Topic - 18
Quantum Computing and Information
RSA Algorithm

Dipan Kumar Ghosh
Indian Institute of Technology Bombay
Powai, Mumbai 400076

April 15, 2017

1 Introduction

Cryptography is the means of encrypting a message (known as plain text) by using a code to covert to to a *cipher text* and transmitting the same over a public channel to an intended recipient. At the receiving end, the receiver decrypts it to reconvert it to the plain text.

Modern cryptography has four essential elements. The first and foremost is *privacy of data*, i.e. the content of the data cannot be understood by anyone other than the person or body for whom the message is intended. The second element is *data integrity* implying that the information should not get altered during transit over a channel which may or may not be secure. Over a public channel it may be safely assumed that the data may be intercepted and/or altered by a person with mala fide intention.If this happens, the sender and the receiver of the message should be aware of the possibility and take steps to minimize such possibility. The third element is *non-repudiation* which means that the sender should not be able to disown the fact of having sent such a message to the receiver and the receiver should not be in a position to deny having received the same. The final element of this process is *authentication* by which the sender and the receiver must be able to confirm each other's identity.

To achieve these, a set of procedures and protocols are established, which is given the collective name of **cryptography**. Historically, codes and ciphers have existed from time immemorial for communication with the armed forces or for communication between lovers avoiding prying eyes and ears of nosy relatives and friends. Julius Caesar is known to have used a simple code to communicate with his forces during Gallic wars. Queen Elizabeth - I is reputed to have established a section for inventing and breaking codes. It is believed that breaking of such a code of a letter written by her incarcerated cousin

Mary, Queen of Scots, was used by Elizabeth to order execution of Mary.

There are two points that has to be appreciated in connection with the protocols. Firstly, it is not necessary that the content of a message must remain a secret for ever. The duration of secrecy is determined by the security needs of the problem. For instance, for a secured communication over the internet for a financial transaction one needs that the instruction to the bank should not broken during the time the transaction is being made. Second point is that even though the data may be sent as ciphers over an insecure channel, initially a protocol needs to be established over a secured channel.

Ideally, a code can be said to be perfectly secure if one cannot get information about the plain text from the cipher text except by one who has a knowledge of the code. It may be remarked that no code is really unbreakable; given enough time every code can be broken. The closest example of an unbreakable code is **Vernam cipher** or a **one time pad**. As the name suggests, the code can be used once, and only once, so that no conclusion can be reached on the code by any repetitive pattern. From a more pedantic version of the pad in which the sender and the receiver agree to use the word sequence in a mutually agreed book to establish a code, a a more modern version consist of using a random sequence of binary digits as the code. For instance, suppose the plain text P is a string of binary digits $P_1, P_2, \ldots, P_n$ and the secret key K is a random sequence of binary digits $K_1, K_2, \ldots, K_n$, one can define the cipher text C to be given by $C_1, C_2, \ldots, C_n$ where

$$C_i = P_i \oplus K_i$$

where $\oplus$ stands for an addition modulo 2 for each i, as seen below

P	1001	1101	1010	1101
K	1100	1010	0110	1111
C	0101	0111	1100	0010

The plain text can be recovered from the cipher text by the inverse process $P = C \oplus K$. The code in practically unbreakable, if used only once. However if one uses it a second time, say for a plain text Q to get cipher text R, the code can be broken as then we have $C \oplus R = P \oplus Q$ and the plain texts usually have some redundancies to enable one to break it with this additional information.

RSA crypto-system was developed in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the MIT. The cryptosystem uses a public key encryption for securing and transmitting sensitive data over the internet. The public key is linked to a private decryption key which is only known to the person who receives the message. It also enables one to authenticate the sender's identity to the receiver. RSA uses what is known as a **trap-door function**, f which is defined as a function which has two characteristics. The function f is easy to compute, i.e., it can be computed in polynomial time. However, the inverse of the function f^{-1} cannot be computed easily from a knowledge of f or vice versa. The name trapdoor function has its origin in the fact that it is easy to fall through a trap door but is not easy to climb back to where one dropped from. (A closely related function is a *hash function* which is almost impossible to invert.) In RSA the trap-door function is multiplication of two large prime numbers, which is obviously easy to compute. However, given the product, there is no known algorithm which can achieve prime factorization in a polynomial time. Euclid's algorithm for factorization (given in the Appendix below) requires of the order of $\sqrt{N}$ steps.

