アルゴリズム論特論 （塩田）

2013年7月18日　離散対数問題

mod p でのべき乗

```
mod 2:
powers of  1:  1

mod 3:
powers of  1:  1  1
powers of  2:  2  1 *

mod 5:
powers of  1:  1  1  1  1
powers of  2:  2  4  3  1 *
powers of  3:  3  4  2  1 *
powers of  4:  4  1  4  1

mod 7:
powers of  1:  1  1  1  1  1  1
powers of  2:  2  4  1  2  4  1
powers of  3:  3  2  6  4  5  1 *
powers of  4:  4  2  1  4  2  1
powers of  5:  5  4  6  2  3  1 *
powers of  6:  6  1  6  1  6  1

mod 11:
powers of  1:  1  1  1  1  1  1  1  1  1  1
powers of  2:  2  4  8  5 10  9  7  3  6  1 *
powers of  3:  3  9  5  4  1  3  9  5  4  1
powers of  4:  4  5  9  3  1  4  5  9  3  1
powers of  5:  5  3  4  9  1  5  3  4  9  1
powers of  6:  6  3  7  9 10  5  8  4  2  1 *
powers of  7:  7  5  2  3 10  4  6  9  8  1 *
powers of  8:  8  9  6  4 10  3  2  5  7  1 *
powers of  9:  9  4  3  5  1  9  4  3  5  1
powers of 10: 10  1 10  1 10  1 10  1 10  1

mod 13:
powers of  1:  1  1  1  1  1  1  1  1  1  1  1  1
powers of  2:  2  4  8  3  6 12 11  9  5 10  7  1 *
powers of  3:  3  9  1  3  9  1  3  9  1  3  9  1
powers of  4:  4  3 12  9 10  1  4  3 12  9 10  1
powers of  5:  5 12  8  1  5 12  8  1  5 12  8  1
powers of  6:  6 10  8  9  2 12  7  3  5  4 11  1 *
powers of  7:  7 10  5  9 11 12  6  3  8  4  2  1 *
powers of  8:  8 12  5  1  8 12  5  1  8 12  5  1
powers of  9:  9  3  1  9  3  1  9  3  1  9  3  1
powers of 10: 10  9 12  3  4  1 10  9 12  3  4  1
powers of 11: 11  4  5  3  7 12  2  9  8 10  6  1 *
powers of 12: 12  1 12  1 12  1 12  1 12  1 12  1
```

```
mod 17:
powers of  1:  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1
powers of  2:  2  4  8 16 15 13  9  1  2  4  8 16 15 13  9  1
powers of  3:  3  9 10 13  5 15 11 16 14  8  7  4 12  2  6  1 *
powers of  4:  4 16 13  1  4 16 13  1  4 16 13  1  4 16 13  1
powers of  5:  5  8  6 13 14  2 10 16 12  9 11  4  3 15  7  1 *
powers of  6:  6  2 12  4  7  8 14 16 11 15  5 13 10  9  3  1 *
powers of  7:  7 15  3  4 11  9 12 16 10  2 14 13  6  8  5  1 *
powers of  8:  8 13  2 16  9  4 15  1  8 13  2 16  9  4 15  1
powers of  9:  9 13 15 16  8  4  2  1  9 13 15 16  8  4  2  1
powers of 10: 10 15 14  4  6  9  5 16  7  2  3 13 11  8 12  1 *
powers of 11: 11  2  5  4 10  8  3 16  6 15 12 13  7  9 14  1 *
powers of 12: 12  8 11 13  3  2  7 16  5  9  6  4 14 15 10  1 *
powers of 13: 13 16  4  1 13 16  4  1 13 16  4  1 13 16  4  1
powers of 14: 14  9  7 13 12 15  6 16  3  8 10  4  5  2 11  1 *
powers of 15: 15  4  9 16  2 13  8  1 15  4  9 16  2 13  8  1
powers of 16: 16  1 16  1 16  1 16  1 16  1 16  1 16  1 16  1

mod 19:
powers of  1:  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1
powers of  2:  2  4  8 16 13  7 14  9 18 17 15 11  3  6 12  5 10  1 *
powers of  3:  3  9  8  5 15  7  2  6 18 16 10 11 14  4 12 17 13  1 *
powers of  4:  4 16  7  9 17 11  6  5  1  4 16  7  9 17 11  6  5  1
powers of  5:  5  6 11 17  9  7 16  4  1  5  6 11 17  9  7 16  4  1
powers of  6:  6 17  7  4  5 11  9 16  1  6 17  7  4  5 11  9 16  1
powers of  7:  7 11  1  7 11  1  7 11  1  7 11  1  7 11  1  7 11  1
powers of  8:  8  7 18 11 12  1  8  7 18 11 12  1  8  7 18 11 12  1
