Example of the Pohlig-Hellman Technique for finding discrete logarithms

Let the prime p = 8101, and a generator of Z_{8101} be a = 6. Find x so that

$$a^x = 7531 \bmod 8101.$$

Observe that p-1 = 8100 = $(2^2)(3^4)(5^2)$, is a product of small primes. We shall determine the numbers $x_2 = x \bmod (2^2)$, $x_3 = x \bmod (3^4)$ and $x_5 = x \bmod (5^2)$.

Determination of x_2.

Since x_2 is a number mod 4, we have $x_2 = c_0 + c_1 (2)$, with the coefficients being either 0 or 1. We determine these coefficients as follows.

$7531^{(p-1)/2} = 7531^{4050} = -1$ and as this = $a^{c_0 (p-1)/2}$, we have $c_0 = 1$.
Now, divide 7531 by a^{c_0} to get
$7531(a^{-1}) = 7531(6751) = 8006 \bmod p$.
$8006^{(p-1)/4} = 8006^{2025} = 1$ and as this = $a^{c_1 (p-1)/2}$, we have $c_1 = 0$.

$x_2 = c_0 + c_1 (2) = 1 + 0(2) = 1$.

Determination of x_3.

Since x_3 is a number mod 81, we have $x_3 = c_0 + c_1 (3) + c_2 (9) + c_3 (27)$, with the coefficients being either 0, 1 or 2. It will be of use to know the numbers $a^{(p-1)/3} = 5883$, and $a^{2(p-1)/3} = 2217$.

$7531^{(p-1)/3} = 2217$, so $c_0 = 2$.
Now divide 7531 by a^{c_0} to get
$7531(a^{-2}) = 6735 \bmod p$.
$6735^{(p-1)/9} = 1$, so $c_1 = 0$.
Now divide 6735 by a^{3c_1} to get
$6735(a^0) = 6735 \bmod p$.
$6735^{(p-1)/27} = 2217$, so $c_2 = 2$.
Now divide 6735 by a^{9c_2} to get
$6735(a^{-18}) = 6992 \bmod p$.
$6992^{(p-1)/81} = 5883$, so $c_3 = 1$.

$x_3 = 2 + 0(3) + 2(9) + 1(27) = 47$.

Determination of x_5.

Since x_5 is a number mod 25, $x_5 = c_0 + c_1$ (5), with the coefficients being either 0, 1, 2, 3 or 4. We need to compute $a^{(p-1)/5} = 3547$, $a^{2(p-1)/5} = 356$, $a^{3(p-1)/5} = 7077$, $a^{4(p-1)/5} = 5221$.

$7531^{(p-1)/5} = 5221$, so $c_0 = 4$.
Divide 7531 by a^{c_0} to get
$7531(a^{-4}) = 7613 \bmod p$.
$7613^{(p-1)/25} = 356$, so $c_1 = 2$.

$x_5 = 4 + 2(5) = 14$.

Determination of x.

We now use the Chinese Remainder Theorem to compute the common solution of the congruences,

- x = 1 mod 4
- x = 47 mod 81
- x = 14 mod 25.

$M_1 = 8100/(4) = 2025$
$y_1 = M_1^{-1} \bmod 4$, $y_1 = 1$.

$M_2 = 8100/81 = 100$
$y_2 = M_2^{-1} \bmod 81$, $y_2 = 64$.

$M_3 = 8100/25 = 324$
$y_3 = M_3^{-1} \bmod 25$, $y_3 = 24$.

x = 1(2025)(1) + 47(100)(64) + 14(324)(24) = **6689** mod 8100.

Return to index (non-frame version)