In deriving the encryption decryption we would need a few theorem from number theory.

Fermat's Little Theorem:

For an prime number p and any integer $a \in \mathbb{Z}$ such that $a \neq 0 \mod p$, i.e. p does not divide a

$$a^{p-1} = 1 \mod p$$

Consider a set S with elements $1, 2, 3 \ldots, (p-1)$. Let r and s be some integers in S, i.e., in the range $1, 2, \ldots (p-1)$. Suppose $ra = sa \mod p$. Thus $(r-s)a = kp$, for some integer k. Since p does not divide a, it must divide $r-s$, so that $r = s \mod p$. However, since both r and s are less than p, it implies that $r = s$. Thus if we multiply each element of S with a, we would generate a sequence S' with elements

$$S' = a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1)$$

No two elements of the above sequence can be the same as we have multiplied a with different integers. It follows that the elements of S', mod p must be identical to those of S, though they may be differently ordered. Hence

$$S = aS \mod p$$

We thus have

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-1) &= (a \cdot 1)(a \cdot 2)(a \cdot 3) \ldots (a \cdot (p-1)) \mod p \\ &= a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \mod p \end{aligned}$$

which implies

$$a^{p-1} = 1 \mod p \tag{1}$$

Euler's Theorem:

We define **Euler's totient function** $\phi(n)$ corresponding to any positive integer n as the number of integers less than n which are relatively prime to n, i.e. which do not have any common factor with n. The number 1 is counted as a member of this set. For instance,corresponding to the number 18, the integers which do not have common factors with 25 are 1,5,7,11,13 and 17, so that $\phi(18) = 6$. Euler's theorem state that for any positive integer m, and an integer a such that a is coprime with m, we have

$$a^{\phi(m)} = 1 \text{ mod } m$$

The proof of Euler's theorem is similar to that given for Fermat's Little theorem. Consider the set of all numbers less than m which are co-prime to m. By definition of the totient function, there are $\phi(m)$ of them:

$$S = (1 \equiv b_1, b_2, \ldots, b_{\phi(m)})$$

where $b_1 < b_2 < \ldots < b_{\phi(m)}$.(Note that if m is a prime, the numbers are simply $1, 2, \ldots (m-1)$. If we multiply the elements of S by a, we would get a set S' whose elements, modulo m are the same as those of S, by argument parallel to that given in Fermat's theorem. Thus $aS = a^{\phi(m)}S$ which gives

$$a^{\phi(m)} = 1 \mod m \tag{2}$$

Chinese Remainder Theorem:
If a set of integers $m_1, m_2, \ldots, m_k$ are relatively primes (i.e., no pair of them have any common factors) and $a_1, a_2, \ldots, a_k$ are integers, then the system of equations

$$x = a_i \mod m_i \text{ for } 1 \le i \le k$$

has a unique solution mod $M = m_1 \cdot m_2 \cdots m_k$ and the solution is given by

$$x = \sum_{i=1}^{k} a_i M_i y_i$$

where $M_i = M/m_i$ and $y_i = (M_i^{-1})\text{mod } m_i$.

Before giving a formal proof we will illustrate the theorem with an example. Consider the system of equations

$$\begin{aligned} x &= 5 \text{ (mod 7)} \\ x &= 3 \text{ (mod 11)} \\ x &= 10 \text{ (mod 13)} \end{aligned}$$

According to the Chinese remainder theorem, this set of equations has a unique solution, which can be obtained as follows. First we calculate $M = 7 \times 11 \times 13 = 1001$. The final solution will consist of sum of three terms, mod 1001. To obtain each term, we calculate $M - 1, M_2$ and M_3

$$\begin{aligned} M_1 &= 11 \times 13 = 143 \\ M_2 &= 7 \times 13 = 91 \\ M_3 &= 7 \times 11 = 77 \end{aligned}$$

We then calculate y_1, y_2 and y_3.

