Discrete Log Algorithms

The Index Calculus

Say we want to compute discrete logs relative to a primitive root for a prime that's not too large.

```
r:=random(10^5); p:=nextprime(r())
```

proc random() ... end

93281

```
alpha:=numlib::primroot(p)
```

3

```
for j from 15 to 2000 do
   t:=powermod(3,j,p):
   if max(numlib::primedivisors(t)) < 100 then
      print(j,t, ifactor(t)) end_if;
end_for
```

16, 44180, $2^2\ 5\ 47^2$

17, 39259, $11\ 43\ 83$

20, 33902, $2\ 11\ 23\ 67$

31, 20252, $2^2\ 61\ 83$

32, 60756, $2^2\ 3\ 61\ 83$

33, 88987, $23\ 53\ 73$

70, 84506, $2\ 29\ 31\ 47$

87, 82289, $19\ 61\ 71$

91, 42458, $2\ 13\ 23\ 71$

112, 69296, $2^4\ 61\ 71$

115, 5372, 2^2 17 79

116, 16116, 2^2 3 17 79

117, 48348, 2^2 3^2 17 79

139, 14600, 2^3 5^2 73

140, 43800, 2^3 3 5^2 73

162, 79373, 7 17 23 29

173, 70577, 13 61 89

184, 51389, 13 59 67

192, 45695, 5 13 19 37

195, 21112, 2^3 7 13 29

196, 63336, 2^3 3 7 13 29

206, 12331, 11 19 59

207, 36993, 3 11 19 59

217, 38480, 2^4 5 13 37

222, 22540, 2^2 5 7^2 23

223, 67620, 2^2 3 5 7^2 23

228, 14204, 2^2 53 67

229, 42612, 2^2 3 53 67

231, 10384, 2^4 11 59

232, 31152, 2^4 3 11 59

233, 175, 5^2 7

234, 525, 3 5^2 7

235, 1575, 3^2 5^2 7

236, 4725, 3^3 5^2 7

237, 14175, 3^4 5^2 7

238, 42525, 3^5 5^2 7

244, 31433, 17 43^2

255, 38918, 2 11 29 61

276, 1435, 5 7 41

277, 4305, 3 5 7 41

278, 12915, 3^2 5 7 41

279, 38745, 3^3 5 7 41

291, 20167, $7\ 43\ 67$

292, 60501, $3\ 7\ 43\ 67$

319, 11767, $7\ 41^2$

320, 35301, $3\ 7\ 41^2$

329, 72695, $5\ 7\ 31\ 67$

331, 1288, $2^3\ 7\ 23$

332, 3864, $2^3\ 3\ 7\ 23$

333, 11592, $2^3\ 3^2\ 7\ 23$

334, 34776, $2^3\ 3^3\ 7\ 23$

337, 6142, $2\ 37\ 83$

338, 18426, $2\ 3\ 37\ 83$

339, 55278, $2\ 3^2\ 37\ 83$

342, 10, $2\ 5$

343, 30, $2\ 3\ 5$

344, 90, $2\ 3^2\ 5$

345, 270, $2\ 3^3\ 5$

346, 810, $2\ 3^4\ 5$

$347, 2430, 2\,3^5\,5$

$348, 7290, 2\,3^6\,5$

$349, 21870, 2\,3^7\,5$

$350, 65610, 2\,3^8\,5$

$357, 22892, 2^2\,59\,97$

$358, 68676, 2^2\,3\,59\,97$

$362, 59177, 17\,59^2$

$382, 24187, 19^2\,67$

$383, 72561, 3\,19^2\,67$

$385, 82, 2\,41$

$386, 246, 2\,3\,41$

$387, 738, 2\,3^2\,41$

$388, 2214, 2\,3^3\,41$

