Oct6

Sunday, October 4, 2020 4:29 PM

Pohlig-Hellman Algorithm Example

Solve $2^x \equiv 6 \mod 11$ ←

Notice $|2| = 2 \cdot 5$

i) 2^5 ← order 2

ii) 2^2 ← order 5

① $(2^5)^x \equiv 6^5 \equiv 10 \mod 11$

10^x

⇝ $x \equiv 1 \mod 2.$

② $4^x \equiv 6^2 \equiv 3 \mod 11$

$$\left.\begin{aligned} 4^1 &= 4 \\ 4^2 &= 16 = 5 \\ 4^3 &= 20 \equiv 9 \\ 4^4 &\equiv 36 \equiv 3 \end{aligned}\right\} \mod 11$$

$x \equiv 4 \mod 5$

$\Downarrow$

$x \equiv 9 \mod 10$

Check $2^9 \equiv 6 \mod 11$

Theorem

Reduce DLP of elt of order p^α in α many DLPs of order p.

Proof $|g| = p^\alpha$. Solve $g^x = h$. *

$x = x_0 + x_1 p + \cdots + x_{\alpha-1} p^{\alpha-1}$ $\quad 0 \le x_i < p$

Find x_i inductively.

Find x_0

* Raise both sides to $p^{\alpha-1}$

$$\underline{h^{p^{\alpha-1}}} = (g^x)^{p^{\alpha-1}} = g^{p^{\alpha-1}(x_0+px_1+\dots+p^{\alpha-1}x_{\alpha-1})}$$

$$= g^{p^{\alpha-1}x_0 + p^{\alpha}(\text{stuff})}$$

$$= \underline{\left(g^{p^{\alpha-1}}\right)^{x_0}} \cdot \cancel{\left(g^{p^{\alpha}}\right)^{(\text{stuff})}}\, e$$

Lemma $|g^{p^{\alpha-1}}| = p$

Find x_0 using order p DLP.

General step

Know $x_0, \dots, x_{i-1}$. Find x_i

$$\underline{h^{p^{\alpha-i}}} = (g^x)^{p^{\alpha-i}} = g^{(p^{\alpha-i})(x_0+\underline{x_1}p+\dots+x_{\alpha-1}p^{\alpha-1})}$$

$$= \underbrace{g^{x_0p^{\alpha-i}}}_{a_0}\underbrace{g^{x_1p^{\alpha-i+1}}}_{a_1}\cdots g^{x_ip^{\alpha-1}}\cancelto{1}{g^{p^{\alpha}(\text{stuff})}}$$

$$\left(g^{p^{\alpha-1}}\right)^{x_i} = \underbrace{h^{p^{\alpha-i}}a_0^{-1}a_1^{-1}\dots a_{i-1}^{-1}}_{\text{Know}}$$

Mod p DLP to find x_i

In total α many mod p DLPs

& find all x_i

so $x = x_0 + x_1 p + x_2 p^2 + \dots + x_{\alpha-1} p^{\alpha-1}$

HW 4 3d

Problem $m^a, m^{ab}, m^b \leftarrow$ know

Find m.

Know $\exists\ a'$ w/ $aa' \equiv 1 \mod p-1$

& b' w/ $bb' \equiv 1 \mod p-1$

Notice $m^a = m^{abb'} = (m^{ab})^{b'}$

$m^b = m^{aba'} = (m^{ab})^{a'}$

Consult w/ DH oracle

Base $g = m^{ab}$ $(= v) \leftarrow$

$g^{a'} = (m^{ab})^{a'}$ $(= w)$

$g^{b'} = (m^{ab})^{b'}$ $(= u)$

Oracle $\Rightarrow g^{a'b'} = m^{aba'b'} = m \mod p$ ✓

DHP $\Longrightarrow$ HW alg.

RSA, integer factorization, & More

Fermat's Little Theorem

p prime. $a \neq 0$ in $(\mathbb{Z}/p\mathbb{Z})^*$

$$\Longrightarrow a^{p-1} \equiv 1 \mod p.$$

Question

If m is not prime is this true?

is $a \neq 0$ in $(\mathbb{Z}/m\mathbb{Z})^*$?

$$\Longrightarrow a^{m-1} \equiv 1 \mod m.$$

NO!!

Examples

$m = 15485207$

$2^{m-1} \equiv 4136685 \mod m \neq 1$

$\Longrightarrow$ m not prime.