$$y_1 = (M_1)^{-1} \mod m_1 = (143)^{-1} \mod 7$$

The solution for y_1 is given by

$$143y_1 = 1 \bmod 7$$

which gives $y_1 = 5$. One can, in a similar fashion obtain $y_2 = 4$ and $y_3 = -1$. The unique solution of the set of equations is then

$$\begin{aligned} x &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \\ &= 5 \cdot 143 \cdot 5 + 3 \cdot 91 \cdot 4 + 10 \cdot 77 \cdot (-1) = 4667 \end{aligned}$$

As the solution is modulus 1001, the final solution is $x = 894 \bmod 1001$. The formal proof of the theorem is obvious. Note that $M_i = M/m_i = \prod_{j\neq i} m_j$. Thus $gcd(M_i, m_i) = 1$. By the the Extended Euclid's algorithm, this implies we can find an integer y_i such that

$$M_iy_i = 1(\text{mod } m_i) \tag{3}$$

Note that, if we have n equations,

$$x = a_1M_1y_1 + a_2M_2y_2 + \ldots + a_kM_ky_k$$

satisfies each of the congruences. This is because the i-th equation is given modulo m_i. So that in the above sum, each term, other than the i-th term has m_i as a factor in the definition of $M_j \ \ (j \neq i)$, as a result of which each term is zero modulo m_i. For the $i-$th term we have $x = a_iM_iy_i$, which equals a_i modulo m_i by virtue of (4).

It is easy to show that the solution is unique. Suppose x_0 and x' are two solutions of the equation system

$$x = a_i \ (\text{mod } m_i) \ \ \forall i = 1, 2, \ldots k$$

Each m_i then divides $x' - x_0$. However, each pair of m_i and m_j are coprimes. Thus we must have,

$$\begin{aligned} x' - x_0 &= m_1N_1 \\ x' - x_0 &= m_2N_2 \\ &\cdots\cdots \\ x' - x_0 &= m_kN_k \end{aligned}$$

where, $N_1, N_2, \ldots$ are integers. This implies $x' - x_0 = 0 \ (\text{mod } m_1m_2 \ldots m_k)$, i.e. $x' = x_0$.

RSA Encryption and Decryption

Consider two primes p and q, whose product N is easily computable and is publicly known, though p and q remain private for the receiver (Bob). Note that Euler's totient function ϕ for p is $p-1$ and for q is $q-1$ as being primes, each number which less than p is coprime with p and likewise for q. The totient function for $N = pq$ is $\phi(N) = (p-1)(q-1)$ because each multiple of p and q are to be subtracted from $N-1$ to get $\phi(N)$. As there are $(p-1)$ multiples of q less than N and $(q-1)$ multiples of P which are less than N. Thus the totient function of N is

$$\phi(N) = (N-1) - [(p-1)+(q-1)] = pq - p - q + 1 = (p-1)(q-1)$$

[Example $N = 35 = 7 \times 5$. $\phi(7) = 6$ and $\phi(5) = 4$. Between 1 to 34, there are 4 factors of 7 and 6 factors of 5, i.e. a total of 10 numbers which are not cop rime to 35. Hence $\phi(35) = 34 - 10 = 24 = (7-1)(5-1)$.]

For encryption, we choose a number e which is coprime with N, i.e. with $(p-1)(q-1)$. Note that since p and q are known only to Bob, without factorizing N (which is hard), no one else can find $\phi(N)$. According to Euler's theorem, if we choose e to be coprime with $\phi(N)$, we have, by definition of coprimes,

$$gcd(e, \phi(N)) = 1$$

Once e is chosen, Bob can publish (e, N) as his public code and any sender, such as Alice will then have to encode the message m which she wishes to send to Bob by this encoder e, i.e. compute the cipher c corresponding to m as

$$c = m^e \pmod{N}$$

Bob also computes the decoder d which satisfies

$$ed = 1 \pmod{\phi(N)}$$

which implies $ed = k\phi(N) + 1$. Note once again that only Bob has a knowledge of $\phi(N)$ and he can easily find such a d. Since, for any m, we must get back the original m from c by raising c to the power d, we must have

