Lecture 12 -- The Pohlig-Hellman attack and Chinese Remainder Theorem

In the last lecture we saw how discrete logarithms could be efficiently solved if $p-1$ was a power of 2. Today we generalize this to the case when $p-1$ is smooth, meaning that it is a product of small primes (exactly “how small” depends on how much time and computing power you have available). Below I typed “$a=b$” when more strictly I meant $a$ is congruent to $b \pmod{p}$, but this is difficult to type in Mathematica.

Let’s try to work with the example of $p = 37$:

```mathematica
p = 37; FactorInteger[p - 1]
{2, 2}, {3, 2}
g = PrimitiveRoot[37]
2
```

We pick a random $h$ from 1 to 36 for this generator $g=2$:

```mathematica
h = RandomInteger[{1, 36}]
33
```

The idea is to think of $g^x = h$, where $x$ is mod 36. If we take both sides to the 18 th power $= 36/2$ th power, we get the value of $x$ mod 2 by trying both possibilities. In general, if we take both sides to the $(p - 1)/k$ - th power, we can determine $x$ mod $k$:

```mathematica
PowerMod[h, 18, p]
1
```

So $x$ is even. Let’s take both sides to the 9 th power to determine $x$ mod 4 (recalling that it is even, so either 0 or 2 mod 4)

```mathematica
PowerMod[h, 9, p]
1
```

Thus $h$ is a multiple of 4. Let’s try the same analysis mod 3, so take to the 12 th power

```mathematica
PowerMod[h, 12, p]
10
```

The possibilities are either $g^{12}$ or $g^{24}$:
Write \( x = 2 + 3y \), so \( g^x = g^2 \cdot g^{3y} = h \), and \( g^{3y} = h^{-1} = g^{28} \)

so \( x \) is 2 mod 3. We can determine it mod 9 (either 2, 5, or 8) by taking both sides to the 4th power

\[
\text{PowerMod}[h^{28}, 4, p]
\]

so \( x \) is 2 mod 3. We can determine it mod 9 (either 2, 5, or 8) by taking both sides to the 4th power

\[
\text{PowerMod}[g, 12, p]
\]

\( 26 \)

\[
\text{PowerMod}[g, 24, p]
\]

\( 10 \)

\[
\text{PowerMod}[h^{28}, 4, p]
\]

\( 1 \)

The possibilities:

\[
\{\text{PowerMod}[g, 0, p], \text{PowerMod}[g, 12, p], \text{PowerMod}[g, 24, p]\}
\]

\( \{1, 26, 10\} \)

So \( x \) is 2 mod 9, and 0 mod 4. Chinese Remainder Theorem says then \( x \) is 20:

\[
\text{PowerMod}[g, 20, p]
\]

\( 33 \)

Another example:

\[
\text{In}[1]= p = 97; \text{FactorInteger}[p - 1]
\]

\[
\text{Out}[1]= \{\{2, 5\}, \{3, 1\}\}
\]

\[
\text{In}[2]= g = \text{PrimitiveRoot}[p]
\]

\[
\text{Out}[2]= 5
\]

\[
\text{h = RandomInteger[\{1, p - 1\}]}
\]

\( 26 \)

Let's try to find the value of \( x \) mod 3, by taking \((p - 1)/3\) rd powers:

\[
\text{In}[4]= \text{PowerMod}[h, (p - 1)/3, p]
\]

\[
\text{Out}[4]= 61
\]

The powers of \( g \) that this could match:

\[
\{\text{PowerMod}[g, (p - 1)/3, p], \text{PowerMod}[g, 2 \cdot (p - 1)/3, p]\}
\]

\( \{35, 61\} \)

so \( x \) is 2 mod 3.

Let's determine it mod 2, then 4, 8, 16, and 32. We write \( x \) mod 32 as a binary expansion \( 16a + 8b + 4c + 2d + e \), each of \( a, b, c, d, \) and \( e \) being equal to 0 or 1. Write
\[ g^x = g^{16a+8b+4c+2d+e} = h, \] and take both sides to the \((p-1)/2\) power, to get \((-1)^d = h^{(p-1)/2}:\]

\[
\text{PowerMod}[h, (p-1)/2, p] \\
96
\]

Thus \(e\) is odd, and write

\[ g^x = g^{16a+8b+4c+2d+e} = 26 \text{ means } g^{16a+8b+4c+2d} = 26 \cdot g^{-1} = 44 \text{ so take both sides to } (p-1)/4 \text{ power:} \]

\[
\text{PowerMod}[44, (p-1)/4, p] \\
96
\]

so \(d\) is odd, and have \(g^{16a+8b+4c} g^2 = 44\) so \(g^{16a+8b+4c} = 44\ \text{ so take both sides to } (p-1)/8 \text{ th power} \]

\[
\text{PowerMod}[91, (p-1)/8, p] \\
1
\]

So \(c\) is even, \(c = 0\), \(g^{16a+8b} = 91\), take both sides to \((p-1)/16\) power

\[
\text{PowerMod}[91, (p-1)/16, p] \\
96
\]

Therefore \(b\) is odd, and we have \(g^{16a} = g^{-8} 91 = 96 = -1.\) Take both sides to the \((p-1)/32=3\text{rd} \) power, and right hand side is -1. Thus \(a\) is odd, \(a=1.\)

We conclude that \(x\) is \(16a+8b+4c+2d+1 = 16+8+2+1=27 \text{ (mod 32), and it is also } 2 \text{ (mod 3). According to the } \text{chinese remainder theorem, it is therefore 59. Indeed, we check:} \]

\[
\text{In[11]}: = \text{PowerMod}[g, 59, p] \\
\text{Out[11]}= 26
\]