Example

$m = 6 \quad m-1 = 5$

$2^5 = 32 \equiv 2 \mod 6$

$3^5 = 243 \equiv 3 \mod 6$

$a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$

$\Updownarrow$

in $(\mathbb{Z}/m\mathbb{Z})^*$

$5^5 = 3125 \equiv 5 \bmod 6$ $\gcd(a,m)=1$

$5 \in (\mathbb{Z}/6\mathbb{Z})^*$

Fermat doesn't hold!

"Coincidence $a^5 \equiv a$ b/c G is small"

↑ think about this

Question

Is there an analogous statement for m a composite #.
↑ to Fermat

Let's do some experiments

Ex $m = 3 \cdot 5 = 15$

Noticed $a \in (\mathbb{Z}/15\mathbb{Z})$

$$a^4 \equiv 1 \bmod 15$$

$$\iff \gcd(a, 15) = 1$$

Remark

If $\gcd(a,m) \neq 1$ shouldn't expect an analog of FLT for a.

Indeed $a^k \equiv 1 \bmod m$ $(k>0)$

Then $(a^{k-1})a \equiv 1 \bmod m$

$$\Longrightarrow a^{-1} = a^{k-1} \bmod m$$

$$\Longrightarrow a \in (\mathbb{Z}/m\mathbb{Z})^* \quad (\gcd(a,m)=1)$$

Summary

① For a generalizion of FLT to make sense, only can involve $a \in (\mathbb{Z}/m\mathbb{Z})^*$

② The correct exponent cannot be $m-1$ in general

③ For $m=15$, the correct exponent is 4.

Explain ③ $15 = 3 \cdot 5$

$$\begin{tikzcd}
 & a^4 \equiv 1 \bmod 3 \arrow[dl, leftrightarrow] \\
a^4 \equiv 1 \bmod 15 & \\
 & a^4 \equiv 1 \bmod 5 \arrow[ul, leftrightarrow]
\end{tikzcd}$$

(Philosophically this is CRT)

Proof

$\Longrightarrow$ ✓

$\Longleftarrow$ If 3 & 5 divide $a^4 - 1$ so 15 does too

* $a^4 \equiv 1 \bmod 5 \longleftarrow$ Fermat $p=5$
$p-1=4$

* $a^4 \equiv (a^2)^2 \equiv 1 \bmod 3 \longleftarrow$ Fermat $p=3$
$p-1=2$

Idea

1* $\boxed{4}$ is a multiple of $p-1$ for $p=3$ & $p=5$

2* $a^4 \equiv 1 \bmod p$ holds $p=3$ & $p=5$ (By Fermat).

3* $a^4 \equiv 1 \bmod 3 \cdot 5$ holds (CRT)

$* \; m-1 = 14$ doesn't satisfy $1*$.

A generalization of Fermat's Little Theorem for $m = pq$ $\quad p \neq q$.

Theorem (Euler's Theorem)

$p \neq q$ prime numbers $\quad g$ a divisor of $p-1$ & $q-1$

$m = p \cdot q$.

$\left[\text{e.g. } g = \gcd(p-1, q-1)\right.$

Then $a \in (\mathbb{Z}/m\mathbb{Z})^*$

$$a^{\frac{(p-1)(q-1)}{g}} \equiv 1 \mod m.$$

in particular $\left.a^{(p-1)(q-1)} \equiv 1\right.$

FLT

Pf/
$$a^{\frac{(p-1)(q-1)}{g}} = \left(a^{p-1}\right)^{\frac{q-1}{g}} \equiv 1^{\frac{q-1}{g}} \mod p$$
$$\equiv 1 \mod p$$

$$a^{\frac{(p-1)(q-1)}{g}} \equiv 1 \mod q$$

So p, q divide $a^{\frac{(p-1)(q-1)}{g}}$

So pq does too

Rmk Lagrange's thm $\left|(\mathbb{Z}/pq\mathbb{Z})^*\right| = (p-1)(q-1)$

$\Rightarrow a^{(p-1)(q-1)} = 1$ by Lagrange.

Euler gives a better bound.

Recall

*Diffie-Hellman & Elgamal relied on difficulty of computing logs. (mod p)

i.e. solving $a^x \equiv b \mod p$
for x knowing a, b, p.

* RSA relies on the difficulty of computing roots mod N

$$x^e \equiv c \mod N \quad *$$

know e, c, N. Find x.