$$c^d = m^{ed} = m \mod N$$

or, equivalently,

$$m^{ed-1} = 1 \implies m^{k\phi(N)} = 1$$

Let us rewrite the above condition as

$$(m^{k(p-1)})^{(q-1)} = 1$$

We have two cases. If m is not a multiple of q, we have by Fermat's little theorem

$$(m^{k(p-1)})^{(q-1)} = 1 \pmod{q}$$

Suppose, on the other hand, m is a multiple of q then $m^{de} = 1$ (mod q. By interchanging p and q and using parallel argument, we have

$$(m^{k(q-1)})^{(p-1)} = 1 \pmod{p}$$

if p does not divide m and $m^{de} = 1$ if p divides m. Since p and q are both primes, we have $m^{de} = 1 \pmod N$. We have shown that $x =\equiv (m^e)^d = m \bmod p$ and $x =\equiv (m^e)^d = m \bmod q$. By the Chinese remainder theorem, the solution is unique.

Example:

Let $p = 11$ and $q = 3$, so that $N = 33$. We have $(p-1)(q-1) = 10 \times 2 = 20$. We choose $e = 7$ which is coprime with $(p-1)(q-1)$. The pair $(e, N) = (7, 33)$ are public. The decryption is obtained by taking $ed = 1$, mod 20, which makes $d = 3$.

Let us use it to encrypt $m = 6$. We have

$$\begin{aligned} c &= m^2 \bmod 33 \\ &= (6)^7 = 30 \end{aligned}$$

To decrypt $c = 30$, we use $d = 3$. We have

$$c^d = 30^3 \bmod 33 = (-3)^3 \bmod 33 = -27 \bmod 33 = 6$$

which is what we started with.

APPENDIX

Euclid's Algorithm:

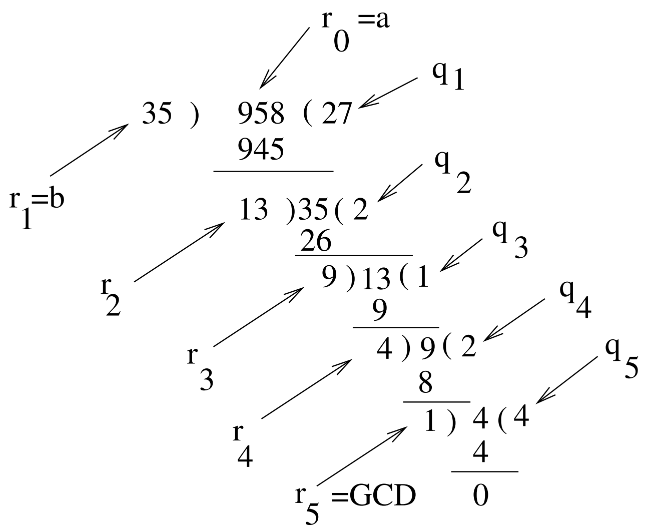
Euclid's algorithm calculates the greatest common divisor (gcd) of two numbers a and b. Note that the greatest common divisor, by definition, is the greatest number which is a factor of both a and b. The algorithm is based on two observations. Let $b < a$.

1. If b divides a then $gcd(a, b) = b$, because b is the largest factor of itself.
2. If b does not divide a, then let us divide a by b with q as the quotient and r as the remainder: $a = qb + r$. Clearly, a common factor of a and b will also be a common factor of r with b. Thus $gcd(a, b) = gcd(b, r)$.

Euler's algorithm uses the above to devise an algorithm of repeated division till the division terminates. An example will illustrate the process. Consider the gcd of 35 with 84.

84	= 35× 2 + 14	gcd(84,35)= gcd(35,14)
35	=14× 2 + 7	gcd(35,14)= gcd(14,7)
14	= 7× 2	gcd(14,7)= 7

Yet another example, consider gcd of 958 and 35.



