Finding a generator in $Z_p^* = \{1, 2, 3, \ldots, p-1\}$

For all $g \in \Gamma$, when Γ is a set of generators
$g^q \neq 1 \bmod p$; and $g^2 \neq 1 \bmod p$.

To compute $u/i \bmod (p-1)$ it is replaced by the following relation $u * i^{-1} \bmod (p-1)$ when gcd(i,p-1) = 1, since

$$u / i \bmod (p-1) = u * i^{-1} \bmod (p-1).$$

```
>> p=11;
>> i=8;
>> i_m1=mulinv(i,p-1)
i_m1 = Inverse element does not exist
>> gcd(i,p-1)  % gcd(8,10)=2 =/=1
ans = 2
>> i=9;
>> gcd(i,p-1)
ans = 1
>> i_m1=mulinv(i,p-1)
i_m1 = 9
>> mod(i*i_m1,p-1)
ans = 1
>> 1/9
ans = 0.1111
```

```
>> i=3;
>> i_m1=mulinv(i,p-1)
i_m1 = 7
>> mod(i*i_m1,p-1)
ans = 1
>> d*d_m1   % 3*7 = 21
ans = 21
>> mod(ans,p-1)   % mod(21,10) = 1
ans = 1
```

Example 1: Let for given integers u, x and h in $Z_{p-1} = \{0, 1, 2, \ldots, p-2\}$ we compute exponent s of generator g by the expression

$$s = u + xh.$$

Then

$$g^s \bmod p = g^{s \bmod (p-1)} \bmod p.$$

Therefore, s can be computed **mod** $(p-1)$ in advance, to save a multiplication operations, i.e.

$$s = u + xh \bmod (p-1).$$

```
>> p=genstrongprime(28)
p = 242502683
>> q=(p-1)/2
q = 121251341
>> isprime(q)
1                % therefore p is strong prime
                 % since p = 2*q +1 and q is prime
>> g=2   % find a generator in Z_p* = {1, 2, 3, ..., p-1}
g = 2
>> mod_exp(g,q,p)   % verification of criteria
                    % g^q ≠ 1 mod p;
                    % the second criteria is
                    % satisfied automatically
ans = 242502682
```

```
>> x=randi(p-1)
x = 4.8906e+07
>> x=int64(randi(p-1))
x = 165532552

>> u=int64(randi(p-1))
u = 74661797
>> h=int64(randi(p-1))
h = 194373549
>> xh=mod(x*h,p-1)
xh = 218184446
>> upxh=mod(u+xh,p-1)
upxh = 50343561
>> s=upxh
```

```
>> upxh=mod(u+x*h,p-1)
% check if the result is the same ??
upxh = 50343561

>> snr=int64(u+x*h)
snr = 32175149681928845
>> mod(snr,p-1)
ans = 50343561
```

s = 50343561

Example 2: Exponent ***s*** computation including subtraction by ***xr*** **mod** (***p***-1) and division by ***i*** in Z_{p-1} when gcd(***i***, ***p***-1) = 1.

$s = (h - xr)i^{-1} \bmod (p-1)$.

Firstly $d = xr \bmod (p-1)$ is computed:
Secondly $-d = -xr \bmod (p-1) = (p-1-d)$ is found.
Thirdly $i^{-1} \bmod (p-1)$ is found.
And finally exponent $s = (h + (p-1-d))i^{-1} \bmod (p-1)$ is computed.

```
>> x = int64(165532552)
x = 165532552
>> h = int64(194373549)
h = 194373549
>> r=int64(randi(p-1))
r = 212560238
>> xr=mod(x*r,p-1)
xr = 98263592
>> mxr=mod(-xr,p-1)
mxr = 144239090
>> xrpmr=mod(xr+mxr,p-1)
xrpmr = 0
>> hpmxr=mod(h+mxr,p-1)
hpmxr = 96109957
```

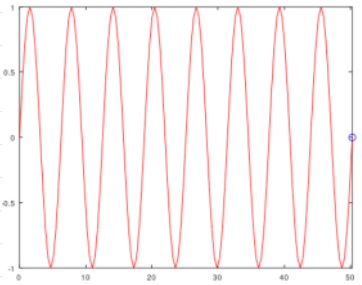
```
>> i=int64(randi(p-1))
i = 64538497
>> gcd(i,p-1)
ans = 1          % then i^-1 mod (p-1) exists

>> i_m1=mulinv(i,p-1)
i_m1 = 196196855
>> mod(i*i_m1,p-1)
ans = 1

>> s=mod(hpmxr*i_m1,p-1)
s = 131208547
```

p128sin.m

```
>> p128sin
xrange = 16 * pi;
step = xrange/128;
x = 0:step:xrange;
y = sin(x);
comet(x, y)
```



p128def.m

```
>> p128def    % Strong prime number  p=2*q+1 = 2*63+1
              % q is prime as well
p = 127;
g = 23;
x = 0:p-1;
a = mod_expv(g, x, p);
comet(x, a)
```