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.

```plaintext
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::primesdivisors(t)) < 100 then
        print(j, t, ifactor(t)) end_if;
end_for

  2  2
16, 44180, 2 5 47

17, 39259, 11 43 83

20, 33902, 2 11 23 67

  2
31, 20252, 2 61 83

  2
32, 60756, 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

  4
112, 69296, 2 61 71
```
115, 5372, 2 17 79

116, 16116, 2 3 17 79

117, 48348, 2 3 17 79

139, 14600, 2 5 73

140, 43800, 2 3 5 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 7 13 29

196, 63336, 2 3 7 13 29

206, 12331, 11 19 59

207, 36993, 3 11 19 59

217, 38480, 2 5 13 37

222, 22540, 2 5 7 23

223, 67620, 2 3 5 7 23
228, 14204, 2 53 67

229, 42612, 2 3 53 67

231, 10384, 2 11 59

232, 31152, 2 3 11 59

233, 175, 5 7

234, 525, 3 5 7

235, 1575, 3 5 7

236, 4725, 3 5 7

237, 14175, 3 5 7

238, 42525, 3 5 7

244, 31433, 17 43

255, 38918, 2 11 29 61

276, 1435, 5 7 41

277, 4305, 3 5 7 41

278, 12915, 3 5 7 41

279, 38745, 3 5 7 41
291, 20167, 7 43 67

292, 60501, 3 7 43 67

\[2\]
319, 11767, 7 41

\[2\]
320, 35301, 3 7 41

329, 72695, 5 7 31 67

\[3\]
331, 1288, 2 7 23

\[3\]
332, 3864, 2 3 7 23

\[3 \ 2\]
333, 11592, 2 3 7 23

\[3 \ 3\]
334, 34776, 2 3 7 23

337, 6142, 2 37 83

338, 18426, 2 3 37 83

\[2\]
339, 55278, 2 3 37 83

342, 10, 2 5

343, 30, 2 3 5

\[2\]
344, 90, 2 3 5

\[3\]
345, 270, 2 3 5

\[4\]
346, 810, 2 3 5
347, 2430, 2 3 5

348, 7290, 2 3 5

349, 21870, 2 3 5

350, 65610, 2 3 5

357, 22892, 2 59 97

358, 68676, 2 3 59 97

362, 59177, 17 59

382, 24187, 19 67

383, 72561, 3 19 67

385, 82, 2 41

386, 246, 2 3 41

387, 738, 2 3 41

388, 2214, 2 3 41

389, 6642, 2 3 41

390, 19926, 2 3 41

391, 59778, 2 3 41
407, 20368, 2 19 67

408, 61104, 2 3 19 67

415, 56056, 2 7 11 13

418, 21016, 2 37 71

419, 63048, 2 3 37 71

432, 17152, 2 67

433, 51456, 2 3 67

438, 4154, 2 31 67

439, 12462, 2 3 31 67

440, 37386, 2 3 31 67

457, 53720, 2 5 17 79

466, 30625, 5 7

467, 91875, 3 5 7

468, 89063, 13 17 31

547, 72197, 23 43 73

555, 3599, 59 61
556, 10797, 3 59 61

2
557, 32391, 3 59 61

561, 11803, 11 29 37

562, 35409, 3 11 29 37

3
575, 1750, 2 5 7

3
576, 5250, 2 3 5 7

2 3
577, 15750, 2 3 5 7

3 3
578, 47250, 2 3 5 7

2
590, 88298, 2 7 17 53

3
608, 41261, 11 31

2
613, 45356, 2 17 23 29

2
618, 14350, 2 5 7 41

2
619, 43050, 2 3 5 7 41

621, 14326, 2 13 19 29

622, 42978, 2 3 13 19 29

5
646, 12064, 2 13 29
647, 36192, $2^3 \cdot 13 \cdot 29$

648, 15295, $5 \cdot 7 \cdot 19 \cdot 23$

649, 45885, $3 \cdot 5 \cdot 7 \cdot 19 \cdot 23$

657, 33698, $2 \cdot 7 \cdot 29 \cdot 83$

661, 24389, $29$

662, 73167, $3 \cdot 29$

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

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

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

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

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

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

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

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

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

690, 72900, $2^2 \cdot 3 \cdot 5$
727, 820, \(2 \ 5 \ 41\)

