

The integral solutions of a Diophantine equation $f(x,y)=0$ represents 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.

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

THEOREM

Let the convergents of the finite continued fraction of a/b be as follows:

$[C_0,C_1,C_2,...,C_n]$ = a/b and gcd(a,b) = d.

Then the integer solution in x and y of the ax-by = d is

$x = (-1)^{n-1} Q_{n-1}$ and $y = (-1)^{n-1} P_{n-1}$.

EXAMPLE: 364x - 227y = 1.
Since 364/227 = [1,2,3/2,5/3,8/5,85/53,93/58,364/227].
We have

$x = (-1)^6\ 58 = 58$

$y = (-1)^6\ 93 = 93$

That is $364\times58 - 227\times93 = 1$.

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].

We have $x = (-1)^7\ 3012 = -3012$

$y = (-1)^7\ 4499 = -4499$

That is $20719\times(-3012) - 13871\times(-4499) = 1$.

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 $x = (n-c)/a$

$y = (m-b)/a$