Cryptographic protocols
Exercise 3

Ilja Kuzovkin

December 31, 2010

1 Recover a shared secret

We have 10 parties and their shares. Any 4 of them can restore secret. We know that up to 3 parties may be adversaries and provide us with wrong shares. In the script you find in the attachment I restore secret in all 210 possible ways (combinations 4 out of 10). AS we can see in appendix B most often secret is being restored to 100, which means it is the original one. If result is not 100, then one or more parties involved in the process has to be corrupted. Just by looking on the output we can see that every time P_3, P_5 or P_9 are involved in the computation the result is not 100. If those parties are not present, secret is being restored to 100.
So I conclude: $v = 100$, parties P_1, P_2, P_4, P_6, P_7, P_8, P_10 are honest and P_3, P_5, P_9 are corrupted.

A Python script

```
import itertools

### http://en.wikipedia.org/wiki/Modular_multiplicative_inverse#Practical_
### Implementation_in_Python
def xgcd(a, b):
  x,y, u,v = 0,1, 1,0
  while a != 0:
    q,r = b/a,b%a; m,n = x-u*q,y-v*q
    b,a, x,y, u,v = a,r, u,v, m,n
  return b, x, y

def modinv(a, m):
  if (a < 0):
    a = a % m
  g, x, y = xgcd(a, m)
    if g != 1:
      return None
    else:
      return x % m


def lagrange(s1, s2, s3, s4, i1, i2, i3, i4, mod):
  return
    (s1 * (i2*modinv(i2-i1, mod)) * (i3*modinv(i3-i1, mod)) * (i4*modinv(i4-i1, mod)) +
     s2 * (i1*modinv(i1-i2, mod)) * (i3*modinv(i3-i2, mod)) * (i4*modinv(i4-i2, mod)) +
     s3 * (i1*modinv(i1-i3, mod)) * (i2*modinv(i2-i3, mod)) * (i4*modinv(i4-i3, mod)) +
```

```
     s4 * (i1*modinv(i1-i4, mod)) * (i2*modinv(i2-i4, mod)) * (i3*modinv(i3-i4, mod)))
     % mod

shares = [389, 834, 291, 527, 329, 404, 168, 779, 621, 144]

for comb in itertools.combinations(range(10), 4):
  print
    str(comb) + ' -> ' +
    'lagrange(' + str(shares[comb[0]]) + ', ' + str(shares[comb[1]]) +
    ', ' + str(shares[comb[2]]) + ', ' + str(shares[comb[3]]) + ', ' +
    str(comb[0] + 1) + ', ' + str(comb[1] + 1) + ', ' + str(comb[2] + 1) +
    ', ' + str(comb[3] + 1) + ', ' + str(911) + '))\t-> ' +
    str(lagrange(shares[comb[0]], shares[comb[1]], shares[comb[2]],
    shares[comb[3]], comb[0] + 1, comb[1] + 1, comb[2] + 1,
    comb[3] + 1, 911))
```

B Script output

```
(0, 1, 2, 3) -> lagrange(389, 834, 291, 527, 1, 2, 3, 4, 911)) -> 833
(0, 1, 2, 4) -> lagrange(389, 834, 291, 329, 1, 2, 3, 5, 911)) -> 667
