Problem 1:

```
(%i1) p:53047;
(%o1) 53047

(%i2) a:3;
(%o2) 3

(%i3) b:8576;
(%o3) 8576

(%i4) x:1234;
(%o4) 1234

(%i5) power_mod(a, x, p);
(%o5) 8576
```

Problem 2:

```
(%i6) p:31;
(%o6) 31

(%i7) a:3;
(%o7) 3

(%i8) b:24;
(%o8) 24

(%i9) power_mod(b, 15, p);
(%o9) 30

(%i10) power_mod(a, 15, p);
(%o10) 30

(%i11) for k: 3 step 2 thru 29 do display( power_mod(a, k, p));
power_mod(3,3,31)=27
power_mod(3,5,31)=26
power_mod(3,7,31)=17
power_mod(3,9,31)=29
power_mod(3,11,31)=13
power_mod(3,13,31)=24
power_mod(3,15,31)=30
power_mod(3,17,31)=22
power_mod(3,19,31)=12
power_mod(3,21,31)=15
power_mod(3,23,31)=11
power_mod(3,25,31)=6
power_mod(3,27,31)=23
power_mod(3,29,31)=21
```

Problem 3:

```
(%o11) done

→ p:3989;
(%o12) 3989

→ a:2;
(%o13) 2

→ b1:3925;
(%o14) 3925

→ x1:2000;
(%o15) 2000

→ power_mod(a, x1, p);
(%o16) 3925

→ b2:1046;
(%o17) 1046

→ x2:3000;
(%o18) 3000

→ power_mod(a, x2, p);
(%o19) 1046

→ b3:b1·b2;
(%o20) 4105550

→ mod(b3, p);
(%o21) 869

→ x3:x1+x2;
(%o22) 5000
```

```
→ p:3989;
(%o12) 3989

→ a:2;
(%o13) 2

→ b1:3925;
(%o14) 3925

→ x1:2000;
(%o15) 2000

→ power_mod(a, x1, p);
(%o16) 3925

→ b2:1046;
(%o17) 1046

→ x2:3000;
(%o18) 3000

→ power_mod(a, x2, p);
(%o19) 1046

→ b3:b1·b2;
(%o20) 4105550

→ mod(b3, p);
(%o21) 869

→ x3:x1+x2;
(%o22) 5000

→ power_mod(a, x3, p);
(%o23) 869
```

Problem 4

```
(%i24) p:1201;
(%o24) 1201

(%i25) alpha:11;
(%o25) 11

(%i26) f(x):=power_mod(alpha, (p−1)/x, p);
(%o26) f(x):=power_mod(alpha, (p−1)/x, p)

(%i27) for i in [2, 3, 5] do display(f(i));
                              f(2)=1200
                               f(3)=570
                              f(5)=1062
(%o27)                         done

(%i28) f(1);
(%o28) 1

(%i29) gcd(1200, p);
(%o29) 1

(%i30) gcd(2, p);
(%o30) 1

(%i31) gcd(3, p);
(%o31) 1

(%i32) gcd(5, p);
(%o32) 1

(%i33) power_mod(alpha, (p−1)/2, p);
(%o33) 1200
```

```
(%o45) 1200

→ x1:1;
(%o46) 1

→ beta2:mod(beta1·power_mod(inv_mod(alpha, p), q·x1, p), p);
(%o47) 729

→ power_mod(beta2, (p−1)/(q^3), p);
(%o48) 1

→ power_mod(alpha, (p−1)/2, p);
(%o49) 1200

→ x2:2;
(%o50) 2

→ beta3:mod(beta2·power_mod(inv_mod(alpha, p), q^2·x2, p), p
(%o51) 177

→ power_mod(beta2, (p−1)/(q^4), p);
(%o52) 1200

→ power_mod(alpha, (p−1)/2, p);
(%o53) 1200

→ x3:1;
(%o54) 1

→ x:mod(x0+2·x1+4·x2+8·x3, 16);
(%o55) 4

→ q:3;
(%o56) 3

→ r:1;
```

```
→ r:1;
(%o57) 1

→ power_mod(beta, (p−1)/q, p);
(%o58) 570

→ power_mod(alpha, (p−1)/q, p);
(%o59) 570

→ x0:1;
(%o60) 1

→ q:5;
(%o61) 5

→ r:2;
(%o62) 2

→ power_mod(beta, (p−1)/q, p);
(%o63) 105

→ power_mod(alpha, 7·(p−1)/q, p);
(%o64) 105

→ x0:7;
(%o65) 7

→ beta1:mod(beta·power_mod(inv_mod(alpha, p), x0, p), p);
(%o66) 292

→ power_mod(beta1, (p−1)/(q^2), p);
(%o67) 1

→ power_mod(alpha, (p−1)/2, p);
(%o68) 1200

→ x1:2;
```

(%o68) 1200

```
→ x1:2;
(%o69) 2

→ x:mod(x0+5·x1, q^r);
(%o70) 17

→ x:17·4;
(%o71) 68

→ 48·25;
(%o72) 1200

→ power_mod(11, x, p);
(%o73) 601

→ mod(68, 1200);
(%o74) 68
```