728, 2460, \(2 \ 3 \ 5 \ 41\)

729, 7380, \(2 \ 3 \ 5 \ 41\)

730, 22140, \(2 \ 3 \ 5 \ 41\)

731, 66420, \(2 \ 3 \ 5 \ 41\)

742, 11524, \(2 \ 43 \ 67\)

743, 34572, \(2 \ 3 \ 43 \ 67\)

757, 874, \(2 \ 19 \ 23\)

758, 2622, \(2 \ 3 \ 19 \ 23\)

759, 7866, \(2 \ 3 \ 19 \ 23\)

760, 23598, \(2 \ 3 \ 19 \ 23\)

761, 70794, \(2 \ 3 \ 19 \ 23\)

770, 6724, \(2 \ 41\)

771, 20172, \(2 \ 3 \ 41\)

772, 60516, \(2 \ 3 \ 41\)

780, 41540, \(2 \ 5 \ 31 \ 67\)
781, 31339, 7 11 37

5
782, 736, 2 23

5
783, 2208, 2 3 23

5
784, 6624, 2 3 23

5
785, 19872, 2 3 23

5
786, 59616, 2 3 23

2
800, 25823, 7 17 31

2
801, 77469, 3 7 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

2
846, 8415, 3 5 11 17

3
847, 25245, 3 5 11 17

4
848, 75735, 3 5 11 17

3
857, 61625, 5 17 29
5
866, 32032, 2 7 11 13

2
877, 89474, 2 7 11 83

2
881, 64757, 7 11 29

887, 7667, 11 17 41

888, 23001, 3 11 17 41

2
889, 69003, 3 11 17 41

897, 35990, 2 5 59 61

2
905, 36179, 11 13 23

2 4
917, 17500, 2 5 7

2 4
918, 52500, 2 3 5 7

920, 6095, 5 23 53

921, 18285, 3 5 23 53

2
922, 54855, 3 5 23 53

3 2
926, 59048, 2 11 61

2
940, 15275, 5 13 47

2
941, 45825, 3 5 13 47

963, 49979, 23 41 53
963, 49979, 23 41 53

982, 10658, 2 73

983, 31974, 2 3 73

992, 70616, 2 7 13 97

1026, 1000, 2 5

1027, 3000, 2 3 5

1028, 9000, 2 3 5

1029, 27000, 2 3 5

1030, 81000, 2 3 5

1041, 50456, 2 7 17 53

1069, 8200, 2 5 41

1070, 24600, 2 3 5 41

1071, 73800, 2 3 5 41

1099, 8740, 2 5 19 23

1100, 26220, 2 3 5 19 23

1101, 78660, 2 3 5 19 23

1104, 71638, 2 7 17 43
1108, 19256, 2 29 83
1109, 57768, 2 3 29 83
1112, 67240, 2 5 41
1113, 15158, 2 11 13 53
1114, 45474, 2 3 11 13 53
1124, 7360, 2 5 23
1125, 22080, 2 3 5 23
1126, 66240, 2 3 5 23
1137, 27166, 2 17 47
1138, 81498, 2 3 17 47
1142, 71668, 2 19 23 41
1151, 45962, 2 7 67
1164, 78242, 2 19 29 71
1167, 60352, 2 23 41
1186, 9350, 2 5 11 17
1187, 28050, 2 3 5 11 17
1188, 84150, 2351117