(0, 1, 2, 5) -> lagrange(389, 834, 291, 404, 1, 2, 3, 6, 911)) -> 11
(0, 1, 2, 6) -> lagrange(389, 834, 291, 168, 1, 2, 3, 7, 911)) -> 136
(0, 1, 2, 7) -> lagrange(389, 834, 291, 779, 1, 2, 3, 8, 911)) -> 211
(0, 1, 2, 8) -> lagrange(389, 834, 291, 621, 1, 2, 3, 9, 911)) -> 864
(0, 1, 2, 9) -> lagrange(389, 834, 291, 144, 1, 2, 3, 10, 911)) -> 557
(0, 1, 3, 4) -> lagrange(389, 834, 527, 329, 1, 2, 4, 5, 911)) -> 694
(0, 1, 3, 5) -> lagrange(389, 834, 527, 404, 1, 2, 4, 6, 911)) -> 100
(0, 1, 3, 6) -> lagrange(389, 834, 527, 168, 1, 2, 4, 7, 911)) -> 100
(0, 1, 3, 7) -> lagrange(389, 834, 527, 779, 1, 2, 4, 8, 911)) -> 100
(0, 1, 3, 8) -> lagrange(389, 834, 527, 621, 1, 2, 4, 9, 911)) -> 336
(0, 1, 3, 9) -> lagrange(389, 834, 527, 144, 1, 2, 4, 10, 911)) -> 100
(0, 1, 4, 5) -> lagrange(389, 834, 329, 404, 1, 2, 5, 6, 911)) -> 120
(0, 1, 4, 6) -> lagrange(389, 834, 329, 168, 1, 2, 5, 7, 911)) -> 719
(0, 1, 4, 7) -> lagrange(389, 834, 329, 779, 1, 2, 5, 8, 911)) -> 615
(0, 1, 4, 8) -> lagrange(389, 834, 329, 621, 1, 2, 5, 9, 911)) -> 704
(0, 1, 4, 9) -> lagrange(389, 834, 329, 144, 1, 2, 5, 10, 911)) -> 714
(0, 1, 5, 6) -> lagrange(389, 834, 404, 168, 1, 2, 6, 7, 911)) -> 100
(0, 1, 5, 7) -> lagrange(389, 834, 404, 779, 1, 2, 6, 8, 911)) -> 100
(0, 1, 5, 8) -> lagrange(389, 834, 404, 621, 1, 2, 6, 9, 911)) -> 690
(0, 1, 5, 9) -> lagrange(389, 834, 404, 144, 1, 2, 6, 10, 911)) -> 100
(0, 1, 6, 7) -> lagrange(389, 834, 168, 779, 1, 2, 7, 8, 911)) -> 100
(0, 1, 6, 8) -> lagrange(389, 834, 168, 621, 1, 2, 7, 9, 911)) -> 677
(0, 1, 6, 9) -> lagrange(389, 834, 168, 144, 1, 2, 7, 10, 911)) -> 100
(0, 1, 7, 8) -> lagrange(389, 834, 779, 621, 1, 2, 8, 9, 911)) -> 638
(0, 1, 7, 9) -> lagrange(389, 834, 779, 144, 1, 2, 8, 10, 911)) -> 100
(0, 1, 8, 9) -> lagrange(389, 834, 621, 144, 1, 2, 9, 10, 911)) -> 794
(0, 2, 3, 4) -> lagrange(389, 291, 527, 329, 1, 3, 4, 5, 911)) -> 748
(0, 2, 3, 5) -> lagrange(389, 291, 527, 404, 1, 3, 4, 6, 911)) -> 278
(0, 2, 3, 6) -> lagrange(389, 291, 527, 168, 1, 3, 4, 7, 911)) -> 28
(0, 2, 3, 7) -> lagrange(389, 291, 527, 779, 1, 3, 4, 8, 911)) -> 789
(0, 2, 3, 8) -> lagrange(389, 291, 527, 621, 1, 3, 4, 9, 911)) -> 191
(0, 2, 3, 9) -> lagrange(389, 291, 527, 144, 1, 3, 4, 10, 911)) -> 97
```

```
(0, 2, 4, 5) -> lagrange(389, 291, 329, 404, 1, 3, 5, 6, 911)) -> 484
(0, 2, 4, 6) -> lagrange(389, 291, 329, 168, 1, 3, 5, 7, 911)) -> 309
(0, 2, 4, 7) -> lagrange(389, 291, 329, 779, 1, 3, 5, 8, 911)) -> 209
