Divisibility and Primes

Denis TRYSTRAM

Lecture notes **Maths for Computer Science** – *MOSIG 1 – 2017*

1 Preliminaries

Number Theory is a field where the problems to solve are very easy to formalize and to understand, but very hard to prove! We recall below some well-known examples:

- Perfect numbers conjecture: is there an odd perfect number? Perfect numbers are numbers which are equal to the sum of their prime factors (for instance $28 = 1 + 2 + 4 + 7 + 14$).
- Goldbach's conjecture: every even number can be written as a sum of two primes.
- Twin primes: are there an infinite number of primes in the form $(n, n+2)$?

The underlying techniques of number theory are very important in many problems, including cryptography. We will investigate several classical results and some related properties.

2 Perfect divisibility

2.1 Basic results and definitions

Let a and b be two integers. a divides b if there is an integer k such that $ak = b$. We also say that b is a multiple of a (notice here that a may be negative). Let remark that according to this definition, every number divides 0.

The following properties are straightforward by applying directly the definitions:

1. If $a \mid b$ then $a \mid bc$ $\forall$ integers c
2. If $a \mid b$ and $b \mid c$ then $a \mid c$
3. If $a \mid b$ and $a \mid b + c$ then $a \mid c$
4. $\forall c \neq 0$, $a \mid b$ *iif* $ac \mid bc$
5. If $a \mid b$ and $a \mid c$ then $a \mid sb + tc$ $\forall$ integers s and t

For instance for proving the last one, remark that there exist k_1 and k_2 such that $a.k_1 = b$ and $a.k_2 = c$, which implies $a(k_1.s + k_2.t) = sb + tc$ for any s and t.

2.2 Greatest Common Divisor

Definition. $GCD(a, b)$ is the largest number that is a divisor of both a and b.

Proposition. $GCD(a, b)$ is equal to the smallest positive linear combination of a and b[1].

The proof considers m as the smallest positive linear combination of a and b. We prove respectively that $m \geq GCD(a, b)$ and $m \leq GCD(a, b)$ by using the general previous properties.

1. By definition, $GCD(a, b) \mid a$ and $GCD(a, b) \mid b$, then, $GCD(a, b) \mid sa + tb$ for any s and t (and thus, in particular for the smallest combination). Then, $GCD(a, b)$ divides m and $m \geq GCD(a, b)$.

2. First, remark that $m \leq a$ because $a = 1.a + 0.b$ is a particular linear combination. We show that $m \mid a$.

   By the division theorem, there exists a decomposition $a = q.m + r$ (where $0 \leq r < m$). Recall also that $m = sa + tb$ for some s and t. Thus, r can be written as $(1 - qs)a + (-qt)b$ which is a combination of a and b. However, as m is the smallest, we get $r = 0$.

   Symmetrically m divides also b.

   Then, $m \leq GCD(a, b)$.

■

Corollary. Every linear combination of a and b is a multiple of $GCD(a, b)$ and vice-versa.

Properties of the GCD

- Every common divisor of a and b divides GCD(a,b)
- GCD(ak,bk)=k.GCD(a,b) for all $k > 0$
- if GCD(a,b)=1 and GCD(a,c)=1 then GCD(a,bc)=1
- if $a \mid bc$ and GCD(a,b)=1 then $a \mid c$
- GCD(a,b) = GCD(b,rem(a,b))

[1] This result is also known as Bezout identity.

In this last property, rem denotes the reminder of the euclidian division of a by b. It is detailed in the next section. The property is useful for quickly compute the GCD of two numbers. This is in fact the basis of the well-known Euclid's algorithm! Let us prove it.

The idea is to show that the set of common divisors of a and b (called D) is equal to the set of the common divisors of b and $rem(a, b)$ (called D').

- If $d \in D$, $d \mid a$ and $d \mid b$.

  As $a = q.b + rem(a, b)$, from property 3 of section 2.1 above, we have $d \mid rem(a, b)$. Then, $d \in D'$.

- If $d' \in D'$, $d' \mid b$ and $d' \mid rem(a, b)$.

  From property 5 above, d' divides any linear combination of them, in particular $q.b + 1.rem(a, b)$ thus, $d' \mid a$ which proves that $d' \in D$.

■

Figures 1 and 2 give a geometrical interpretation of the euclidian division and the CGD. It corresponds to the largest surface unit to obtain a tessellation of the rectangle $a \times b$.

