As the second example to illustrate how DSA digital signature algorithm works, let's try it with another prime divisor q=11 and prime modulus p=23.

The process of generating the public key and private key can be illustrated as:

q = 11 # selected prime divisor

p = 23 # computed prime modulus: (p-1) mod q = 0

g = 4 # computed: 1 < g < p, g\*\*q mod p = 1:

# and g = h\*\*((p–1)/q) mod p

# 4\*\*11 mod 23 = 1: 4194304 mod 23 = 1

x = 7 # selected: 0 < x < q

y = 8 # computed: y = g\*\*x mod p = 4\*\*7 mod 23

{23,11,4,8} # the public key: {p,q,g,y}

{23,11,4,7} # the private key: {p,q,g,x}

With the private key {p,q,g,x}={23,11,4,7}, the process of generating a digital signature out a message hash value of h=3 can be illustrated as:

h = 3 # the hash value as the message digest

k = 5 # selected: 0 < k < q

r = 1 # computed: r = (g\*\*k mod p) mod q = (4\*\*5 mod 23) mod 11

i = 9 # computed: k\*i mod q = 1: 5\*i mod 11 = 1

s = 2 # computed: s = i\*(h+r\*x) mod q = 9\*(3+1\*7) mod 11

{1,2} # the digital signature: {r,s}

The process of verifying the digital signature {r,s}={1,2} with the public key {p,q,g,y}={23,11,4,8} can be illustrated as:

h = 3 # the hash value as the message digest

w = 6 # computed: s\*w mod q = 1: 2\*w mod 11 = 1

u1 = 7 # computed: u1 = h\*w mod q = 3\*6 mod 11 = 7

u2 = 6 # computed: u2 = r\*w mod q = 1\*6 mod 11 = 6

v = 1 # computed: v = (((g\*\*u1)\*(y\*\*u2)) mod p) mod q

# = (((4\*\*7)\*(8\*\*6)) mod 23) mod 11 = 2

# = 16384\*262144 mod 23 mod 11 = 1

v == r # verification passed

Very nice. The verification value matches the expected value with no problem.