(0, 2, 4, 8) -> lagrange(389, 291, 329, 621, 1, 3, 5, 9, 911)) -> 504
(0, 2, 4, 9) -> lagrange(389, 291, 329, 144, 1, 3, 5, 10, 911)) -> 227
(0, 2, 5, 6) -> lagrange(389, 291, 404, 168, 1, 3, 6, 7, 911)) -> 64
(0, 2, 5, 7) -> lagrange(389, 291, 404, 779, 1, 3, 6, 8, 911)) -> 900
(0, 2, 5, 8) -> lagrange(389, 291, 404, 621, 1, 3, 6, 9, 911)) -> 516
(0, 2, 5, 9) -> lagrange(389, 291, 404, 144, 1, 3, 6, 10, 911)) -> 554
(0, 2, 6, 7) -> lagrange(389, 291, 168, 779, 1, 3, 7, 8, 911)) -> 800
(0, 2, 6, 8) -> lagrange(389, 291, 168, 621, 1, 3, 7, 9, 911)) -> 855
(0, 2, 6, 9) -> lagrange(389, 291, 168, 144, 1, 3, 7, 10, 911)) -> 725
(0, 2, 7, 8) -> lagrange(389, 291, 779, 621, 1, 3, 8, 9, 911)) -> 275
(0, 2, 7, 9) -> lagrange(389, 291, 779, 144, 1, 3, 8, 10, 911)) -> 281
(0, 2, 8, 9) -> lagrange(389, 291, 621, 144, 1, 3, 9, 10, 911)) -> 744
(0, 3, 4, 5) -> lagrange(389, 527, 329, 404, 1, 4, 5, 6, 911)) -> 220
(0, 3, 4, 6) -> lagrange(389, 527, 329, 168, 1, 4, 5, 7, 911)) -> 170
(0, 3, 4, 7) -> lagrange(389, 527, 329, 779, 1, 4, 5, 8, 911)) -> 457
(0, 3, 4, 8) -> lagrange(389, 527, 329, 621, 1, 4, 5, 9, 911)) -> 722
(0, 3, 4, 9) -> lagrange(389, 527, 329, 144, 1, 4, 5, 10, 911)) -> 140
(0, 3, 5, 6) -> lagrange(389, 527, 404, 168, 1, 4, 6, 7, 911)) -> 100
(0, 3, 5, 7) -> lagrange(389, 527, 404, 779, 1, 4, 6, 8, 911)) -> 100
(0, 3, 5, 8) -> lagrange(389, 527, 404, 621, 1, 4, 6, 9, 911)) -> 841
(0, 3, 5, 9) -> lagrange(389, 527, 404, 144, 1, 4, 6, 10, 911)) -> 100
(0, 3, 6, 7) -> lagrange(389, 527, 168, 779, 1, 4, 7, 8, 911)) -> 100
(0, 3, 6, 8) -> lagrange(389, 527, 168, 621, 1, 4, 7, 9, 911)) -> 258
(0, 3, 6, 9) -> lagrange(389, 527, 168, 144, 1, 4, 7, 10, 911)) -> 100
(0, 3, 7, 8) -> lagrange(389, 527, 779, 621, 1, 4, 8, 9, 911)) -> 331
(0, 3, 7, 9) -> lagrange(389, 527, 779, 144, 1, 4, 8, 10, 911)) -> 100
(0, 3, 8, 9) -> lagrange(389, 527, 621, 144, 1, 4, 9, 10, 911)) -> 39
(0, 4, 5, 6) -> lagrange(389, 329, 404, 168, 1, 5, 6, 7, 911)) -> 906
(0, 4, 5, 7) -> lagrange(389, 329, 404, 779, 1, 5, 6, 8, 911)) -> 20
(0, 4, 5, 8) -> lagrange(389, 329, 404, 621, 1, 5, 6, 9, 911)) -> 564
(0, 4, 5, 9) -> lagrange(389, 329, 404, 144, 1, 5, 6, 10, 911)) -> 40
(0, 4, 6, 7) -> lagrange(389, 329, 168, 779, 1, 5, 7, 8, 911)) -> 357
(0, 4, 6, 8) -> lagrange(389, 329, 168, 621, 1, 5, 7, 9, 911)) -> 763
(0, 4, 6, 9) -> lagrange(389, 329, 168, 144, 1, 5, 7, 10, 911)) -> 65