$389, 6642, 2\,3^4\,41$

$390, 19926, 2\,3^5\,41$

$391, 59778, 2\,3^6\,41$

407, 20368, 2^4 19 67

408, 61104, 2^4 3 19 67

415, 56056, 2^3 7^2 11 13

418, 21016, 2^3 37 71

419, 63048, 2^3 3 37 71

432, 17152, 2^8 67

433, 51456, 2^8 3 67

438, 4154, 2 31 67

439, 12462, 2 3 31 67

440, 37386, 2 3^2 31 67

457, 53720, 2^3 5 17 79

466, 30625, 5^4 7^2

467, 91875, 3 5^4 7^2

468, 89063, 13^2 17 31

547, 72197, 23 43 73

555, 3599, 59 61

556, 10797, $3\ 59\ 61$

557, 32391, $3^2\ 59\ 61$

561, 11803, $11\ 29\ 37$

562, 35409, $3\ 11\ 29\ 37$

575, 1750, $2\ 5^3\ 7$

576, 5250, $2\ 3\ 5^3\ 7$

577, 15750, $2\ 3^2\ 5^3\ 7$

578, 47250, $2\ 3^3\ 5^3\ 7$

590, 88298, $2\ 7^2\ 17\ 53$

608, 41261, $11^3\ 31$

613, 45356, $2^2\ 17\ 23\ 29$

618, 14350, $2\ 5^2\ 7\ 41$

619, 43050, $2\ 3\ 5^2\ 7\ 41$

621, 14326, $2\ 13\ 19\ 29$

622, 42978, $2\ 3\ 13\ 19\ 29$

646, 12064, $2^5\ 13\ 29$

647, 36192, $2^5\ 3\ 13\ 29$

648, 15295, 5 7 19 23

649, 45885, 3 5 7 19 23

657, 33698, 2 7 29 83

661, 24389, 29^3

662, 73167, $3\ 29^3$

673, 12880, $2^4\ 5\ 7\ 23$

674, 38640, $2^4\ 3\ 5\ 7\ 23$

679, 61420, $2^2\ 5\ 37\ 83$

684, 100, $2^2\ 5^2$

685, 300, $2^2\ 3\ 5^2$

686, 900, $2^2\ 3^2\ 5^2$

687, 2700, $2^2\ 3^3\ 5^2$

688, 8100, $2^2\ 3^4\ 5^2$

689, 24300, $2^2\ 3^5\ 5^2$

690, 72900, $2^2\ 3^6\ 5^2$

727, 820, 2^2 5 41

728, 2460, 2^2 3 5 41

729, 7380, 2^2 3^2 5 41

730, 22140, 2^2 3^3 5 41

731, 66420, 2^2 3^4 5 41

742, 11524, 2^2 43 67

743, 34572, 2^2 3 43 67

757, 874, 2 19 23

758, 2622, 2 3 19 23

759, 7866, 2 3^2 19 23

760, 23598, 2 3^3 19 23

761, 70794, 2 3^4 19 23

770, 6724, 2^2 41^2

771, 20172, 2^2 3 41^2

772, 60516, 2^2 3^2 41^2

780, 41540, 2^2 5 31 67

781, 31339, $7\ 11^{2}\ 37$

782, 736, $2^{5}\ 23$

783, 2208, $2^{5}\ 3\ 23$

784, 6624, $2^{5}\ 3^{2}\ 23$

785, 19872, $2^{5}\ 3^{3}\ 23$

786, 59616, $2^{5}\ 3^{4}\ 23$

800, 25823, $7^{2}\ 17\ 31$

801, 77469, $3\ 7^{2}\ 17\ 31$

835, 57761, 11 59 89

841, 38038, 2 7 11 13 19

844, 935, 5 11 17

845, 2805, 3 5 11 17

846, 8415, $3^{2}\ 5\ 11\ 17$

847, 25245, $3^{3}\ 5\ 11\ 17$

848, 75735, $3^{4}\ 5\ 11\ 17$

857, 61625, $5^{3}\ 17\ 29$

$866, 32032, 2^5\ 7\ 11\ 13$

$877, 89474, 2\ 7^2\ 11\ 83$