Euler's algorithm starts by defining $r_0 = a$ and $r_1 = b$. We define the successive long divisions by the recursive formula

$$r_{i+1} = r_{i-1} - q_i r_i$$

The algorithm ends when $r_n = 0$. The GCD is given by r_{n-1}. In the above example

$$\begin{aligned}
r_0 &= a = 958 \\
r_1 &= b = 35 \\
r_2 &= 958 - 27 \times 35 = 13 \\
r_3 &= 35 - 2 \times 13 = 9 \\
r_4 &= 13 - 1 \times 9 = 4 \\
r_5 &= 9 - 2 \times 4 = 1
\end{aligned}$$

The algorithm ends in the next step, giving $r_6 = 0$ so that the gcd is $r_5 = 1$.

Corollary: Extended Euler Algorithm

For two integers a and b, one can always find two integers x and y such that $ax + by = gcd(a, b)$, i.e. $ax = gcd(a, b)$ mod b. (The proof of this is found in any algebra text book. Though the pair x and y may not be unique, written in the second form (i.e. in terms of mod b, the integer x is unique).

The algorithm works the same way as the Euler's algorithm. However, we run the sequence backward to get the gcd of a and b in terns of a and b. In the example above, the gcd is $r_5 = 1$. We can write,

$$\begin{aligned} r_5 = 1 &= 9 - 2 \times (4) \\ &= 9 - 2 \times (13 - 1 \times 9) = 3 \times 9 - 2 \times 13 \\ &= 3 \times (35 - 2 \times 13) - 2 \times 13 = 3 \times 35 - 8 \times 13 \\ &= 3 \times 35 - 8 \times (958 - 27 \times 35) \\ &= -8 \times 958 + 219 \times 35 \end{aligned}$$

Chinese Remainder Theorem:
If a set of integers $m_1, m_2, \ldots, m_k$ are relatively primes (i.e., no pair of them have any common factors) and $a_1, a_2, \ldots, a_k$ are integers, then the system of equations

$$x = a_i \mod m_i \text{ for } 1 \le i \le k$$

has a unique solution mod $M = m_1 \cdot m_2 \cdots m_k$ and the solution is given by

$$x = \sum_{i=1}^{k} a_i M_i y_i$$

where $M_i = M/m_i$ and $y_i = (M_i^{-1})\text{mod } m_i$.

Before giving a formal proof we will illustrate the theorem with an example. Consider the system of equations

$$\begin{aligned} x &= 5 \text{ (mod 7)} \\ x &= 3 \text{ (mod 11)} \\ x &= 10 \text{ (mod 13)} \end{aligned}$$

According to the Chinese remainder theorem, this set of equations has a unique solution, which can be obtained as follows. First we calculate $M = 7 \times 11 \times 13 = 1001$. The final solution will consist of sum of three terms, mod 1001. To obtain each term, we calculate $M - 1, M_2$ and M_3

$$\begin{aligned} M_1 &= 11 \times 13 = 143 \\ M_2 &= 7 \times 13 = 91 \\ M_3 &= 7 \times 11 = 77 \end{aligned}$$

We then calculate y_1, y_2 and y_3.

$$y_1 = (M_1)^{-1} \text{ mod } m_1 = (143)^{-1} \text{ mod } 7$$

The solution for y_1 is given by

$$143 y_1 = 1 \text{ mod } 7$$

which gives $y_1 = 5$. One can, in a similar fashion obtain $y_2 = 4$ and $y_3 = -1$. The unique solution of the set of equations is then

$$\begin{aligned} x &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \\ &= 5 \cdot 143 \cdot 5 + 3 \cdot 91 \cdot 4 + 10 \cdot 77 \cdot (-1) = 4667 \end{aligned}$$

As the solution is modulus 1001, the final solution is $x = 894 \bmod 1001$. The formal proof of the theorem is obvious. Note that $M_i = M/m_i = \prod_{j\neq i} m_j$. Thus $gcd(M_i, m_i) = 1$. By the the Extended Euclid's algorithm, this implies we can find an integer y_i such that

$$M_iy_i = 1(\text{mod } m_i) \tag{4}$$

Note that, if we have n equations,

$$x = a_1M_1y_1 + a_2M_2y_2 + \ldots + a_kM_ky_k$$

satisfies each of the congruences. This is because the i-th equation is given modulo m_i. So that in the above sum, each term, other than the i-th term has m_i as a factor in the definition of $M_j \ \ (j \neq i)$, as a result of which each term is zero modulo m_i. For the $i-$th term we have $x = a_iM_iy_i$, which equals a_i modulo m_i by virtue of (4).