(0, 4, 7, 8) -> lagrange(389, 329, 779, 621, 1, 5, 8, 9, 911)) -> 374
(0, 4, 7, 9) -> lagrange(389, 329, 779, 144, 1, 5, 8, 10, 911)) -> 377
(0, 4, 8, 9) -> lagrange(389, 329, 621, 144, 1, 5, 9, 10, 911)) -> 153
(0, 5, 6, 7) -> lagrange(389, 404, 168, 779, 1, 6, 7, 8, 911)) -> 100
(0, 5, 6, 8) -> lagrange(389, 404, 168, 621, 1, 6, 7, 9, 911)) -> 495
(0, 5, 6, 9) -> lagrange(389, 404, 168, 144, 1, 6, 7, 10, 911)) -> 100
(0, 5, 7, 8) -> lagrange(389, 404, 779, 621, 1, 6, 8, 9, 911)) -> 222
(0, 5, 7, 9) -> lagrange(389, 404, 779, 144, 1, 6, 8, 10, 911)) -> 100
(0, 5, 8, 9) -> lagrange(389, 404, 621, 144, 1, 6, 9, 10, 911)) -> 403
(0, 6, 7, 8) -> lagrange(389, 168, 779, 621, 1, 7, 8, 9, 911)) -> 769
(0, 6, 7, 9) -> lagrange(389, 168, 779, 144, 1, 7, 8, 10, 911)) -> 100
(0, 6, 8, 9) -> lagrange(389, 168, 621, 144, 1, 7, 9, 10, 911)) -> 858
(0, 7, 8, 9) -> lagrange(389, 779, 621, 144, 1, 8, 9, 10, 911)) -> 401
(1, 2, 3, 4) -> lagrange(834, 291, 527, 329, 2, 3, 4, 5, 911)) -> 910
(1, 2, 3, 5) -> lagrange(834, 291, 527, 404, 2, 3, 4, 6, 911)) -> 812
```

```
(1, 2, 3, 6) -> lagrange(834, 291, 527, 168, 2, 3, 4, 7, 911)) -> 723
(1, 2, 3, 7) -> lagrange(834, 291, 527, 779, 2, 3, 4, 8, 911)) -> 123
(1, 2, 3, 8) -> lagrange(834, 291, 527, 621, 2, 3, 4, 9, 911)) -> 667
(1, 2, 3, 9) -> lagrange(834, 291, 527, 144, 2, 3, 4, 10, 911)) -> 88
(1, 2, 4, 5) -> lagrange(834, 291, 329, 404, 2, 3, 5, 6, 911)) -> 665
(1, 2, 4, 6) -> lagrange(834, 291, 329, 168, 2, 3, 5, 7, 911)) -> 901
(1, 2, 4, 7) -> lagrange(834, 291, 329, 779, 2, 3, 5, 8, 911)) -> 813
(1, 2, 4, 8) -> lagrange(834, 291, 329, 621, 2, 3, 5, 9, 911)) -> 815
(1, 2, 4, 9) -> lagrange(834, 291, 329, 144, 2, 3, 5, 10, 911)) -> 588
(1, 2, 5, 6) -> lagrange(834, 291, 404, 168, 2, 3, 6, 7, 911)) -> 867
(1, 2, 5, 7) -> lagrange(834, 291, 404, 779, 2, 3, 6, 8, 911)) -> 567
(1, 2, 5, 8) -> lagrange(834, 291, 404, 621, 2, 3, 6, 9, 911)) -> 905
(1, 2, 5, 9) -> lagrange(834, 291, 404, 144, 2, 3, 6, 10, 911)) -> 94
(1, 2, 6, 7) -> lagrange(834, 291, 168, 779, 2, 3, 7, 8, 911)) -> 167
(1, 2, 6, 8) -> lagrange(834, 291, 168, 621, 2, 3, 7, 9, 911)) -> 478
(1, 2, 6, 9) -> lagrange(834, 291, 168, 144, 2, 3, 7, 10, 911)) -> 778
(1, 2, 7, 8) -> lagrange(834, 291, 779, 621, 2, 3, 8, 9, 911)) -> 97
(1, 2, 7, 9) -> lagrange(834, 291, 779, 144, 2, 3, 8, 10, 911)) -> 824
(1, 2, 8, 9) -> lagrange(834, 291, 621, 144, 2, 3, 9, 10, 911)) -> 594
(1, 3, 4, 5) -> lagrange(834, 527, 329, 404, 2, 4, 5, 6, 911)) -> 420