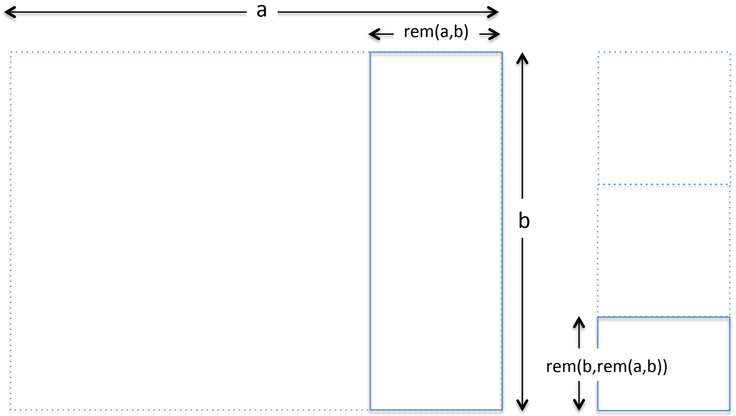


Figure 1: Geometric interpretation of the euclidian division of a by b. The first step is on the left, the second one on the right.

3 Euclidian division and Primes

As we remarked in the previous section, divisibility is not always perfect. As we learned in the elementary school, if one number does not evenly divide another, there is a remainder left over.

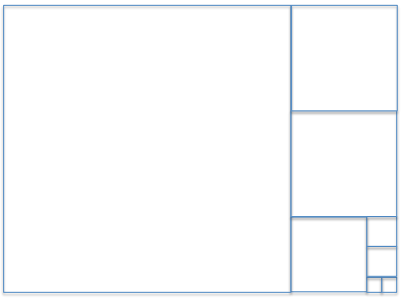


Figure 2: Final step of the geometric interpretation of GCD(a,b) as the smallest area to pave the a by b rectangle.

Division theorem. Let a and b be two integers such that $b > 0$, then there exists a unique pair of integers q and r such that $a = qb + r$ and $0 \leq r < b$.

Proving this theorem is two-fold: first the existence, and then the uniqueness.

- Let E be the set of all positive integers in the form $n = a - b.z$. E is not empty (well, for instance, it contains a) and $E \subset \mathbb{N}$, thus, it has a smallest element. Let denote it r.

  We should verify that $r < b$. It is easy by remarking that $r = a - b.z$ for some z and $r - b$ does not belong to E because r is the smallest one. Thus, $r - b < 0$.

- Let us prove this part by contradiction. Suppose there exist two such pairs of integers: $a = q_i.b + r_i$ for $i = 1, 2$.

  Then, $(q_1 - q_2).b + r_1 - r_2 = 0$.

  Thus, b divides $r_1 - r_2$ and $0 \leq r_1 < b$ and $0 \leq r_2 < b$

  $r_1 - r_2 = 0$ and thus, $q_1 = q_2$.

■

Notations. $rem(a, b)$ denotes the remainder of a by b.

Definition. A *prime* is an integer with no positive divisor other than 1 and itself (otherwise, it is said a *composite*). 1 is neither a prime nor a composite.

Fundamental theorem of Arithmetic.

Every positive integer n can be written in an unique way as a product of primes: $n = p_1p_2...p_j$ $(p_1 \leq p_2 \leq ... \leq p_j)$.

We have again two results to prove: first that every integer can be written as the product of primes, and second that this factorization is unique.

- The first part will be proved easily by a strong induction: let assume that all numbers can be decomposed accordingly up to n and let consider $n+1$. If it is prime the decomposition exists (it is it-self), if it is a composite, each factor can be expressed as a product of primes by the induction hypothesis.

- The uniqueness is obtained by contradiction: Let us first order the primes of the decomposition by increasing values. Assume there are two distinct decompositions into primes. Consider now the first prime which is not the same in both products. One is the smallest and it is easy to remark that it can divides the products of primes of the second number, which is a contradiction.

■

The fundamental theorem provides a (partial) answer to the distribution of prime numbers. Let $\pi(n)$ the number of primes that are lower or equal to n. The theorem states that the limit of $\pi(n)$ when n goes to infinity is $\frac{n}{log(n)}$. This result was guessed by Legendre in 1798 and proved one century later.

Euclide proved that there are an infinity of primes by a simple argument (contradiction about the largest prime over a finite set). Then, Euler proved in the XIXth century the same result (using the fundamental theorem of arithmetic).

4 Fermat little theorem

Statement:

For all prime number p and for all integer a, $a^p - a$ is divisible by p (another way to write this theorem is $a^p \equiv a[p]$).

The classical proof is obtained by recurrence on a, applying the Newton binomial decomposition:

- The basis of the induction is straightforward since $1^p \equiv 1[p]$

- Assuming $a^p \equiv a[p]$ holds, let us write $(a+1)^p = a^p + \Sigma_{1 \leq k \leq p} a^k \binom{p}{k}$

  There is an interesting property on the binomial coefficients when p is prime that is clear while looking at the Pascal triangle modulo $[p]$ in Figure 3. Apart the two extreme coefficients, they are all multiples of p.

