## ***greatest common divisor*** القاسم المشترك الأكبر

**Euclid's algorithm**, is an efficient method for computing the greatest common divisor (GCD) of two numbers, the largest number that divides both of them without leaving a remainder.

The *greatest common divisor* of integers a and b, denoted by *gcd(a,b)*, is the largest integer that divides (without remainder) both a and b. So, for example:

$$\gcd(15, 5) = 5, \quad \gcd(7, 9) = 1, \quad \gcd(12, 9) = 3, \quad \gcd(81, 57) = 3.$$

The gcd of two integers can be found by repeated application of the division algorithm, this is known as the ***Euclidean Algorithm***. You repeatedly divide the divisor by the remainder until the remainder is 0. The gcd is the last non-zero remainder in this algorithm. The following example shows the algorithm.

Finding the gcd of 81 and 57 by the Euclidean Algorithm:

$$81 = 1(57) + 24$$
$$57 = 2(24) + 9$$
$$24 = 2(9) + 6$$
$$9 = 1(6) + \mathbf{3}$$
$$6 = 2(3) + 0.$$

It is well known that if the gcd(a, b) = r then there exist integers p and s so that:

$$p(a) + s(b) = r.$$

By reversing the steps in the Euclidean Algorithm, it is possible to find these integers p and s. We shall do this with the above example:

Starting with the next to last line, we have:

$$\mathbf{3} = 9 - 1(6)$$

From the line before that, we see that 6 = 24 - 2(9), so:

**3** = 9 - 1(24 - 2(9)) = 3(9) - 1(24).

From the line before that, we have 9 = 57 - 2(24), so:

**3** = 3( 57 - 2(24)) - 1(24) = 3(57) - 7(24).

And, from the line before that 24 = 81 - 1(57), giving us:

**3** = 3(57) - 7( 81 - 1(57)) = 10(57) -7(81).

So we have found p = -7 and s = 10.

The procedure we have followed above is a bit messy because of all the back substitutions we have to make. It is possible to reduce the amount of computation involved in finding p and s by doing some auxillary computations as we go forward in the Euclidean algorithm (and no back substitutions will be necessary). This is known as the ***extended Euclidean Algorithm***.

**The Extended Euclidean Algorithm for finding the inverse of a number mod n.**

We will number the steps of the Euclidean algorithm starting with step 0. The quotient obtained at step i will be denoted by $q_i$. As we carry out each step of the Euclidean algorithm, we will also calculate an auxillary number, $p_i$. For the first two steps, the value of this number is given: $p_0 = 0$ and $p_1 = 1$. For the remainder of the steps, we recursively calculate $p_i = p_{i-2} - p_{i-1} q_{i-2} \pmod n$. Continue this calculation for one step beyond the last step of the Euclidean algorithm.

The algorithm starts by "dividing" n by x. If the last non-zero remainder occurs at step k, then if this remainder is 1, x has an inverse and it is $p_{k+2}$. (If the remainder is not 1, then x does not have an inverse.) Here is an example:

**Find the inverse of 15 mod 26.**

Step 0: 26 = 1(15) + 11 $p_0 = 0$

Step 1: 15 = 1(11) + 4 $p_1 = 1$

Step 2: 11 = 2(4) + 3 $p_2 = 0 - 1( 1) \bmod 26 = 25$

Step 3: $4 = 1(3) + 1$ $p_3 = 1 - 25(1) \bmod 26 = -24 \bmod 26 = 2$

Step 4: $3 = 3(1) + 0$ $p_4 = 25 - 2(2) \bmod 26 = 21$

$p_5 = 2 - 21(1) \bmod 26 = -19 \bmod 26 = 7$

Notice that $15(7) = 105 = 1 + 4(26) \equiv 1 \pmod{26}$.

القاسم المشترك الأكبر لعددين طبيعيين A ، B يساوي القاسم المشترك الأكبر للعدد الثاني B وباقي قسمة A على B ، ونكرر العملية نفسها حتى يصبح باقي القسمة مساويا الصفر، عندئذ يكون القاسم المشترك الأكبر هو العدد الآخر

$$GCD(A,B) = GCD(B,r) \cdots\cdots GCD(N,0).$$

حيث r هو باقي قسمة A على B . و N هو القاسم المشترك الأكبر.

$A = q_0 B + r_0$

**Ex: a = 1071 and b = 462**

$1071 = 2 \times 462 + 147$

$462 = 3 \times 147 + 21$

$147 = 7 \times 21 + 0$

**خوارزمية أقليدس** هي واحدة من أقدم الخوارزميات الجارية الاستعمال لايجاد القاسم المشترك الاكبر. ظهرت في كتاب الأصول لإقليدس في حوالي عام 300 قبل الميلاد.

**أوجد العوامل المشتركه بين العددين 18 ، 24**

**طريقة اخرى :أختار أصغر العددين**

**عوامـــل 18 هـــي الأعـــداد التـــى تقبـــل 18 القســـمة عليهـــا وهـــى 1، 2، 3 ، 6 ، 9 ، 18**
**وحيـــث أن العـــدد الأخـــر وهـــو الـــ 24 يقبـــل القســـمة علـــى كـــل مـــن 1، 2، 3 ، 6**

**إذا العوامل المشتركة هى 1، 2، 3 ، 6 وأعلى عامل مشترك هو 6**

**طريقة اخرى**

**نبحث عن كل الأعداد التى حاصل ضربها 24**

**نبدأبجدول العدد : 1× 24**

**ثم جدول العدد 2 : 2 × 12**

**ثم جدول العدد 3 : 3 × 8**

**ثم جدول العدد 4 : 4 × 6**

**إذا عوامل العدد 24 هى 1، 2 ، 3 ، 4 ، 6 ، 8 ، 12 ، 24**

**أما بالنسبة للعدد 18**

**فنبحث عن كل الأعداد التى حاصل ضربها 18**

**نبدأ بجدول العدد1: 1× 18**

**ثم جدول العدد 2: 2 × 9**

**ثم جدول العدد 3: 3 × 6**

**إذا عوامل العدد 18 هى 1، 2 ، 3 ، 6 ، 9 ،18**

**إذا العوامل المشتركة هى 1، 2، 3 ، 6 وأعلى عامل مشترك هو 6**