powers of  9:  9  5  7  6 16 11  4 17  1  9  5  7  6 16 11  4 17  1
powers of 10: 10  5 12  6  3 11 15 17 18  9 14  7 13 16  8  4  2  1 *
powers of 11: 11  7  1 11  7  1 11  7  1 11  7  1 11  7  1 11  7  1
powers of 12: 12 11 18  7  8  1 12 11 18  7  8  1 12 11 18  7  8  1
powers of 13: 13 17 12  4 14 11 10 16 18  6  2  7 15  5  8  9  3  1 *
powers of 14: 14  6  8 17 10  7  3  4 18  5 13 11  2  9 12 16 15  1 *
powers of 15: 15 16 12  9  2 11 13  5 18  4  3  7 10 17  8  6 14  1 *
powers of 16: 16  9 11  5  4  7 17  6  1 16  9 11  5  4  7 17  6  1
powers of 17: 17  4 11 16  6  7  5  9  1 17  4 11 16  6  7  5  9  1
powers of 18: 18  1 18  1 18  1 18  1 18  1 18  1 18  1 18  1 18  1

mod 23:
powers of  1:  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1
powers of  2:  2  4  8 16  9 18 13  3  6 12  1  2  4  8 16  9 18 13  3  6 12  1
powers of  3:  3  9  4 12 13 16  2  6 18  8  1  3  9  4 12 13 16  2  6 18  8  1
powers of  4:  4 16 18  3 12  2  8  9 13  6  1  4 16 18  3 12  2  8  9 13  6  1
powers of  5:  5  2 10  4 20  8 17 16 11  9 22 18 21 13 19  3 15  6  7 12 14  1 *
powers of  6:  6 13  9  8  2 12  3 18 16  4  1  6 13  9  8  2 12  3 18 16  4  1
powers of  7:  7  3 21  9 17  4  5 12 15 13 22 16 20  2 14  6 19 18 11  8 10  1 *
powers of  8:  8 18  6  2 16 13 12  4  9  3  1  8 18  6  2 16 13 12  4  9  3  1
powers of  9:  9 12 16  6  8  3  4 13  2 18  1  9 12 16  6  8  3  4 13  2 18  1
powers of 10: 10  8 11 18 19  6 14  2 20 16 22 13 15 12  5  4 17  9 21  3  7  1 *
powers of 11: 11  6 20 13  5  9  7  8 19  2 22 12 17  3 10 18 14 16 15  4 21  1 *
powers of 12: 12  6  3 13 18  9 16  8  4  2  1 12  6  3 13 18  9 16  8  4  2  1
powers of 13: 13  8 12 18  4  6  9  2  3 16  1 13  8 12 18  4  6  9  2  3 16  1
```

```
powers of 14: 14 12  7  6 15  3 19 13 21 18 22  9 11 16 17  8 20  4 10  2  5  1 *
powers of 15: 15 18 17  2  7 13 11  4 14  3 22  8  5  6 21 16 10 12 19  9 20  1 *
powers of 16: 16  3  2  9  6  4 18 12  8 13  1 16  3  2  9  6  4 18 12  8 13  1
powers of 17: 17 13 14  8 21 12 20 18  7  4 22  6 10  9 15  2 11  3  5 16 19  1 *
powers of 18: 18  2 13  4  3  8  6 16 12  9  1 18  2 13  4  3  8  6 16 12  9  1
powers of 19: 19 16  5  3 11  2 15  9 10  6 22  4  7 18 20 12 21  8 14 13 17  1 *
powers of 20: 20  9 19 12 10 16 21  6  5  8 22  3 14  4 11 13  7  2 17 18 15  1 *
powers of 21: 21  4 15 16 14 18 10  3 17 12 22  2 19  8  7  9  5 13 20  6 11  1 *
powers of 22: 22  1 22  1 22  1 22  1 22  1 22  1 22  1 22  1 22  1 22  1 22  1
```

mod p で底 a の生成する部分群 $\langle a \rangle$

```
mod 2:
< 1> =  [1] *

mod 3:
< 1> =  [1]
< 2> =  [1, 2] *

mod 5:
< 1> =  [1]
< 2> =  [1, 2, 3, 4] *
< 3> =  [1, 2, 3, 4] *
< 4> =  [1, 4]

mod 7:
< 1> =  [1]
< 2> =  [1, 2, 4]
< 3> =  [1, 2, 3, 4, 5, 6] *
< 4> =  [1, 2, 4]
< 5> =  [1, 2, 3, 4, 5, 6] *
< 6> =  [1, 6]

mod 11:
< 1> =  [1]
< 2> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] *
< 3> =  [1, 3, 4, 5, 9]
< 4> =  [1, 3, 4, 5, 9]
< 5> =  [1, 3, 4, 5, 9]
< 6> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] *
< 7> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] *
< 8> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10] *
< 9> =  [1, 3, 4, 5, 9]