1189, 65888, 22971

1190, 11102, 271361

1191, 33306, 2371361

1195, 85918, 271719

1203, 10915, 53759

1204, 32745, 353759

1220, 72352, 271719

1226, 40843, 114779

1229, 76670, 25111741

1232, 17908, 21137

1233, 53724, 231137

1245, 60928, 2717

1246, 89503, 374159

1250, 67106, 2132989

1251, 14756, 271731

1252, 44268, 2371731
1259, 81719, 11 17 19 23
1262, 60950, 2 5 23 53
1270, 90584, 2 13 67
1277, 71645, 5 7 23 89
1284, 68816, 2 11 17 23
1292, 21736, 2 11 13 19
1293, 65208, 2 3 11 13 19
1298, 81055, 5 13 29 43
1317, 18304, 2 11 13
1318, 54912, 2 3 11 13
1323, 4433, 11 13 31
1324, 13299, 3 11 13 31
1325, 39897, 3 11 13 31
1328, 51128, 2 7 11 83
1332, 37004, 2 11 29
1340, 66082, 2 19 37 47
1343, 11875, 5 19
<table>
<thead>
<tr>
<th>Number</th>
<th>Value</th>
<th>Count</th>
<th>Prime Factors</th>
<th>Last Two Digits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1343</td>
<td>11875</td>
<td>5</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>1344</td>
<td>35625</td>
<td>3 5</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>1358</td>
<td>39479</td>
<td>11</td>
<td>37 97</td>
<td></td>
</tr>
<tr>
<td>1365</td>
<td>55648</td>
<td>2 37</td>
<td>47</td>
<td></td>
</tr>
<tr>
<td>1368</td>
<td>10000</td>
<td>2</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>1369</td>
<td>30000</td>
<td>2 3 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1370</td>
<td>90000</td>
<td>2 3 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1386</td>
<td>4094</td>
<td>2 2 3</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td>1387</td>
<td>12282</td>
<td>2 3 23</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td>1388</td>
<td>36846</td>
<td>2 3 23</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td>1411</td>
<td>82000</td>
<td>2 5 41</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1418</td>
<td>47918</td>
<td>2 13 19</td>
<td>97</td>
<td></td>
</tr>
<tr>
<td>1421</td>
<td>81133</td>
<td>13 79</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1434</td>
<td>4945</td>
<td>5 23 43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1435</td>
<td>14835</td>
<td>3 5 23</td>
<td>43</td>
<td></td>
</tr>
<tr>
<td>1436</td>
<td>44505</td>
<td>3 5 23</td>
<td>43</td>
<td></td>
</tr>
<tr>
<td>1441</td>
<td>87400</td>
<td>2 5 19</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1443, 40352, 2</td>
<td>13</td>
<td>97</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1458, 81577, 29</td>
<td>97</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1466, 73600, 2</td>
<td>5</td>
<td>23</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 1467, 34238, 2 | 17 | 19 | 53 |
| 1472, 17825, 5 | 23 | 31 |
| 1473, 53475, 3 | 5 | 23 | 31 |

| 1477, 40549, 23 | 41 | 43 |
| 1483, 83425, 5 | 47 | 71 |

| 1484, 63713, 13 | 29 |
| 1492, 28832, 2 | 17 | 53 |

| 1493, 86496, 2 | 3 | 17 | 53 |

| 1496, 3367, 7 | 13 | 37 |
| 1497, 10101, 3 | 7 | 13 | 37 |

| 1498, 30303, 3 | 7 | 13 | 37 |

| 1499, 90909, 3 | 7 | 13 | 37 |

| 1523, 59885, 5 | 7 | 29 | 59 |
1527, 73, 73
1528, 219, 3 73
1529, 657, 3 73
1530, 1971, 3 73
1531, 5913, 3 73
1532, 17739, 3 73
1533, 53217, 3 73
1555, 40936, 2 7 17 43
1602, 26264, 2 7 67
1603, 78792, 2 3 7 67
1608, 23851, 17 23 61
1609, 71553, 3 17 23 61
1620, 3887, 13 23
1621, 11661, 3 13 23
1622, 34983, 3 13 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 29 59
1635, 92394, 2 3 29 59
1641, 6344, 2 13 61
1642, 19032, 2 3 13 61
1643, 57096, 2 3 13 61
1646, 49096, 2 17 19
1656, 82786, 2 11 53 71
1665, 44330, 2 5 11 13 31
1671, 41344, 2 17 19
1677, 10013, 17 19 31
1678, 30039, 3 17 19 31
1679, 90117, 3 17 19 31
1696, 34816, 2 17
1702, 8432, 2 17 31
1703, 25296, $2^4$ 3 17 31