$881, 64757, 7\ 11\ 29^2$

$887, 7667, 11\ 17\ 41$

$888, 23001, 3\ 11\ 17\ 41$

$889, 69003, 3^2\ 11\ 17\ 41$

$897, 35990, 2\ 5\ 59\ 61$

$905, 36179, 11^2\ 13\ 23$

$917, 17500, 2^2\ 5^4\ 7$

$918, 52500, 2^2\ 3\ 5^4\ 7$

$920, 6095, 5\ 23\ 53$

$921, 18285, 3\ 5\ 23\ 53$

$922, 54855, 3^2\ 5\ 23\ 53$

$926, 59048, 2^3\ 11^2\ 61$

$940, 15275, 5^2\ 13\ 47$

$941, 45825, 3\ 5^2\ 13\ 47$

$963, 49979, 23\ 41\ 53$

963, 49979, 23 41 53

982, 10658, $2\ 73^2$

983, 31974, $2\ 3\ 73^2$

992, 70616, $2^3\ 7\ 13\ 97$

1026, 1000, $2^3\ 5^3$

1027, 3000, $2^3\ 3\ 5^3$

1028, 9000, $2^3\ 3^2\ 5^3$

1029, 27000, $2^3\ 3^3\ 5^3$

1030, 81000, $2^3\ 3^4\ 5^3$

1041, 50456, $2^3\ 7\ 17\ 53$

1069, 8200, $2^3\ 5^2\ 41$

1070, 24600, $2^3\ 3\ 5^2\ 41$

1071, 73800, $2^3\ 3^2\ 5^2\ 41$

1099, 8740, $2^2\ 5\ 19\ 23$

1100, 26220, $2^2\ 3\ 5\ 19\ 23$

1101, 78660, $2^2\ 3^2\ 5\ 19\ 23$

1104, 71638, $2\ 7^2\ 17\ 43$

1108, 19256, 2^3 29 83

1109, 57768, 2^3 3 29 83

1112, 67240, 2^3 5 41^2

1113, 15158, 2 11 13 53

1114, 45474, 2 3 11 13 53

1124, 7360, 2^6 5 23

1125, 22080, 2^6 3 5 23

1126, 66240, 2^6 3^2 5 23

1137, 27166, 2 17^2 47

1138, 81498, 2 3 17^2 47

1142, 71668, 2^2 19 23 41

1151, 45962, 2 7^3 67

1164, 78242, 2 19 29 71

1167, 60352, 2^6 23 41

1186, 9350, 2 5^2 11 17

1187, 28050, 2 3 5^2 11 17

1188, 84150, $2\ 3^2\ 5^2\ 11\ 17$

1189, 65888, $2^5\ 29\ 71$

1190, 11102, 2 7 13 61

1191, 33306, 2 3 7 13 61

1195, 85918, $2\ 7\ 17\ 19^2$

1203, 10915, 5 37 59

1204, 32745, 3 5 37 59

1220, 72352, $2^5\ 7\ 17\ 19$

1226, 40843, 11 47 79

1229, 76670, 2 5 11 17 41

1232, 17908, $2^2\ 11^2\ 37$

1233, 53724, $2^2\ 3\ 11^2\ 37$

1245, 60928, $2^9\ 7\ 17$

1246, 89503, 37 41 59

1250, 67106, 2 13 29 89

1251, 14756, $2^2\ 7\ 17\ 31$

1252, 44268, $2^2\ 3\ 7\ 17\ 31$

1259, 81719, $11\ 17\ 19\ 23$

1262, 60950, $2\ 5^{2}\ 23\ 53$

1270, 90584, $2^{3}\ 13^{2}\ 67$

1277, 71645, $5\ 7\ 23\ 89$

1284, 68816, $2^{4}\ 11\ 17\ 23$

1292, 21736, $2^{3}\ 11\ 13\ 19$

1293, 65208, $2^{3}\ 3\ 11\ 13\ 19$

1298, 81055, $5\ 13\ 29\ 43$

1317, 18304, $2^{7}\ 11\ 13$

1318, 54912, $2^{7}\ 3\ 11\ 13$

1323, 4433, $11\ 13\ 31$

1324, 13299, $3\ 11\ 13\ 31$

