**Euclud’s algorithm**

(3rd century B.C., from Alexandria)

One of the basic techniques of number theory is Euclid’s algorithm, which is a simple procedure for determining the greatest common divisor of two positive numbers.

**Greatest common divisor**

We will use notation gcd(a,b) to mean the greatest common divisor of a and b. The positive integer c is said tob the greatest common divisor of a and b if

1. c is a divisor of a and of b
2. any divisor of a and b is a divisor of c

An equivalent definition is the following:

gcd(a,b)=max[k, such that k|a and k|b]

Because we require that the greatest common divisor be positive, gcd(a,b)=gcd(a,-b)=gcd(-a,b)=gcd(-a,-b). In general, gcd(a,b)=gcd(|a|,|b|).

gcd(60,24)=gcd(60,-24)=12

Also, because all nonzero integers divide 0, we have gcd(a,0)=|a|.

**Greatest common divisor (CONT 1)**

We stated that two integers are relatively prime if their only common positive integer factor is 1. This is equivalent to saying that a and b are relatively prime if gcd(a,b)=1.

8 and 15 are relatively prime because the positive divisors of 8 are 1,2,4, and 8, and the positive divisors of 15 are 1,3,5, and 15, so 1 is the only integer on both lists.

**Finding the greatest common divisor**

Euclid’s algorithm is based on the following theorem: For any nonnegative integer a and any positive integer b,

gcd(a, b)=gcd(b, a mod b) (4.3)

*gcd(55,22)=gcd(22, 55 mod 22) = gcd(22,11) = 11*

To see, that (4.3) works, let d=gcd(a,b). Then, by the definition of gcd, d|a and d|b. For any positive integer b, a can be expressed in the form

a = kb+rr mod b

a mod b = r

with k, r integers. Therefore, (a mod b) = a-kb for some integer k. But because d|b, it also divides kb. We also have d|a. Therefore, d|(a mod b). This shows, that d is a common divisor of b and (a mod b). Conversely, if d is a common divisor of b and (a mod b), then d|kb and thus d|[kb+(a mod b)], which is equivalent to d|a. Thus, the set of common divisors of a and b is equal to the set of common divisors of b and (a mod b). Therefore, the gcd of one pair is the same as the gcd of the other pair, proving the theorem.

*Equation (4.3) can be used repetitively to determine the greatest common divisor:*

*gcd(18,12)=gcd(12,6)=gcd(6,0)=6*

*gcd(11,10)=gcd(10,1)=gcd(1,0)=1*

Euclid’s algorithm makes repeated use of (4.3) to determine the greatest common divisor, as follows. The algorithm assumes a>b>0. It is acceptable to restrict the algorithm to positive integers because gcd(a,b) = gcd(|a|,|b|)

**EUCLID’S ALGORITHM**

EUCLID(a,b)

1. A:=a; B:=b
2. if B=0 return A=gcd(a,b)
3. R=A mod B
4. A:=B
5. B:=R
6. goto 2

The algorithm has the following progression:

A1=B1xQ1+R1

A2=B2xQ2+R2

A3=B3xQ3+R3

*To find gcd(1970,1066)*

*1970=1x1066+904 gcd(1066,904)*

*1066=1x904+162 gcd(904,162)*

*904=5x162+94 gcd(162,94)*

*162=1x94+68 gcd(94,68)*

*94=1x68+26 gcd(68,26)*

*68=2x26+16 gcd(26,16)*

*26=1x16+10 gcd(16,10)*

*16=1x10+6 gcd(10,6)*

*10=1x6+4 gcd(6,4)*

*6=1x4+2 gcd(4,2)*

*4=2x2+0 gcd(2,0)*

*Therefore, gcd(1970,1066)=2*

This process should terminate, otherwise we would get an endless sequence of positive integers, each one is strictly smaller than the one before, and this is clearly impossible.

**FINITE FIELDS OF THE FORM GF(p)**

Finite fields play crucial role in many crypto algorithms. It can be shown that the order of a finite field must be a power of a prime pn, where n is a positive integer. Prime is an integer whose only positive integer factors are itself and 1. The finite field of order pn is usually denoted by GF(pn); GF stands for Galois field in honor of the French mathematician Evarist Galois (1811-1832, <http://scienceworld.wolfram.com/biography/Galois.html> ).

**Finite Fields of Order p**

For a given prime p, GF(p) is defined as the set Zp={0,1,..,p-1} of integers together with arithmetic operations modulo p. For such prime numbers, holds (M7) - Multiplicative inverse axiom.

Because elements w of Zp are relatively prime to p, if we multiply all the elements of Zp by w, the resulting residues are all of elements Zp, permuted. Thus, exactly one of the residues has the value 1, respective multiplier is just the inverse element for w, designated w-1. Now, equation (4.2) can be written without condition:

If  then  (4.4)

Consequence is obtained by multiplication of both parts of (4.4) by a-1.

The simplest finite field is GF(2):

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| + | 0 | 1 |  | X | 0 | 1 |  | w | -w | w-1 |
| 0 | 0 | 1 |  | 0 | 0 | 0 |  | 0 | 0 | - |
| 1 | 1 | 0 |  | 1 | 0 | 1 |  | 1 | 1 | 1 |

Addition Multiplication Inverses

**Finite Fields of Order p (CONT 1)**

Next is for GF(7):



**Finding the Multiplicative Inverse in GF(p)**

Table 4.3b may be used to find multiplicative inverse, but for large values of p it is not practical.

If gcd(m,b)=1, then b has a multiplicative inverse modulo m. That is, for positive integer b<m, there exists a b-1<m such that b b-1=1 mod m. Euclid’s algorithm can be extended so that, in addition to finding gcd(m,b), if the gcd is 1, the algorithm returns the multiplicative inverse of b.

**Finding the Multiplicative Inverse in GF(p) (CONT 1)**

EXTENDED EUCLID(m,b)

1. (A1,A2,A3):=(1,0,m); (B1,B2,B3):=(0,1,b);
2. if B3=0 return A3=gcd(m,b); no inverse
3. if B3=1 return B3 = gcd(m,b); B2= b-1 mod m
4. Q=
5. (T1,T2,T3):=(A1-QB1, A2-QB2, A3-QB3)
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

Throughout the computation, the following relationships hold:

mT1+bT2=T3 mA1+bA2=A3 mB1+bB2=B3

To see that algorithm correctly returns gcd(m,b), note that if we equate A and B in Euclid’s algorithm with A3 and B3 in the extended Euclid’s algorithm, then the treatment of the two variables is identical. Note also that if gcd(m,b)=1, then on the final step we would have B3=0 and A3 =1. Therefore, on the preceding step, B3=1. But if B3=1, then we can say the following:

mB1+bB2=B3

mB1+bB2=1

bB2=1-mB1

bB21 mod m

Hence, B2 is the multiplicative inverse of b.

Table 4.4 is an example of the execution of the algorithm. It shows that gcd(550,1759)=1 and that the multiplicative inverse of 550 is 355; that is, 550x3551 mod 1759.

**Finding the Multiplicative Inverse in GF(p) (CONT 2)**

