TW314 Lecture 31 (We. 3 May 2017)

The square-and-multiply algorithm

Let b have binary representation

$$b = b_0 + 2b_1 + 2^2 b_2 + \cdots + 2^{l-1} b_{l-1}$$

To find $c \equiv a^b \pmod n$:

Step 1 Set $i = l-1$ and $z_{l-1} = 1$.

Step 2 Let $y_i \equiv z_i^2 \pmod n$.

Step 3 Let $z_{i-1} \equiv a y_i \pmod n$ if $b_i = 1$

and $z_{i-1} \equiv y_i \pmod n$ if $b_i = 0$.

Step 4 If $i > 0$, decrement i by 1

and go to Step 2.

Step 5 Put $c = z_{-1}$. Stop.

Example: Find $3^{75} \pmod{10}$.

$75 = 1001011_2$, so $\ell = 7$

and $b_0 = 1,\ b_1 = 1,\ b_2 = 0,\ b_3 = 1,\ b_4 = 0,\ b_5 = 0,\ b_6 = 1$.

i	b_i	z_i	y_i
6	1	1	1
5	0	3	9
4	0	9	1
3	1	1	1
2	0	3	9
1	1	9	1
0	1	3	9

z_{-1} $\boxed{7}$

So $3^{75} \equiv 7 \pmod{10}$.

Proof that the algorithm determines $a^b \pmod n$:

The algorithm gives the recurrence relation

$$Z_{l-1} = 1, \quad Z_{i-1} = a^{b_i} Z_i^2 \quad \text{for} \quad i = l-1, l-2, \ldots, 2, 1, 0.$$

This gives us

$$Z_{l-2} = a^{b_{l-1}} Z_{l-1}^2 = a^{b_{l-1}}$$

$$Z_{l-3} = a^{b_{l-2}} Z_{l-2}^2 = a^{b_{l-2}} a^{2b_{l-1}}$$

$$Z_{l-4} = a^{b_{l-3}} Z_{l-3}^2 = a^{b_{l-3}} a^{2b_{l-2}} a^{2^2 b_{l-1}}$$

$$\vdots$$

$$Z_{l-k} = a^{b_{l-k+1}} a^{2b_{l-k+2}} a^{2^2 b_{l-k+3}} \cdots a^{2^{k-2} b_{l-1}}$$

Let $k = l+1$, then

$$Z_{-1} = a^{b_0} a^{2b_1} a^{2^2 b_2} \cdots a^{2^{l-1} b_{l-1}}$$

$$= a^{[b_0 + 2b_1 + 2^2 b_2 + \cdots + 2^{l-1} b_{l-1}]}$$

$$= a^b$$

We illustrate the "square-and-multiply" algorithm for finding $c \equiv a^b \pmod{n}$ with two examples:

Example 1 Find $3^{75} \pmod{10}$

solution:
$$3^{75} \equiv 3 \times (3^2)^{37} \equiv 3 \times 9^{37} \pmod{10}$$
$$\equiv 3 \times 9 \times (9^2)^{18} \equiv 7 \times 1^{18} \pmod{10}$$
$$\equiv 7 \pmod{10}$$

Example 2 Find $77^{77} \pmod{100}$

solution:
$$77^{77} \equiv 77 \times (77^2)^{38} \equiv 77 \times 29^{38} \pmod{100}$$
$$\equiv 77 \times (29^2)^{19} \equiv 77 \times 41^{19} \pmod{100}$$
$$\equiv 77 \times 41 \times (41^2)^9 \equiv 57 \times 81^9 \pmod{100}$$
$$\equiv 57 \times 81 \times (81^2)^4 \equiv 17 \times 61^4 \pmod{100}$$
$$\equiv 17 \times (61^2)^2 \equiv 17 \times 21^2 \pmod{100}$$
$$\equiv 17 \times 41 \equiv 97 \pmod{100}.$$