It is easy to show that the solution is unique. Suppose x_0 and x' are two solutions of the equation system

$$x = a_i \text{ (mod } m_i) \ \ \forall i = 1, 2, \ldots k$$

Each m_i then divides $x' - x_0$. However, each pair of m_i and m_j are coprimes. Thus we must have,

$$\begin{aligned} x' - x_0 &= m_1N_1 \\ x' - x_0 &= m_2N_2 \\ &\cdots\cdots \\ x' - x_0 &= m_kN_k \end{aligned}$$

where, $N_1, N_2, \ldots$ are integers. This implies $x' - x_0 = 0 \text{ (mod } m_1m_2\ldots m_k)$, i.e. $x' = x_0$.

RSA Encryption and Decryption

Consider two primes p and q, whose product N is easily computable and is publicly known, though p and q remain private for the receiver (Bob). Note that Euler's totient function ϕ for p is $p-1$ and for q is $q-1$ as being primes, each number which less than p is coprime with p and likewise for q. The totient function for $N = pq$ is $\phi(N) = (p-1)(q-1)$ because each multiple of p and q are to be subtracted from $N-1$ to get $\phi(N)$. As there are $(p-1)$ multiples of q less than N and $(q-1)$ multiples of P which are less than N. Thus the totient function of N is

$$\phi(N) = (N-1) - [(p-1) + (q-1)] = pq - p - q + 1 = (p-1)(q-1)$$

[Example $N = 35 = 7 \times 5$. $\phi(7) = 6$ and $\phi(5) = 4$. Between 1 to 34, there are 4 factors of 7 and 6 factors of 5, i.e. a total of 10 numbers which are not cop rime to 35. Hence $\phi(35) = 34 - 10 = 24 = (7-1)(5-1)$.]
For encryption, we choose a number e which is coprime with N, i.e. with $(p-1)(q-1)$. Note that since p and q are known only to Bob, without factorizing N (which is hard), no one else can find $\phi(N)$. According to Euler's theorem, if we choose e to be coprime with $\phi(N)$, we have, by definition of coprimes,

$$gcd(e, \phi(N)) = 1$$

Once e is chosen, Bob can publish (e, N) as his public code and any sender, such as Alice will then have to encode the message m which she wishes to send to Bob by this encoder e, i.e. compute the cipher c corresponding to m as

$$c = m^e \pmod{N}$$

Bob also computes the decoder d which satisfies

$$ed = 1 \pmod{\phi(N)}$$

which implies $ed = k\phi(N) + 1$. Note once again that only Bob has a knowledge of $\phi(N)$ and he can easily find such a d. Since, for any m, we must get back the original m from c by raising c to the power d, we must have

$$c^d = m^{ed} = m \mod N$$

or, equivalently,

$$m^{ed-1} = 1 \implies m^{k\phi(N)} = 1$$

Let us rewrite the above condition as

$$(m^{k(p-1)})^{(q-1)} = 1$$

We have two cases. If m is not a multiple of q, we have by Fermat's little theorem

$$(m^{k(p-1)})^{(q-1)} = 1 \pmod{q}$$

Suppose, on the other hand, m is a multiple of q then $m^{de} = 1$ (mod q. By interchanging p and q and using parallel argument, we have

$$(m^{k(q-1)})^{(p-1)} = 1 \pmod{p}$$

if p does not divide m and $m^{de} = m$ if p divides m. Since p and q are both primes, we have $m^{de} = m$ (mod N). We have shown that $x =\equiv (m^e)^d = m \bmod p$ and $x =\equiv (m^e)^d = m \bmod q$. By the Chinese remainder theorem, the solution is unique.
Example:

Let $p = 11$ and $q = 3$, so that $N = 33$. We have $(p-1)(q-1) = 10 \times 2 = 20$. We choose $e = 7$ which is coprime with $(p-1)(q-1)$. The pair $(e, N) = (7, 33)$ are public. The decryption is obtained by taking $ed = 1$, mod 20, which makes $d = 3$.
Let us use it to encrypt $m = 6$. We have

$$\begin{aligned} c &= m^2 \text{ mod } 33 \\ &= (6)^7 = 30 \end{aligned}$$

To decrypt $c = 30$, we use $d = 3$. We have

$$c^d = 30^3 \text{ mod } 33 = (-3)^3 \text{mod } 33 = -27 \text{ mod } 33 = 6$$

which is what we started with.