(1, 3, 4, 6) -> lagrange(834, 527, 329, 168, 2, 4, 5, 7, 911)) -> 894
(1, 3, 4, 7) -> lagrange(834, 527, 329, 779, 2, 4, 5, 8, 911)) -> 141
(1, 3, 4, 8) -> lagrange(834, 527, 329, 621, 2, 4, 5, 9, 911)) -> 758
(1, 3, 4, 9) -> lagrange(834, 527, 329, 144, 2, 4, 5, 10, 911)) -> 814
(1, 3, 5, 6) -> lagrange(834, 527, 404, 168, 2, 4, 6, 7, 911)) -> 100
(1, 3, 5, 7) -> lagrange(834, 527, 404, 779, 2, 4, 6, 8, 911)) -> 100
(1, 3, 5, 8) -> lagrange(834, 527, 404, 621, 2, 4, 6, 9, 911)) -> 232
(1, 3, 5, 9) -> lagrange(834, 527, 404, 144, 2, 4, 6, 10, 911)) -> 100
(1, 3, 6, 7) -> lagrange(834, 527, 168, 779, 2, 4, 7, 8, 911)) -> 100
(1, 3, 6, 8) -> lagrange(834, 527, 168, 621, 2, 4, 7, 9, 911)) -> 331
(1, 3, 6, 9) -> lagrange(834, 527, 168, 144, 2, 4, 7, 10, 911)) -> 100
(1, 3, 7, 8) -> lagrange(834, 527, 779, 621, 2, 4, 8, 9, 911)) -> 628
(1, 3, 7, 9) -> lagrange(834, 527, 779, 144, 2, 4, 8, 10, 911)) -> 100
(1, 3, 8, 9) -> lagrange(834, 527, 621, 144, 2, 4, 9, 10, 911)) -> 351
(1, 4, 5, 6) -> lagrange(834, 329, 404, 168, 2, 5, 6, 7, 911)) -> 731
(1, 4, 5, 7) -> lagrange(834, 329, 404, 779, 2, 5, 6, 8, 911)) -> 494
(1, 4, 5, 8) -> lagrange(834, 329, 404, 621, 2, 5, 6, 9, 911)) -> 354
(1, 4, 5, 9) -> lagrange(834, 329, 404, 144, 2, 5, 6, 10, 911)) -> 851
(1, 4, 6, 7) -> lagrange(834, 329, 168, 779, 2, 5, 7, 8, 911)) -> 178
(1, 4, 6, 8) -> lagrange(834, 329, 168, 621, 2, 5, 7, 9, 911)) -> 299
(1, 4, 6, 9) -> lagrange(834, 329, 168, 144, 2, 5, 7, 10, 911)) -> 614
(1, 4, 7, 8) -> lagrange(834, 329, 779, 621, 2, 5, 8, 9, 911)) -> 845
(1, 4, 7, 9) -> lagrange(834, 329, 779, 144, 2, 5, 8, 10, 911)) -> 535
(1, 4, 8, 9) -> lagrange(834, 329, 621, 144, 2, 5, 9, 10, 911)) -> 603
(1, 5, 6, 7) -> lagrange(834, 404, 168, 779, 2, 6, 7, 8, 911)) -> 100
(1, 5, 6, 8) -> lagrange(834, 404, 168, 621, 2, 6, 7, 9, 911)) -> 222
(1, 5, 6, 9) -> lagrange(834, 404, 168, 144, 2, 6, 7, 10, 911)) -> 100
(1, 5, 7, 8) -> lagrange(834, 404, 779, 621, 2, 6, 8, 9, 911)) -> 509
(1, 5, 7, 9) -> lagrange(834, 404, 779, 144, 2, 6, 8, 10, 911)) -> 100
(1, 5, 8, 9) -> lagrange(834, 404, 621, 144, 2, 6, 9, 10, 911)) -> 272
(1, 6, 7, 8) -> lagrange(834, 168, 779, 621, 2, 7, 8, 9, 911)) -> 588
(1, 6, 7, 9) -> lagrange(834, 168, 779, 144, 2, 7, 8, 10, 911)) -> 100
```

```
(1, 6, 8, 9) -> lagrange(834, 168, 621, 144, 2, 7, 9, 10, 911)) -> 401
(1, 7, 8, 9) -> lagrange(834, 779, 621, 144, 2, 8, 9, 10, 911)) -> 788
(2, 3, 4, 5) -> lagrange(291, 527, 329, 404, 3, 4, 5, 6, 911)) -> 841