1325, 39897, $3^{2}\ 11\ 13\ 31$

1328, 51128, $2^{3}\ 7\ 11\ 83$

1332, 37004, $2^{2}\ 11\ 29^{2}$

1340, 66082, $2\ 19\ 37\ 47$

1343, 11875, $5^{4}\ 19$

1343, 11875, 5^{4} 19

1344, 35625, 3 5^{4} 19

1358, 39479, 11 37 97

1365, 55648, 2^{5} 37 47

1368, 10000, 2^{4} 5^{4}

1369, 30000, 2^{4} 3 5^{4}

1370, 90000, 2^{4} 3^{2} 5^{4}

1386, 4094, 2 23 89

1387, 12282, 2 3 23 89

1388, 36846, 2 3^{2} 23 89

1411, 82000, 2^{4} 5^{3} 41

1418, 47918, 2 13 19 97

1421, 81133, 13 79^{2}

1434, 4945, 5 23 43

1435, 14835, 3 5 23 43

1436, 44505, 3^{2} 5 23 43

1441, 87400, 2^{3} 5^{2} 19 23

1443, 40352, 2^5 13 97

1458, 81577, 29^2 97

1466, 73600, 2^7 5^2 23

1467, 34238, 2 17 19 53

1472, 17825, 5^2 23 31

1473, 53475, 3 5^2 23 31

1477, 40549, 23 41 43

1483, 83425, 5^2 47 71

1484, 63713, 13^3 29

1492, 28832, 2^5 17 53

1493, 86496, 2^5 3 17 53

1496, 3367, 7 13 37

1497, 10101, 3 7 13 37

1498, 30303, 3^2 7 13 37

1499, 90909, 3^3 7 13 37

1523, 59885, 5 7 29 59

1527, 73, 73

1528, 219, 3 73

1529, 657, 3^{2} 73

1530, 1971, 3^{3} 73

1531, 5913, 3^{4} 73

1532, 17739, 3^{5} 73

1533, 53217, 3^{6} 73

1555, 40936, 2^{3} 7 17 43

1602, 26264, 2^{3} 7^{2} 67

1603, 78792, 2^{3} 3 7^{2} 67

1608, 23851, 17 23 61

1609, 71553, 3 17 23 61

1620, 3887, 13^{2} 23

1621, 11661, 3 13^{2} 23

1622, 34983, 3^{2} 13^{2} 23

1627, 12298, 2 11 13 43

1628, 36894, $2\ 3\ 11\ 13\ 43$

1632, 3422, $2\ 29\ 59$

1633, 10266, $2\ 3\ 29\ 59$

1634, 30798, $2\ 3^{2}\ 29\ 59$

1635, 92394, $2\ 3^{3}\ 29\ 59$

1641, 6344, $2^{3}\ 13\ 61$

1642, 19032, $2^{3}\ 3\ 13\ 61$

1643, 57096, $2^{3}\ 3^{2}\ 13\ 61$

1646, 49096, $2^{3}\ 17\ 19^{2}$

1656, 82786, $2\ 11\ 53\ 71$

1665, 44330, $2\ 5\ 11\ 13\ 31$

1671, 41344, $2^{7}\ 17\ 19$

1677, 10013, $17\ 19\ 31$

1678, 30039, $3\ 17\ 19\ 31$

1679, 90117, $3^{2}\ 17\ 19\ 31$

1696, 34816, $2^{11}\ 17$

1702, 8432, $2^{4}\ 17\ 31$

1703, 25296, 2^4 3 17 31

1704, 75888, 2^4 3^2 17 31

1728, 40940, 2^2 5 23 89

1733, 60634, 2 7 61 71

1746, 2209, 47^2

1747, 6627, 3 47^2

1748, 19881, 3^2 47^2

1749, 59643, 3^3 47^2

1754, 34694, 2 11 19 83

1760, 12775, 5^2 7 73

1761, 38325, 3 5^2 7 73

1776, 49450, 2 5^2 23 43