<10> =  [1, 10]

mod 13:
< 1> =  [1]
< 2> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12] *
< 3> =  [1, 3, 9]
< 4> =  [1, 3, 4, 9, 10, 12]
< 5> =  [1, 5, 8, 12]
< 6> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12] *
< 7> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12] *
```

```
< 8> =  [1, 5, 8, 12]
< 9> =  [1, 3, 9]
<10> =  [1, 3, 4, 9, 10, 12]
<11> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12] *
<12> =  [1, 12]

mod 17:
< 1> =  [1]
< 2> =  [1, 2, 4, 8, 9, 13, 15, 16]
< 3> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] *
< 4> =  [1, 4, 13, 16]
< 5> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] *
< 6> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] *
< 7> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] *
< 8> =  [1, 2, 4, 8, 9, 13, 15, 16]
< 9> =  [1, 2, 4, 8, 9, 13, 15, 16]
<10> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] *
<11> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] *
<12> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] *
<13> =  [1, 4, 13, 16]
<14> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] *
<15> =  [1, 2, 4, 8, 9, 13, 15, 16]
<16> =  [1, 16]

mod 19:
< 1> =  [1]
< 2> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18] *
< 3> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18] *
< 4> =  [1, 4, 5, 6, 7, 9, 11, 16, 17]
< 5> =  [1, 4, 5, 6, 7, 9, 11, 16, 17]
< 6> =  [1, 4, 5, 6, 7, 9, 11, 16, 17]
< 7> =  [1, 7, 11]
< 8> =  [1, 7, 8, 11, 12, 18]
< 9> =  [1, 4, 5, 6, 7, 9, 11, 16, 17]
<10> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18] *
<11> =  [1, 7, 11]
<12> =  [1, 7, 8, 11, 12, 18]
<13> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18] *
<14> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18] *
<15> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18] *
<16> =  [1, 4, 5, 6, 7, 9, 11, 16, 17]
<17> =  [1, 4, 5, 6, 7, 9, 11, 16, 17]
<18> =  [1, 18]

mod 23:
< 1> =  [1]
< 2> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
< 3> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
< 4> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
< 5> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
< 6> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
< 7> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
< 8> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
```

```
< 9> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
<10> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
<11> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
<12> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
<13> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
<14> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
<15> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
<16> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
<17> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
<18> =  [1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]
<19> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
<20> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
<21> =  [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] *
<22> =  [1, 22]
```