(2, 3, 4, 6) -> lagrange(291, 527, 329, 168, 3, 4, 5, 7, 911)) -> 880
(2, 3, 4, 7) -> lagrange(291, 527, 329, 779, 3, 4, 5, 8, 911)) -> 619
(2, 3, 4, 8) -> lagrange(291, 527, 329, 621, 3, 4, 5, 9, 911)) -> 644
(2, 3, 4, 9) -> lagrange(291, 527, 329, 144, 3, 4, 5, 10, 911)) -> 355
(2, 3, 5, 6) -> lagrange(291, 527, 404, 168, 3, 4, 6, 7, 911)) -> 388
(2, 3, 5, 7) -> lagrange(291, 527, 404, 779, 3, 4, 6, 8, 911)) -> 77
(2, 3, 5, 8) -> lagrange(291, 527, 404, 621, 3, 4, 6, 9, 911)) -> 708
(2, 3, 5, 9) -> lagrange(291, 527, 404, 144, 3, 4, 6, 10, 911)) -> 112
(2, 3, 6, 7) -> lagrange(291, 527, 168, 779, 3, 4, 7, 8, 911)) -> 877
(2, 3, 6, 8) -> lagrange(291, 527, 168, 621, 3, 4, 7, 9, 911)) -> 37
(2, 3, 6, 9) -> lagrange(291, 527, 168, 144, 3, 4, 7, 10, 911)) -> 566
(2, 3, 7, 8) -> lagrange(291, 527, 779, 621, 3, 4, 8, 9, 911)) -> 779
(2, 3, 7, 9) -> lagrange(291, 527, 779, 144, 3, 4, 8, 10, 911)) -> 474
(2, 3, 8, 9) -> lagrange(291, 527, 621, 144, 3, 4, 9, 10, 911)) -> 776
(2, 4, 5, 6) -> lagrange(291, 329, 404, 168, 3, 5, 6, 7, 911)) -> 561
(2, 4, 5, 7) -> lagrange(291, 329, 404, 779, 3, 5, 6, 8, 911)) -> 175
(2, 4, 5, 8) -> lagrange(291, 329, 404, 621, 3, 5, 6, 9, 911)) -> 804
(2, 4, 5, 9) -> lagrange(291, 329, 404, 144, 3, 5, 6, 10, 911)) -> 203
(2, 4, 6, 7) -> lagrange(291, 329, 168, 779, 3, 5, 7, 8, 911)) -> 875
(2, 4, 6, 8) -> lagrange(291, 329, 168, 621, 3, 5, 7, 9, 911)) -> 303
(2, 4, 6, 9) -> lagrange(291, 329, 168, 144, 3, 5, 7, 10, 911)) -> 409
(2, 4, 7, 8) -> lagrange(291, 329, 779, 621, 3, 5, 8, 9, 911)) -> 869
(2, 4, 7, 9) -> lagrange(291, 329, 779, 144, 3, 5, 8, 10, 911)) -> 857
(2, 4, 8, 9) -> lagrange(291, 329, 621, 144, 3, 5, 9, 10, 911)) -> 842
(2, 5, 6, 7) -> lagrange(291, 404, 168, 779, 3, 6, 7, 8, 911)) -> 33
(2, 5, 6, 8) -> lagrange(291, 404, 168, 621, 3, 6, 7, 9, 911)) -> 877
(2, 5, 6, 9) -> lagrange(291, 404, 168, 144, 3, 6, 7, 10, 911)) -> 333
(2, 5, 7, 8) -> lagrange(291, 404, 779, 621, 3, 6, 8, 9, 911)) -> 10
(2, 5, 7, 9) -> lagrange(291, 404, 779, 144, 3, 6, 8, 10, 911)) -> 287
(2, 5, 8, 9) -> lagrange(291, 404, 621, 144, 3, 6, 9, 10, 911)) -> 861
(2, 6, 7, 8) -> lagrange(291, 168, 779, 621, 3, 7, 8, 9, 911)) -> 676
(2, 6, 7, 9) -> lagrange(291, 168, 779, 144, 3, 7, 8, 10, 911)) -> 833
(2, 6, 8, 9) -> lagrange(291, 168, 621, 144, 3, 7, 9, 10, 911)) -> 346
(2, 7, 8, 9) -> lagrange(291, 779, 621, 144, 3, 8, 9, 10, 911)) -> 761