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

1728, 40940, $2^2$ 5 23 89

1733, 60634, 2 7 61 71

1746, 2209, 47

1747, 6627, 3 47

1748, 19881, 3 47

1749, 59643, 3 47

1754, 34694, 2 11 19 83

1760, 12775, 5 7 73

1761, 38325, 3 5 7 73

1776, 49450, 2 5 23 43

1779, 29216, 2 11 83

1780, 87648, 2 3 11 83

1816, 18473, 7 13 29

1817, 55419, 3 7 13 29
<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
<th>Factor 1</th>
<th>Factor 2</th>
<th>Factor 3</th>
<th>Factor 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1838</td>
<td>33670</td>
<td>2 5 7 13 37</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1852</td>
<td>9086</td>
<td>2 7 11 59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1853</td>
<td>27258</td>
<td>2 3 7 11 59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1854</td>
<td>81774</td>
<td>2 3 7 11 59</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1866</td>
<td>24211</td>
<td>11 31 71</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1867</td>
<td>72633</td>
<td>3 11 31 71</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1869</td>
<td>730</td>
<td>2 5 73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1870</td>
<td>2190</td>
<td>2 3 5 73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1871</td>
<td>6570</td>
<td>2 3 5 73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1872</td>
<td>19710</td>
<td>2 3 5 73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1873</td>
<td>59130</td>
<td>2 3 5 73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1905</td>
<td>64408</td>
<td>2 83 97</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1912</td>
<td>5986</td>
<td>2 41 73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1913</td>
<td>17958</td>
<td>2 3 41 73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1914</td>
<td>53874</td>
<td>2 3 41 73</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1947</td>
<td>1924</td>
<td>2 13 37</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1948</td>
<td>5772</td>
<td>2 3 13 37</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1949, 17316, 2 3 13 37

1950, 51948, 2 3 13 37

1952, 1127, 7 23

1953, 3381, 3 7 23

1954, 10143, 3 7 23

1955, 30429, 3 7 23

1956, 91287, 3 7 23

1958, 75335, 5 13 19 61

1962, 38870, 2 5 13 23

1972, 55625, 5 89

1974, 34220, 2 5 29 59

1978, 66671, 11 19 29

1981, 27778, 2 17 19 43

1982, 83334, 2 3 17 19 43

1983, 63440, 2 5 13 61

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

$\mod\left(\text{powermod}(3,-1,p-1) \cdot 661,p-1\right)$
Check:
\[
powermod(3,\%,p)
\]
29

Then since \(1458 = 2L(29) + L(97)\), \(L(97)\) 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".
\[
N:=\text{ceil}(\sqrt{p-1})
\]
306

Say we want to find \(L(1374)\).
\[
b:=1374
\]
1374

\[
\text{firstlist := matrix}(1,N):
\text{firstlist}[1,1]:=1:
\text{for j from 2 to N do}
\quad \text{firstlist}[1, j] := \text{mod}(\text{firstlist}[1, j-1]*3, p):
\text{end_for}
\]
78244

Now we compare \(b^\alpha^{Nk}\) with the numbers in the first list and look for a match.
\[
t:=b:
\]
\[
c:=\text{powermod}(\alpha, -N, p):
\]
\text{for k from 0 to N-1 do}
\quad \text{for j from 1 to N do}
\quad \quad \text{if } t = \text{firstlist}[1,j] \text{ then print}(N\times k+j-1); \text{ break; break;}
\quad \text{end_if; end_for;}
\text{t:=\text{mod}(t*c, p)}:
\text{end_for:}
52943

Let's check:
\[
powermod(\alpha, 52943, p)
\]
\texttt{powermod(alpha, 52943, p)}

1374

It works!