Rmk

- ⇝ HW saw square roots mod p are easy *
- ⇝ Factor m, CRT reduces (square) roots mod m to those mod p. *

Formalize the remark

Prop p - prime. $e \geq 1$. $\boxed{\gcd(e, p-1) = 1}$

Let $d = e^{-1} \mod (p-1)$ $\quad (de \equiv 1 \mod p-1)$

Then $x^e \equiv c \mod p$ has a unique solution $x = c^d \mod p$.

(Easy to compute $\sqrt[e]{c}$. just $\boxed{e^{-1}}$)

Proof $de = 1 + k(p-1)$

$$(c^d)^e = c^{de} = c^{1+k(p-1)} = c\,\overset{1}{\cancel{(c^{p-1})}}{}^k$$

$$\equiv c \mod p.$$

"c^d is an e'th root of c"

Uniqueness (showed $z^{de} = z \mod p \quad \forall z$)

suppose x_1, x_2 both e'th roots of c

$$x_1 = x_1^{de} = (x_1^e)^d = c^d = (x_2^e)^d = x_2^{de} \equiv x_2 \mod p.$$

Rmk Square roots weren't unique!! if p odd.

(but $\gcd(2, p-1) = 2$)

In general $\gcd(e, p-1) = g$

Then if 1 e'th root exists g do.

Rmk Notice RSA problem ($x^e \equiv c \mod N$.) is not very hard if N is prime.

Next goal

Use factorization of N to reduce RSA problem to prime case where it is easy.

($N = pq \quad p \neq q$)

Prop Let p, q distinct. $e \geq 1$.

$\gcd(e, (p-1)(q-1)) = 1$.

Let $d = e^{-1} \mod (p-1)(q-1)$

i.e. $ed \equiv 1 \mod (p-1)(q-1) \Leftarrow de = 1 + k(p-1)(q-1)$

The $x^e \equiv c \mod pq$ has a unique

solution $x \equiv c^d \mod pq$.

Pf/ $c^d = \underline{x^{de}} = x\cdot\Big(\underset{\substack{1\\ \text{(Euler)}}}{\cancel{x^{(p-1)(q-1)}}}\Big)^k = \underline{x} \mod pq$

So c^d is an e'th root of c.

$$(c^d)^e = c^{de} = c^{1+(p-1)(q-1)k}$$
$$= c\cdot\Big(\overset{1}{\cancel{c^{(p-1)(q-1)}}}\Big)^k = c$$

Uniqueness

(showed $z^{de} \equiv z \mod pq$)

u another e'th root of c

$u = u^{de} = (\underline{u^e})^d = c^d \mod pq$

Rmk Get an algorithm for computing $\sqrt[e]{c} \mod N$. (know $N = pq$)

Step 1 Find $d = e^{-1} \mod (p-1)(q-1)$ (EEA)

Step 2 Compute c^d. mod pq (FP)

↑ that's x.

How hard is Step 1?

Example

* $x^3 = 7 \mod 15$

$\downarrow$

$3^{-1} \bmod (p-1)(q-1) = \bmod 8.$

$3^{-1} \equiv 3 \bmod 8$

$\downarrow$

$7^3 = 343 \equiv 13 \bmod 15$

Check

$13^3 \equiv 2197 \equiv 7 \bmod 15$

so $\sqrt[3]{7} = 13 \bmod 15.$

Moral

Computing $x^e \equiv c \bmod N$ hard.
If I know $N = pq$ it caves down to computing $e^{-1} \bmod (p-1)(q-1)$.

RSA

- Setup $N = pq$. $e, c \in \mathbb{Z}$
- Problem: Solve $\underline{x^e \equiv c \bmod N}$
- Hard: In general to do w/o knowing p, q.
- Easy: If I know p & q easy to solve for x.

Rmk Rely on it being difficult to factor N.

RSA exploits this in the following way

RSA

Alice wants to send Bob a message.

Bob

Eve

Alice

- * Bob chose secret (large) primes $p \neq q$.
- * Bob chooses an encryption exponent e w/ $\gcd(e,(p-1)(q-1))=1$
- * Bob publishes $N=pq$ & e. →

Alice has a message m.

Alice computes ciphertext $c=m^e \bmod N$

sends c to Bob.

- * Bob computes $d = e^{-1} \bmod (p-1)(q-1)$

To decrypt Bob computes $\boxed{c^d} = \bmod N$

↑ this is m.

Rmk Questions does Eve need p & q? or just the product $(p-1)(q-1)$?

Next time we will show these two bits of knowledge are equivalent.