(3, 4, 5, 6) -> lagrange(527, 329, 404, 168, 4, 5, 6, 7, 911)) -> 242
(3, 4, 5, 7) -> lagrange(527, 329, 404, 779, 4, 5, 6, 8, 911)) -> 642
(3, 4, 5, 8) -> lagrange(527, 329, 404, 621, 4, 5, 6, 9, 911)) -> 53
(3, 4, 5, 9) -> lagrange(527, 329, 404, 144, 4, 5, 6, 10, 911)) -> 51
(3, 4, 6, 7) -> lagrange(527, 329, 168, 779, 4, 5, 7, 8, 911)) -> 568
(3, 4, 6, 8) -> lagrange(527, 329, 168, 621, 4, 5, 7, 9, 911)) -> 139
(3, 4, 6, 9) -> lagrange(527, 329, 168, 144, 4, 5, 7, 10, 911)) -> 451
(3, 4, 7, 8) -> lagrange(527, 329, 779, 621, 4, 5, 8, 9, 911)) -> 108
(3, 4, 7, 9) -> lagrange(527, 329, 779, 144, 4, 5, 8, 10, 911)) -> 888
(3, 4, 8, 9) -> lagrange(527, 329, 621, 144, 4, 5, 9, 10, 911)) -> 41
(3, 5, 6, 7) -> lagrange(527, 404, 168, 779, 4, 6, 7, 8, 911)) -> 100
(3, 5, 6, 8) -> lagrange(527, 404, 168, 621, 4, 6, 7, 9, 911)) -> 806
(3, 5, 6, 9) -> lagrange(527, 404, 168, 144, 4, 6, 7, 10, 911)) -> 100
(3, 5, 7, 8) -> lagrange(527, 404, 779, 621, 4, 6, 8, 9, 911)) -> 152
(3, 5, 7, 9) -> lagrange(527, 404, 779, 144, 4, 6, 8, 10, 911)) -> 100
```

```
(3, 5, 8, 9) -> lagrange(527, 404, 621, 144, 4, 6, 9, 10, 911)) -> 35
(3, 6, 7, 8) -> lagrange(527, 168, 779, 621, 4, 7, 8, 9, 911)) -> 191
(3, 6, 7, 9) -> lagrange(527, 168, 779, 144, 4, 7, 8, 10, 911)) -> 100
(3, 6, 8, 9) -> lagrange(527, 168, 621, 144, 4, 7, 9, 10, 911)) -> 214
(3, 7, 8, 9) -> lagrange(527, 779, 621, 144, 4, 8, 9, 10, 911)) -> 751
(4, 5, 6, 7) -> lagrange(329, 404, 168, 779, 5, 6, 7, 8, 911)) -> 309
(4, 5, 6, 8) -> lagrange(329, 404, 168, 621, 5, 6, 7, 9, 911)) -> 440
(4, 5, 6, 9) -> lagrange(329, 404, 168, 144, 5, 6, 7, 10, 911)) -> 29
(4, 5, 7, 8) -> lagrange(329, 404, 779, 621, 5, 6, 8, 9, 911)) -> 218
(4, 5, 7, 9) -> lagrange(329, 404, 779, 144, 5, 6, 8, 10, 911)) -> 740
(4, 5, 8, 9) -> lagrange(329, 404, 621, 144, 5, 6, 9, 10, 911)) -> 26
(4, 6, 7, 8) -> lagrange(329, 168, 779, 621, 5, 7, 8, 9, 911)) -> 833
(4, 6, 7, 9) -> lagrange(329, 168, 779, 144, 5, 7, 8, 10, 911)) -> 777
(4, 6, 8, 9) -> lagrange(329, 168, 621, 144, 5, 7, 9, 10, 911)) -> 707
(4, 7, 8, 9) -> lagrange(329, 779, 621, 144, 5, 8, 9, 10, 911)) -> 617
(5, 6, 7, 8) -> lagrange(404, 168, 779, 621, 6, 7, 8, 9, 911)) -> 783
(5, 6, 7, 9) -> lagrange(404, 168, 779, 144, 6, 7, 8, 10, 911)) -> 100
(5, 6, 8, 9) -> lagrange(404, 168, 621, 144, 6, 7, 9, 10, 911)) -> 385
(5, 7, 8, 9) -> lagrange(404, 779, 621, 144, 6, 8, 9, 10, 911)) -> 361
(6, 7, 8, 9) -> lagrange(168, 779, 621, 144, 7, 8, 9, 10, 911)) -> 329
```