1779, 29216, 2^5 11 83

1780, 87648, 2^5 3 11 83

1816, 18473, 7^2 13 29

1817, 55419, 3 7^2 13 29

1838, 33670, $2\ 5\ 7\ 13\ 37$

1852, 9086, $2\ 7\ 11\ 59$

1853, 27258, $2\ 3\ 7\ 11\ 59$

1854, 81774, $2\ 3^{2}\ 7\ 11\ 59$

1866, 24211, $11\ 31\ 71$

1867, 72633, $3\ 11\ 31\ 71$

1869, 730, $2\ 5\ 73$

1870, 2190, $2\ 3\ 5\ 73$

1871, 6570, $2\ 3^{2}\ 5\ 73$

1872, 19710, $2\ 3^{3}\ 5\ 73$

1873, 59130, $2\ 3^{4}\ 5\ 73$

1905, 64408, $2^{3}\ 83\ 97$

1912, 5986, $2\ 41\ 73$

1913, 17958, $2\ 3\ 41\ 73$

1914, 53874, $2\ 3^{2}\ 41\ 73$

1947, 1924, $2^{2}\ 13\ 37$

1948, 5772, $2^{2}\ 3\ 13\ 37$

$1949,\ 17316,\ 2^2\ 3^2\ 13\ 37$

$1950,\ 51948,\ 2^2\ 3^3\ 13\ 37$

$1952,\ 1127,\ 7^2\ 23$

$1953,\ 3381,\ 3\ 7^2\ 23$

$1954,\ 10143,\ 3^2\ 7^2\ 23$

$1955,\ 30429,\ 3^3\ 7^2\ 23$

$1956,\ 91287,\ 3^4\ 7^2\ 23$

$1958,\ 75335,\ 5\ 13\ 19\ 61$

$1962,\ 38870,\ 2\ 5\ 13^2\ 23$

$1972,\ 55625,\ 5^4\ 89$

$1974,\ 34220,\ 2^2\ 5\ 29\ 59$

$1978,\ 66671,\ 11^2\ 19\ 29$

$1981,\ 27778,\ 2\ 17\ 19\ 43$

$1982,\ 83334,\ 2\ 3\ 17\ 19\ 43$

$1983,\ 63440,\ 2^4\ 5\ 13\ 61$

This is enough to compute discrete logs of some small numbers.
For example, 233=2*L(5)+L(7), 342=L(5)+L(2), 661=3*L(29), and 1972=4*L(5)+L(89) (all mod p-1 = 93280). So L(29) must be 3^{-1}*661 or:

```
_mod(powermod(3,-1,p-1)*661,p-1)
```

62407

Check:

```
powermod(3,%,p)
```

29

Then since 1458 = 2*L(29) + L(97), L(97) is:

```
_mod(1458-2*62407,p-1)
```

63204

Check:

```
powermod(3,%,p)
```

97

Baby Step, Giant Step Method

This time we first find N for the "giant steps".

```
N:=ceil(sqrt(p-1))
```

306

Say we want to find L(1374).

```
b:=1374
```

1374

```
firstlist := matrix(1,N):
firstlist[1,1]:=1:
for j from 2 to N do
   firstlist[1, j] := _mod(firstlist[1, j-1]*3, p):
end_for
```

78244

Now we compare b*alpha^{-Nk} with the numbers in the first list and look for a match.

```
t:=b:
c:=powermod(alpha, -N, p):
for k from 0 to N-1 do
   for j from 1 to N do
   if t = firstlist[1,j] then print(N*k+j-1); break; break;
   end_if; end_for;
t:=_mod(t*c, p):
end_for:
```

52943

Let's check:

```
powermod(alpha, 52943, p)
```

```
powermod(alpha, 52943, p)
```

1374

It works!