APPENDIX

Euclid's Algorithm:
Euclid's algorithm calculates the greatest common divisor (gcd) of two numbers a and b. Note that the greatest common divisor, by definition, is the greatest number which is a factor of both a and b. The algorithm is based on two observations. Let $b < a$.

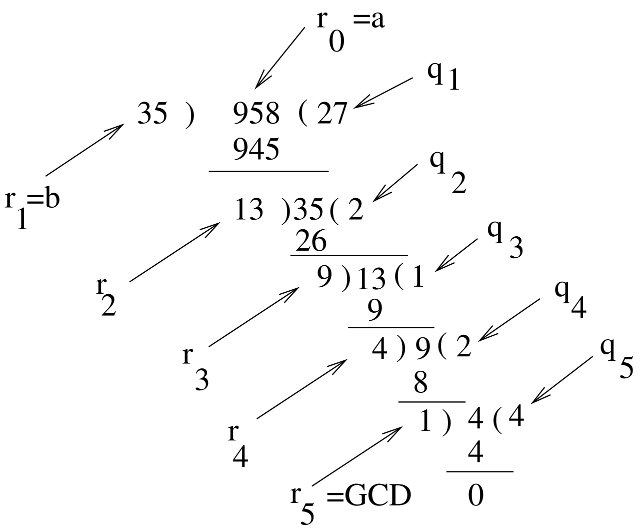
1. If b divides a then $gcd(a, b) = b$, because b is the largest factor of itself.

2. If b does not divide a, then let us divide a by b with q as the quotient and r as the remainder: $a = qb + r$. Clearly, a common factor of a and b will also be a common factor of r with b. Thus $gcd(a, b) = gcd(b, r)$.

Euler's algorithm uses the above to devise an algorithm of repeated division till the division terminates. An example will illustrate the process. Consider the gcd of 35 with 84.

84	= 35× 2 + 14	gcd(84,35)= gcd(35,14)
35	=14× 2 + 7	gcd(35,14)= gcd(14,7)
14	= 7× 2	gcd(14,7)= 7

Yet another example, consider gcd of 958 and 35.



Euler's algorithm starts by defining $r_0 = a$ and $r_1 = b$. We define the successive long divisions by the recursive formula

$$r_{i+1} = r_{i-1} - q_i r_i$$

The algorithm ends when $r_n = 0$. The GCD is given by r_{n-1}. In the above example

$$\begin{aligned}
r_0 &= a = 958\\
r_1 &= b = 35\\
r_2 &= 958 - 27 \times 35 = 13\\
r_3 &= 35 - 2 \times 13 = 9\\
r_4 &= 13 - 1 \times 9 = 4\\
r_5 &= 9 - 2 \times 4 = 1
\end{aligned}$$

The algorithm ends in the next step, giving $r_6 = 0$ so that the gcd is $r_5 = 1$.

Corollary: Extended Euler Algorithm

For two integers a and b, one can always find two integers x and y such that $ax + by = gcd(a, b)$, i.e. $ax = gcd(a, b) \bmod b$. (The proof of this is found in any algebra text book. Though the pair x and y may not be unique, written in the second form (i.e. in terms of mod b, the integer x is unique).

The algorithm works the same way as the Euler's algorithm. However, we run the sequence backward to get the gcd of a and b in terns of a and b. In the example above, the gcd is $r_5 = 1$. We can write,

$$\begin{aligned}
r_5 = 1 &= 9 - 2 \times (4) \\
&= 9 - 2 \times (13 - 1 \times 9) = 3 \times 9 - 2 \times 13 \\
&= 3 \times (35 - 2 \times 13) - 2 \times 13 = 3 \times 35 - 8 \times 13 \\
&= 3 \times 35 - 8 \times (958 - 27 \times 35) \\
&= -8 \times 958 + 219 \times 35
\end{aligned}$$