1.
```
def past-pow(a, e, m):
    result = 1
    while (e > 0):
        if e%2==1:
            a = a%m
            result *= a
        a = a*a
        e// 2
    return result
```

result =

1726337951052995266587377453047496920693080667448691995741034764803416503319973

2.
```
def exgcd(a,b):
    if b==0:
    return a, 1, 0
    else:
        gcd, x1, y1 = exgcd(b, a%b)
        x = y1
        y = x1 - (a//b)* y1
        return gcd, x, y
```

x =
41200623673777417421300360372702978793016376279472912929714463504140441945848,
y =
-384881533506059102101273442177371406663360435678362140099629615416260579186964073750644039436519118410311121695688458737024479701617313453674615258279478204294408528818259213600898896667370118629882826262629841282161015461089211725392507 79

gcd = 1

3.

$s_i a + t_i b = r_i$

$s_{i+1} a + t_{i+1} b = r_{i+1}$

$s_{i+2} a + t_{i+2} b = r_{i+2}$

$r_i - \lfloor \frac{r_i}{r_{i+1}} \rfloor r_{i+1} = r_{i+2}$

$a(s_i t_{i+1} - t_i s_{i+1}) = r_i t_{i+1} - r_{i+1} t_i$

$r_i(s_{i+1} + t_{i+1}) = r_{i+1}(s_i + t_i)$

(1) $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$

$s_0 = 1 \quad t_0 = 0$

$s_1 = 0 \quad t_1 = 1$

$s_2 = s_0 - q_1 s_1 \quad t_2 = t_0 - q_1 t_1$

$s_0 t_1 - t_0 s_1 = 1$

$s_1 t_2 - t_1 s_2 = -(s_0 - q_1 s_1) = -1$

$s_i t_{i+1} - t_i s_{i+1} = (-1)^i$

$s_{i+1} t_{i+2} - t_{i+1} s_{i+2} = s_{i+1}(t_i - q t_{i+1}) - t_{i+1}(s_i - q s_{i+1})$

$= s_{i+1} t_i - t_{i+1} s_i$

$= -(s_i t_{i+1} - s_{i+1} t_i)$

So $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$

(2) $t_i t_{i+1} \le 0$ and $|t_i| \le |t_{i+1}|$

(归纳法)

$t_0 t_1 \le 0$

if $t_i t_{i-1} \le 0$, for $t_i t_{i+1}$:

$t_{i+1} = t_{i-1} - q_i t_i$

$\Rightarrow t_i t_{i+1} = t_i t_{i-1} - q_i t_i^2 \le 0$

$t_{i+1} = t_{i-1} - q t_i$

if $t_i > 0 \Rightarrow t_{i-1} < 0, -t_i < 0 \Rightarrow |t_{i+1}| = |t_{i-1}| + q|t_i|$

$\ge |t_i|$

else $t_i < 0 \Rightarrow t_{i-1} > 0, -t_i > 0 \quad |t_{i+1}| = |t_{i-1}| + q|t_i| \ge |t_i|$

4. $r_{i-1}|t_i| \le a$ and $|t_i| \le a$

in Problem 3.

$a(s_i t_{i+1} - t_i s_{i+1}) = r_i t_{i+1} - r_{i+1} t_i$

so $a = |r_i t_{i+1} - r_{i+1} t_i| = |r_i t_{i+1}| + |r_{i+1} t_i| \ge |r_i t_{i+1}|$

异号.

so $r_{i-1}|t_i| \le a$

hence $r_{i-1} \ge 1$. so $|t_i| \le a$.

5.

the number of iterations is bounded by : $O(\log b)$

This follows from the fact : $a_{i+1} = a_i \bmod a_{i-1}$

dividing an n-bit number by an m-bit number has complexity $O(nm)$ bit operations.

Thus, at each step, if a initially has $l(a)$ bits and b has $l(b)$ bits, the cost of computing a mod b is at most $O(l(a) l(b))$