  This can be proved by applying the definition
  $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{1}{k!} p.(p-1)(p-k+1)$

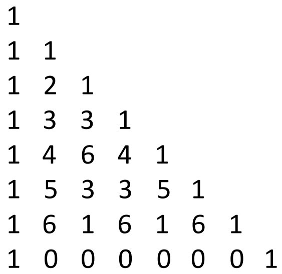
Thus, p divides $k! \binom{p}{k}$ but it has no common divisor with $k!$ since $k \leq p-1$.

This shows that p divides $\binom{p}{k}$.

$(a+1)^p \equiv a^p + 1[p]$

As $a^p \equiv a[p]$ by applying the induction hypothesis, we obtain $(a+1)^p \equiv a+1[p]$.

■



1							
1	1						
1	2	1					
1	3	3	1				
1	4	6	4	1			
1	5	3	3	5	1		
1	6	1	6	1	6	1	
1	0	0	0	0	0	0	1

Figure 3: Pascal Triangle modulo a prime number (7).

5 Perfect numbers

5.1 Definition

A perfect number (*PN* in short) is a number which is equal to the sum of its proper divisors.

For instance, the first perfect numbers are the following:

- 6, which has 3 proper divisors, namely, 1, 2 and 3.

  $1+2+3=6$.

- 28 whose 5 proper divisors are: 1, 2, 4, 7 and 14.

  $1+2+4+7+14=28$.

- 496 has 9 proper divisors, namely, 1, 2, 4, 8, 16, 31, 62, 124 and 248.

  $1+2+4+8+16+31+62+124=496$.

A *Mersenne number* is a prime which has the following expression: $2^\alpha - 1$ for some given integer α.

For instance, $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$ are primes while $15 = 2^4 - 1$ is not prime... Obviously, there exist primes which are not Mersenne's numbers (like $5, 13$ etc.).

Property 1.
Show that $2^\alpha - 1$ is only prime if α is prime.

The proof is based on the little Fermat theorem which was proved in the previous section.

Notice that there are number of this form where α is prime and $2^\alpha - 1$ is not (for instance $\alpha = 6$ and $2^6 - 1 = 63 = 7 \times 9$).

The objective of the next section is to study some characterizations of perfect numbers. It remains several open questions like the existence of odd perfect numbers or if there are an infinite number of such numbers.

Let us first prove some properties about even PM.

5.2 Properties

We are now going to prove the main result:

Property 2.
α is a prime. Let denote by PN_α the number obtained by the following expression: $2^{\alpha-1}(2^\alpha - 1)$ where $2^\alpha - 1$ is a prime.

PN_α is a perfect number and all the perfect numbers have this form.

Proof.

The list of factors Φ_i (for $0 \leq i \leq \alpha - 1$) of $2^{\alpha-1}$ is: $1, 2, 4, ..., 2^{\alpha-1}$.

The other factors of PN_α are obtained by: $\Phi_i.(2^\alpha - 1)$.

Summing up all these factors, we obtain the following expression:
$\Sigma_{i=0,\alpha-2}(2^i + 2^\alpha - 1) = \Sigma_{i=0,\alpha-2}2^i(1 + 2^\alpha - 1)$
$= 2^\alpha \Sigma_{i=0,\alpha-2}2^i$
$= 2^{\alpha-1}\Sigma_{i=0,\alpha-2}2^{i+1}$
$= 2^{\alpha-1}\Sigma_{i=1,\alpha-1}2^i$
$= 2^{\alpha-1}\frac{2^\alpha-1}{2-1}$.
This property was proved by Euclide in *Principae IX-36.*

There are nice properties behind perfect numbers, for instance it is easy to show that the last digit of any perfect number (in usual decimal notation) is 6 or 8.

Property 3 (coding PN by binary representation).
The binary representation of $NP_3 = 28$ and NP_5 are respectively $(11100)_2$ and $(111110000)_2$. It is natural to deduce the binary representation of any NP_α.
$PN_\alpha = (11...10...0)_2$ (α times 1 followed by $\alpha - 1$ times 0).

Proof. The left part comes from $2^\alpha - 1$ and the right part comes from the shifts corresponding to the multiplication by $2^{\alpha-1}$.

Property 4 (link with triangular numbers Δ_n).
Let remark that $PN_2 = 6 = \Delta_3$, $PN_3 = 28 = \Delta_7$.
It is easy to show more generally that $PN_\alpha = \Delta_{2^\alpha-1}$.

Proof. The proof is straightforward by using the basic expression $\Delta_n = \frac{n(n+1)}{2}$ for $n = 2^\alpha - 1$.
$\Delta_{2^\alpha-1} = \frac{(2^\alpha-1)(2^\alpha-1+1)}{2} = \frac{(2^\alpha-1)(2^\alpha)}{2} = (2^\alpha - 1)2^{\alpha-1}$